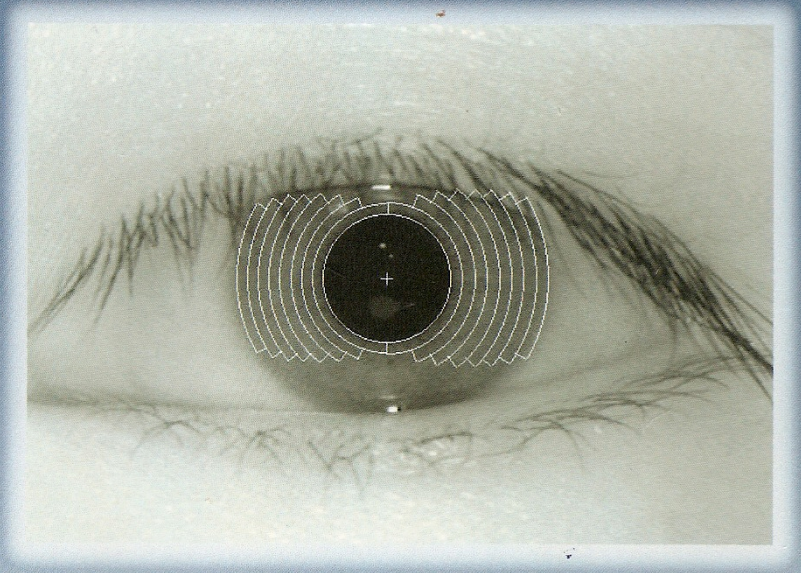
Dr Neđeljko Lekić
prof. dr Zoran Mijanović

IDENTIFIKACIONI SISTEMI



ELEKTROTEHNIČKI FAKULTET

TEMPUS
Education and Culture
JEP CD Tempus 40017 2005

Dr Neđeljko Lekić
Prof. dr Zoran Mijanović
Elektrotehnički fakultet Podgorica

IDENTIFIKACIONI SISTEMI

Osnovni udžbenik

TEMPUS CD_40017 EDICIJA, 2008

Podgorica, novembar 2008.

Dr Neđeljko Lekić
Prof. dr Zoran Mijanović
Elektrotehnički fakultet Podgorica

IDENTIFIKACIONI SISTEMI

Izdavači:
Elektrotehnički fakultet Podgorica
i
Tempus projekat JEP-CD-40017-2005

Za izdavača:
Prof. dr Radovan D. Stojanović

Štampa:
Sten doo Podgorica

Tiraž:
100

SADRŽAJ

GLAVA III

GLAVA IV

GLAVA V

GLAVA VI

PREDGOVOR

Identifikacioni sistemi služe da prepoznaju korisnika i omoguće ostvarenje njegovih prava i obaveza. Postoji mnogo vrsta identifikacionih sistema. Neki se zasnivaju na čitanju kontaktne kartice, a neki pomoću radio-talasa (RFID sistemi) razmjenjuju podatke sa korisnikom bez direktnog kontakta. Postoje i biometrijski identifikacioni sistemi koji identifikaciju vrše na osnovu prepoznavanja fizičkih ili karakteristika ponašanja čovjeka (prepoznavanje otiska prsta, dužice oka, lica, glasa i slično).

Oblast primjene identifikacionih sistema je veoma široka. Mogu se upotrebiti za kontrolu pristupa, praćenje ljudi, životinja ili stvari, magacinska poslovanja, u zdravstvu, za bezgotovinska plaćanja, zaštitu od krađe, kontrolu kvalitete proizvoda, kontrolu hrane, poboljšanje produktivnosti, za borbu protiv terorizma, itd.

Knjiga identifikacioni sistemi namijenjena je za studente koji istoimeni kurs imaju na postdiplomskim studijama na Elektrotehničkom fakultetu, smjer Elektronika, II semestar, kao i postdiplomskim studijama Studija primijenjenog računarstva, III semestar.

Knjiga je nastala kao plod dugogodišnjeg iskustva autora u radu u ovoj oblasti. U osnovi ona pokriva kurs od jednog semestra.

Knjiga se sastoji iz 6 segmenata, odnosno 6 glava.

U prvoj glavi dat je kratak pregled postojećih identifikacionih tehnika.

U dugoj glava su detaljnije opisane optičke identifikacione tehnike. Najviše prostora dato je trakastim kodovima, kao najprimjenjivanijoj optičkoj identifikacionoj tehnici. Detalaljnije su opisani česte korišteni jednodimenzioni trakasti kodovi, kao što su: UPC/EAN, Interleaved 2 of 5, Code 128, Code 39, itd.. Posebno veliki prostor dodijeljen je UPC/EAN trakastom kodu, kao kodu koji se koristi za označavanje proizvoda u maloprodaji i ima daleko najveću primjenu. Dat je i kratak pregled dvodimenzionih trakatih kodova odnosno matričnih kodova. Ukazano je na razloge njihovog uvođenja i navedene osnovne karakteristika najčešće korištenih simbola iz ove kategorije. Zadnji dio teksta o trakastim kodovima posvećen je tehnikama očitavanja trakastog koda. Objašnjeni su osnovni principi čitača sa fiksiranim zrakom, čitača sa pokretnim zrakom i CCD čitača. Kraj ove glave sadrži podatke o optičkim identifikacionim karticama (laserskim karticama). Ukazano je na osnovne razlike između optičkih identifikacionih kartica i optičkih diskova. Dat je krakat opis memoriskog medija laserske kartice. Čitači optičkih identifikacionih kartica takođe su kratko opisani. Na kraju su navedena osnovna područja primjene ove identifikacione tehnike.

Treće glava je posvećena identifikacionoj tehnici u kojoj identifikator i čitač podatke razmjenjuju beskontaktno, pomoću radio talasa. Ova tehnika se naziva RFID (Radio-Frequency Identification). Dat je jezgrovit prikaz

osnovnih karakteristike ove identifikacione tehnologije koja se danas brzo razvija. Prikazane su različite realizacije RF identifikatora i RF čitača. Posebno detaljno je opisana Mifare® 1 S50 beskontaktna identifikaciona kartica. To je RF identigikator jednostavna konstrukcije sa širokim poljem primjene. Na kraju je dat pregled mogućih aplikacija ove identifikacione tehnike.

U četvrtoj glavi riječ je o pametnim karticama. Data je osnovna definicija, što je to pametna kartica, kao i pregled postojećih vrsta pametnih kartica. Dominanatan dio poglavljua posvećen je kriptovanju podataka u pametnim karticama. Dat je opis simetričnog i asimatričnog kriptovanja. U okviru simetričnog kriptovanja detaljnije je opisan DES (Data Encryption Standard) algoritam. Kod asimetričnog kriptovanja dat je opis RSA algoritma, kao i osnovni principi upotrebe digitalnog potpisa. Na kraju glave dat je pregled primjena pametnih kartica.

Peta glava sadrži pregled biometrijskih identifikacionih tehnika. U pregledu je ukazano na osnovnu podjelu bimetrijskih tehnika na tehnike koje prepoznavanje vrše na osnovu fizičkih karakteristika i na tehnike koje prepoznavanje vrše na osnovu karakteristika ponašanja čovjeka. Navedene su osnovne prednosti i nedostaci ovih tehnika u odnosu na tradicionalne identifikacione tehnike. Poseban prostor je dodijeljen tehnici prepoznavanja otiska prsta, kao najstarijoj i biometrijskoj tehnici koja se danas najčešće primjenjuje. Dalje je nešto više rečeno o tehnici prepoznavanja dužice oka. U odnosu na druge biometrijske tehnike, koje se koriste u identifikacionim sistemima, ova prepoznavanje dužice se odlikuje najvećim stepenom pouzdanosti identifikacije. Prepoznavanje lica je još jedna biometrijska tehnika kojoj je dat prostor u ovom izdanju. Od biometrijskih tehnika zasnovanih na karakteristikama ponašanja nešto više je rečeno o prepoznavanju glasa.

Nakon pregleda najčešće korištenih identifikacionih tehnika u šestoj glavi se govori o identifikacionom sistemu kao cjelini. Ukazano je da jedan kompletan identifikacioni sistem, osim identifikatora i čitača, sadrži i puno drugih komponenti kao što su: logeri, baza podataka, aplikativni softver, besprekidno napajanje, komunikaciona infrastruktura, itd.. Opis tih komponenti i njihove uloge u sistemu čini okosnicu ovog dijela knjige.

Na kraju knjige dat je pregled korištene literature.

ZAHVALNOST

Autori se zahvaljuju studentima postdiplomcima: **Laković Milanu**, **Mariji Mirković** i **Nikolić Nikoli**. Oni su pomogli u izradi pojedinih segmenata ove knjige. Laković Milan dao je značajan doprinos u dijelu u kojem se opisuje biometrijska tehnika prepoznavanja otiska prsta. Mirković Marija je dala doprinos u opisu DES algoritma i biometrijskoj tehnici

prepoznavanja dužice oka, dok je Nikolić Nikola pomogao u opisu RSA algoritma.

Posebnu zahvalnost autori duguju **European Commission for Education and Culture** i **Prof. Dr Radovanu Stojanoviću**, koji su kroz realizaciju projekta **JEP CD TEMPUS 40017/2005** pomogli u pojavljivanju ovog udžbenika.

GLAVA I

1. PREGLED IDENTIFIKACIONIH TEHNIKA

Postojeće identifikacione tehnike se mogu podijeliti u dvije osnovne grupe:

- Tradicionalne identifikacione tehnike i
- Briometrijske identifikacione tehnike.

U tradicionalnim identifikacionim tehnikama, objektu čije se prepoznavanje vrši, dodjeljuje se neki identifikator. U biometrijskim identifikacionim tehnikama prepoznavanje čovjeka vrši se na osnovu njegovih jedinstvenih fizičkih i/ili karakteristika ponašanja.

Najčešće korištene tradicionalne identifikacione tehnike kao identifikator upotrebljavaju:

- Trakasti kod,
- Magnetski zapis,
- ″Pametni″ identifikator.

Tradicionalni identifikacioni sistemi se upotrebljavaju za identifikaciju predmeta, životinja i ljudi. Svaki objekat, u ovim sistemima, mora posjedovati identifikator. Identifikator može biti različitog oblika i dimenzija. U identifikaciji proizvoda u maloprodaji, identifikator sa trakastim kodom štampa se na omotu proizvoda (Slika 1.1).

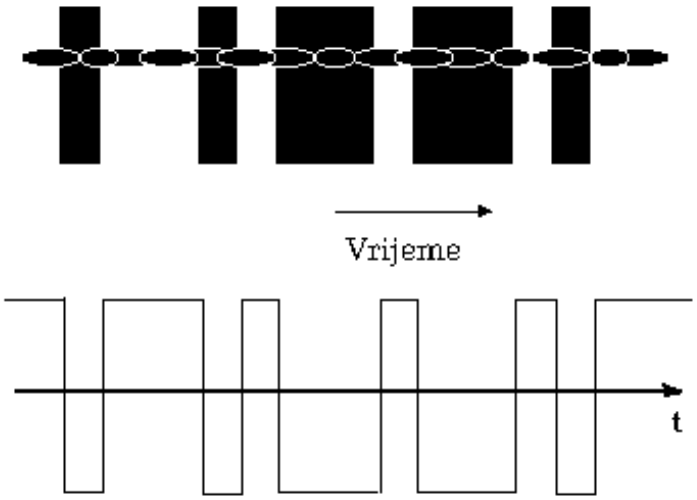
Slika 1.1 Trakasti kod oštampan na prozvodu

U slučaju identifikacije čovjeka, identifikator je često standardnog oblika kartice (Slika 1.2).

Slika 1.2 Različite identifikacione kartice

Redosljed kojim su identifikacioni sistemi navedenu na početku poglavlja je redosljed kojim su se oni pojavljivali u širokoj primjeni.

Trakasti kod je jedan od prvih načina predstavljanja informacija u mašinski čitljivom obliku. Njime se vrši razmjena podataka, svedenih na štampani oblik. Kompjuter generiše štamapnu sliku simbola trakastog koda na papiru ili drugom grafičkom medijumu. Ovaj simbol se zatim prezentuje čitaču trakastog koda. Čitač osvjetljava simbol trakastog koda i ispituje segment po segment u simbolu, da bi odredio da li je visoke refleksije (međuprostor) ili niske refleksije (traka). Na osnovu toga čitač konvertuje simbol trakastog koda u digitalni signal. Ovaj digitalni signal se zatim prevodi u originalnu karakter poruku. Slika 1.3 ilustruje osnovni princip čitanja trakastog koda.

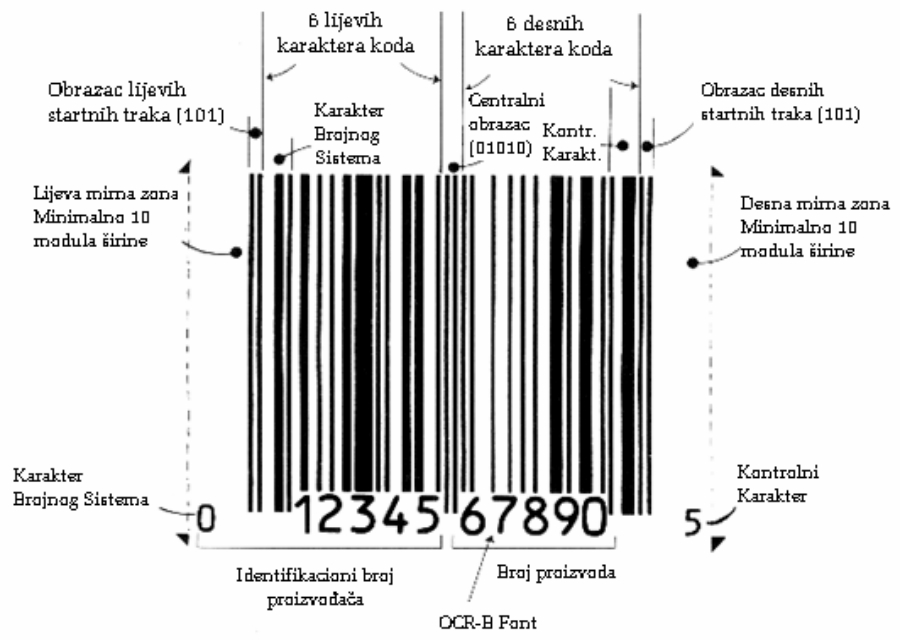


Slika 1.3 Osnovni princip čitanja trakastog koda

Ideja primjene trakastih kodova u sistemima za identifikaciju proizvoda u maloprodaji pojavila se već četrdesetih godina prošlog vijeka. U dvadesetom vijeku došlo je do prave ekplozije u smislu porasta količine i raznovrsnosti roba kojom se trguje. To je uzrokovalo da cijene logistike i kontrole inventara višestruko naraste, naročito u supermarketima. Zato su oni među prvima dali podršku razvoju sistema za automatsku identifikaciju proizvoda. Krenulo se sa stanovišta da bi jednostavna oznaka, mašinski čitljiva, omogućila trgovcima da saznaju sadržaj paketa proizvoda bez potrebe za pojedinačnom provjerom svakog paketa. Mogućnost da se brzo odredi sadržaj paketa ubrzala bi razmjenu robe i smanjila troškove transporta, kontrole inventara i logistike.

1949 godine, Norman Woodland, diplomirani student na Drexel Institute of Technology, zainteresovao se za ovaj problem i prihvatio se traženja rješenja. Woodland je problem povezao sa Morse-ovim kodom. Poruke Morse-ovog koda sastojale su se od ″tačaka i crtica″ koje su se mogle čitati automatski ili od strane čovjeka. Postoji priča, da, dok je razmatrao problem na plaži, Woodland je pisao poruke Morse-ovog koda u pijesku. Onda je produžio tačke i crtice naniže – praveći uske i široke linije. Tako je došao do ideje za, danas opšte poznati, trakasti kod [1].

Sljedećih 20 godina pojavljivali su se trakasti kodovi različitih oblika [1, 2]. 1969 godine konzorcijum za distribuciju hrane osnovao je asocijaciju nazvanu Uniform Code Council (UCC) [3] koja je počela sa koncipiranjem standardizovanog trakastog koda za sve potrošačke artikle. Ovaj kod je nazvan Universal Product Code (UPC) [4]. UPC je linearan (jednosdimenzioni), trakasti kod. (Slika 1.4).



Slika 1.4. Kompletan simbol U.P.C koda – verzija A

Simbol UPC koda sadrži podatke o proizvođaču i proizvodu (Slika 1.3). 1974 godine UCC je prihvatio UPC kod i razvio prateću tehnologiju [3]. 1974-06-26, UPC simbol se pojavio na pakovanju od 10 Wrigley guma i skeniran je u supermarketu u Ohio. Taj događaj predstavlja početak modernog doba u identifikaciji proizvoda. Od tada se počelo sa primjenom trakastih kodova svuda u maloprodajnim objektima, gdje su i danas široko rasprostranjeni. Nalaze se na gotovo svakom komercijalnom artiklu.

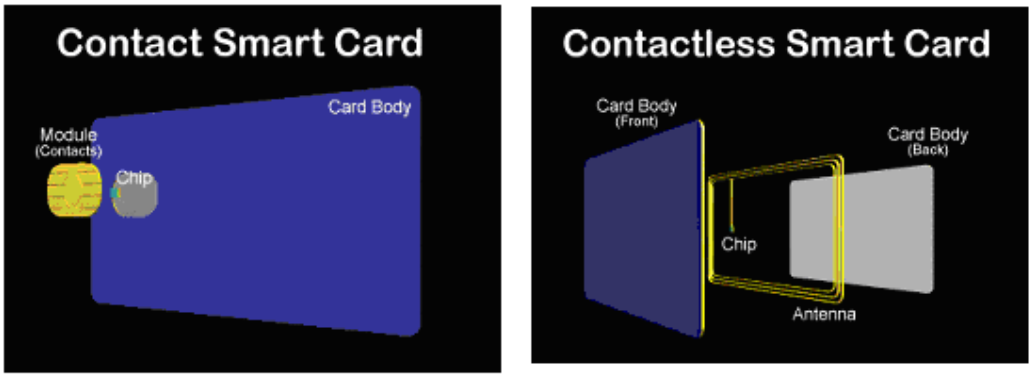
Druga faza razvoja trakastih kodova ogleda se u pojavi dvodimenzionalnih i matričnih kodova. Dvodimenzionalni i matrični kodovi omogućavaju smještanja više podataka na manjoj površini. Često se koriste za označavanje proizvoda malih dimenzija, kao i tamo gdje je na maloj površini potrebno smjestiti više podataka (npr. audio zapis na filmskim trakama) [5].

Danas svuda prisutne, magnetne trake, prvi put su se pojavile ranih 60-tih godina kao prevozne karte u londonskom metrou. Rukovodstvo londonskog prevoza je obložilo zadnju stranu vozne karte, magnetskim zapisom koji je sadržavao šifriranu vrijednost karte. Svaki put kada bi kartica bila provučena kroz čitač na prevoznoj stanici, na magnetsku traku se upisivala nova šifrirana vrijednost koja je u odnosu na raniju umanjena za cijenu prevoza. Sistem je kasnije prerađen. Reduciran je prostor sa magnetskim zapisom na standardni format trake (Slika 1.5) [6, 7].

Slika 1.5 Kartica sa magnetskim zapisom oblika trake i čitač Mini123 MSR500m(ur)

Kartice sa magnetnim zapisom (magnetne trake) i dalje se široko koriste kao finansijske kartice, prevozne karte i identifikacione kartice. Pod finansijskim karticama podrazumijevaju se kreditne i debitne kartice, koje se koriste kod automatskih blagajni i terminala na prodajnim mjestima. Prevozne karte sa magnetskim zapisom koriste se u gotovo svim vidovima saobraćaja (željeznici, autobuskom saobraćaju, avionskom saobraćaju itd.). Magnetni zapis kao identifikator se koristi kod vozačkih dozvola, članskih karata, kartica ključeva i slično [8, 9].

Identifikacioni sistemi zasnovani na primjeni ″pametnih″ identifikatora sve su prisutniji u našoj svakodnevici. ″Pametni″ identifikatori imaju ugrađen jedan ili više mikročipova. Čip može sadržati mikroprocesor sa internom memorijom ili može biti samo memorijski [10, 11]. Prema načinu na koji komuniciraju sa čitačem ″pametni″ identifikatori mogu biti kontaktni ili bekontaktni. Na slici 2.5 prikazan je kontaktni i bezkontaktni identifikator oblika kreditne kartice [10, 12].



Slika 1.5 Kontaktne i beskonraktne (RF) kartice

″Pametne″ identifikatore karakteriše visoka zaštićenost podataka. U samom čipu ugrađene su funkcije zaštite. Imaju inteligentnu interakciju sa čitačem [10, 13, 14].

Identifikacioni sistemi zasnovani na ″pametnim″ identifikatorima danas ubrzano dobijaju na popularnosti i sve više potiskuju druge tradicionalne identifikacione sisteme. Koriste se širom svijeta u finasijskum poslovima, telekomunikacijama, tranzitu, maloprodaji, zdravstvu, kontroli pristupa itd. [15, 16, 17].

Posebno su interesantni beskontakni ″pametni″ identifikatori i sistemi zasnovani na njihovoj primjeni (RFID sistemi). Zahvaljujući svojim prednostima, kao što su nepostojanje kontakata, nepostojanje potrebe za direktnom vidljivošću, otpornost na prljavštinu i ogrebotine ova identifikaciona tehnila u poslednje vrijeme nalaze sve brojnije primjene [18,12].

Biometriski identifikacioni sistemi koriste se za identifikaciju čovjeka na osnovu prepoznavanja njegovih fizičkih karakteristika ili karakteristika ponašanja. Kod ovih sistema nije potreban dodatni identifikator, već je on sastvani dio čovjeka. Danas postoje biometrijski identifikacioni sistemi koji identifikaciju vrše na osnovu prepoznavanja:

- otiska prsta,
- dužice oka,
- mrežnjače oka,
- karakteristika lica,
- karakteristika glasa,

- karakteristika šake,
- potpisa, itd.

U poslednjih desetak godina ostvaren je bitan napredak u razvoju biometrijskih identifikacionih sistema. Njihovo područje primjene se neprestalno proširuje [19, 20].

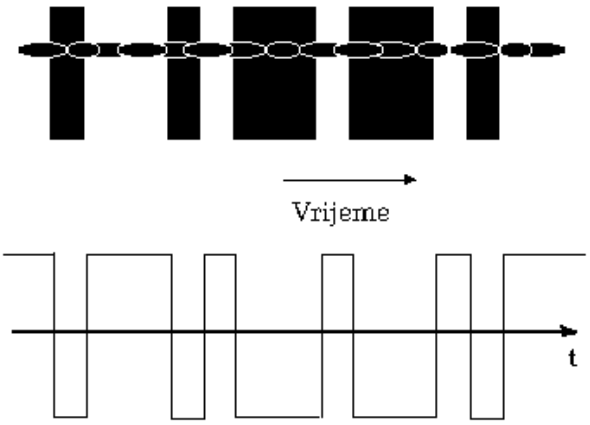
GLAVA II

2. OPTIČKE IDENTIFIKACIONE TEHNIKE

2.1 TRAKASTI KODOVI

Trakasti kodovi, koji su u početku služili za poboljšanje produktivnosti u maloprodajnim objektima, razvili su se u nešto što danas predstavlja standard u oblasti prikupljanja podataka. Ovaj koncept se prvi put pominje 1949. godine kada je N. J. Woodland dao prvi trakasti kod (Cirkular). Danas su trakasti kodovi zastupljeni u najvećem broju ako ne i u svim segmentima industrije, elektronike, brige o zdravlju, avionskog transporta, maloprodaje i dr..

Trakastim kodovima vrši se razmjena podataka, svedenih na štampani oblik. Kompjuter generiše štamapnu sliku simbola trakastog koda na papiru ili drugom grafičkom medijumu. Ovaj simbol se zatim prezentuje uređaju za skeniranje odnosno čitaču trakastog koda. Čitač osvjetljava simbol trakastog koda i ispituje segment po segment u simbolu, da bi odredio da li je visoke refleksije (međuprostor) ili niske refleksije (traka). Tako čitač detektuje prelaske iz svijetle u tamnu i iz tamne u svijetlu zonu. Dužina vremena u kome detektor "vidi" svijetlo ili mrak konvertuje se u digitalni signal. Ovaj digitalni signal se zatim prevodi u originalnu karakter poruku. Slika 2.2.1 ilustruje osnovni princip čitanja trakastog koda.



Slika 2.1.1. Čitanje trakastog koda

Najuži element u trakastom kodu konvencionalno je nazvan 'X'. U dvoširinskim kodovima, odnos širokog (W) i uskog (N) prostora treba da se

kreće opsegu od 2.4 : 1 do 3.2 : 1, pri čemu se preporučuje 3.0:1. Kako su šire trake čitljive sa veće daljine to tipična uska traka ne smije biti uža od 0.25 mm. Preporučljivo je uzeti širinu između 0.3 i 0.5 mm.

Slika 3.2. pokazuje tipičan simbol trakastog koda. Svaki simbol na početku i na kraju sadrži mirnu zonu, čija je širina obično 10 puta veća od širine uskog elementa ili otprilike 6mm (ponekad i više). Minimalna visina simbola je 15 procenata njegove dužine. Često se preoporučuje minimalno 12.5mm. Veća visina simbola pomaže čitanju, naročito kada treba prevazići neizbježan šum koji potiče od prljavštine i habanja na simbolu.

ANSI (American National Standard Institute) definiše *simbol* trakastog koda kao ”prostor pravougaonih traka i međuprostora, koji su raspoređeni po utvrđenom obrascu i služe za prezentaciju elementarnih podatka odnosno karaktera”. Simbol trakastog koda sadrži vodeću mirnu zonu, startni karakter, karaktere podatka i kontrolni karakter (ako postoji), stop karakter i završnu mirnu zonu. *Simbologija* je jezik traka i međuprostora u oštampanom simbolu. Danas ima preko 50 različitih simbologija, ali samo četiri (U.P.C/EAN, Code 39, Code 128 i Interleaved 2 of 5) imaju značajnu primjenu u maloprodaji i industriji. Sredinom 1993 godine pojavljuju se PDF 417, DataMatrix i Code 6 kao vodeći kodovi u transportnoj, hemijskoj i elektronskoj industriji. PDF 417 primjenjuje se tamo gdje je potrabna velika gustina podataka i ručno skeniranje. DataMatrix se primjenjuje tamo gdje se simboli laserski ugraviraju (npr. mala pakovanja). Code 6 se upotrebljava u sortation-style aplikacijama.

Slika 2.1.2. Mirne zone na početku i na kraju simbola trakastog koda

Mirne zone se smještaju na početku i na kraju svakog simbola (Slika 2.2.2) i služe za davanje referentnog nivoa optičkom detektoru unutar skenera. Ovaj referentni nivo omogućava skeneru da prepozna što je traka a što međuprostor u simbolu trakastog koda.

Start-Stop karakter ili start-stop obrazac slijedi neposredno iza mirne zone i daje čitaču informacije kao što su:

- smjer čitanja,
- širina uskog elemeta,

- početak ili završetak simbola.

Svaka *simbologija* sadrži jedinstven set pravila za predstavljanje podataka. Pravila definišu:

- tip informacije, odnosno, da li je ona samo numerička, slovna i numerička zajedno ili sadrži i znakove specijalne namjene,
- model širokih i uskih traka i međuprostora koji predstavljaju informaciju,
- dužinu poruke (fiksna ili promjenljiva dužina),
- gustinu kojom su podaci upakovani u datu dužinu.

Na primjer, Code 39 (alfanumerička simbologija) zahtijeva devet elmenata (pet traka i četiri međuprostora) od kojih su tri široka i šest uskih, za predstavljanje pojedinog karaktera. Za razliku od njega, alfanumerički kod Code 128 prikazuje karaktere sa tri trake i tri međuprostora u više širina. Različite simbologije imaju različitu relativnu gustinu karaktera (broj karaktera koji se može smjestiti u jedinicu dužine).

Simbologije se dijele na kontinualne i diskretne. Svaki karakter u diskretnoj simbologiji počinje sa trakom i završava sa trakom. Između svaka dva karaktera postoji međuprostor. Ovaj međuprostor može biti različite širine, obično između 1 i 5,3 puta širine najužeg elementa (trake ili međuprostora) (najčešće 1). Code 39 i Codebar su diskretne simbologije. Kontinualni kodovi za razliku od diskretnih nemaju međuprostor između karaktera. Takvi su U.P.C/EAN, Interleaved 2 of 5 i Code 128.

Sistemi sa trakastim kodom su rapidno smanjili količinu grešaka u odnosu na sisteme gdje se unos podataka vrši tastaturom i to sa jedne greške u 300 unesenih karaktera na manje od jedne greške u milion unesenih karaktera. Tome je, između ostalog, doprinijelo i uvođenje tzv. *kontrolnog* karaktera. To je matematički izračunata vrijednost koja se dodaje svakom simbolu trakastog koda. Obično se smješta na kraju simbola, prije stop karaktera. *Kontrolni* karakter može uspješno eliminisati svaki oblik greške u podacima bilo da je ona unešena u simbol ili da se pojavila prilikom skeniranja.

Da bi se obezbijedila sigurnost čitanja simboli trakastog koda imaju posebnu sigurnosnu strukturu. Takva struktura obezbjeđuje da pojedini defekt štampe u simbolu ne izazove da karakter sa defektom bude pročitan kao drugi važeći karakter u simbologiji. Ova osobina se naziva *self-checking.* Code 93 nema *self-checking* na nivou karaktera ali posjeduje dva *kontrolna* karaktera kojima obezbjeđuje integritet podataka.

Trakasti kodovi se često čitaju uređajima sa promjenljivom brzinom čitanja. Svjetlosna olovka (*light pen*), na primjer, može varirati u brzini od 3 do 30 inča u sekundi, a i kod lasera se javljaju izvjesne varijacije u brzini. Da bi se obezbijedila sigurnost čitanja, u ovim uslovima, broj traka i međuprostora kao i njihova relativna širina po katakteru mora biti konstantna. Takvi simboli se nazivaju *self-clocking.*

Poznato je da je simbologija definisana kao ”set pravila za predstavljanje podatataka u obliku simbola trakastog koda”. Međutim prije nego što

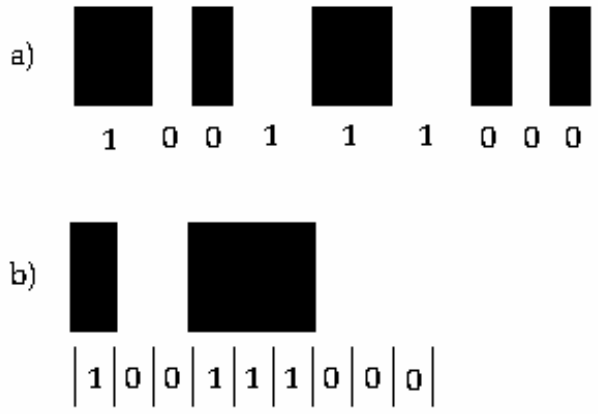
razmotrimo kako izabrati određenu simbologiju moramo uočiti razliku između riječi ”kod” i ”simbol”. Prije mnogo godina je, nažalost pogrešno, izabran termin ”bar kod tehnologija” koji su naši savremenici ovjekovječili kroz imena simbologija Code 39, Code 49, Code 93 i Code 128. Mnogo precizniji i pravilniji termin bi bio ”bar simbol tehnologija”.

Jednostavno, *kod* je uređeni skup slova, brojeva i specijalnih znakova i predstavlja poruku. Na primjer, broj socijalnog osiguranja je kod koji je jedinstven za svaku individuu. Kod proizvoda identifikuje određeni proizvod izmađu svih ostalih proizvoda. Dalje, identifikacioni kod proizvođača je jedinstven za pojedinog proizvođača.

Na drugoj strani, simboli su reprezenti koda. Na primjer H_2O je hemijski simbol za ”bezbojnu prozirnu tečnost koja se na zemlji pojavljuje u rijekama, morima, okeanima, itd., i pada iz oblaka u vidu kiše”- ili kreće vodu. Trakasti simboli predstavljaju kodove pomoću traka i međuprostora.

Postoje dva osnovna načina za predstavljanje informacija u obliku tradicionalnih simbola trakastog koda. U prvom načinu svaki bit predstavljamo trakom ili međuprostorom i to tako što, ako je bit ”″1”″ elemnat je širok a ako je bit ”″0”″ element je uzan. Iako, je ovakav kod opšte-poznat kao ”binarni kod”, mi ćemo ga nazivati ”širinski kod” zato što ovaj termin bliže opisuje šemu kodiranja (a i zbog široke upotrebe riječi ”binaran” u računarskoj literaturi).

Drugi metod dijeli trake i međuprostore u intervale koje nazivamo *moduli*. Moduli označeni jedinicom predstavljaju trake, a moduli označeni nulom predstavljaju međuprostore. Pojedina traka ili međuprostor može biti sastavljena iz više modula. Ovakav metod nazivamo delta kodiranje, a tako dobijeni kod ”delta kod”. Slika 2.2.3a prikazuje kodiranje binarnog niza 100111000 u širinski kod. Slika 2.2.3b prikazuje isti niz u obliku delta koda. Kao što se može vidijeti iz ovih slika, delta kodovi (U.P.C., Code 93, Code 128, Code 16K, Code 49 i PDF417) imaju veću gustinu nego širinski kodovi (Code 39, Interleaved 2 of 5, Codabar i MLC 2D).



Slika 2.1.3. a) Širinsko kodiranje; b) Delta kodiranje

Danas postoje međunarodni sporazumi i standardi u upotrebi trakastih kodova [21]. Poštovanje tih standarda je obavezno u situacijama kada se isti simboli trakastih kodova namjeravaju upotrebljavati među više partnera (kupci, trgovci, prevoznici i posrednici) odnosno u tzv ”otvorenim sistemima”. Manje je kritično u slučajevima kada se simboli upotrebljavaju samo u vlastitoj organizaciji odnosno samo za internu upotrebu (”zatvoreni sistemi”).

2.1.1 JEDNODIMENZIONI TRAKASTI KODOVI

U ovom dijelu je dat osvrt na neke najčešće korištene jednodimenzione trakaste kodove.

2.1.1.1 U.P.C: Universal Product Code

U.P.C je ubjedljivo najrasprostranjeniji simbol trakastog koda pa će, stoga, biti nešto detaljnije opisan.

U.P.C. se u početku koristio za označavenje proizvoda u U.S. prodavnicama hrane, da bi se kasnije proširio i na trgovinu na veliko, farmaceutiku, knjige, časopise, elektronske proizvode, ustanove, softver i hardver. U.P.C simbol se sastoji od :

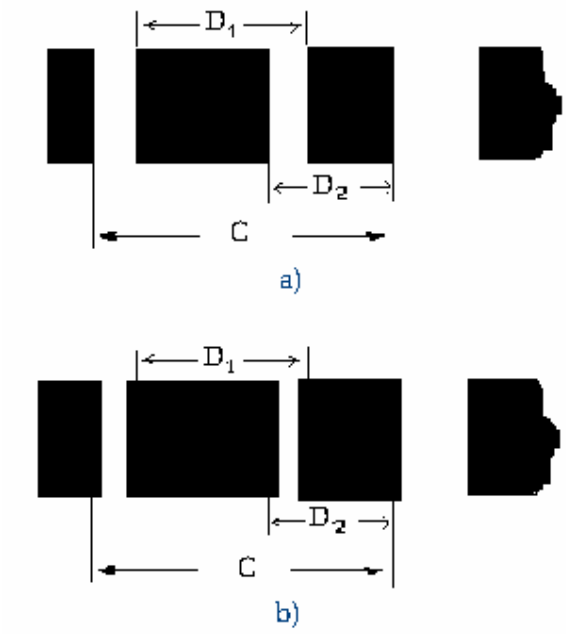
- šest cifara koje predstavljaju identifikacioni broj (ID) proizvođača (dodjeljuje ga UCC -Uniform Code Council).
- pet cifara koje predstavljaju ID pojedinog proizvoda (dodjeljuje sam proizvođač).
- kontrolna cifra koja se izračunava iz prethodnih jedanaest cifara.

Znači, U.P.C simbol sadrži 12 cifara od kojih je svega pet na raspolaganju proizvodjaču pa je najveći problem svakog proizvođača odrediti šemu po kojoj će numerisati svoje proizvode. Često proizvođači svoj asortiman dijele u grupe proizvoda i za svaku grupu fiksiraju prvu cifru identifikacionog broja. Zatim proizvode određene grupe dijele po boji, veličini ili materijalu u podgrupe za koje fiksiraju drugu cifru ID itd. Međutim brojna struktura U.P.C za identifikaciju proizvoda je predvidijela samo pet cifara što omogućava 100000 mogućih permutacija. Fiksiranjem bilo koje cifre značajno umanjujemo broj permutacija. Uzmimo na primjer kompaniju koja se bavi obradom drveta, metala i plastike. Neka svi drvni proizvodi počinju sa “1”, svi metalni proizvodi sa “2” i svi plastični proizvodi sa “3”. Time je broj permutacija sveden sa 100000 na 30000. Ako bi još specificirali boju i veličinu? Dakle vidimo da bilo koji inteligentni način kodiranja redukuje broj mogućih kodova i donosi opasnost da ih broj proizvoda prevaziđe. Zato je ponakad bolje koristiti slučajno označavanje proizvoda (na primjer od 00000 pa dalje) jer na taj način možemo numerisati 100000 proizvoda prije nego što nam zatreba još

jedan ID proizvođača [4].

Strukrura U.P.C. simbola mora zadovoljavati određene kriterijume. Osnovni kriterijum je da se omogući štamparskim kompanijama da ga mogu štamapti, na omotu proizvoda, zajedno sa promotivnim materijalom, bez povećanja cijene štampe. Dalje, U.P.C. simbol, pri višesmjernom skeniranju, mora biti čitljiv pri bilo kakvoj orijentaciji prema skeneru. I na kraju, broj grešaka pri prvom skeniranju ne smije biti veći od jedne greške u 10000 skeniranih simbola [4].

Proces štampanja uvijek prati pojava ”razlivanja mastila”, zbog čega je širina trake veća od širine odgovarajućeg međuprostora. Koliko će ova pojava biti prisutna zavisi od vrste i uslova štampe, viskoznosti mastila i drugih faktora koje je teško precizno kontrolisati. IBM je predložio metodu, zvanu *delta distance* [1], kojom je moguće učiniti simbol trakastog koda neosjetljivijim na pojavu uniformnog razlivanja mastila [21].

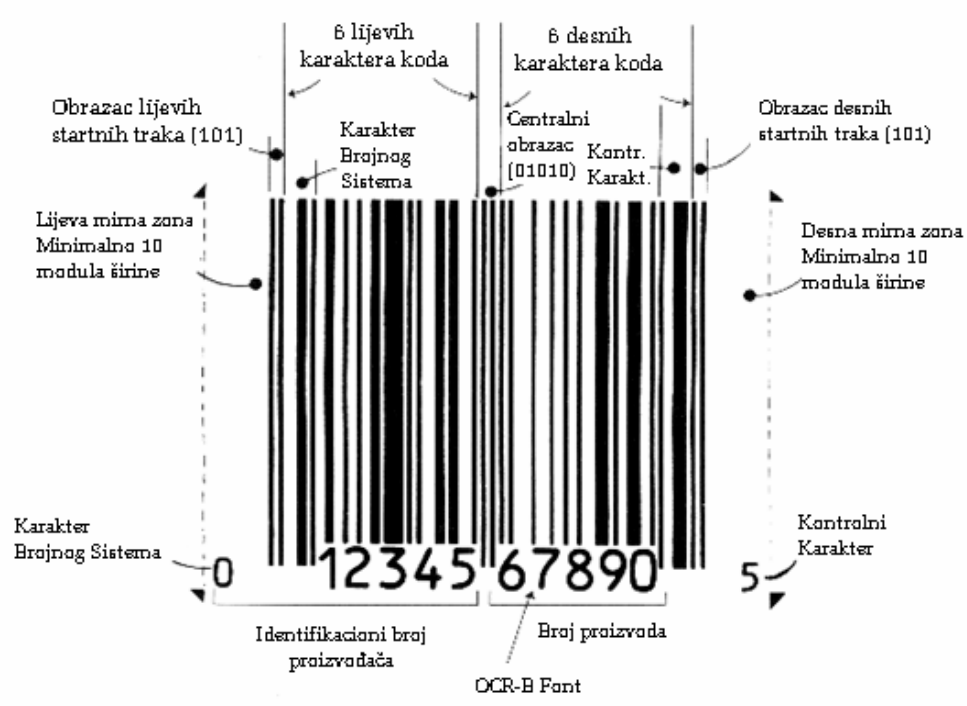


Slika 2.1.4 Razlivanje mastila i delta distance metod

Ova metoda se primjenjuje kod U.P.C. simbola i prikazana je na slici 2.4. Dimenzija D_1 je uzeta od rastuće ivice prve trake do rastuće ivice druge trake, dok je dimenzija D_2 uzeta od opadajuće ivice prve trake do opadajuće ivice druge trake. Dimenzija C je rastojanje od rastuće ivice prve trake do rastuće ivice trake susjednog karaktera. Ove dimenzije se ne mijenjaju pod uticajem ″razlivanja mastila″. Međutim, ako je ″razlivanje mastila″ toliko izraženo da neki međuprostori postanu tako mali da ih čitač ne može raspoznati , simbol će biti nečitljiv.

VERZIJA A

Kompletan U.P.C simbol (verzija A) dat je na slici 2.2.5.



Slika 2.1.5. Kompletan simbol U.P.C koda – verzija A

Duže trake u sredini simbola dijele simbol na lijevu i desnu polovinu. Trake u svakoj polivini simbola moraju biti dovoljno duge da bi povećale pouzdanost čitanja simbola i smanjile potrebu za njegovom preciznom orijentacijom prema simbolu.

Problem nekih proizvođača je što dizajn njihovih proizvoda, umetanjem U.P.C. simbola potrebne veličine biva narušen. Često proizvođači ovaj problem rješavaju tako što umanje simbol skraćivanjem visine traka. Takav postupak se reflektuje u smanjenoj pouzdanosti čitanja i zahtijeva preciznije orijentisanje simbola prema čitaču. Na slici 2.1.6 prikazan je skraćeni simbol U.P.C. trakastog koda, verzije A.

Slika 2.1.6 Skraćeni simbol U.P.C. koda – verzija A

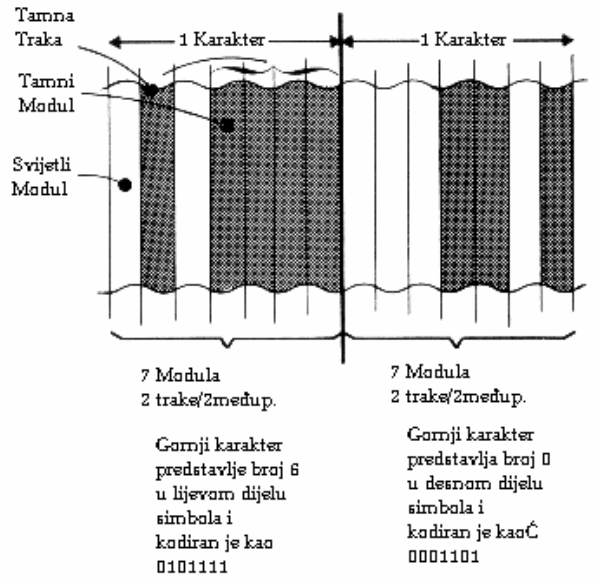
U.P.C./EAN karakteri su konstruisani iz kombinacije dvije trake i dva međuprostora. Oni zauzimaju ukupno sedam modula, kako je pokazano na slici 2.1.7. Tamni moduli odgovaraju binarnoj jedinici a svijetli moduli odgovaraju binarnoj nuli, tako da je zbir bitova jednak broju tamnih modula u katakteru. Krakteri lijevo od centralnog obrasca imaju neparan broj tamnih modula (3 ili 5) i nazivamo ih neparnim karakterima. Karakteri na desnoj strani od centralnog obrasca imaju paran broj tamnih modula (dva ili četiri i nazivamo ih parnim karakterima) (Tabela 2.1.1). Znači, moguće je konstruisati 20 različitih karaktera na lijevoj i 20 različitih karaktera na desnoj strani U.P.C. simbola. U Verziji A U.P.C. simbola koristi se deset karaktera na lijevoj i deset karaktera na desnoj strani. Kao što se vidi sa slike 2.1.5, svaka polovina simbola sadrži ukupno šest cifara, sa zadnjom cifrom na desnoj strani simbola, koja predstavlja kontrolni karakter. Kontrolni karakter se izračunava iz prethodnih jedanaest karaktera (cifara). Simboli, U.P.C Verzija A, imaju dva nivoa kontrole. Prvi nivo je ispitivanje parnosti broja traka u svakom karakteru unutar obije polovine simbola. Drugi nivo predstavlja kontrolni karakter u simbolu. Izračunavanje kontrolnog karaktera za U.P.C. vrši se po modulu 10 na sljedeći način:

1) Saberu se sve cifre na neparnim pozicijama i dobijeni zbir pomnoži sa 3.
2) Na rezultat iz tačke 1. se saberu sve cifre na parnim pozicijama.
3) Dobijeni rezultat se podijeli sa 10 i ostatak dijeljenja oduzme od 10.
4) Ukoliko je rezultat 10 uzima se 0.

Primjer: Za UPC-A kod "03600029145X" izračunati kontrolnu cifru X.
Rješenje:

1. Sabiranje svih cifara na neparnim pozicijama: 0+6+0+2+1+5 = 14
   Množenje rezultata sa 3: 14x3=42
2. Dodavanje cifara sa prnih pozicija: 42+3+0+0+9+4 = 58
3. Izračunavanje ostatka po modulu 10: 58 mod 10 = 8
   Oduzimanje od 10: 10 - 8 = 2 (ukoliko je rezultat 10 uzima se 0).

Konačno zaključujemo da je vrijednost kontrolne cifre, **X = 2**.
Pravac skeniranja U.P.C./EAN simbola određen je parnošću karaktera (ne Start/Stop obrascem).



Slika 2.1.7 Karakteri u U.P.C. simbolu trakastog koda

Tabela 2.1.1 Karakteri u simbolu U.P.C. koda – verzija A		
Vrijednost karaktera	**Karakter u lijevom dijelu simbola (Neparan broj tamnih modula) L - kod**	**Karakter u desnom dijelu simbola (Paran broj tamnih modula) R-kod**
0	0001101	1110010
1	0011001	1100110
2	0010011	1101100
3	0111101	1000010
4	0100011	1011100
5	0110001	1001110
6	0101111	1010000
7	0111011	1000100
8	0110111	1001000
9	0001011	1110100

VERZIJA E

Postoji skraćena verzija U.P.C. simbola. To je Verzija E koja kodira šest cifara podataka, i prikazana je na Slici 2.1.8. Samo simboli koji upotrebljavaju brojni sistem ″0″ za proizvođački identifikacioni kod mogu biti kodirani u Verziji E (to je predstavljeno na Slici 2.1.8 vodećom nulom). Simboli Verzije E upotrebljavaju karaktere kodirane po obrascu datom u Tabeli 2.1.2.

Slika 2.1.8. Simbol U.P.C. trakastog koda – verzija E

Tabela 2.1.2 Karakteri u simbolu U.P.C. koda – verzija E		
Vrijednost karaktera	Neparan broj modula u karakteru (O)	Paran broj modula u karakteru (E)
0	0001101	0100111
1	0011001	0110011
2	0010011	0011011
3	0111101	0100001
4	0100011	0011101
5	0110001	0111001
6	0101111	0000101
7	0111011	0010001
8	0110111	0001001
9	0001011	0010111

Ni jedan karakter u U.P.C. Verzija E kodu nije, eksplicitno, kontrolni karakter. Kontrola je ostvarena kroz permutacije parnosti kodiranih karaktera, kao što pokazuje Tabela 2.1.3.

Tabela 2.1.3 Permutacije parnosti						
Kontrolni karakter	**Pozicija karaktera podataka u simbolu**					
Vrijednost	**1**	**2**	**3**	**4**	**5**	**6**
0	E	E	E	O	O	O
1	E	E	O	E	O	O
2	E	E	O	O	E	O
3	E	E	O	O	O	E
4	E	O	E	E	O	O
5	E	O	O	E	E	O
6	E	O	O	O	E	E
7	E	O	E	O	E	O
8	E	O	E	O	O	E
9	E	O	O	E	O	E

Šest karaktera u simbolu U.P.C. Verzija E su realizovani iz U.P.C. koda na sljedeći način:

Prvi slučaj: Ako se proizvođački broj završava sa 000 ili 100 ili 200, proizvođač ima na raspolaganju 1000 brojeva za svoje proizvode, i to između 00000 i 00999. Šest karaktera se dobijaju iz prva dva karaktera proizvođačkog broja, zatim slijede zadnja tri karaktera od broja artikla i zadnji karakter je treći karakter proizvođačkog broja.

Drugi slučaj: Ako se proizvođački broj završava sa 300, 400, 500, 600, 700, 800 ili 900, proizvođač ima na raspolaganju 100 brojeva za svoje proizvode i to između 00000 i 00099. Karakteri U.P.C. verzije E se dobijaju iz prva tri karaktera proizvođačkog broja, zatim zadnja dva karaktera broja artikla, i zadnji karakter je ″3″.

Treći slučaj: Ako se proizvođački broj završava sa 10, 20, 30, 40, 50, 60, 70, 80 ili 90 na raspolaganju je 10 brojeva za identifikaciju proizvoda. To su brojevi između 00000 i 00009. Šest karaktera se dobija iz prva četiri karaktera proizvođačkog broja, zadnjeg karaktera od broja proizvoda i karaktera ″4″.

Četvrti slučaj: Ako se proizvođački broj ne završava sa nulom, onda su na raspolaganju 5 brojeva za identifikaciju proizvoda (00005 do 00009).Karakteri Verzije E se sastavljaju iz svih pet karaktera proizvođačkog broja, dok je zadnji karakter broj proizvoda.

U primjeru na slici 2.1.8, kod je ″00783491″. Prvi karakter je nula i označava brojni sistem (Verzija E postoji samo za brojni sistem ″0″). Zadnja cifra ″1″ je kontrolni karakter koji određuje obrazac parnosti karaktera u simbolu. Preostaju ″078349″. Zadnji karakter nije ″0″, ″1″ ili ″2″ (Prvi slučaj), niti ″3″ (Drugi slučaj), niti ″4″ (Treći slučaj). To znači da je proizvođački kod ″007834″ i da je kod proizvoda ″00009″. Kada se

pročitani kod prosljeđuje kompjuterskom sistemu prosljeđuje se ″007834000091″ a ne ″00783491″, što omogućava bazi podataka jednostavno identifikovanje proizvođača i njegovog prooizvoda.

Izračunavanje kontrolnog karaktera vrši se na sljedeći način:

1. Saberu se brojevi na neparnim pozicijama u proširenom nizu (s′lijeva na desno) 0+7+3+0+0+9=19
2. Dobijena suma se pomnoži sa ″3″ 19·3=57
3. Saberu se parne pozicije (slijeva na desno) 0+8+4+0+0=12
4. Saberu se rezultati koraka 2 i 3, i to je: 57+12=69
5. Dobijeni rezultat se oduzima od najbližeg većeg umnoška broja deset (70-69=1)
6. Rezultujući kontrolni karakter je =1
7. Znači koristimo ″1″ kodni obrazac parnosti iz Tabele 2.2b).
8. Karaktere kodiramo na sljedeći način:

   ″0″ (Paran)
   ″7″ (Paran)
   ″8″ (Neparan)
   ″3″ (Paran)
   ″4″ (Neparan)
   ″9″ (Neparan)

BROJNI SISTEMI

Karakter koji određuje brojni sistem u simbolu U.P.C. služi kao sredstvo pomoću koga se određuje kojeg je tipa artikal čiji simbol čitamo. Karakteri brojnog sistema su definisani u Tabeli 2.1.4.

Tabela 2.1.4 Karakteri brojnog sistema

″0″	Označava standardne maloprodajne i nemaloprodajne artikle
″1″	Rezervisano za buduću upotrebu
″2″	Označava artikle koji se prodaju po težini (riba, meso, sir, voće itd.)
″3″	Služi za kodiranje National Drug Code (NDC) i National Healt Related Items Code (NHRIC) artikle koji imaju 10 cifarske kodove kontrolisane od strane FDA
″4″	Koristi sa u maloprodaji za internu upotrebu
″5″	Koristi se za označavanje kupona (karata)
″6″	Koristi se za maloprodajne i nemaloprodajne artikle
″7″	Koristi se za maloprodajne i nemaloprodajne artikle
″8″	Rezervisano za buduću upotrebu
″9″	Rezervisano za buduću upotrebu

Detaljna analizu simbola sa svim pomenutim vrijednostima karaktera brojnog sistema može se naći u [4].

U.P.C. SIMBOL SA DVIJE DODATE CIFRE ZA PERIODIČNOST

Ovaj simbol se koristi za označavanje periodičnih trgovačkih isporuka. Omogućje trgovcu praćenje isporuka. Najviše sistema na prodajnim mjestima, ne čita dva dodata karaktera i identifikuje samo proizvođača i artikal. Zato se moraju primijeniti specijalizovani čitači, koji uzimaju u obzir i dvije dodatne cifre i osim proizvođača i artikla identifikuju i datum izdavanja artikla. Ako se isporuke vrše sedmično dodati broj se kreće između 1 i 52, ako se vrše polumjesečno dodati broj se kreće između 1 i 24, a ako se isporuke vrše mjesečno dodati broj se kreće između 1 i 12. Na Slici 2.1.9 dat je U.P.C. simbol u verziji A, gdje je izdavač identifikovan sa ″001234″ a atrikal sa ″56789″, i u slučaju da se radi o mjesečnim isporukama, riječ je o decembarskoj isporuci.

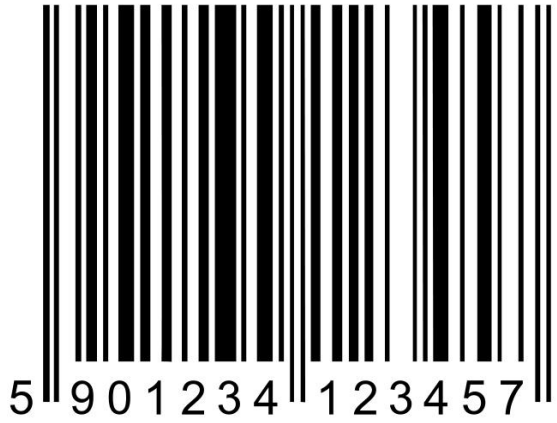
Slika 2.1.9 UPC-A. simbol sa dvije dodatne cifre za periodičnost

Slično, na Slici 2.1.10 je dat U.P.C. Simbol Verzija E sa dva dodata karaktera, gdje je izdavač određen sa ″072440″, a artikal sa ″00004″ i, ako je riječ o polumjesečnoj isporuci, to je isporuka iz prve polovine januara.

Slika 2.1.10 UPC-E simbol sa dvije dodatne cifre za periodičnost

INTERNACIONALNO NUMERISANJE ARTIKALA
(EAN –– International Article Numbering)

Na principima U.P.C. koda, 1974 godina utvrđeno je internacionalno numerisanje artikala (EAN). Osnovna razlika između U.P.C. i EAN je u tome što U.P.C. ima dvanaestocifarski, a EAN trinaestocifarski kod. Oznaka EAN-13 govori da je riječ o punom trinaestocifarskom kodu. Slika 2.1.11 prikazuje primjer U.P.C./EAN-13 simbola.



Slika 2.1.11 Primjer U.P.C./EAN-13 simbola.

U.P.C. i EAN su međusobno kompatibilne simbologije i skeneri koji čitaju jedan od ova dva simbola mogu čitati i drugi. Zapravo U.P.C. se može smatrati podskupom EAN-13.

Prvih dva ili tri karaktera EAN simbola koriste se za određivanje ″brojnog sistema″. To je u stvari jedinstveni fiksirani kod, koji se dodjeljuje državama, koje na omotima svojih proizvoda štamapaju simbole trakastih

kodova. Kako je broj država na Zemlji veći od 100 to za ovu namjenu nije dovoljno predvidjeti dvocifarski kod. Neke zemlje koriste više različitih brojnih sistema, shodno njihovim potrebama. Sjedinjenim Američkim Državama pripadaju brojevi od 00 do 09. Osim za identifikaciju države fiksirani kod se dodjeljuje i za označavanje knjiga, kupona, odnosno, tiketa i za identifikaciju periodičnih simbola. U Tabeli 2.1.6 izlistani su fiksirani kodovi (brojni sistemi) nekih država.

Tabela 2.1.6 Brojni sistemi nekih država

EAN Brojni sistemi (Fiksirani kodovi)	**Država**
00-09	Sjedinjene Američke Države
10-19	Rezervisano
20-29	EAN meloprodaja (sl. Brojnom Sistemu ″4″ kod UPC)
30-37	Francuska
40-43	Njemačka
440	Njemačka
49	Japan
50	Velika Britanija i Irska
520	Grčka
529	Kipar
54	Belgija i Luksemburg
57	Danska
599	Mađarska
600-601	Južna Afrika
76	Švajcarska
779	Argentina
789	Brazil
80-83	Italija
84	Španija
87	Holandija
888	Singapur
90-91	Austria
93	Australia
977	Periodični kodovi
978-979	Knjige (ISBN)
98-99	Brojevi kupona (tiketa)

EAN simboli, kao i U.P.C. simboli, imaju dvije trake i dva međuprostora unutar jednog karaktera koda i isti početni, krajnji i centralni obrazac. Iako

U.P.C simbol ima 12 cifara a EAN simbol 13 cifara, oba simbola imaju po 30 traka i 29 međuprostora. Karakteri na desnoj strani simbola EAN (pozicije $X_6X_5X_4X_3X_2X_1$ čitano s′desna na lijevo gdje je X_1 kontrolni karakter) kodirani na isti način kao i karakteri na desnoj strani U.P.C. simbola). Karakteri na lijevoj strani EAN simbola $X_{12}X_{11}X_{10}X_9X_8X_7$ konstruisani su slično U.P.C. simbolu Verzija E. Trinaesti karakter (najljeviji karakter) EAN-13 simbola se ne kodira vec njegova vrijednost određuje na koji način će pojedini karakter iz prve grupe od 6 karaktera biti kodiran. Drugim riječima, ovaj karakter određuje obrazac parnosti karaktera od X_7 do X_{12} (Tabela 2.1.7 i Tabela 2.1.8).

Tabela 2.1.7 Obrasci kodranja karaktera u EAN-13 trakastom kodu

Vrijednost karaktera	Brojni Set L	Brojni Set G	Brojni Set R
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Tabela 2.1.8 Obrazac parnosti $X_{12}X_{11}X_{10}X_9X_8X_7$ karakter i zavisnosti od vrijednosti prve cifre

Vrijednost 13-te Cifre	Brojni set cifara od 7 do 12					
	12	11	10	9	8	7
0	L	L	L	L	L	L
1	L	L	G	L	G	G
2	L	L	G	G	L	G
3	L	L	G	G	G	L
4	L	G	L	L	G	G
5	L	G	G	L	L	G
6	L	G	G	G	L	L
7	L	G	L	G	L	G
8	L	G	L	G	G	L
9	L	G	G	L	G	L

EAN brojni set G je isti kao U.P.C. Verzija E brojni set sa parnim brojem tamnih modula. Brojni set L je isti kao set za lijeve karaktere u

U.P.C. Verzija A simbolu. Brojni set R je isti kao set za desne karaktere u U.P.C. Verzija A simbolu. Najviše U.P.C./EAN skenirajućih sistema smještaju U.P.C. kod u trinaestocifarsko polje, sa desnim podešavanjem (nula se smješta u s′lijeva). Znači da U.P.C. karaktere brojnog sistema smještaju kao 00 do 09. Na osnovu toga i Tabele 2.1.8 jasno je da će obrazac parnosti i karakter set lijevih karaktera U.P.C. simbola biti ispravno prepoznat od strane EAN skenera.

Pokazana su dva primjera. Prvi primjer, (Tabela 2.1.9), pokazuje strukturu koda EAN simbola prikazanog na Slici 2.1.11. Drugi primjer, (Tabela 2.1.10), pokazuje strukturu kod U.P.C. simbola prikazanog na Slici 2.1.5.

Tabela 2.1.9 Kodna struktura EAN-13 simbola sa slike 2.1.11

Pozicija karaktera	13	12	11	10	9	8	7	6	5	4	3	2	1
Brojni set		L	G	G	L	L	G	R	R	R	R	R	R
Karakter	5	9	0	1	2	3	4	1	2	3	4	5	7

Tabela 2.1.10 Kodna struktura U.P.C simbola sa slike 2.1.5

Pozicija Karaktera	13	12	11	10	9	8	7	6	5	4	3	2	1
Brojni set		L	L	L	L	L	L	R	R	R	R	R	R
Karakter	0	0	1	2	3	4	5	6	7	8	9	0	5

EAN-8

EAN-8 je osmocifarski kod čije dvije prve cifre s lijeva predstavljaju fiksirani kod (EAN Interbational Coding Authority) a prva cifra s′desna predstavlja kontolnu cifru izračunatu iz prijethodnih sedam cifara (po modulu 10 - Prilog 2). Preostalih pet cifara koriste se za identifikaciju proizvođača i artikla. Na taj načim, moguće je kodirati svega 100000 različitih EAN-8 simbola sa jednim fiksiranim kodom, pa se EAN-8 simbol uglavnom primjenjuje tamo gdje nema dovoljno prostora za štampanje simbola EAN-13.

EAN-8 simboli se mogu koristiti u maloprodaji za internu upotrebu, slično U.P.C simbolima sa brojnim sistemom ″4″ ili EAN-13 simbolima sa fiksiranim kodom izmađu 20 i 29. Prva cifra slijeva, EAN-8 simbola, koji se koriste za te namjene je ″2″ a zadnja cifra je kontrolna cifra izračunata na isti način kao i kod drugih EAN-8 simbola. Preostalih šest cifara se koriste za označavanje proizvoda. Cifra ″2″ na početku EAN-8 simbola govori da je taj simbol namijenjen za internu upotrebu i ne može se koristiti izvan određenog maloprodajnog mjesta.

Na slici 2.1.12 dat je primjer simbola EAN-8 koda.

Slika 2.1.12 Primjer simboa EAN-8 koda

Tabela 2.1.11 pokazuje strukturu EAN-8 simbola.

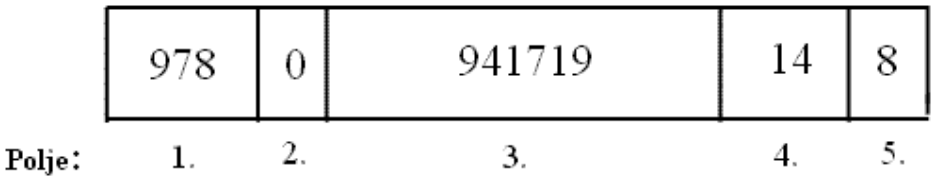
Tabela 2.1.11 Struktura EAN-8 simbola								
ozicija karaktera	8	7	6	5	4	3	2	1
Brojni set parnosti	A	A	A	A	C	C	C	C
Karakter	2	0	1	2	3	4	5	1

EAN za identifikaciju KNJIGA
(Bookland EAN)

ISBN (International Standard Book Number) sistem je međunarodno prihvaćen sistem za jedinstveno numerisanje knjiga. Ključni element u sistemu je International Standard Book Number, koji se obično označava skraćenicom ″ISBN″. To je u stvari fiksirani dio koda, čija je namjena da, povećanjem tačnosti i brzine izvođenja, smanji cijenu identificiranja i distribucije publikovanih proizvoda.

Od Novembra 1985 godine Book Industry Systems Advisoty Committee (BISAC) preporučuje da se na publikovanim knjigama, na zadnjoj korici u donjem desnom uglu, štampa simbol trakastog koda, poznat kao ″Bookland EAN″.

Struktura Bookland EAN simbola data je na slici 2.1.13.



Slika 2.1.13 Struktura Bookland EAN simbola

Prve tri cifre s lijeva čine EAN prefiks ″978″ ili ″979″ (ISBN) (Polje 1).

Polje 2 predstavlje identifikator grupe, koji je određen od strane International Standard Book Number Agency. Za englesko govorno područje identifikator grupe je ″0″ ili ″1″.

Polje 3 je identifikator izdavača. Ovo polje varira u dužini u zavisnosti od broja naslova koji je izdavač predvidio.

Dužina identifikatora izdanja (Polje 4) određena je kao razlika broja 9 i zbira dužina identifikatora grupe i izdavača. Ako je identifikator grupe ″0″, Tabela 2.1.12 pokazuje kako se određuju dužine identifikatora izdavača i identifikatora izdanja. Ako je identifikator grupe ″1″, može se koristiti Tabela 2.1.13.

Peto polje sadrži kontrolnu cifru izračunava se iz prethodnih 12 cifara, po formuli:

$$x_{13} = [10 - ([x_1 + 3x_2 + x_3 + 3x_4 + \cdots + x_{11} + 3x_{12}] \bmod 10)]$$

Tabela 2.1.12 Određivanje dužine identifikatora izdavača i izdanja, ako je identifikator grupe ″0″

Ako su 5ta i 6ta cifra u rangu:	Dužina koda Izdavača	Dužina koda Naslova
00-19	2 cifre	6 cifre
20-69	3 cifre	5 cifre
70-84	4 cifre	4 cifre
85-89	5 cifre	3 cifre
90-94	6 cifre	2 cifre
95-99	7 cifre	1 cifre

Tabela 2.1.13 Određivanje dužine identifikatora izdavača i izdanja, ako je identifikator grupe ″1″

Ako su 4ta , 5ta, 6ta i 7ma cifra u rangu:	Dužina koda Izdavača	Dužina koda Naslova
0000- 5499	Rezervisano za ubuduće	Rezervisano za ubuduće
5500-8697	5 cifara	3 cifre
8698-9989	6 cifara	2 cifre
9990-9999	7 cifara	1 cifre

Ponekad se Bookland EAN kodu dodaju pet cifara koje predstavljaju cijenu izdanja. Takav simbol se označava sa Bookland EAN/5 čiji primjer je dat na Slici 2.1.14. Vodeća cifra (prva s′lijeva) u Velikoj Britaniji je ″0″ (označava funtu), a u U.S.A. vodeća cifra je ″5″ (označava dolar). Ovaj simbol treba razlikovati od sličnog U.P.C. simbola sa dodatnih pet cifara poznatom kao Price-Point U.P.C (Slika 2.1.15).

Slika 2.1.14 Simbol Bookland EAN/5 koda

Slika 2.1.15 Simbol Price-Point UPC koda

National Association of College Stores preporučuje, da za knjige koje nemaju unaprijed fiksiranu cijenu, pet dodatnih cifara se može koristiti za neku drugu potrebu izdavača, s′tim što u tom slučaju prva cifra mora biti ″9″. U ovom slučaju izdavaču su na raspolaganju kodovi u opsego od 90000 do 98999. Ako izdavač ništa ne kodira u dodatnih pet cifara preporučuje sa da taj kod bude ″90000″.

2.1.1.2 2 of 5 Code i Interleaved 2 of 5 simbologije

2 of 5 Code je razvio Gerry Woolf iz Idention Corporation 1968. godine. Kod je našao primjenu u rukovanju magacinskim inventarom i markiranju avionskih karata i prtljaga. Dizajn 2 of 5 Code koda je takav, da sve informacije su sadržane u širini traka, sa međuprostorima koji služe samo da odvoje pojedine trake. Trake mogu biti uske ili široke, pri čemu je, obično, šira traka trostruko veće širine od uske trake. Svaki karakter 2 of 5 Code simbola sadrži pet traka, od čega su dvije široke. Otuda potiče i naziv koda. Međuprostori mogu biti bilo koje razumljive širine. Obično su širine jednake širini uske trake. Uske trake označavaju binarnu nulu a široke trake

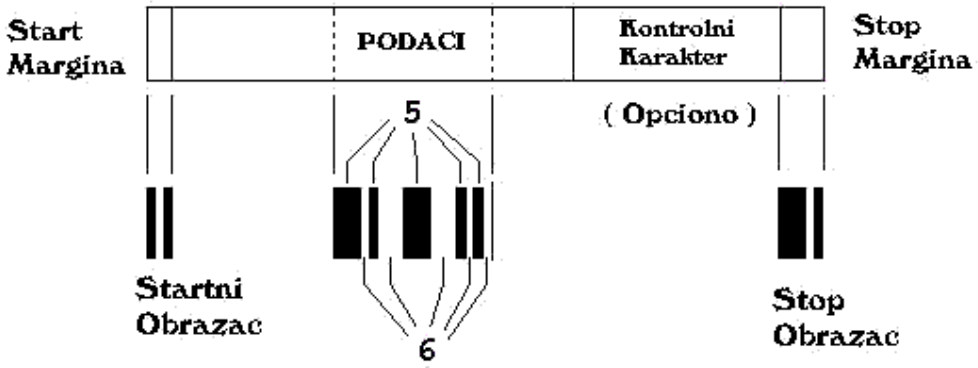
binarnu jedinicu. Usvojena pravila kodiranja za 2 of 5 Code kod data su u Tabeli 2.1.14.

Tabela 2.1.14 Tabela kodiranja 2 of 5 Code simbologiju	
Karakter	Binarni kod 1247P
0	00110
1	10001
2	01001
3	11000
4	00101
5	10100
6	01100
7	00011
8	10010
9	01010
Start	110
Stop	101

Kodna struktura, vezano za težinu pozicije široke trake, gledano s′lijeva na desno, je 1,2,4,7, i bit parnosti. Tako je ″5″ predstavljeno sa širokom trakom na pozicijama težine ″1″ i ″4″ (1+4=5). Od ovog pravila odstupaju karakteri nula, start i stop.

2 of 5 Code je diskretni kod. To znači da svaki karakter u simbolu počinje sa trakom i završava se sa trakom. Između svaka dva karaktera postoji međuprostor koji ih razdvaja. Kod se mogao uspješno štampati i sa jednostavnom štamparskim mašinama, što ga je, do pojave savremenih kompjuterskih štampača, činilo popularnim. Nakon toga 2 of 5 Code, gubi svoju popularnost jer sve više dolaze do izražaja njegovi nadostaci, kao što su mala gustina informacija i velika dužina koda koji je nepodesan za čitanje laserskim čitačima.

Kao rješenje ovih problema, Dr. David Allais predlaže Interleaved 2 of 5 simbologiju. Interleaved 2 of 5 je široko prihvaćen kao simbol trakastog koda na grupnim ambalažama (na primjer paketima cigareta i dr.). Tehnika kodiranja za Interleaved 2 of 5 je ista kao za 2 of 5 Code sa jednim izuzetkom –– i trake i međuprostori su nosioci informacija. Cifre koje su na neparnim pozicijama, gledano s′lijeva na desno, u kodu, predstavljene su trakama, dok su cifre, na parnim pozicijama u kodu predstavljene međuprostorima. Startni obrazac se nalazi na lijevom početku simbola i sastavljen je od uske trake, uskog međuprostora i uske trake. Stop karakter se nalazi na desnom početku simbola i predstavljen je sa širokom trakom, uskim međuprostorom i uskom trakom (Slika 2.15).



Slika 2.1.16 Struktura Interleaved 2 of 5 simbola

Simbol Interleaved 2 of 5 koda sadrži paran broj cifara. U slučaju da treba kodirati broj sa neparanim brojem cifara, prije kodiranja dodaje se vodeća nula. Interleaved 2 of 5 je *self-checking* i za razliku od 2 of 5 Code, kontinualan je. Preporučuje se da nominalni odnos širina elemenata koda bude u opsegu 2.5:1 do 3:1. U.P.C. Shipping Container Symbol je odredio odnos 2.5:1.

Ovako definisan, Interleaved 2 of 5 simbol nije dovoljno zaštićen. Iskustvo je pokazalo da se javlja problem nazvan "*"short scan"* (nepotpuno očitavanje). *Short scan* se može desiti kada se vrši dijagonalno skeniranje, na primjer kada se koristi ručni laserski skener. *Short scan* ne presiječe sve trake i međuprostore simbola, ali pročitane podatke prepozna kao ispravne. Konstrukcija karaktera Interleaved 2 of 5 simbola i start/stop obrazaca omogućuje prosljeđivanje ″nekorektnih podataka″ kompjuterskom sistemu, pri dijagonalnom skeniranju. Mogućnost, takvog, pogrešnog skeniranja raste sa porastom dužine simbola.

Postoje tri različita rješenja koja sprječavaju pojavu nepotpunog očitavanja. Prvo rješenje je dodavanje simbolu kontrolnog karaktera izračunatog po modulu 10. Međutim, dodavanjem kontrolnog karaktera on postaje dio dekodirane poruke i ako Interleaved 2 of 5 kod ima paran broj cifara, kontrolni karakter će taj broj učiniti neparnim. Pošto Interleaved 2 of 5 zahtijeva paran broj cifara, mora se na početku koda dodati nula. Ipak, upotreba kontrolne cifre izračunate po modulu 10 u Interleaved 2 of 5 simbolima je preporučljiva.

Drugo rješenje za prepoznavanje nepotpunog očitavanja simbola je fiksna dužina Interleaved 2 od 5 koda. Ako dekoder očekuje tačno određeni broj cifara, vrijednost dekodiranja kratkim skenom će biti odbačena i skeniranje će se ponoviti.

Treće rješenje je dodavanje po jedne trake. sa gornje i donje strane Interleaved 2 of 5 simbola. Dodate trake moraju biti normalne na trake u simbolu i u fizičkom kontaktu sa njima. Širina traka mora biti najmanje jednaka širini šire trake u simbolu a preporučuje se da bude jednaka četvorostrukoj širini uske trake. Struktura Interleaved 2 of 5 simbola je

takva da startni karakter počunje uskom trakom a stop karakter se završava uskom trakom. Prisustvo, opisanih, ivičnih traka iznad i ispod simbola onemogućiće da, pri ″kratkom skenu″, bude detektovan validni start i stop obrazac. To znači da će podaci dobijeni od ″kratkog skena″ biti odbačeni i skeniranje će se morati ponoviti.

Osim što eliminišu *short scan* okvirne trake pomažu kada se štampanje vrši tehnikom koja koristi ″mokro mastilo″, tako što smanjuju mogućnost da simbol, usljed razlivanja mastila, dođe u kontakt sa okolnom štampom ili drugim simbolom. Ako se prilikom štampanja Interleaved 2 of 5 simbola koristi ″mokro mastilo″, okolne trake obavijaju čitavi simbol (Slika 2.1.17). U slučajevima kada Interleaved 2 of 5 simbol ne štampamo ovakvim postupkom okvirne trake trabaju biti samo na vrhu i na dnu simbola (slika 2.1.18).

Slika 2.1.17 Okolne trake obavijaju kompletan Interleaved 2 of 5 simbol

Slika 2.1.18 Okolne trake samo na vrhu i dnu Interleaved 2 of 5 simbola

1981. godine Uniform Code Council je odredio 14-cifarski format (ITF-14) Interleaved 2 of 5 simbola za markiranje utovarnih kontejnera,

odnosno, grupnih ambalaži. Dužina Interleaved 2 of 5 simbola može se izračunati na sljedeći način:

$$L = (((D \cdot (2 \cdot N + 3) + (6 + N)) \cdot X) + 2Q$$

gdje je:
L= dužina simbola uključujući mirne zone;
D= broj cifara;
N= odnos širina uskog i širokog elementa;
X= širina uskog elementa;
Q= širina mirne zone.

Primjer ITF-14 simbola dat je na slici 2.1.17. Sa slike vidimo za se simbol sastoji od indikatora pakovanja, U.P.C. identifikacinog broja proizvođača, broja proizvoda kojeg (određuje proizvođač), i kontrolnog karaktera izračunatog po modulu 10.

Namjena indikatora pakovanja je da definiše količinu skeniranog proizvoda, da bi se što tačnije i brže mogla ažurirati baza podataka u kompjuterskom sistemu. Tako se ″7″ koristi kao indikator pakovanja koji identifikuje jedinicu punjenja. Indikator pakovanja ″5″ je standardni identifikator za utovarne kontejnere. Broj ″3″ bi se mogao upotrijebiti kao identifikator grupnih pakovanja unutar utovarnog kontejnera itd.. Za precizno definisanje značenja pojedine vrijednosti identifikatora pakovanja labelar je dužan konsultovati svoje bazične kupce.

2.1.1.3 Code 128

Razvijen od strane Ted Wilijams-a, a zatim od Computer Identics-a, Code128 se pojavio krajem 1981. godine, kao odgovor na potrebu za kompaktnim alfanumeričkim trakastim kodom, koji bi bio u mogućnosti kodirati složene identifikacione znake.

Code 128 kodira kompletan ASCII karakter set (Tabela 2.1.15), ima promjenjivu dužinu simbola i mogućnost da poveže jednu poruku sa drugom u cilju dobijanja kompletne informacije. Ako simbol predstavlja skup numeričkih podataka, Code128 može kodirati par cifara (00 do 99) umjesto alfanumeričkog karaktera (Tabela 2.1.15-Code C). Ova mogućnost smanjuje dužinu simbola Code128 za pola, odnosno, udvostručuje gustinu informacija u simbolu. Kada u poruci postoji šest ili više uzastopnih numeričkih podataka, kodiranje se vrši u cifarskim parovima. Prilikom dekodiranja, dobijena informacija se provjerava na nekolika nivoa. Prvi nivo je, ispitivanje parnosti u svakom pojedinačnom karakteru. Drugi nivo je poređenje dekodirane traka/međuprostor vrijednosti sa vrijednosti ivica-slična ivica. Treći nivo je kontrola kompletne poruke na osnovu provjere kontrolnog karaktera sa kraja poruke.

Code 128 slijedi opšti format trakastog koda, odnosno, sastoji se iz vodeće mirne zone, start koda, karaktera podataka, kontrolnog karaktera, stop koda i završne mirne zone (Slika 2.1.19). ″X″ dimenzija se bira na osnovu mogućnosti raspoložive opreme za skeniranje i štampanje. Code 128 karakteri se satoje od tri trake i tri međuprostora i od ukupno 11 modula. Trake i međuprostori mogu biti širine jedan, dva, tri ili četiri modula. 103 različite traka/međuprostor kombinacije (kodne riječi) predstavljaju karaktere u Code 128 karakter setu, plus tri različita start karaktera i stop karakter. Izbor start koda određuje jedan od tri moguća karakter seta, tako da se može predstaviti čitav ASCII 128 karakter set. Karakter set Code C obezbjeđuje da svaka kodna riječ predstavlja dvocifarski broj tako da se dobije dvostruka gustina koda kada su kodirani podaci čisto numerički. Različite kontrolne funkcije i šiftne kodne riječi omogućavaju promjenu karakter seta unutar jednog simbola. Dužina simbola Code128 može se izračunati na iz sljedeće formule:
gdje je:

$$L = (((5.5D + 11C + 35) \cdot X)) + 2Q$$

L= dužina simbola;
D= broj cifra u numeričkom polju;
C= broj karaktera koji nijesu uključeni u numeričko polje, plus broj funkcijskih i šift
karaktera;
X= širina uskog elementa (X dimenzija)
Q= širina mirne zone.

■CODE-128

	CODE A	CODE B	CODE C	Simbol karaktera	Kod kar B S B S B S		CODE A	CODE B	CODE C	Simbol karaktera	Kod kar B S B S B S
0	SP	SP	00		2 1 2 2 2 2	54	V	V	54		3 1 1 1 2 3
1	!	!	01		2 2 2 1 2 2	55	W	W	55		3 1 1 3 2 1
2	"	"	02		2 2 2 2 2 1	56	X	X	56		3 3 1 1 2 1
3	#	#	03		1 2 1 2 2 3	57	Y	Y	57		3 1 2 1 1 3
4	$	$	04		1 2 1 3 2 2	58	Z	Z	58		3 1 2 3 1 1
5	%	%	05		1 3 1 2 2 2	59	[	[	59		3 3 2 1 1 1
6	&	&	06		1 2 2 2 1 3	60	\	\	60		3 1 4 1 1 1
7	'	'	07		1 2 2 3 1 2	61	]	]	61		2 2 1 4 1 1
8	(	(	08		1 3 2 2 1 2	62	^	^	62		4 3 1 1 1 1
9	)	)	09		2 2 1 2 1 3	63	_	_	63		1 1 1 2 2 4
10	*	*	10		2 2 1 3 1 2	64	NUL	`	64		1 1 1 4 2 2
11	+	+	11		2 3 1 2 1 2	65	SOH	a	65		1 2 1 1 2 4
12	,	,	12		1 1 2 2 3 2	66	STX	b	66		1 2 1 4 2 1
13	-	-	13		1 2 2 1 3 2	67	ETX	c	67		1 4 1 1 2 2
14	.	.	14		1 2 2 2 3 1	68	EOT	d	68		1 4 1 2 2 1
15	/	/	15		1 1 3 2 2 2	69	ENQ	e	69		1 1 2 2 1 4
16	0	0	16		1 2 3 1 2 2	70	ACK	f	70		1 1 2 4 1 2
17	1	1	17		1 2 3 2 2 1	71	BEL	g	71		1 2 2 1 1 4
18	2	2	18		2 2 3 2 1 1	72	BS	h	72		1 2 2 4 1 1
19	3	3	19		2 2 1 1 3 2	73	HT	i	73		1 4 2 1 1 2
20	4	4	20		2 2 1 2 3 1	74	LF	j	74		1 4 2 2 1 1
21	5	5	21		2 1 3 2 1 2	75	VT	k	75		2 4 1 2 1 1
22	6	6	22		2 2 3 1 1 2	76	FF	l	76		2 2 1 1 1 4
23	7	7	23		3 1 2 1 3 1	77	CR	m	77		4 1 3 1 1 1
24	8	8	24		3 1 1 2 2 2	78	SO	n	78		2 4 1 1 1 2
25	9	9	25		3 2 1 1 2 2	79	SI	o	79		1 3 4 1 1 1
26	:	:	26		3 2 1 2 2 1	80	DLE	p	80		1 1 1 2 4 2
27	;	;	27		3 1 2 2 1 2	81	DC1	q	81		1 2 1 1 4 2
28	<	<	28		3 2 2 1 1 2	82	DC2	r	82		1 2 1 2 4 1
29	=	=	29		3 2 2 2 1 1	83	DC3	s	83		1 1 4 2 1 2
30	>	>	30		2 1 2 1 2 3	84	DC4	t	84		1 2 4 1 1 2
31	?	?	31		2 1 2 3 2 1	85	NAK	u	85		1 2 4 2 1 1
32	@	@	32		2 3 2 1 2 1	86	SYN	v	86		4 1 1 2 1 2
33	A	A	33		1 1 1 3 2 3	87	ETB	w	87		4 2 1 1 1 2
34	B	B	34		1 3 1 1 2 3	88	CAN	x	88		4 2 1 2 1 1
35	C	C	35		1 3 1 3 2 1	89	EM	y	89		2 1 2 1 4 1
36	D	D	36		1 1 2 3 1 3	90	SUB	z	90		2 1 4 1 2 1
37	E	E	37		1 3 2 1 1 3	91	ESC	{	91		4 1 2 1 2 1
38	F	F	38		1 3 2 3 1 1	92	FS	|	92		1 1 1 1 4 3
39	G	G	39		2 1 1 3 1 3	93	GS	}	93		1 1 1 3 4 1
40	H	H	40		2 3 1 1 1 3	94	RS	~	94		1 3 1 1 4 1
41	I	I	41		2 3 1 3 1 1	95	US	DEL	95		1 1 4 1 1 3
42	J	J	42		1 1 2 1 3 3	96	FNC 3	FNC 3	96		1 1 4 3 1 1
43	K	K	43		1 1 2 3 3 1	97	FNC 2	FNC 2	97		4 1 1 1 1 3
44	L	L	44		1 3 2 1 3 1	98	SHIFT	SHIFT	98		4 1 1 3 1 1
45	M	M	45		1 1 3 1 2 3	99	CODE C	CODE C	99		1 1 3 1 4 1
46	N	N	46		1 1 3 3 2 1	100	CODE B	FNC 4	CODE B		1 1 4 1 3 1
47	O	O	47		1 3 3 1 2 1	101	FNC 4	CODE A	CODE A		3 1 1 1 4 1
48	P	P	48		3 1 3 1 2 1	102	FNC 1	FNC 1	FNC 1		4 1 1 1 3 1
49	Q	Q	49		2 1 1 3 3 1	103	START(CODE A)				2 1 1 4 1 2
50	R	R	50		2 3 1 1 3 1	104	START(CODE B)				2 1 1 2 1 4
51	S	S	51		2 1 3 1 1 3	105	START(CODE C)				2 1 1 2 3 2
52	T	T	52		2 1 3 3 1 1						B S B S B S B
53	U	U	53		2 1 3 1 3 1		STOP				2 3 3 1 1 1 2

Tabela 2.1.15 Code 128 karakter set

Napomena: Ako numeričko polje sadrži šest ili više cifara, vrši se šiftovanje na kodni set Code C, da bi se smanjila dužina simbola. Ako u numeričkom nizu postoji neparan broj cifara, zadnja cifra u nizu kodira se kodnim setom Code A ili Code B. Za izračunavanje dužine simbola, parni broj cifara će se uračunati u D, a zadnja cifra će se uključiti u C.

Slika 2.1.19 Struktura Code 128 simbola

Dekodiranje svakog karaktera Code128 počinje sa određivanjem razmaka između susjednih rastućih i susjednih opadajućih ivica u karakteru (Slika 2.1.20). Dekodiranje se sastoji iz sljedećih koraka:

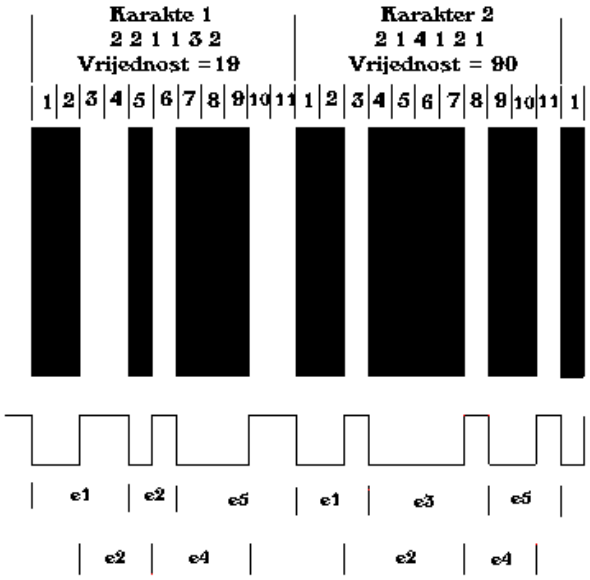
1. Skeniranje simbola sa optičkim uređajem koji mjeri količinu reflektovane svjetlosti od simbola. Količina reflektovane svjetlosti od trake, različita je od količine reflektovane svjetlosti od međuprostora, pa se na izlazu skenirajućeg sistema dobija analogni talasni oblik.
2. Digitalizovanje analognog signala, tj njegovo pretvaranje u povorku pravougaonih impulsa.
3. Dekodiranje svakog karaktera na osnovu traka/međuprostor obrasca, i provjera da li svaki karakter zadovoljava uslove parnosti traka i međuprostora.
4. Provjera dali je broj elemenata (traka i međuprostora) jednak šestostukom broju dekodiranih karaktera plus jedan za stop karakter.
5. Izračunavanje širina e_1, e_2, e_3, e_4 i e_5 i konvertovanje dobijenih vrijednosti u najbliže cijele brojeve E_1, E_2, E_3, E_4 i E_5.
6. Dekodiranje karaktera upotrebom pet dobijenih vrijednosti E_1, E_2, E_3, E_4 i E_5 kao ključa. U primjeru sa slike 2.1.20 prvom karakteru pripada niz “″221132″ i ako je korektno odštampan za njega se dobijaju sljedeće vrijednosti razmaka: E_1=4, E_2=3, E_3=2, E_4=4 i E_5=5.
7. Poslednji korak je izračunavanje kontrolnog karaktera po modulu 103 (Prilog 2) i njegovo poređenje sa dekodiranim karakterom sa kraja simbola.

Karakteri sa Slike 2.1.20 mogu sadržavati različite informacije, što zavisi od izbora startnog karaktera (koji će im prethoditi).

Ako se za startni karakter izabere Start A (Kodna riječ 103) dekodirani niz će biti ″3 (Sub)″ (gdje je (Sub) ASCII Substitute karakter).

Ako se za startni karakter izabere Start B (Kodna riječ 104) dekodirani niz će biti ″3z″.

Ako se za startni karakter izabere Strat C (Kodna riječ 105) dekodirani niz će biti ″1990″.



Slika 2.1.20 Očitavanje karaktera Code 128 simbola

Na slici 2.1.21 je pokazano kako se jedan Code 128 simbol koji ima identične simbole karaktera podataka a različite START karaktere dekodira u različite nizove podataka.

Slika 2.1.21 Code 128 simboli koji imaju identične karaktere podataka a različite START karaktere kodiraju različite nizove podataka.

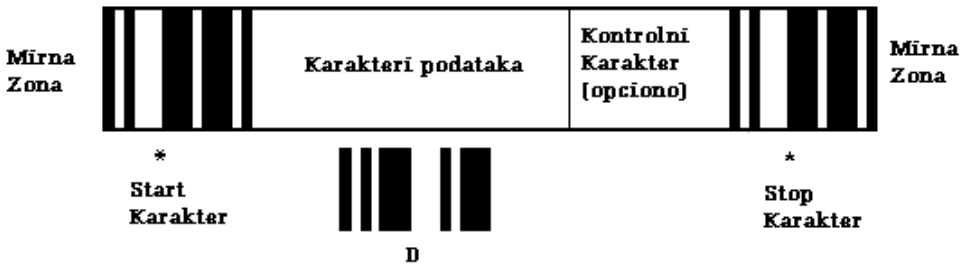
Code 39

Često korištena simbologija trakastog koda je i Code 39. Code 39 (ranije poznat kao Code 3 of 9 i 3 of 9 Code) je širinski kod, razvijen 1975. godine od strane Dr. David Allais i Ray Stevens iz Interface Mechanisms (kasnije Intermec). Ime Code 39 ukazuje da je originalni karakter set imao 39 karaktera (danas Code 39 ima 43 karaktera) i govori o strukturi koda. Naime, svaki karakter u Code 39 karakter setu predstavljen je sa 5 traka i 4 međuprostora i od ukupno devet elemenata tri su široka a šest je uskih (3 of 9). Kompletan karakter set je pokazan u Tabeli 2.1.16 i uključuje sart/stop karakter (predstavljen sa ″*″), 43 karaktera podataka od čega je 10 cifara i 26 slova alfabeta, SPACE, i šest simbola (-, ., $, /, + i %).

Char.	Obrazac	Bars	Spaces	Char.	Obrazac	Bars	Spaces
1		10001	0100	M		11000	0001
2		01001	0100	N		00101	0001
3		11000	0100	O		10100	0001
4		00101	0100	P		01100	0001
5		10100	0100	Q		00011	0001
6		01100	0100	R		10010	0001
7		00011	0100	S		01010	0001
8		10010	0100	T		00110	0001
9		01010	0100	U		10001	1000
0		00110	0100	V		01001	1000
A		10001	0010	W		11000	1000
B		01001	0010	X		00101	1000
C		11000	0010	Y		10100	1000
D		00101	0010	Z		01100	1000
E		10100	0010	-		00011	1000
F		01100	0010	.		10010	1000
G		00011	0010	Space		01010	1000
H		10010	0010	*		00110	1000
I		01010	0010	$		00000	1110
J		00110	0010	/		00000	1101
K		10001	0001	+		00000	1011
L		01001	0001	%		00000	0111

Tabela 2.1.16 Code 39 Karakter set

Kod Code 39 je promjenljive dužine. Maksimalna dozvoljena dužina simbola zavisi od upotrijebljene opreme za čitanje. Code 39 je diskretan kod, što znači da svaki karakter u kodu počinje i završava se sa trakom i svaka dva karaktera u simbolu mora razdvajati međuprostor. Kod je bidirekcion, odnosno, može se skenirati s′lijeva na desno i s′desna na lijevo. Jedinstveni karakter, obično predstavljen ″*″, koristi se kao start i stop karakter. Simbol Code 39 sastoji se iz vodeće mirne zone, startnog karaktera, odgovarajućih karaktera podataka, kontrolnog karaktera (opciono), stop karaktera i završne mirne zone (Slika 2.1.22).



Slika 2.1.22 Struktura Code 39 simbola

Dužina Code 39 simbola može se izračunati iz sljedeće formule:

$$L = (((C + 2) \cdot (3 \cdot N + 6) \cdot X + ((C + 1) \cdot I)) + 2Q$$

gdje je:
L= dužina simbola;
C= broj karaktera podataka;
X= širina uskog elementa (X dimenzija);
N= odnos širina širokog i uskog elementa;
I = širina razdvojnog međuprostora;
Q= širina mirne zone.

Iako neki industrijski standardi preporučuju da odnos širina širokog i uskog elementa u simbolu bude između 2:1 i 3:1, preporučljivo je uzeti odnos 3:1.

Važan parametar Code 39 koda je nominalna širina uskog elementa i nominalni odnos širokog i uskog elementa. Minimalna nominalna širina uskog elementa (X dimanzija) je 0.6mm pri direktnom štampanju na naboranu površinu. Inače, minimalna nominalna širina uskog elementa je 0.33mm i ne preporučuje se da bude manja od 0.25mm. Nominalna širina elemenata kao i odnos širina širokog i uskog elementa ne smiju se mijanjati unutar jednog simbola.

Snažna zaštita na nivou kraktera (*self-checking*) omogućuje da Code 39 ima visok nivo bezbjednosti podataka. Sa korektnom opremom za čitanje koda i veoma dobro oštampanim simbolom, može se očekivati samo jedna greška zamjene (pročitan jedan karakter umjesto drugog) u nekoliko miliona očitanih karaktera.

1991. godine Center for Automatic Identification u Ohio University (pod sponzorstvom AIM-USA) i Health Industry Business Communications Council (HIBCC) izvršili su testiranje simbologija trakastog koda. Između ostalog, vršeno je ispitivanje pouzdanosti očitavanja Code 39, Code 128 i U.P.C.-A simbologija, skeniranih pod istim uslovima. Dobijeni rezultati dati su u Tabeli 2.1.17

Tabela 2.1.17 Rezultati ispitivanja pouzdanosti očitavanja Code 39, Code 128, U.P.C simbologija		
Simbologije	**Najgori slučaj**	**Najbolji slučaj**
Code 39	1 greška u 2.500.000	1 greška u 34.000.000
Code 128	1 greška u 2.800.000	1 greška u 37.000.000
U.P.C.-A	1 greška u 394.000	1 greška u 800.000

Ovaj koeficijent greške je toliko bolji, nego kada se unos podataka vrši pomoću tastature, da upotreba kontrolnog karaktera može izgledati suvišna. Međutim, snažan podsticaj za uvođenje kontrolnog karaktera je mogućnost da zbog nekog razloga simbol trakastog koda ne može biti ispravno pročitan. U tom slučaju, kontrolni karakter služi da se prepozna ta situacija i za kontrolu tačnosti podataka unijetih pomoću tastature.

Kontrolni karakter koda Code 39 obično se izračunava tako što se sabere vrijednost modula svakog karaktera i podijeli sa 43. Ostatak dijeljenja predstavlje vrijednost modula kontrolnog karaktera. Ovakav, jednostavani postupak, će dati isti kontrolni karakter za nizove karaktera 123456 i 123546 (moduo 21 ili karakter L). Znači kontrolni karakter izračunat primjenom tradicionalnog modula 43 neće registrovati bilo kakvu permutaciju unuta niza karaktera podataka. Zamjena mjesta karakterima je česta greška kod unosa podataka sa tastature, naročito kada dužina niza karaktera poraste. Zbog toga je neophodno razlikovati pozicije karaktera u nizu karaktera, na primjer, na način što će se svakoj poziciji dodijeliti odgovarajuća težina. Na taj način dobijamo izračunavanje kontrolnog karaktera po težinskom modulu 43 [1].

2.1.1.4 Druge jednodimenzione simbologije

Osim do sada pokazanih, postoji oko pedeset drugih simbologija trakastog koda. U ovom odjeljku biće, kratko opisano sljedećih šest simbologija: Codabar, Code 93, Plessey, BC412 i BC309 i Postnet code. Ovih šest simbologija je odabrano jer imaju značajnu primjenu u današnjim sistemima sa trakastim kodom. Codabar je prikazan zbog njegove široke upotrebe od strane U. S. Federal Express-a i zajednice za obradu krvi. Code 93 je opisan zato što prilikom kodiranja alfanumeričkih informacija ima veću gustinu od Code 128 (u čisto numeričkim informacijama Code 128 ima veću gustinu). Plessey je diskutovan zato se njegova primjena, od najprije samo na policama nakih maloprodajnih objekata, kasnije znatno proširila. BC412 kod i njemu sličan BC309 kod su pokazani zato što predstavljaju standard za markiranje poluprovodničkih pločica. Postnet je opisan zato što se koristi u U.S. Postal Service.

CODABAR

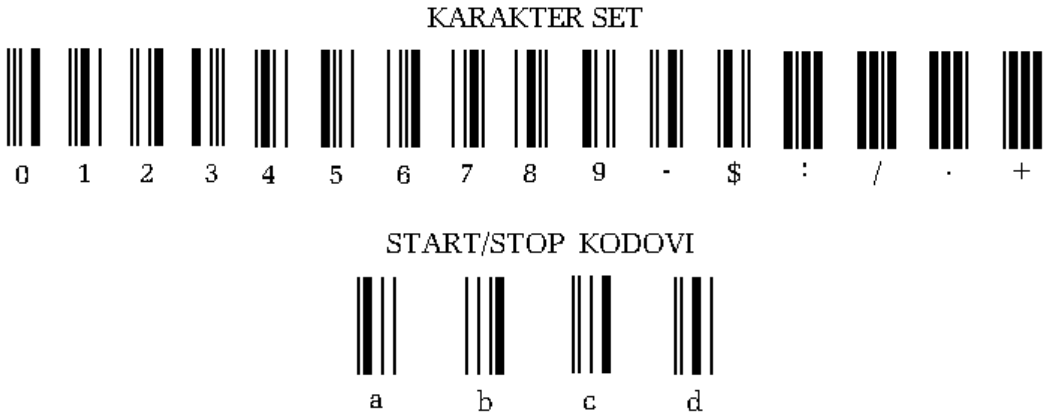
Codabar se pojavio 1972. godine. Razvio ga je Monarch Marking System i namijenio za cjenovne etikete u maloprodajnim objektima. Međutim kako je kasnije za ove namjene opšte prihvaćen U.P.C. kod Codabar se preusmjerio za markiranja u industriji.

U 1977. godini je formalno usvojeno, od strane Committee for Commonality in Blood Banking Automation (CCBBA), da se Codabar koristi za markiranje proizvoda krvi.

Codabar ima četiri karaktera koja mogu predstavljati START ili STOP karakter. Ovo omogućava 16 različitih kombinacija koje se mogu iskoristiti za jedinstveno identifikovanje različitih tipova podataka. CCBBA kombinuje START i STOP kodove sa najviše još jednim dodatnim identifikatorom (iza START koda i ispred STOP koda) za specificiranje namjene koda (na primjer: kod za identifikaciju krvne grupe, identifikaciju uzoraka krvi, itd.).

Codabar je diskretni, širinski, self-checking kod promjenjive dužine. Karkater set sadrži 16 karaktera (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, -, $, :, /, . i +) plus četiri karaktera za predstavljenje start/stop obrazaca. Karakteri se sastoje od četiri trake i tri međuprostora između i pokazani su na slici 2.1.23. Na slici 2.1.24 dat je primjer Codabar simbola. 12 osnovnih karaktera (0 do 9, - i $) konstruisani su kao kodovi 2 od 7, što znači da su od sedam raspoloživih elemenata dva široka (jedna traka i jedan međuprostor). Ostala četiri karaktera, zajedno sa četiri start/stop karaktera, konstruisani su kao 3 od 7. Odnos širokih i uskih elemenata je između 2:1 ili 3:1 (preporučuje se 3:1). Iidentification Manufactures (AIM) specificira da minimalna X dimenzija na smije biti manja od 0.2mm (preporuka: 0.33mm). Širina razdvojnog međuprostoraje između 1X i 5.3X.

Da bi poboljšao tačnost unosa podataka pomoću tastature kada simbol nije moguće skenirati, Codabar ponekad primjenjuje kontrolni karakter izračunat po modulu 16.



Slika 2.1.23 Codebar karakter set

Slika 2.1.25 Primjer Codabar simbola

CODE 93

Code 93 je uveden 1982 godine, od strane Intermec-a, kao konkurentna simbologija Code 128 simbologiji i za obezbjeđivanje dopunskog karakter seta, karakter setu Code 39 (Code 128 je uveden 1981 u cilju dobijanja koda veće gustine nego li kod Code 39).

Svaki karakter sadrži 9 modula, aranžiranih u tri trake i tri međuprostora. Ovako oraganizovan Code 93 može kodirati 56 različitih karaktera. Karakter set je pokazan u Tabeli 2.1.18 sadrži samo 48 od tih 56 karaktera (43 od njih se poklapaju sa Code 39 karakter setom a četiri se koriste kao kontrolni karakteri kada se kodira kompletan ASCII karakter set (prošireni Code 93).

	Karakt	Simbol karaktera	Binarni oblik karaktera		Karakt	Simbol karaktera	Binarni oblik karaktera
0	0		100010100	24	O		100101100
1	1		101001000	25	P		100010110
2	2		101000100	26	Q		110110100
3	3		101000010	27	R		110110010
4	4		100101000	28	S		110101100
5	5		100100100	29	T		110100110
6	6		100100010	30	U		110010110
7	7		101010000	31	V		110011010
8	8		100010010	32	W		101101100
9	9		100001010	33	X		101100110
10	A		110101000	34	Y		100110110
11	B		110100100	35	Z		100111010
12	C		110100010	36	-		100101110
13	D		110010100	37	.		111010100
14	E		110010010	38	SPACE		111010010
15	F		110001010	39	$		111001010
16	G		101101000	40	/		101101110
17	H		101100100	41	+		101110110
18	I		101100010	42	%		110101110
19	J		100110100	43	($)		100100110
20	K		100011010	44	(%)		111011010
21	L		101011000	45	(/)		111010110
22	M		101001100	46	(+)		100110010
23	N		101000110		START		101011110
					STOP		1010111101

Tabela 2.1.18 Code 93 karakter set

Code 93 je kontinualan kod promjenjive dužine ali bez *self-checking*-a. Simbol posjeduje dva kontrolna karaktera izračunata po modulu 47. Širine traka i međuprostora mogu biti jedan, dva, tri, četiri ili pet modula. Da bi se obezbijedila imunost o;itavanja na pojavu ″razlivanja mastila″ koristi se pomenuta tehnika dekodiranja ″ivica-susjedna slična ivica″ (edge-to-similar-edge) [1].

Ako je Code 39 oštampan sa 2:1 odnosom širokog i uskog elementa, pojedini karakter koda je širine 12 modula (12xX). Uz to Code 39 je diskretni kod, što znači da ima i međuprostor za odvajanje karaktera, koji ako je širine 1X povećava broj modula po karakteru na 13. Za razliku od Code 39, Code 128 je kontinualni simbol i svaki njegov karakter sadrži 11 modula. Code 93 je takođe kontinualni kod čiji je karakter širine 9 modula pa je znatno efikasniji pri kodiranju alfanumeričkih podataka. Međutim za numeričke podatke Code 128 je duple gustine što prevazilazi gustinu koda Code 93.

PLESSEY

Plessey Code i njegove varijante (MSI Code, Texon Code i Anker Code) imaju korijene u PWM (Pulse Width Modulatied) kodu koga je razvila Plessey Company Limited of Dorset, England. Kod se koristio za markiranje polica u bakalnicama. PWM kod predstavlja svaki bit informacije sa parom traka/međuprostor. Nulti bit se predstavlja uskom trakom koju slijedi široki međuprostor, dok jedinica sadrži široku traku i uski međuprostor.

Svaka decimalna cifra predstavljena je BCD (binary code decimal) karakterom koji sadrži četiri bita (kao što pokazuje Tabela 2.1.19). PWD kodovi nemaju *self-checking* već koriste kontrolne karaktere. MSI Code primjenjuje kontrolni karakter izračunat po modulu 10. Za start i stop karaktere Plessey i Anker kodovi koriste 1101 karakter. MSI koristi par traka/međuprostor za predstavljanje jedinice kao start karakter i par traka/međuprostor za predstavljanje nule kao stop karakter.

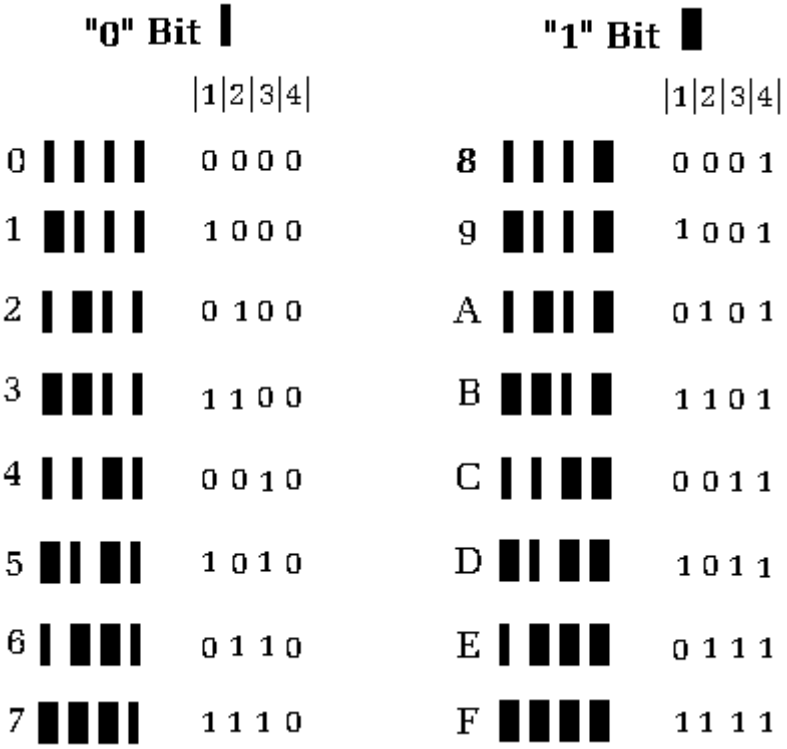


Tabela 2.1.19 Cifre BCD koda kodirane Plessey kodom

POSTNET CODE

Postnet trakasti kod je razvijen od strane U.S. Postal Service (USPS) da bi se obezbijedio sistem kodiranja informacije na pismima, koje bi se mogle čitati sa relativno jeftinim sorterima trakastih kodova. Kod se štampa u donjem desnom uglu pisama i predstavlja podatke (ZIP Code ili ZIP+4 code) pomoću dugih i kratkih traka. Prvu specifikaciju za Postnet kod dao je Mason Lilly iz U.S. Postal Service-a 1980. godine. Međutim još kasnih šesdesetih godina, pravljen je pokušaj primjene koncepta dugih i kratkih traka, ali je propao zbog nedostatka adekvatne opreme za čitanje takvih simbola.

ZIP+4 Postnet trakasti kod se sastoji od devet cifara plus kontrolna cifra. Svaka cifra se kodira sa pet traka od kojih su dvije duge, a ostale tri duplo kraće. Za različite cifre različit je i raspored dugih i kratkih traka koje ih predstavljaju. Duga traka predstavlja binarnu ″1″, a kratka traka predstavlja binarnu ″0″. Kodna struktura Postnet koda je data u Tabeli 2.1.20.

Tabela 2.1.20 Postnet Code karakter set	
Karakter	Postnet simbol
0	11000
1	00011
2	00101
3	00110
4	01001
5	01010
6	01100
7	10001
8	10010
9	10100

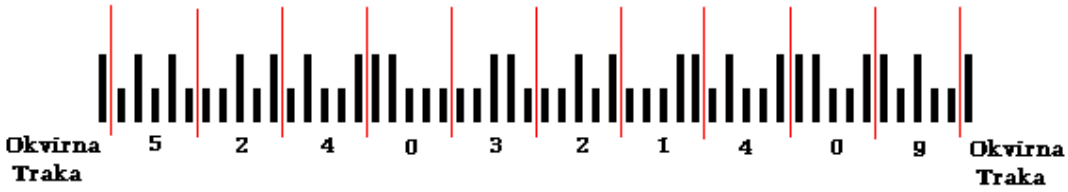
Kompletan ZIP+4 Postnet simbol sadrži 50 traka koje predstavljaju devet cifara ZIP+4 koda i jedan kontrolni karakter i plus dvije okvirne trake na oba kraja simbola. Kontrolni karakter se izračunava tako što oduzmemo sumu svih cifara po modulu 10 od 10. Na primjer , kontrolni karakter ZIP+4 koda 52403-2140 izračunavamo iz sljedeđih koraka:

Prvi korak: 5+2+4+0+3+2+1+4+0=21.

Drugi korak: 21/10=2 sa ostatkom =1.

Treći korak 10-1=9=kontrolni karakter.

Pojedine trake koje čine Postnet trakasti kod, štamapju se tako da duga traka bude visine 3.175mm±0.254mm, a kratke traka visine 1.27mm±0.127mm. Širina traka iznosi 0.508mm±0.12mm. Na osnovu ovih dimenzija, može se zaključiti da je gustina Postnet koda 8±1 traka po cm duzine. Prostor između centralnih linija susjednih traka je između1.143mm i 1.27mm. Primjer devetocifarskog ZIP+4 Postnet koda (52404-2140) je dat na Slici 2.1.26.



Slika 2.1.26 Primjer simbola devetocifarski ZIP+4 Postnet koda

Osim Postnet koda USPS primjenjuje i FIM (Facing Identification Mark) obrasce. FIM je obrazac koji sadrži 9 pozicija u kojima se može nalaziti traka. Postoji 4 FIM obrasca (A, B, C, D) i koristi se u poslovnoj pošti. Ovi obrasci su dati na Slici 2.1.27. Visina FIM traka je obično 15.876mm±3.175mm. Širina FIM trake je 0.7874mm±0.2032mm.

Slika 2.1.27 FIM obrasci

BC412

Semiconductor Equipment and Materials International (SEMI) publikovao je skicu standarda, koja je 1993. godine adaptirana za markiranje zadnje strane silikonskih pločica. Skica standarda opisuje simbol trakastog koda, nazvanog BC412, koji je varijanta FIM traka/ne obrasca. Dok u Postnet kodu ima devet pozicija u kojima se nalazi ili ne nalazi traka u BC412 postoji 12 takvih pozicija i uvijek na tačno četiri pozicije postoji traka.

BC412 je jednoširinski trakasti kod, tj kod u kojem su sve trake iste širine. Takav kod je idealan za identifikaciju poluprovodničkih ploča na koje se serijski broj urezuje pulsirajućim laserom. U poređenju sa konvencionalnim višeširinskim trakastim kodovima, jednoširinski trakasti kod omogućava bolji kvalitet markiranja, kraće vrijeme urezivanja, veću gustinu podataka i veći koeficijent pouzdanosti (štampane ploče imaju manji kontrast).

Primjena višeširinskog koda, Code 39 na primjer, u takvim aplikacijama donijela bi probleme jer pulsirajući laser pravi trake slabog kvaliteta kada je širina bara veća od prečnika njegove svjetlosne mrlje i teško može precizno ispoštovati odnos uske i široke trake u cijelom simbolu.

Relativno novi jednodimenzioni BC412 trakasti kod razvijen je od strane Computer Identics i IBM 1988. godine. Upotrijebljen za markiranje poluprovodničkih ploča, kod ima sljedeće osobine:

- može kodirati 36 alfanumeričkih karaktera,
- dvanaset modula po karakteru,
- četiri trake po karakteru
- osam modula su međuprostori,
- prvi modul u svakom karakteru je traka (sinhronizaciona traka),
- zadnji modul u svakom karakteru je međuprostor.

Sinhronizirajuća traka obezbjeđuje kodu *self-checking*, za razliku od Postnet koda koji za sinhronizaciju koristi posebno markiranje. Bidirekcionost koda je postignuta start (traka – međuprostor – međuprostor) i stop (traka- međuprostor – traka) obrascem.

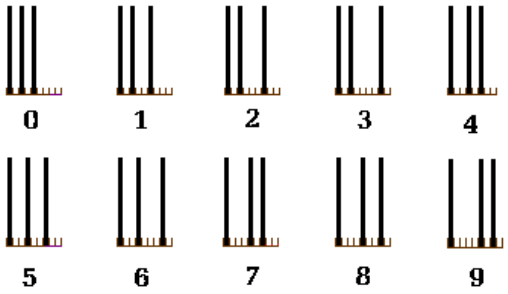
Za obezbjeđenje integriteta podataka koristi se kontrolni karakter izračunat po modulu 35 (Prilog 2). Kontrolni karakter se, takođe, može upotrijebiti za otkrivanje nečitljivih karaktera. Karakter može biti nečitljiv iz više razloga, na primjer, ako broj traka u 12-–to modulskom simbolu nije

tačno četiri, ili ako prvi modul nije traka, ili ako zadnji modul nije međuprostor. Algoritam za korekciju greške se koristi da rekonstruiše nečitjivi karakter na osnovu identifikacije njegove pozicije u kodu

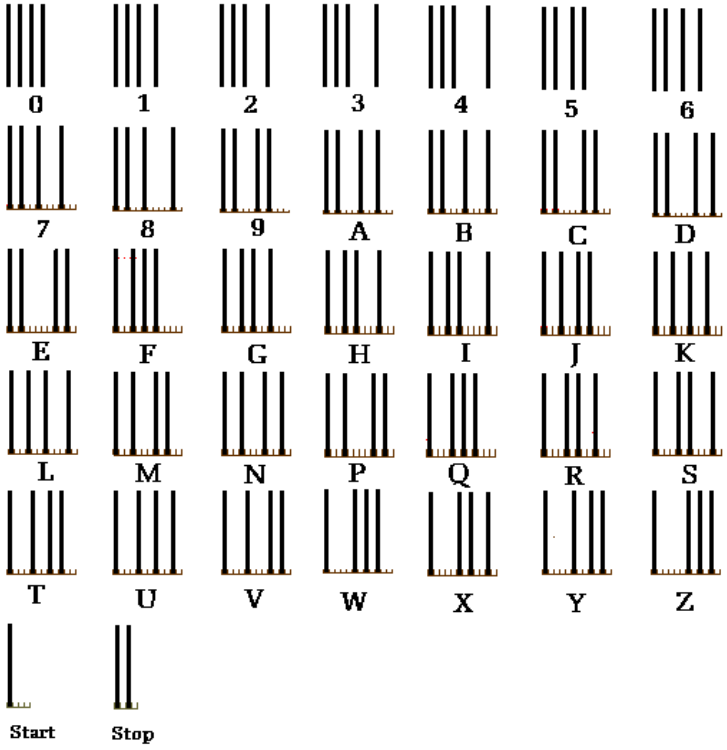
Novi trakasti kod BC412 se može uspješno primijeniti za identifikaciju pločica u poluprovodničkoj industriji. Druge, moguće, primjene BC412 koda su CD-ROM-ovi ili staklo, gdje je veome mali prostor na raspolaganju za urezivanje podataka.

Na Slici 2.1.29 prikazan je karakter set BC412 koda.

U aplikacijama koje zahtijevaju isključivo numeričke podatke može se koristiti slična simbologija zvana BC309. Dok BC412 ima četiri trake u 12 modula širokom karakteru, BC 309 ima tri trake u devet modula širokom karakteru. BC309 karakter set je pokazan na Slici 2.1.28.



Slika 2.1.28 Karakter set BC412 koda



Slika 2.1.29 Karakter set BC412 koda

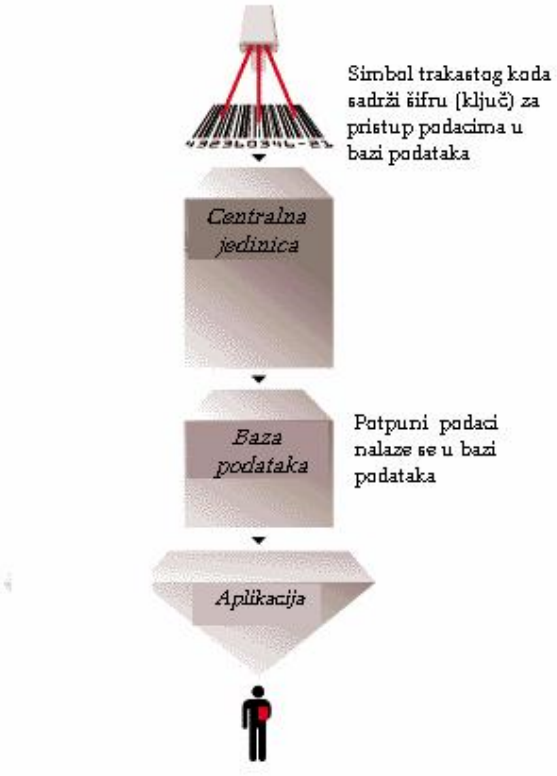
2.1.2 DVODIMENZIONALNI (MATRIČNI) TRAKASTI KODOVI

2.1.2.1 Uvod

S protokom vremena i proširivanjem spectra aplikacija, postajali su sve brojniji zahtjevi za smještanje više informacija u simbol trakastog koda. Najveći broj aplikacija trakastog koda koriste trakasti kod samo kao identifikator elementa (artikla), dok se svi ostali podaci vezani za taj element nalaze u bazi podataka (trakasti kod služi kao ključ za pristup tim podacima). Poznati primjer ovakvog pristupa je upotreba Universal Product Code (UPC) simbola u maloprodaji. Dvanaesto-cifarski kod identifikuje proizvođača i proizvod, dok se opis proizvoda, cijena, oporezovanost, informacije o inventaru i drugi podaci nalaze u bazi podataka kompjuterskog sistema (slika 2.27). Ovakva upotreba trakastog koda ima dvije značajne prednosti i to:

♦ mogućnost korišćenja velikog broja infirmacija o pojedinom elementu upotrebom
relativno kratkog koda (simbola) i

♦ mogućnost promjene podataka vezanih za element bez potrebe za promjenom
trakastog koda.



Slika 2.1.30 Jednodimnzioni trakasti kod i aplikacija na PC-u.

Ovakav pristup nije upotrebljiv u aplikacijama u kojima je nepraktično smještati potrebne podatke o elementima u bazu podataka, odnosno, tamo gdje nije moguć pristup bazi podataka. Ovo može biti slučaj, zato što element može dospjeti na mjesto gdje nije moguć pristup glavnom kompjuteru u kojem su smješteni podaci o elementu.

Alternativa za ovakve slučajeve bi bila upotreba dužih trakastih kodova koji bi sadržavali sve potrebne informacije, kao što su ime proizvoda, proizvođač, cijena, težina, datum proizvodnje, itd. Na ovaj način podaci bi bili na raspolaganju bez potrebe za pristupom bazi podataka. Međutim, povećenjem dužine trakastog koda javlja se problem njegovog štampanja na male elemente (na primjer poluprovodničke komponente i sklopove).

Drugo rješenje ovog problema moglo bi biti korišćenje elektronske razmjene podataka između udaljenih računara. Ideja se satoji u tome da se, upotrebom standardnih protokola i formata, sa udaljenog računara podaci prenesu lokalnom računaru kada mu zatrebaju. Problemi sa ovim pristupom su što on poskupljuje i usporava upotrebu trakastih kodova (aplikaciju).

Treća mogućnost, za rješenje ovog problema, je povećanje gustine informacija u simbolu trakastog koda. Osnovni problem prilikom kodiranja informacija, na nekom medijumu, je obezbjeđenje što niže cijene kodiranja. Tu se susrijeću sljedeći konfliktni zahtjevi:

- ♦ Simbol treba da ima veliku gustinu informacija;
- ♦ Simbol mora biti pouzdano čitljiv;
- ♦ Kreiranje (štampanje) simbola treba biti što jeftinije;
- ♦ Simbol treba da bude čitljiv i sa relativno jeftinom opremom.

Kako je potpuno zadovoljenje svih ovih zahtjeva nemoguće, mora se ići na optimalni kompromis.

Zbog široke upotrebe riječi karakter, da bi se smanjila mogućnost zabune, u daljem tekstu ćemo karakter trakastog koda nazivati ″kodna riječ″.

Kod svih širinskih kodova , kao što u Interleaved 2 of 5, Code 39, i Codeabar, u svakoj kodnoj riječi postoji isti broj elemenata (m) od kojih je, uvijek, w širokih. Zato se kodna riječ često predstavlje kao uređeni par (m,w). Code 39, na primjer, ima devet elemenata od kojih su tri široka pa se kodna riječ može predstaviti kao uređeni par (9,3). Tabela 2.1.21 pokazuje neke osnovne karakteristike širinskih kodova Interleaved 2 of 5, Code 39, i Codeabar. U Tabeli 2.1.21 predpostavlje se da je odnos širokog i uskog elemnta u svim simbolima svih kodova 2.5:1. Količina informacija je dobivena kao funkcija broja modula u kodnoj riječi i broja kodnih riječi koje mogu biti generisane [22].

Tabela 2.1.21 Karakteristike nekih širinskih kodova					
(m,w)	**Broj mogućih kodnih riječi**	**Broj korišćenih Kodnih riječi**	**Ukupna širina (u modulima)**	**Količina Informacije**	**Naziv koda**
5,2	10	10	8	0.415	Interleaved 2of 5
9,3	84	44	13.5	0.404	Code 39
7,2	21	16	10	0.400	Codabar

Unutar svake kodne riječi, kod delta kodova, kao što su U.P.C., Code 49, Code 93, Code 128, Code 16K, i PDF417, postoji konstantan broj modula i konstantan broj traka i međuprostora. Code 93, na primjer, ima devet modula u kodnoj riječi, tri trake i tri međuprostora. Delta kodovi se takođe mogu predstaviti uređenim parom ″(n, k)″, gdje je ″n″ broj modula a ″k″ broj traka/međuprostora. Broj mogućih kodnih riječi koje mogu biti konstruisane za dati delta kod (C) izračunava se kao:

$$C = \frac{(n-1)!}{(2k-1)!(n-2k)!}$$

Kao primjer, izračunati ćemo broj kodnih riječi za U.P.C. kod. Znamo da je kodna riječ U.P.C. sastavljena iz sedam modula, dvije trake i dva međuprostora i može se predstaviti parom (7,2). Izračunavanjem vrijednosti svake zagrade imamo:

$$(n-1)!=(7-1)!=6!=6\cdot5\cdot4\cdot3\cdot2\cdot1=720$$
$$(2k-1)!=(2\cdot2-1)=(4-1)!=3!=6$$
$$(n-2k)!=(7-2\cdot2)!=(7-4)!=3!=6$$

pa se za C dobija

$$C = \frac{720}{6\cdot6} = 20$$

U.P.C. koristi svih 20 kodnih riječi i to 10 za lijevu stranu simbola i 10 za desnu stranu simbola. Tabela 2.1.22 pokazuje neke karakteristike pomenutih delta kodova.

Tabela 2.1.22 Karakteristike nekih Delta kodova					
(n,k)	Broj mogućih Kodnih riječi	Broj korišćenih kodnih riječi	Ukupna širina (u modilima)	Količina informac.	Naziv koda
7,2	20	20	7	0.617	U.P.C./EAN
9,3	56	48	9	0.645	Code 93
11,3	252	106	11	0.725	Code 128
16,4	6435	4802	16	0.791	Code 49
11,3	252	106	11	0.725	Code 16K
17,4	11440	929	17	0.793	PDF417

Postoji više načina da se poveća gustina informacija u simbolima trakastog koda. Jedan od načina je da se razvije novi jednodimenzionalani simbol primjenom delta kodiranja. Tehnika delta kodiranja omogućava veću gustinu informacija nego širinsko kodiranje. Tako kodovi Code 128 i Code 93 imaju približno 43 postotka veću gustinu od širinskih kodova, pod uslovom da su im moduli istih širina.

Drugi način je smanjenje širine modula (uže X). Međutim smanjenjem X dimenzije takođe se smanjuje i tolerancija prilikom štampanja, zahtijeva se mnogo preciznije kreiranje simbola, a kao posljedica toga povećava se cijena.

Gustinu informacija u simbolu trakastog koda moguće je povećati i smanjenjem visine traka i zatim slaganjem simbola jedan na vrh drugoga. Tako su kreirani dvodimenzionalni kodovi MLC 2D, Code 16K i neke vrste Code 49. Nedostatak ovih kodova ogleda se u postojanju razdvojne trake između posloženih redova. Razdvojna traka smanjuje smanjuje količinu informacija koja može biti smještena u određenom prostoru, ali sprječava interferenciju između redova (Slika 2.1.31).

Razvojem tehnike skeniranja redova bez razdvojne trake između njih i mogućnosti povezivanja tako dobijenih informacija dovela je do pojave kodova bez razdvojne trake. Najpoznatiji takav dvodimenzionalni kod je PDF417 za čije korištenje je potreban znatno snažnija računarska podrška.

Upotrebom dvodimenzionalnih kodova moguće je na malom prostoru smjestiti stotine karaktera podataka. Na taj način je moguće osim samo šifre proizvoda i proizvođača (U.P.C./EAN) u simbol trakastog koda smjestiti i razne druge podatke i tako minimizirati potrebu za pristupanje udaljenoj bazi podataka. Ovakvi trakasti kodovi postaju zapravo prenosivi fajlovi podataka. Ključ za pristup detaljnijim podacima sadržan je i u ovim simbolima.

U ostatku ovog poglavlja dat je detaljniji pregled neki poznatijih dvodimenzionalnih kodova.

2.1.2.2 MLC 2D

1989. godine njemačka firma ICS Identcode napravila je tri verzije dvodimenzionalnog višelinijskog koda MLC 2D – (Multi-line Code two-dimensional).

Verzija Codablock A satoji se od redova trakastog koda Code 39 posloženih jedan na vrh drugog, pri čemu su trake i međuprostori skraćeni i postoji razdvojna horizontana traka. Simbol ove verzije MLC 2D trakastog koda, može sadržavati do 1320 karaktera koji se kodiraju u najviše 22 reda.

Verzija Codablock F koristi Code 128 u svojoj strukturi, sa svim alfanumeričkim kodnim riječima i numeričkim kodnim riječima, dvostruke gustine.

Verzija Codablock N u svojoj strukturi (redovima koda) koristi Interleaved 2 of 5 simbologiju i može kodirati do 600 karaktera u jedan do dest redova.

Svaki simbol MLC 2D koda posjeduje strukturu neke jednodimenzione simbologije, start i stop kodni obrazac i dva karaktera u svakom redu koji daju informaciju koji je to red.

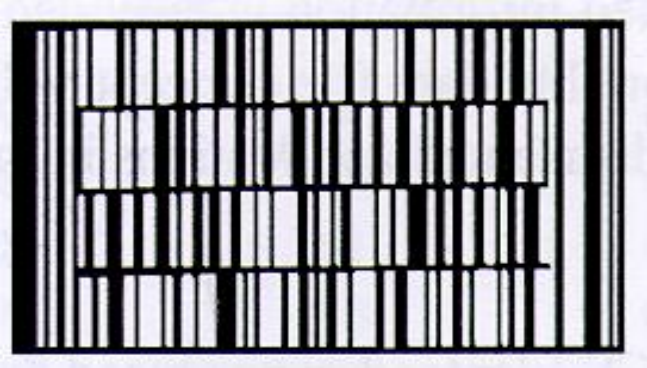
Veličinu simbola definiše oprema za štamapanje i oprema za čitanje koda. ICS Identprint MLC 2D štamparski program predlaže 0.2 mm širinu najuže trake sa 2:1 i 3:1 odnosom širina i 7 mm visinu trake.

U Codablock A verziji u jednom redu koda može biti od 2 do 61 kodne riječi.

Zbirne krakteristike MLC 2D kodova date su u Tabeli 2.1.23, a primjer Codablock A verzije dat je na Slici 2.1.31.

MLC 2D kod se skenira red po red, a za povezivanje tako dobijenih podataka koriste se kodne riječi koji označavaju broj reda. Prve primjene ovog koda bile su za etiketiranje u medicini i elektronici (medicinske informacije – hemijski sastav supstance i sl.)

Tabela 2.1.23 Karakteristike MLC 2D koda					
MLC 2D kod	**Kodirajući Karakter Set**	**Osnovna Simbologija u redovima**	**Tip Koda**	**Maximalna Gustina Karaktera**	**Maximalan Broj karaktera u simbolu**
Codablock A	Alfa-numericki (velika slova) –,·,Space,$ /,+ i %	Code 39	Diskretni	Određena nedefinisanom visinom trake	1320 u 1 do 22 reda
Codablock F	Potpuni alfanumerički, numericki duple gustine, 3 start, 1stop kod 4 kontrolna koda	Code 128	Kontinualni	Određena nedefinisanom visinom trake	420 u 1 do 7 reda
Codablock N	Numeričke Cifre 1 - 9	Interleaved 2 of 5	Kontinualni	Određena nedefinisanom Visinom trake	2728 u 1 do 62 reda



Slika 2.1.31 Primjer MLC 2D Codablok A simbola

2.1.2.3 Code 16K

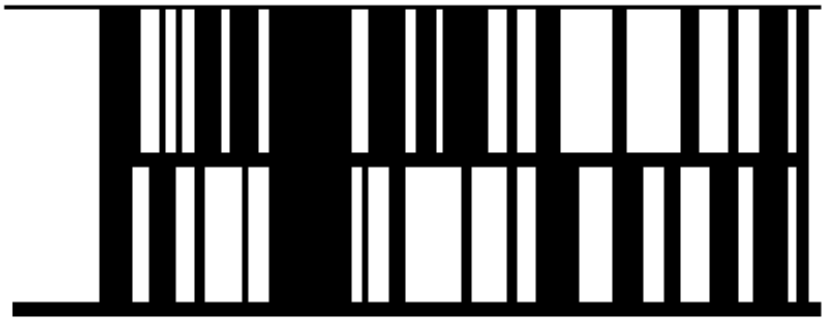
U 1988. godini Laserlight Systems uvodi kod Code 16K. Code 16K može imati između 2 i 16 redova. Redovi 1 do 8 imaju uzastopne startne obrazace razvijene iz UPC/EAN Number Set L (0 do 6 i 9) i uzastopne stop obrasce razvijene iz UPC/EAN Number Set R (0 do 6 i 9). Redovi 9 do 16 imaju uzastopne startne obrasce razvijene iz UPC/EAN Number Set L (0 do 6 i 9) i uzastopne stop obrasce razvijene iz UPC/EAN Number Set R (4 do 6, 9, 0 do 3). Ovi obrasci obezbjeđuju numerisanje redova.

Svaki red ima vodeću mirnu zonu, dužine 10X, startni obrazac (7 modula), sinhronizacionu traku (1X), 5 kodnih riječi iz invertovanog Code 128 karakter seta (11 modula svaki), stop obrazac (7 modula), i završnu mirnu zonu minimalne širine 1X. Svaki red u simbolu koda sadrži 70 modula, plus 11 za mirne zone. Simboli koji imaju između dva i deset redova imaju minimalnu visinu reda 8X. Maksimalna visina simbola ne smije preći 80X, da bi se mogla uspješno skenirati dvosdimenzionalnom skenirajućom glavom, na primjer, matričnim CCD uređajem. Zadnji red sadrži dva kontrolna karaktera po modulu 107 [23]. Kontrolni karakteri smanjuju, za dva, broj kodnih riječi u zadnjem redu. Karakter set za Code 16K uključuje svih 103 Code 128 karaktera, plus kodne riječi za ″pad″,″shift″, ″double shift″, i ″triple shift″, ukupno 107 kodnih riječi. Kodne riječi shift, double shift, triple shift omogućuju pomjeranje na drugi kodni set i zatim vraćanje nazad na originalni kodni set. Karakteri iz Code 128 karakter seta se u Code 16K kodu koriste sa invertovanim traka/međuprostor obrascem. Ne primjer, Code 128 obrazac BSBSBS, u kodu Code 16K je SBSBSB (B – traka, S-međuprostor).

Osnovne krakteristike koda Code 16K grupisane su u Tabeli 2.1.24

Primjer koda Code 16K dat je na slici 2.29.

Tabela 2.1.24 Karakteristike koda Code 16K
Kodni karakter setovi: Code Set A –ASCII Alfabet (velika slova), Brojevi, Interpunkcija i Kontrolni karakteri Code Set B – ASCII Alfabet (velika i mala slova), Brojevi, i Interpunkcijski karakteri Code Set C – Brojevi dvostruke gustine
Tip Koda: Kontinualni
Samokontrola karaktera: Postoji
Veličina simbola: Promjenjiva
Bidirekciono Dekodiranje: Da
Broj karaktera za indikaciju reda u jednom redu: 2 uključena u start/stop obrazac
Najmanja nominalna širina elementa: Limitirana jedino od strane tehnologije štampanja i tehnologije čitanja.
Najmanja nominalna visina elementa: 0.254mm
Maximalna gustina podataka: Karakter setovi A i B (alfanumerički modeli) – 18 ASCII karaktera po kvadratnom cm Karakter set C (numerički model) – 36 numeričkih karaktera po kvadratnom cm
Maksimalan broj karaktera podataka u Simbolu: Karakter setovi A i B (alfanumerički modeli) – 78 ASCII karaktera Karakter set C (numerički model) – 158 numeričkih karaktera



Slika 2.1.32 Code16K simbol

2.1.2.4 Code 49

Code 49 je dizajnirao Dr. David Allais. Uveden je od Intermec-a 1987. godine. Ovaj kod je jedan od prvih koji je koristio prednosti velike gustine delta kodiranja u naslaganoj (dvodimenzionalnoj) strukturi. Code 49 kodira 49 karaktera (0 do 9, A do Z,–, ., space, $, /, +, %, Shift 1, Shift 2, F1, F2, F3, i Numeric Shift (ns)). Upotrebom Shift 1 i Shift 2 Code 49 može kodirati čitav ASCII karakter set. Code 49 može imati od 2 do 8 redova. Svaki red sadrži 70 modula. Startni obrazac je širine dva modula a stop obrazac je širine četiri modula. Redovi su međusobno odvojeni horizontalnom trakom širine jednog modula. Minimalna visina trake je 8X.

Svaki red sadrži četiri kodne riječi. Svaka kodna riječ sadrži dva karaktera. Zadnji karakter u svakom redu je kontrolni karakter izračunat po modulu 49 za prvih sedam karaktera u redu. Ako simbol kodira broj karaktera koji ne popunjavaju do kraja zadnji red u simbolu, on se popunjava sa ″ns″ (Numeric Shift) karakterima. Code 49, takođe kodira broj reda, na osnovu jedinstvenog obrasca parnosti, pridruženog svakom redu. Tabela 2.1.25 prikazuje obrazac parnosti pridružen svakoj kodnoj riječi unutar svakog kodnog reda u simbolu. Traba zapaziti da poslije sedmog reda ne dolazi osmi red već zadnji red. Zadnji red u simbolu, bez obzira da li simbol sadrži 2, 3, 4, 5, 6, 7, ili 8 redova, ima obrazac parnosti zadnjeg reda u Tabeli 2.1.25.

Tabela 2.1.25 Obrasci parnosti za indikaciju broja reda u Code 49

	Kodna riječ 1	**Kodna riječ 2**	**Kodna riječ 3**	**Kodna riječ 4**
Red 1	Neparan	Paran	Paran	Neparan
Red 2	Paran	Neparan	Paran	Neparan
Red 3	Neparan	Neparan	Paran	Paran
Red 4	Paran	Paran	Neparan	Neparan
Red 5	Neparan	Paran	Neparan	Paran
Red 6	Paran	Neparan	Neparan	Paran
Red 7	Neparan	Neparan	Neparan	Neparan
Zadnji red	Paran	Paran	Paran	Paran

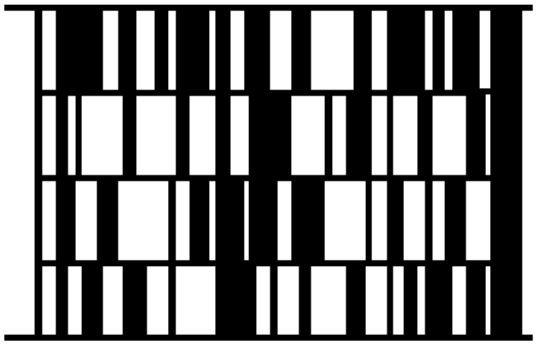
U simbolima koji imaju manje od sedam redova, zadnji red sadrži dvije kontrolne kodne riječi. Simboli koji imaju sedam ili osam redova u zadnjem redu imaju tri kontrolne riječi. Kontrolne riječi (karakteri) su izračunati po modulu 2401 [23]. Preostala kodna riječ u zadnjem redu kazuje broj redova u simbolu i mod simbola.

Postoji sedam modova Code 49. Jedan od njih je regularni alfanumerički mod (Mod 0) sa dva karaktera u jednoj kodnoj riječi. Drugi je numerički mod (Mod 2) gdje se deset cifara smješta u tri kodne riječi.

Sa jednim kontrolnim karakterom na kraju svakog reda i dvije ili tri kontrolne kodne riječi unutar svakog simbola, Code 49 spada i veoma sigurne kodove.

Sažet prikaz osnovnih karakteristika Code 49 koda dat je u Tabeli 2.1.26, a primjer koda dat je na Slici 2.1.33.

Tabela 2.1.26 Karaketristike koda Code 49
Kodni karakter setovi: Normalni mod: 0 do 9, Ado Z, –, ·, Space, $, /, +, %, Shift1, Shift2, F1, F2,F3, i Numeric Shift (ns) ASCII mod: Svih 128 ASCII karaktera (Shift 1 i Shift 2) Numerički mod: 100 brojnih vrijednosti
Tip koda: Kontinualni
Samokontrola karaktera: Ne postoji
Veličina simbola: Promjenjiva
Bidirekciono dekodiranje: Da
Broj karaktera za indikaciju reda u redu: Indikacija reda je ostvarena obrascem parnosti reda
Najmanja nominalna širina elementa: Ograničena jedino tehnologijom štampanja i tehnologijom čitanja.
Najmanja, preporučljiva, nominalna visina elementa: 0.254mm
Maksimalna gustina karaktera podataka: Alfa Mod ili ASCII: 14.4 Akfa/ASCII karaktera po kvadratnom cm Numerički model: 81 numerički karakter
Broj karaktera koji ne sadrže podatak: Jedan karakter po redu, plus 4 do 6 karaktera po simbolu
Dodatne funkcije: Edge-to-edge dekodiranje Sposobnost povezivanja Redovi mogu biti skenirani u bilo kom redosljedu Visoka sigurnost podataka



Slika 2.1.33 Code 49 Simbol

2.1.2.5 PDF 417

PDF 417 je dvodimenzionalni trakasti kod koji u jednom simbolu može kodirati oko hiljadu bajtova. Maximalan broj ASCII karaktera koji mogu biti kodirani u jednom simbolu, zavisi od šeme za kompresiju podataka. Postoji 12 šema (modova) kompresije PDF417 koda. Dva moda su standardni, i nazivaju se *printable ASCII mod* i *Binarni mod*. Preostalih 10 su korisnički modovi, koje može definisati korisnik u skladu sa specifičnom primjenom PDF417 koda. Svaki korisnički mod može kodirati 900 različitih entiteta (riječi, brojevi, etc.). Modovi se mogu mijenjati unutar simbola u skladu sa zahtjevima aplikacije.

U printable ASCII modu, maksimalan broj ASCII karaktera u simbolu je 1848. U Binarnom modu, taj broj je 1108 karaktera. U modovima koje definiše korisnik, maksimalan broj ASCII karaktera u simbolu može biti mnogo veći nego u printable ASCII modu. Ako količina podataka prelazi maksimalan kapacitet simbola, moguće je nekoliko pojadinačnih simbola povezati u oblik fajla podataka. Tako dobijeni simbol naziva se *macro* PDF417 čiji kapacitet nema logičkih ograničenja (ipak u praksi se uvijek teži da simbol bude što je moguće manji).

Svaki PDF417 simbol je sastavljen od više redova. Svaki red sadrži nekoliko kodnih riječi. Svaka kodna riječ je sastavljena iz 17 modula raspoređenih u četiri trake i četiri međuprostora. Sve kodne riječi su podijeljene u tri međusobno isključive podgrupe, takozvane klastere. Svaki klaster kodira 929 PDF417 kodnih riječi sa različitim traka/međuprostor obrascem, tako da se jedan klaster ne može zamijeniti drugim. Svaki red koristi samo jedan od tri klastera. Isti klaster se ponavlje svakog trećeg reda u simbolu. Svaka dva susjedna reda koriste različiti klaster, pa dekoder može povezati nepotpune skenove dok dekodira PDF417 simbole velike gustine.

Prva i zadnja kodna riječ u svakom redu PDF417 simbola predstavljaju indikatore reda. PDF417 posjeduje dvije kontrolne sume. Na Slici 2.1.34

dat je primjer PDF417 simbola. Osnovne karakteristike PDF417 koda date su u Tabeli 2.1.27.

Najmanja nominalna širina elementa zavisi od procesa štampanja koji je upotrijebljen, a ne od PDF417 simbologije. Moguće je štampati PDF417 simbol toliko mali koliko oprema za štampanje može realizovati, odnosno oprema za čitanje može raspoznati.

Najmanja, preporučljiva, nominalna visina elementa zavisi od karakteristika laserskog čitača koji se koristi za čitanje simbola. Ako se za čitanje koristi CCD čitač, nominalna visina može biti koliko i nominalna širina elementa.

Čitač PDF417 simbola može biti laserski skener ili CCD kamera. 1992 Symbol Technologies objavljuje PDF1000 skener, koji može obaviti 15 miliona instrukcija u sekundi i ima brzinu skeniranja od 560 skenova/sekundi [24].

Slika 2.1.34 PDF417 simbol

Tabela 2.27 Karakteristika PDF147
Kodni karakter set: Svih 128 ASCII karaktera i binarni podaci
Tip koda: Kontinualni karaktere
Veičina simbola: Promjenjiva
Bidirekciono dekodiranje: Da
Broj karaktera za indikaciju reda u pojedinom redu: 2
Minimalni broj redova u simbolu: 3
Maksimalni broj redova u simbolu: 90
Minimalni broj kolona podataka: 1
Maksimlni broj kolona podataka: 30
Broj kodnih riječi za opisivanje dužine simbola: 1
Broj kodnih riječi koje ne sadrže podatke: Četiri kodne riječi po redu + tri kodne riječi po simbolu
Dodatne funkcije: Edge–to–edge dekodiranje Povezivanje djelimičnih skenova Sposobnost korekcije greške

2.1.2.6 Code 1

Code 1, kojeg je izumio Ted Williams 1992. godine, je prva matrična simbologija. U ovom kodu trake i međuprostori realizuju se u obliku malih kodnih kvadratića. Svaki kvadratić kodira jedan bit podatka. Bijeli kvadratić označava ″0″ a crni kvadratić označava ″1″. Ovi kvadratići kodiraju 8-bitni bajtove podataka u obliku prvougaonih prostora sa dva reda od po četiri kvadratića. Bit najveće težine, u bajtu, smješta se u gornji lijevi ugao pravougaunika. Bitovi niže težine se zatim smještaju s′lijeva na desno u gornjem redu a zatim u istom smjeru u donjem redu. Bit najmanje težine smješta se u donjem desnom uglu pravoudaonika.

Code 1 može kodirati puni ASCII 128 karakter set i neke funkcijske karaktere. Simbol Code 1 se izvodi u osam različitih veličina. Najmanji simbol sadrži 160 kodnih kvadratića, a najveći 16320 kodnih kvadratića. Verzije su Code 1A, 1B, 1C, 1D, 1E, 1F, 1G, i 1H. Code 1A je najmanji simbol a Code 1H je najveći simbol. Simbol Code 1H može sadržavati 2182 alfanumerička karaktera ili 3493 cifre.

Svaki simbol se satoji od segmanata, koji predstavljaju kodirane podatke u obliku dvodimenzionalnih obrazaca. Code 1A, 1B, 1C, 1D i 1E simboli imaju šest segmenata podataka, a Code 1F, 1G i 1H imaju 16 segmenata. Svaka verzija simbola ima jedinstveni obrazac traka i međuprostora u centru simbola i taj obrazac se naziva centralni obrazac. Ovaj obrazac dijeli simbol na gornju i donju polovinu.

Parovi vertikalnih susjednih traka i međuprostora upotrebljavaju se da odvoje segmente podataka. Code 1F, G i H imaju i horizontalne obrasce za odvajanje segmenata podatka. Svaki vertikalni i horizontalni obrazac je završen sa kratkim, normalnim na njega, linijskim segmantom zvanim kapa, koji se koristi kao mjera veličine simbola za dekodiranje.

U Tabeli 2.1.28 je dat broj horizontalnih i vertikalnih kvadratića , kao i broj bajtova u simbolu za različite verzije simbola.

Tabela 2.1.28 Broj kvadratića i bajtova u različitim verzijama Code 1 simbola

Verzija Code 1	Broj kvadratića po horizontali	Broj kvadratića po vertikali	Broj bajtova u simbolu
A	16	10	20
B	20	14	35
C	28	20	70
D	36	30	135
E	48	42	252
F	68	60	510
G	92	88	1012
H	136	120	1040

U Tabeli 2.1.29 dat je kratak pregled osnovnih karakteristika koda Code 1, a na Slici 2.1.35 dat je primjer ovog koda.

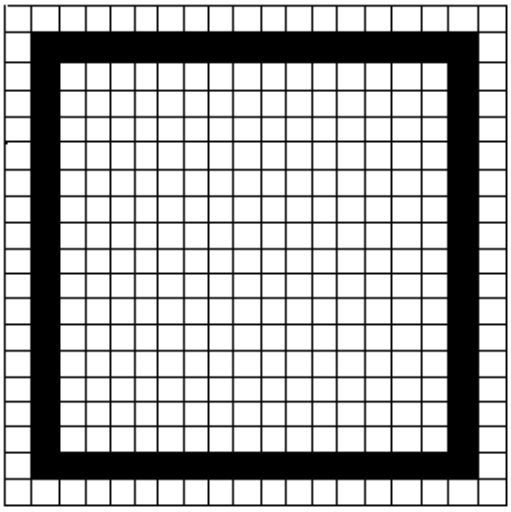
Detaljnije podatke o ovom kodu mogu se naći u [22].

Tabela 2.1.29 Karakteristike koda Code 1
Kodni karakter set: Svih 128 ASCII karaktera, 4 funkcijska karaktera i 1 Pad karakter
Kontrola na nivou karaktera: Postoji
Veličina simbola: Promjenjiva
Bideirakciono kodiranje: Da
Broj segmenata u simbolu: 1 – 16
Broj potrebnih kontrolnih karaktera: 10 – 560
Maksimalan broj bajtova u simbolu: • Code 1A = 10 bajtova podataka i 10 kontrolnih bajtova • Code 1B = 19 bajtova podataka i 16 kontrolnih bajtova • Code 1C = 44 bajtova podataka i 26 kontrolnih bajtova • Code 1D = 91 bajtova podataka i 44 kontrolnih bajtova • Code 1E = 182 bajtova podataka i 70 kontrolnih bajtova • Code 1F = 370 bajtova podataka i 140 kontrolnih bajtova • Code 1G = 732 bajtova podataka i 280 kontrolnih bajtova • Code 1H = 1480 bajtova podataka i 560 kontrolnih bajtova
Dodatne funkcije: Edge–to–edge dekodiranje Sposobnost korekcije greške

Slika 2.1.35 Code 1 simbol

2.1.2.7 Vericode

1990 godine Carl, Roberts Anselmo i Daid Hooper su dobili nagradu za U.S. patent broj 4924078, dat 1987 godine, koji je danas poznat kao Vericode. Vericode je dvodimenzionalni trakasti kod sastavljen od ćelija podataka kako pokazuje Slika 2.1.36. Osim ćelija na granici simbola, sve ostale ćelije u simbolu mogu imati vrijednosti ″on″ (″1″) ili ″off″ (″0″). Spoljne ćelije podataka (ćelije izvan graničnih ćelija) mogu se upotrijebiti za određivanje orijentacije simbola, za sinhronizaciju, ili za identifikaciju simbola. Unutrašnje ćelije (ćelije unutar graničnog kvadrata na Slici 2.1.36) su ćelije koje kodiraju podatke u simbolu. Slika 2.1.36 pokazuje unutrašnju matricu ćelija podataka od 15 kolona i 15 vrsta, koja omogućuje kodiranje 2224 različita simbola.

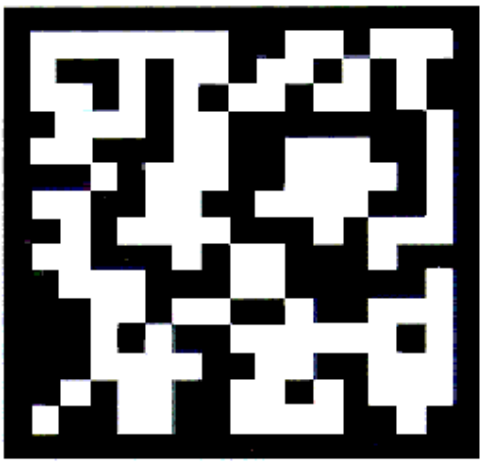


Slika 2.1.36 Vericode matrica

Upotrebom simbola iste veličine, gustina simbola se može mijenjati promjenom veličine ćelije podatka. Isto tako, uzimanjem konstantne gustine simbola njegova veličina se mijenja zavisno od broja bajtova koje treba kodirati. Simbol može biti biko koje veličine koja se može optički pročitati. Zbog binarne prirode ćelije podatka, moguće je dodati bit parnosti za povećanje sigurnosti čitanja. Simbol posjeduje redudansu takvu da više od 50% simbola može biti izbrisano a da simbol bude čitljiv (ne dođe do gubitka podataka). Pogrešni podaci se rekonstruišu uz pomoć računara i specifičnog algoritma.

Kompletan Vericode simbol koji kodira 22 karaktera prikazan je na Slici 2.1.37. Ćelije u gornjem lijevom i gornjem desnom uglu su ″off″ i ćelija u donjem desnom uglu je ″off″. ćelija u donjem desnom uglu je ″on″. Ovakav raspored ćelija u uglovima simbola omogućava da pri bilo kakvoj poziciji

unutar 360° može biti ispravno dekodiran. Vericode simbol može kodirati između 1 i 5000 karaktera.



Slika 2.1.37 Vericode simbol – kodira 22 kodne riječi (karaktera)

2.1.2.8 Data Matrix

DataMatrix kod je razvijen 1989 godine od strane International DataMatrix of Clearwater, Florida. To je dvodimenzioni trakasti kod dizajniran tako da može kodirati veliku količinu podataka u veoma malom prostoru. Za razliku of Verocode koda koji ima okvir sastavljen od crnih ćelija (″on″ bita) kod DataMatrix koda dvije susjedne stranice okvira koda se sastoje od crnih ćelija dok se u preostale dvije susjedne stranice crna i bijela polja (ćelije) naizmjenično smjenjuju (Slika 2.1.38). Ovakav okvir omogućava određivanje orijentacije simbola i veličine ćelije, odnosno, gustine koda.

Veličina simbola se kreće između 0.0254mm po stranici i 35.56cm po stranici. DataMatrix može kodirati od jednog do 2000 karaktera. Simbol može imati maximalnu teoretsku gustinu od 500 miliona karaktera na 25.4mm. Naravno, u parksi, gustina koda je limitirana rezolucijom tehnologije štamapanja, odnosno, tehnologije čitanja koda. 500 karaktera se može kodirati sa 24-pinskim matričnim štampačem u kvadratu čija je stranica 25.4mm ako se kodiraju brojevi, odnosno 35.56mm za puni ASCII karakter set.

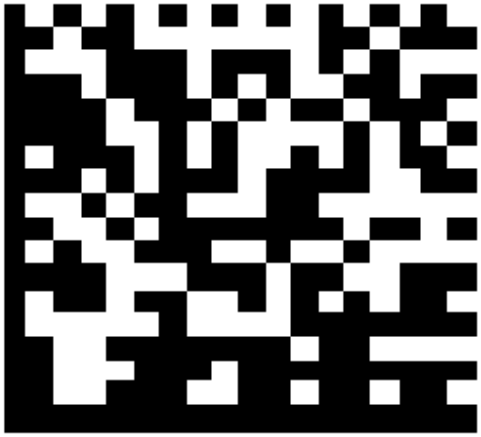
Kod je manje osjetljiv ne defekte štampe nego li tradicionalni trakasti kodovi [26]. Šema kodiranja ima veliku redudansu (podaci su rasuti po simbolu) koja omogućava da se kod ispravno pročita čak i ako je njegov dio pogrešan (oštećen ili izbrisan).

Svi DataMatrix simboli se mogu podijeliti i dvije grupe. Prva grupa simbola se označava sa ECC-000 do ECC-140 i oni imaju neparan broj

ćelija duž svake stranice kvadrata simbola. Ovi simboli koriste konvoluciono kodiranje za korekciju greške [27], i korišćeni su najviše početnih primjena DataMatrix kodova. Druga grupa simbola se označava sa ECC-200. Ovi simboli imaju paran broj ćelija duž svake linije koda i koriste Reed-Solomon tehniku za korekciju greške (Prilog 2). Maksimalni kapacitet ECC-200 simbola je 3116 cifara ili 2335 alfanumeričkih karaktera u simbolu sa 144 ćelije.

Zahvaljujući činjenici da simbol DataMatrix koda veličine 2 do 3 mm može kodirati oko petnaest karaktera, ovaj kod se najviše koristi za identifikaciju malih elemenata kao sto su integrisana kola, male štampane ploče, sitni medicinski instrumenti i slično.

Primjer DataMatrix simbola dat je na Slici 2.1.38.



Slika 2.1.38 Data Matrix simbol

Na slici 2.1.39 prikazan je DataMatrix simbol na Mini PCI kartici. U ovoj primjeni simbol kodira serijski broj kartice.

Slika 2.1.39 DataMatrix simbol na Mini PCI kartici

2.1.2.9 MaxiCode

MaxiCode (izvorno nazvan UPSCode) je matrični kod razvijen od strane United Parcel Service 1992 godine. To je dvo-dimenzionalna simbologija koja može kodirati oko 100 karaktera podataka u prostoru od 25.4 mm^2 (1 $inch^2$). Unutar tog malog prostora postoje dvije MaxiCode komponente. To su bijeli i crni šestouglovi koji pakuju informacije u dva smjera. U sredini MaxiCode simbola nalazi se okrugli prozor koji omogućuje skeneru da odredi položaj simbola bez obzira na njegovu orijentaciju.

Simbol MaxiCode je fiksne veličine, što mu omogućava visoku pouzdanost čitanja i kada se kreće velikom brzinom. Upotreba šestougaonih elemenata, po čemu je Maxi Code jedinstven, omogućuje gusto pakovanje binarnih podataka. U jednom simbolu, za kodiranje karaktera, aranžirano je 864 šestougaonih elemenata u 144 šestobitnih simbol karaktera, koji se koriste za kodiranje podataka, korekciju greške i kontrolne funkcije čitača. Simbol krakteri sadrže šest elemenata koji su organizovani u tri reda od po dva elementa od kojih je lijevi niže a desni više težine.

MaxiCode simboli su podijeljeni u tri segmenta, od kojih svaki sadrži bitove podataka i bitove korekcije greške. Segmenti se koriste za efikasnije izračunavanje korekcije greške i nemaju značaja prilikom kodiranja podataka.

Segment 1, koji se naziva Primarna Poruka, sadrži 120 bitova, od kojih je 54 bita upotrijebljeno za kodiranje 9 karaktera podataka, 4 bita su upotrijebljena kao indikatori moda simbola, 2 bita se ne koriste a 60 bitova je upotrijebljeno za korekciju greške.

Segmenti 2 i 3 obrazuju Sekundarnu Poruku koja sadrži svih preostalih 744 bitova i može biti konfigurisana za Standardnu i Povećanu korekciju greške. Sa standardnom korekcijom greške, sekundarna poruka može maksimalno kodirati 84 karaktera podataka, dok sa povećanom korekcijom greške maksimalno 64 karaktera podataka.

MaxiCode koristi Reed-Solomon kodove za korekciju greške i rekonstrukciju podataka. Osim toga obezbjeđuje i dva posebna nivoa korekcije greške i to: Standard Error Correction (SEC) i Enhanced Error Correction (EEC) [5, 21].

Standard Error Correction (SEC) koristi se u sekundarnoj poruci i uključuje 20 karaktera za korekciju greške. Ovo omogućuje potpunu rekonstrukciju podataka kada je do 16% simbol karaktera u sekundarnoj poruci oštećeno.

Enhanced Error Correction (EEC) primjenjuje jedan karakter za korekciju greške na svaki karakter podatka i obezbjeđuje maksimalni kapacitet korekcije greške od oko 25%.

Četiri bita u primarnoj poruci su upotrijebljena kao indikatori moda. Indikatori moda se koriste da ukažu na korišćenje EEC u sekundarnoj poruci, na strukturu primarne poruke i na to da li je simbol usamljen ili je

povezan sa više drugih MaxiCode simbola. Osam MaxiCode simbola se mogu povezati u struktuisani format.

Na slici 2.1.40 prikazan je primjer MaxiCode simbola. Detaljnije informacije o ovom kodu mogu se pogledati u [22].

Slika 2.1.40 MaxiCode simbol

2.1.2.10 UltraCode

UltraCode je uveden kao četvrta generacija linearnih simbologija. To je, zapravo, linearno matrična simbologija, koja uz primjenu Reed-Solomon korekcije greške, može kodirati srednju količinu podataka. UltraCode simbologija se razlikuje od većine dvodimenzionalnih simbologija, sa korekcijom greške, u tome što što su njegovi simboli dugački u odnosu na visinu simbola, slično podstojećim linearnim trakastim kodovima. Nijesu postavljeni kao simbologije velikog kapaciteta (Slika 2.1.41).

UltraCode predstavlja dvodimenzionalnu matričnu simbologiju sa konstantnim brojem redova. UltraCode simbol je konstantne visine, čija dužina zavisi od količine kodiranih podataka i upotrijebljenog nivoa korekcije greške.

UltraCode može kodirati kompletan 20-bitni karakter set ISO 10646-1, uključujući 16-bitnu Osnovnu Multijezičku Matricu(=Unicode 2.0 karakter set). Takođe, kodira ISO/IEC 4873 i ISO 8859 serije osmobitnih karakter setova, kao i specifične karakter setove kodova Code 39, Code 49, Code 93, Code 128, Codebar, Interleaved 2 of 5, UPS/EAN, UCC/EAN-128, i Codeablock F.

Za predstavljanje svakog podataka koristi par vertikalnih kolona sa sedam monohromatskih ili osam višebojnih ćelija (Slika 2.1.41). Nivoi korekcije greške su: četiri nivoa Reed-Solomon korekcije greške plus još jedan nivo za korekciju greše [22].

Veličina simbola izražena brojem ćelija u simbolu kreće se između 7Yx25X ćelija minimalno i 7Yx4275X ćelija maksimalno za monohromatski simbol. Za višebojni simbol imamo minimalno 9Yx25X i 9Yx2136X maksimalno ćelija.

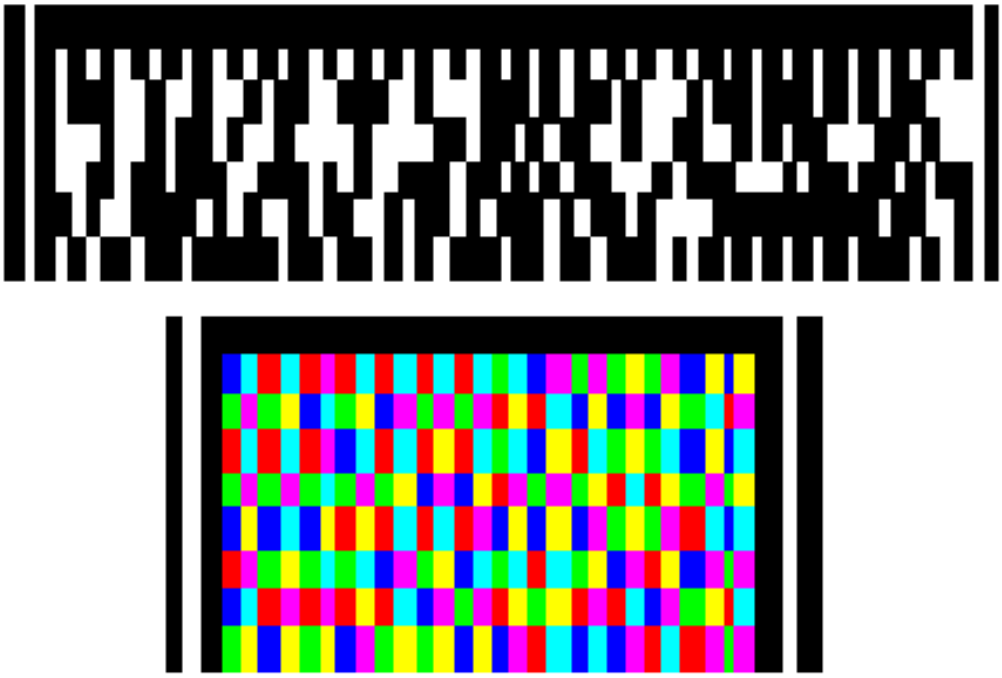
Broj karaktera podataka u simbolu maksimalne veličine zavisi od nivoa korekcije graške. Za nulti novo korekcije greške imamo maksimalno 1882 kodne riječi, što odgovara maksimalno 1882 alfanumeričkih karaktera u bilo kojemu alfabetu; 313 kineskih, japanskih ili koreanskih idiografskih karaktera; 1140 cifara; ili 1175 bajtova u binarnom modu.

Simbol može biti ma kakve orijentacije i može se čitati bez obzira da li je slika izvedena crno na bijelo ili bijelo na crno. Fajl podataka se može logički i kontinualno koditati u do 23 UltraCode simbola. Originalni podaci se mogu korektno rekonstruisati baz obzira na redosljed skeniranja simbola. Korekcije oštećenja simbola zasnovane su na strukturnim pravilima za odabir simbola karaktera.

UltraCode primjenjuje novi konceptualni metod dijeljenja jezika u jezičke grupe i kodne površine, što omogućava kodiranje najpopularnijih jezika sa UltraCode simbologijom, uključujući višejezičnost unutar UltraCode simbola.

UltraCode simboli sa korekcijom greške mogu se koristiti za emulaciju najpopularnijih linearnih odnosno grupisanih (naslaganih) simbologija trakastih kodova (Code 39, Code 49, Code 93, Code 128, Codebar, Interleaved 2 of 5, UPS/EAN, UCC/EAN-128, i Codeablock F).

Na slici 2.1.41 prikazan je monohromatski i višebojni UltraCode simbol.



Slika 2.1.41 UltraCode simboli

2.1.2.11 Čitači dvodimenzionalnih simbologija

Svi matrični simboli zahtijevaju dvodimenzionalni CCD skener ili dvodimanzionalnu CCD video kameru i ne mogu biti lako pročitani laserskim skenerom. To je zbog toga što nije jednostavno laserskim zrakom presjeći sve ćelije, unutar simbola.

Laserski skeneri zahtijevaju da visina elementa simbola bude veća od širine elementa. Uniform Simbol Specification je odredio za Code 49 i Code 16K da visina njihovog elementa bude osam puta veća od širine elementa. Za PDF417 je specificirano da visina elementa je oko tri puta širina elementa. Code 49, Code 16K i PDF417 mogu biti čitani laserskim skenerom.

CCD skeneri dozvoljavaju da visina segmenta bude jednaka njegovoj širini, što omogućava čitanje kodova mnogo veće gustine.

2.1.3. ČITAČI TRAKASTOG KODA

Kada su Woodland i Silver 1949. Godine dali prvi trakasti kod nazvan *circular* predložili su i uređaj za čitanje simbola toga koda. Taj uređaj se smatra prvim čitačem trakastog koda.

Prvi industrijski sistem sa trakastim kodom instalirala je firma General Atronics (danas Accu-Sort System) u Scott Paper Company–ji. On je koristio dvije fotoćelije za skeniranje dvorednog trakastog koda.

Kada je 1974. godine instaliran prvi sistem sa trakastim kodom u maloprodaji (u Marsh′s Supermarket u Troy, Ohio), koristio je čitač dizajniran od Spectra Physics Retail Systems-a. Ovaj sistem je čitao Universal Grocery Product Identification Code, danas poznat kao UPC.

Za razliku od stacionarnih sistema u supermarketima, wand čitači ili svjetlosne olovke razvijeni su i korišteni sa prenosivim sistemima za prikupljanje podataka. Railroad Retirement Board i US Patent Office su bili prvi značajniji korisnici ovih sistema. Gotovo deceniju su vladali čitači sa prorezom i svjetlosne olovke. Symbol Technologies uvodi 1980. godine prvi ručni helium- neon (He-Ne) laserski čitač. Od tada ovakvi čitači prolaze kroz više faza razvojado današnjeg oblika laserskog čitača sa gasom. 1986. godine pojavljuje se prva generacija laserskih čitača sa diodama. Ovi čitači su manji, niže cijene i troše manje energije od He-Ne laserskih čitača. Druga generacija laserskih čitača sa diodama ili treća generacija laserskih čitača pojavljuje se 1988. godine. Ovi čitači koriste diode koje emituju vidljivu svjetlost čime se omogućuje da simboli mogu diti štampani u boji i mastilo ne mora sadržavati ugljenik. 1990. godine Symbol Technologies uvodi 8500 ALR čitač sposoban da čita simbole sa uskim elementima širine 0.38mm sa udaljenosti od 60 do 250cm. Ovi čitači su sposobni čitati simbole manje gustine (približno 1mm = širina uskog elementa) sa udaljenosti od preko 4.5m.

Takođe 1990. godine, Symbol Technology uvodi ručni skener PDF1000, posebno dizajniran da čita dvodimenzionalne simbole.

Norland Corporation je 1981. godine proizveo prvi ručni CCD čitač (CCD – charge-coupled device). Norand-ov uređaj je koristio ksenonsku cijev za stvaranje svjetlosnog bljeska i osvjetljavanje trakastog simbola. Linearni CCD element sadržao je liniju od preko hiljadu detektora koji trenutno snimaju cijeli simbol. Svaki element linearnog CCD čitača opaža refleksioni prostor (međuprostor) i apsorbcioni prostor (traka).

Druga generacija CCD čitača upotrebljava niz visoko-snažnih LED dioda koje emituju vidljivu svjetlost za osvjetljavanje simbola trakastog koda.

Treća generacija CCD čitača (pojavila se 1990. godine od Symbol Technology) koristi CCD matricu sličnu elementima u CCD video kamerama. Ovi CCD prostori su matrice fotodetektora. Matrični CCD-ovi mogu biti fiksni i ručni. Ovakvi uređaji su sposobni savladati probleme kao što su mrlje, praznine i hrapavost ivica traka. Omogućavaju čitanje simbola

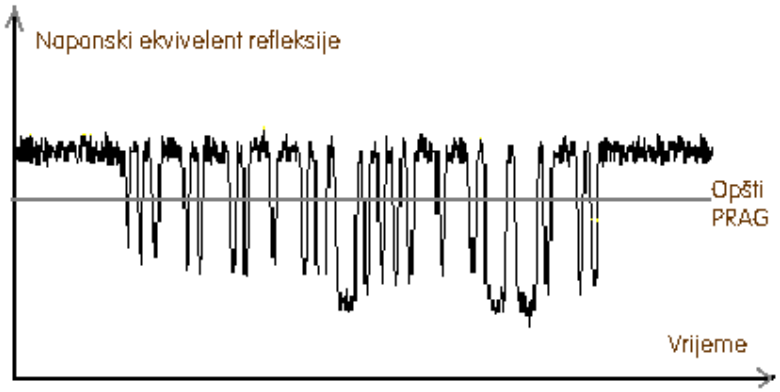
sa velikom gustinim, simbola sa malom gustinom i novih dvodimenzionih simbola.

2.1.3.1 Komponente čitača takastog koda

Osnovni djelovi svakog čitača trakastog koda su *skener* i *dekoder*.

SKENER

Često se čitači trakastog koda nazivaju skeneri. Ovaj naziv nije odgovarajući jer skener predstavlja integralni dio čitača. Skener trakastog koda osvjetljava simbol trakastog koda i daje informaciju o koeficijentu refleksije svjetlosti od simbola. Prostori visoke refleksije su međuprostori a prostori niske reflaksije su trake. Svaki čitač trakastog koda za čitanje upotrebljava elektro-optički sistem. Zajednički hardver za sve čitače uključuje izvor svjetlosti, optiku, fotodetektor i kolo za obradu signala. Izvor svjetlosti osvjetljava simbol trakastog koda od koga se svjetlost reflektuje nazad u fotodetektor. Fotodetektor mjeri količinu reflektovane svjetlosti i konvertuje je u električni signal. Kolo za obradu signala prenosi signal do dekodera koji prevodi signal u upotrebljivu informaciju (Slika 3.1).



Slika 2.1.42 Signal na izlazu skenera jednodimenzionog trakastog koda

DEKODER

Kada fotodetektor konvertuje reflektovani svjetlosni signal, od simbola trakastog koda, u električni signal taj signal se zatim digitalizuje. Digitalizaciju obavlja dijelom hardver dijelom softver dekodera. Proces se sastoji od mjerenja jačine reflektovanog optičkog signala iz skenera i njegovog poređivanja sa odgovarajućim pragom refleksije. Ako je refleksija veća od odgovarajućeg praga onda kažemo da se radi o međuprostoru a ako je refleksija manja od odgovarajućeg praga onda

kažemo da se radi o traci. Tako dekoder prevodi električni signal u binarni niz.

Dekoder obavlja nekoliko funkcija u proesu dekodiranja. Prvo, dekoder određuje širinu svake trake i međuprostora. Mjerenje širine se, najčešće, obavlja tako što se određuje vrijeme u kojem skener vidi visoku ili nisku refleksiju. Drugo, dekoder ispituje da li obavezna mirna zona postoji na oba kraja simbola. Treće, dekoder dodjeljuje kvantizovani broj za izmjerenu širinu kao broj koji toj širini odgovara unutar korištene simbologije. Na primjer, Code 39, Interleaved 2 of 5, Codebar i MLC-2D imaju dvije širine. U.P.C./EAN, Code 128 i Code 16K imaju 4 širine. Code 93 ima 5 širina. Code 49 i PDF-417 imaju 6 širina. Četvrto, dekoder provjerava dali je broj različitih širina u saglasnosti sa pravilima kodiranja za datu simbologiju. Najzad, dekoder poredi dobijene obrasce sa postojećom tabelom obrazaca i tako određuje podatke (karaktere) unutar simbola.

Neki čitači trakastog koda mogu čitati više različitih simbologija [23]. Autodiskriminacija je proces odabiranja određene simbologije. Povećanjem broja algoritama za dekodiranje raznih simbologija raste i matematička vjerovatnoća da štamparska greška u simbolu može učiniti da on bude pročitan kao valjani simbol druge simbologije. Zato je preporučljivo koristiti one simbologije čiji su obrasci značajno različiti.

Mnoge simbologije su bidirekcione. To znači da mogu biti čitane s’′lijeva u desno i s′’desna u lijevo. Smjer čitanja često se određuje start i stop obrascem u simbolu. Na primjer, start/stop obrazac simbola Code 39 je NB WS NB NS WB NS WB NS NB (′N′ je uski element, ′W′ je široki eement, ′B′ je traka i ′S′ je međuprostor). Ako je obrazac, koji vidi dekoder, u gornjem poretku, dekoder zna da je simbol procitan s’′lijeva na desno. Ako je niz obrnut, dekoder zna da je simbol pročitan s’′desna u lijevo. Usvaja se jedan smjer skeniranja (obično s′lijeva u desno) i podaci dobijani čitanjem u suprotnom smjeru prevode se na podatke usvojenog smjera.

Čitači sa pokretnim-zrakom imaju mogućnost da pročitaju simbol više puta u toku jedne sekunde. Oni upoređuju dva različita čitanja. Samo kada tri uzastopna dekodiranja daju isti simbol trakastog koda podaci se dalje prosljeđuju.

Izlaz dekodera je binarni signal koji dalje mora biti prezentiran nekom uređaju za prikupljanje podataka. Najviše dekodera ima RS232C za vezu. Format kodiranja može biti BCD, asinhroni ASCII, prošireni BCD (EBCDIC) itd.

2.1.3.2 Izvori svjetlosti kod čitača trakastog koda

Svi tipovi čitača trakastog koda imaju izvor svjetlosti koji osvjetljava oštampani simbol. Dio te svjetlosti reflektuje se ka fotodetektoru. Optika za

fokusiranje svjetla se obično nalazi između izvora svjetlosti i simbola ili(i) ispred fotodetektora.

Postoje skeneri trakastog koda koji osvjetljavaju simbole sa infracrvenim izvorima svjetlosti, talasne dužine 900 nanometara ili izvorima vidljive svjetlosti talasne dužine između 600 i 700 nanometara. Skeneri koji koriste helium-neon lasere imaju talasnu dužinu svjetlosti 632.8 nanometara. Diode koje emituju vidljivu svjetlost (LED) i upotrebljavaju se u skenerima sa usmjerenim zrakom, emituju svjetlost talasne dužine izneđu 670 i 700 nanometara, najčešće 670 nanometara. Infracrvene LED se takođe koriste u skenerima sa usmjerenim zrakom, i rade u opsegu od 800nm do 950nm. Infracrvene laserske diode koje se koriste u bezkontaktnim čitačima sa fiksiranim i pokretnim zrakom imaju talasnu dužinu emitovane svjetlosti 900nm. Nove laserske diode koje emituju vidljivu svjetlost rade u opsegu 670 do 680 nanometara.

Često čitači trakastog koda koriste izvore crvene vidljive svjetlosti. U tom slučaju dobiće se slab kontrast ako su trake štampane sa mastilom čija boja sadrži crveni pigment. Trake štampane crvenom, žutom, narandžastom, crvenkasto-purpurnom, crvenkasto-braon, neće se dovoljno razlikovati od bijelog međuprostora kada se čita crvenim izvorom svjetlosti, odnosno kada se koristi He-Ne, laserske diode sa crvenom vidljivom svjetlošću i mnogi čitači sa usmjerenim zrakom koji koriste crvene LED.

Drugi se problem javlja kada simbol čitamo skenerom sa infracrvenim izvorom svjetlosti. Traka, oštampana mastilom koje ima nizak sadržaj ugljenika neće biti vidljiva za skener iako je ljudsko oko sasvim dobro opaža. Dalje, simboli oštampani termički na organskom papiru takođe neće biti vidljivi za infracrveni čitač.

Mnogi poluprovodnički elmenti, kao što su laseri, diode koje emituju svjetlost, pa i mjerni pretvarači osjetljivi na svjetlo najefikasnije rade sa infracrvenom svjetlošću talasne dužine iznad 900nm. Na žalost, mnoga često korištena mastila, vidljiva čovjekovom oku, nevidljiva su za infracrvenu svjetlost. Zbog toga, ako je u upotrebi čitač sa infracrvenim zracima simboli trakastog koda moraju biti štampani mastilom koje je na bazi ugljenika. Ugljenična mastila, za razliku od drugih popularnih mastila, nijesu fizički stabilna. Takva mastila mogu izazvati probleme kao što su mrlje u štampi i oštećenje mehanizma za štampanje. Pored toga, ako mašinski čitljivi medij štampamo posebnim mastilom svaki artikal mora proći kroz dva ciklusa štampe- jedan ciklus za text, crteže itd., a drugi ciklus za trakasti kod. Sve to rezultira povećanjem cijene štampanja a osnovni ekonomski uslov je što niža cijena štampanja simbola (zahtijeva se da nanošenje simbola trakastog koda ne povećava cijenu štampe).

Korištenje karbonskih mastila veoma pogoduje čitanju simbola i kada se koristi vidljiva svjetlost. Ipak, danas je preporučljivo koristiti čitače sa vidljivom svjetlošću u svim primjenama. Sistemi koji koriste samo čitače u infracrvenoj oblasti ne mogu pratiti nove tehnologije štampanja [25].

Na kraju zaključujemo da, ukoliko želimo simbole trakastog koda čitati različitim čitačima, najbolje je simbole štampati karbonskim mastilom. S druge strane, ukoliko želimo da isti čitač može čitati različite trakaste kodove, najbolje je koristiti čitač sa izvorom vidljive svjetlosti.

Ako se sistemi sa trakastim kodom primjenjuju u supermarketima imamo mnoge artikle sa, na primjer, aluminijskom oblogom. Ova obloga ima sjajnu metalnu površinu i u simbolu trakastog koda njome su predstavljene trake. Kako, generalno, smatramo da su trake oštampani prostor, ovdje imamo obrnutu situaciju i da bi je razumjeli moramo uočiti razliku između ogledalne refleksije i difuzione refleksije. Ogledalna refleksija se javlja kod glatkih i sjajnih poovršina, poput ogledala. Njena osnovna karakteristika je da ugao kojom sjetlost pada na glatku površinu je jednak i suprotan uglu kojom se svjetlost reflektuje od glatke površine. Difuziona refleksija je proces kada se upadna svjetlost reflektuje u više pravaca. Tako, ukoliko detektor nije u ravni ogledalne refleksije, svjetlost reflektovana sa glatke metalne površine proći će mimo detektora i detektor će je vidijeti kao tamni prostor. Na primjer, skeneri sa usmjerenim zrakom imaju detektor vertikalno iznad površine simbola. Kao posljedica toga, svjetlost reflektovana sa ogledalne površine mimoilazi detektor. Do detektora dolazi samo dio reflektovane svjetlosti od obojene površine pa nju detektor vidi kao međuprostor.

2.1.3.3 Vrste čitača trakastog koda

Čitači trakastog koda se, prema načinu čitanja, mogu svrstati u tri grupe. Prvu grupu čine čitači sa fiksiranim zrakom. Kod njih se skeniranje obavlja tako što se objekat sa simbolom trakastog koda kreće ispred čitača. Drugu grupu čine čitači sa pokretnim zrakom. Ovdje objekat miruje dok se zrak iz skenera kreće po simbolu. Treću grupu čine čitači čije je funkcionisanje slično video ili fotografskoj kameri gdje čitav simbol biva osvijetljen iz izvora svjetlosti koji može biti ksenonska cijev, LED ili laserske diode, i slika se reflektuje ka poluprovodničkoj komponenti poznatoj kao CCD.

2.1.3.3.1 Čitači sa fiksiranim zrakom

Čitanje, kod čitača sa fiksiranim zrakom zavisi od spoljnjeg pokreta. Taj pokret može napraviti operater, prelaženjem čitačem preko simbola ili pomjeranjem simbola ispred čitača. Postoje različiti tipovi čitača sa fiksiranim zrakom. To su svjetlosna olovka, ručni bezkontaktni čitači, transportni čitači sa fiksiranim zrakom i čitači sa fiksiranim zrakom integrisani unutar drugog uređaja. Vrsta čitača sa fiksiranim zrakom su i čitači sa prorezom koji služe za čitanje simbola trakastog koda sa kartice. Kartica se provači kroz prorez, siječe fiksirani zrak čitača i na taj način se dobija električni signal ekvivelentan trakastom kodu.

Čitači sa fiksiranim zrakom obično ne koriste laserski izvor svjetlosti. Umjesto njih, upotrebljavaju se LED. Razlozi su sljedeći. Prvo, zato što su ovi čitači namijenjeni da se instaliraju tamo gdje je prostor dragocjen i gdje je malo rastojanje čitača od simbola. Drugo, LED imaju znatno duži vijek trajanja i nijesu osjetljive na udare i vibracije kao laserske diode. Treće, LED emitiju svjetlost u nekoliko talasnih dužina u vidljivom i nevidljivom opsegu spektra pa je moguće podesiti talasnu dužinu svjetlosti za aplikaciju.

Kao prednost čitača sa fisiranim zrakom u odnosu na laserske čitače može se smatrati i to što ne posjeduju pokretne djelove u mehanizmu skeniranja. To rezultira u manjim dimenzijama, dužem radnom vijeku i nižoj cijeni.

Čiatači sa fiksiranim zrakom mogu čitati sa vrlo malog odstojanja dok laserski čitači sa pokretnim zrakom moraju se dovoljno odmaći od simbola da bi on bio čitav obuhvaćen.

SVJETLOSNA OLOVKA (WAND ČITAČI)

Svjetlosna olovka je dosta korišteni čitač trakastog koda. Njegove prednosti su prenosivost i niska cijena. Čitanje se vrši tako što operater prelazi olovkom poprijeko preko simbola, od uvodne mirne zone preko svih traka i međuprostora i završne mirne zone. Kada operater ne uspije jednim prolaskom, dekodirati simbol trakastog koda sljedeći put, obično, pokuša sporije. Međutim, dobar savjet je da pokuša malo brže, ne sporije. Ubrzanje će smanjiti oscilacije prilikom a oscilacije, upravo, najviše otežavaju čitanje. Svjetlosne olovke podržavaju širok opseg brzina i ubrzanja mada se ove veličine se, najčešće, značajnije ne mijenjaju pri prelasku preko simbola. Svjetlosne olovke su, generalno, u mogućnosti podržati brzine između 80 i 800 mm u sekundi.

Svjetlosne olovke se sastoje od kućišta u obliku olovke, izvora svjetlosti i fotodetektora. Kako operater pokreće olovku preko simbola, javljaju se razlike u refleksiji svjetlosti od traka i od međuprostora koje bivaju detektovane od strane fotodetektora. Ovaj detektor konvertuje pomenute razlike u analogni električni signal koji se zatim prosljeđuje dekoderu.

Svjetlosne olovke se još nazivaju kontaktni čitači pošto zahtijevaju fizički kontakt sa simbolom. Tačnije, dozvoljena je malu distanca ali ne višu od 1.2 mm. Ovo rastojanje nazivamo *dubina polja* čitanja.

Širina otvora kojom svjetlost ide ka detektoru kod svjetlosnih olovki je veoma važna, mnogo važnija nego kod čitača baziranih na laserskoj tehnici. Širina otvora treba biti približno jednaka širini najužeg elementa u simbolu trakastog koda koji se čita. Ukoliko je širina veća to dovodi do smanjenja jasnoće signala, odnosno manje razlike između trake i međuprostora u ekvivalentnom analognom električnom signalu. Ako je širina manja može se desiti da defekt štampe u simbolu bude pročitan kao traka ili međuprostor.

Svjetlosne olovke su konstruisane da pouzdano čitaju kada su postavljene okomito na površinu simbola ili u nekom opsegu uglova oko okomitog položaja. Zato se preporučuju koristiti za čitanje simbola koji su na glatkim, ravnim i tvrdim površinama. Postoje i svjetlosne olovke koje najbolje čitaju kada su pod uglom 75° prema podlozi i sl. [1].

Kao primjer, na Slici 2.1.43 prikazana je svjetlosna olovka CL30. Ovo je čitač trakastog koda izrađen od nerđajućeg čelika sa glatkom kuglicom od sintetičkog rubina na vrhu. Na taj način je čitač zaštićen od habanja, a unutrašnja optika od prašine i prljavštine. Svojim glatkim vrhom CL30, prilikom čitanja, ne oštećuje simbol. Prisustvo optičkog filtra propusnika opsega i električnog filtra čini da se ovaj čitač može koristiti pri dnevnoj svjetlosti a i pri snažnom fluoroscentnom osvjetljaju. Postoje CL30 čitači sa crvenom vidljivom svjetlošću (CL30R-N10x) i sa infracrvenom svjetlošću (CL30I-N10x). Rezolucija CL30 čitača je od 0.10 do 0.40 milimetara, što mu omogućava da čita simbole velike, male i srednje gustine. Zahvaljujući svojoj izdržljivosti i nagibnom uglu od preko pedeset stepeni ovaj čitač se može koristiti u kombinaciji sa prenosivim (ručnim) terminalima. Zahvaljujući posjedovanju brzih kola na izlazu ovog čitača se dobija kvalitetan TTL-signal. Čitač se napaja sa 4.3 –5.5V i 35mA. Izvor svjetlosti je talasne dužine 660nm crvene LED i 940 nm infracrvene LED. Brzina skeniranja je od 34 do 3700 mm/sec, za rezoluciju 0.15mm. Ispravno funkcioniše na temperaturama od -10° C do 50° C i pri vlažnosti 95% bez kondezacije.

Slika 2.1.43 Svjetlosna olovka CL30

Kao drugi primjer na Slici 2.1.44 prikazana je svjetlosna olovka proizvod firme ZEBEX, America, Inc. Namijenjena je za povezivanje sa PC-ijem (dnosno PC/2). Povezuje se sopstvenim kablom između centralne jedinice PC-ija i tastature. Podatke o procitanom trakastom kodu prenosi isto kao da je pritisnuta tipka tastature. Kada čitač nije u upotrebi tastatura normalno funkcionioše. Upotrebljava se za čitanje svih popularnih trakastih kodova (U.P.C./EAN,Code 39, Code 93, Code 128, 2 of 5, Codabar).Napaja se sa +5VDC i 70mA. Napajanje obezbjeđuje kompjuter.

Pouzdano radi na temperaturama od 5°- 50°C i vlažnosti od 10-90%

Slika 2.1.44 Svjetlosna olovka ZEBEX

BEZKONTAKTNI RUČNI ČITAČI SA FIKSIRANIM ZRAKOM

Ovi čitači, takođe, zahtijevaju od operatera pokret prilikom skeniranja ali mu omogućuju veći razmak od simbola. Mnogi od ovih čitača, kao izvor svjetlosti koriste infracrvenu svjetlost koja nije vidljiva ljudskom oku. Vidljiva svjetlost se koristi za navođenje, da bi se olakšalo pozicioniranje.

Bezkontaktni ručni čitači sa fiksiranim zrakom imaju nižu cijenu nego čitači sa pokretnim zrakom, imaju veću dubinu polja čitanja nego svjetlosne olovke, prenosivi su i, na neki način, predstavljaju srednje rješenje.

BESKONTAKTNI NEPOKRETNI ČITAČI SA FIKSIRANIM ZRAKOM

Na nekim transportnim trakama i trakama za sortiranje pošte skeniranje se obavlja kretanjem simbola trakastog koda pored aparature za čitanje. Kretanje se obavlja tako da čitač može da vidi svaku traku i međuprostor u simbolu.

Bezkontaktni nepokretni čitači sa fiksiranim zrakom imaju ograničenu dubinu polja čitanja.

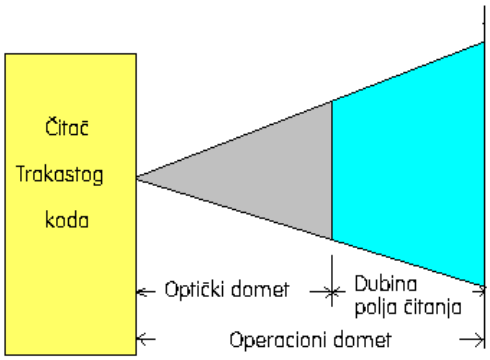
Na transportnim trakama omogućena im je samo jedna prilika da ispravno pročitaju simbol trakastog koda. Zato kada se to ne dogodi objekat se ponovo vraća na traku bilo automatski bilo ručno.

Nedostatak ovih čitača u odnosu na čitače sa pokretnim zrakom i ručne čitače je potreba da položaj simbola na objektu bude striktno kontrolisan. Kao što će se vidijeti iz narednog izlaganja čitači sa pokretnim zrakom postižu bolju čitljivost kada je simbol stepeničast nago kada je oblika ″stubića ograde″ (Slika 2.1.XX). Međutim, kako su čitači sa fiksiranim zrakom prvi razvijeni to su se i standardi za oblik simbola trakastog koda ravnali prema njima. Jednom uspostavljeni standard je kasnije teško promijeniti jer bi to ugrozilo postojeće, instalirane, sisteme. Tako danas,

uglavnom, imamo simbole trakastog koda štampane u obliku ″stubića ograde″.

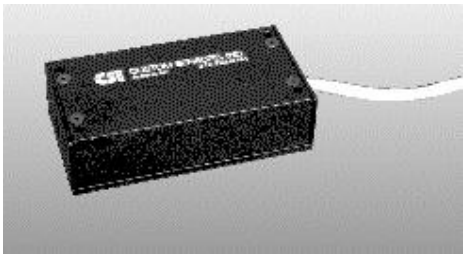
U svakom optičkom sistemu žiža (fokus) je najvažniji parametar za dobijanje čiste i razgovjetne slike. Na primjer, izvan fokusa fotografija je nejasna i objekti na njoj se teško uočavaju. To može da dovede do izobličavanja refleksije od traka i međuprostora do tačke kada više ne mogu biti raspoznati. Širina razmaka u kome je simbol trakastog koda u fokusu je dubina polja čitanja (depth of field – DoF) (Slika 3.4). DoF je razmak između maximalnog i minimalnog rastojanja simbola od čitača u kome simbol trakastog koda može biti pročitan. Jedan metod za određivanje DoF je definisanje optimalnog rastojanja (žižne tačke) i zatim određivanja maksimalnog rastojanja na obije strane od žižne tačke. Kod svjetlosnih olovki dubina polja čitanja se definiše kao maksimalno rastojanje vrha olovke od simbola koji čita. Za razliku od njega kod beskontaktnih čitača sa fiksiranim zrakom žižna tačka je, pomoću sočiva, pomjerena dalje u prostoru tako da objekat može biti dosta udaljen ili sasvim blizu čitača. Razmak od čitača do bliže ivice DoF-a naziva se optički domet (Slika 2.1.45). Kombinacija optičkog dometa i širine polja čitanja naziva se operaciono polje čitača (Slika 2.1.45).

Čitači sa fiksiranim zrakom mogu da čitaju simbole koji se kreću brzinom od 5cm do 5m u sekundi. Širina uskog elementa može ići do 0.254 inč. Simboli sa užim elementima moraju se kretati sporije nego simboli sa širim elementima. Čitači sa fiksiranim zrakom se primjenjuju kod transportnih traka koje se obično kreću brzinom od oko 500cm u sekundi.



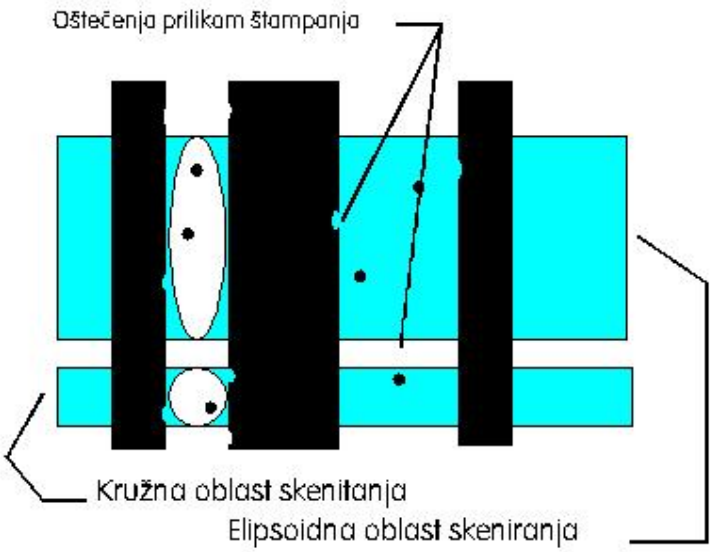
Slika 2.1.45 Optički domet, dubina polja čitanja i operacioni domet

Primjer nepokretnog čitača sa fiksiranim zrakom dat je na Slici 2.1.46.



Slika 2.1.46 Čitač sa fiksiranim zrakom, proizvod firme Custom Sensor, Inc

Čitač je proizvod iz serije BF, firme Custom Sensors, Inc (CSI). Uređaj u sebi sadrži kolo za dekodiranje i na izlazu daje podatke u ASCII formatu. Čitač može biti sa izvorom crvene vidljive svjetlosti ili sa izvorom infracrvene svjetlosti. Svjetlosni trag mu je elipsoidnog oblika pri čemu je duža osa elipse paralelna trakama u simbolu (Slika 2.1.47).



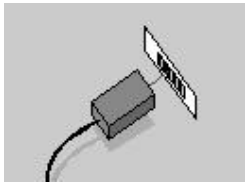
Slika 2.1.47 Svjetlosni trag Custom Sensor nepokretnog čitača sa fiksiranim zrakom

To rezultira u boljem procentu uspješnog čitanja u prvom pokušaju nego kada je svjetlosni trag kružnog oblika.

Sve glavne funkcije čitača daju se podešavati tako da se čitač može koristiti u različitim aplikacijama. Konfiguracioni podaci se čuvaju u EEPROM memoriji čiji sadržaj ostaje sačuvan i pri nestanku električne energije. Uređaj čita i dekodira nekoliko standardnih simbologija trakastog koda i u stanju je automatski raspoznati o kojoj se simbologiji iz pomenute grupe radi.

Uređaj se napaja sa 5V DC i smješten je u anodiranom aluminijskom kućištu.

Čitač je prvenstveno namijenjen za simbole trakastog koda koji prolaze pored njega (Slika 2.1.48)



Slika 2.1.48 Objekat prolazi ispred nepokretnog čitača sa fiksiranim zrakom

Simboli moraju biti propisno orijentisani preme čitaču i na definisanom odstojanju od njega. Najčešće se koristi model sa crvenom vidljivom svjetlošću koji čita kodove u kojima su trake štampane crnom ili nekom drugom bojom, izuzev crvene. Model sa infracrvenom svjetlošću koristi se tamo gdje je ambijent visoko osvijetljen, u fotografiji gdje film mora biti zaklonjen od vidljive svjetlosti ili u situacijama gdje se trakasti kod, radi potrebe skrivanja (zaštite od kopiranja) premazuje slojem koji propušta iznfracrvenu svjetlost.

Izlaz čitača može se direktno vezati za serijski port računara.

INTEGRISANI ČITAČI SA FIKSIRANIM ZRAKOM

Čitači sa fiksiranim zrakom često su integrisani u drugi uređaj koji može biti transportni mehanizam, uređaj za medicinsko dijagnosticiranje ili kod različitih terminala koji kao mašinski čitljiv medij koriste trakasti kod.

ČITAČI SA PROREZOM I FIKSIRANIM ZRAKOM

Čitači trakastog koda sa prorezom i fiksiranim zrakom namijenjeni su za čitanje trakastog koda sa identifikacionih kartica, tiketa, znački i sa bilo kojeg drugog nosioca simbola trakastog koda koji se može provući kroz prorez. Simbol koji se provači kroz prorez, siječe fiksirani zrak čitača i na taj način se dobija električni signal ekvivelentan trakastom kodu.

Kao i kod drugih čitača koji kao izvor svjetlosti koriste LED diode čitači sa prorezom imaju dubinu polja čitanja nekoliko milimetara.

Obično se optički sistem čitača nalazi na odstojanju od 10 do 15 mm od dna proreza pa je preporučljivo da se na toj visini od dna kartice nalazi sredina traka i međuprostora trakastog koda.

Postoje čitači sa prorezom koji kao izvor svjetlosti koriste vidljive LED i čitači koji koriste infracrvene LED.

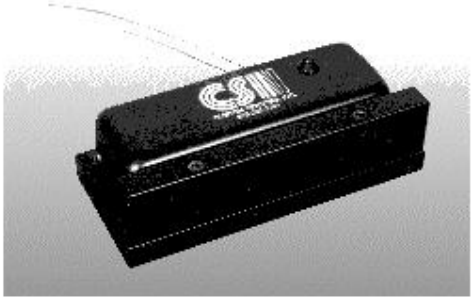
Kao primjer čitača sa prorezom na Slici 2.1.49 dat je čitač BC serije, proizvod firme Custom Sensors, Inc (CSI). Koristi se za čitanje kodova na karticama, značkama ili sličnim dokumentima. Ovaj uređaj čita i dekodira sve često korišćene simbologije. Kao izvor svjetlosti može koristiti LED

koje emituju vidljivu svjetlost i infracrvene LED. Ako koristi LED koje emituju vidljivu crvenu svjetlost, trakasti kod treba biti štampan crnom bojom ili bojom koja ne sadrži crveni pigment. Infracrveni čitač će čitati simbole štampane mastilom na bazi ugljenika, koji su ponekad radi skrivanja još premazani sigurnosnim slojem navidjivim za infracevenu svjetlost. Čitač posjeduje dva protokola za prenos podataka do računara ili drugog inteligentnog periferijskog uređaja. To su RS 232 (namijenjen za prenos podataka na manje daljine) i RS 422 koji se koristi za veće distance. Čitači BC serije smješteni su u crnom anodiziranom aluminijskom kućištu. Napajaju se sa 5VDC.

Ovi čitači se najčešće koriste za evidencije vremena prisustve radnika u fabrikama, kontrolu pristupa određenim objektima i slično.

Osobine:

- Integrisan dekoder
- Crveni vidljivi ili infracrveni model
- LED izvor svjetlosti otporan na udar
- Eliptička polje čitanja- pobaljšava performanse
- Mogučnaost konfigurisanja od strane korisnika
- RS-232 ili RS-422 izlaz
- Čita sve česta korištene simbologije
- Radi na +5VDC
- Aluminijska kučište



Slika 2.1.49 Čitač sa prorezom, proizvod firme Custom Sensor, Inc

Drugi primjer čitača sa prorezom je iz ZB-600 serije, proizvod firme ZEBEX,America,Inc (Slika 2.1.50). Ovaj čitač posjeduje više interfejsa za komunikaciju. To su RS-232, CMOS serijski interfejs i simulator tastature. Minimalna rezolucija čitača je 0.15mm a maximalna debljina kartice, odnosno nosioca koda koji se provlači kroz prorez, je 1,5mm. Posjeduje LED indikator i programabilni biper. Može da čita sve najpopularnije simbologije i može se konfigurisati provlačenjem konfiguracione kartice. Dubina polja čitanja mu je 2mm. Kao izvor svjetlosti koristi LED od 660nm za vidljivi opseg i 940nm za infracrveni opseg. Napaja se sa +5VDC ± 10%. Potrošnja struje mu se, zavisno od modela kreće između 25mA i 95 mA. Čitač pouzdano funkcioniše za temperaturni opseg od 0°C do 40°C a dozvoljena vlažnost je do 85% bez kondenzacije.

Slika 2.1.50 Čitač sa prorezom ZB-600, proizvod firme ZEBEX

2.1.4.4.2 Čitači sa pokretnim zrakom

Današnji **č**itači sa pokretnim zrakom su laserski čitači. Laserskom tehnologijom vrši se generisanje koherentne svjetlosti u uskim ali jakim snopovima. Riječ LASER je skraćenica od Light Amplification by the Stimulated Emission of Radiation. Laserska svjetlost je jednobojna ili monohromatska. Ako je svjetlost jednobojna onda je samo jedne talasne dužine. Ako su, još, talasne dužine snopa u fazi onda se kaže da je snop koherentan. Primjer nekoherentne svjetlosti je obična sijalica koja emituje bijelu svjetlost. Bijela svjetlost je nekoherentna, posjeduje sve vidljive boje i neke koje nijesu vidljive. Takva svjetlost se još naziva panhromatska svjetlost. Ona se prostire u svim pravcima i ne može se koncentrisati odnosno kontrolisati. Laserska svjetlost može biti kontrolisana zato što su njeni zraci iste talasne dužine i međusobno u fazi.

Usmjerenost i koherentna priroda laserske svjetlosti omogućavaju veću dubinu polja čitanja, vaći optički domet a samim tim i veće operaciono polja laserskih čitača. Laserski čitači fokusiraju izvor svjetlosti, dok većina ostalih čitača fokusira reflektovanu svjetlost. Kombinacija fokusirane svjetlosti sa koherentnom prirodom laserske svjetlosti čini da se na prijemu može koristi uskopropusni optički filtar, podešen da propušta samo svjetlost određene talasne dužine. Ovo poboljšava kvalitet signala i čini čitač otpornijim na uticaj spoljnjeg svjetla.

Svjetlost u laserskom zraku je strogo usmjerena. Uz pomoć sočiva ona se fokusira u obliku uskog konusa i emituje u jednom pravcu. Usmjerenst

laserskog zraka ostvaruje se pomoću optike koja se nalazi na kraju izvora svjetlosti u čitaču. U tako uskom snopu koncentrisana je sva snaga izvora svjetlosti što omogućava veće polje čitanja i smanjuje potrebu za preciznim pozicioniranjem simbola prema skeneru.

Žižna daljina laserskog zraka predstavlja rastojanje između skenera i centra polja čitanja. U toj tački prečnik zraka je najmanji i naziva se

$$\sqrt{2}d$$

zrakovni *struk*. Sa d se obilježava prečnik struka. Kada prečnik zraka pređe vrijednost

smatra se da je zrak ima nezadovoljavajuću snagu osvjetljaja, odnosno, da to više nije polje čitanja (Slika 2.1.51). Maximalni prečnik laserskog zraka na smije biti veći od $\sqrt{2}$ puta minimalna širine trake. Povećanje dubine polja čitanja može se ostvariti povećanjem optičkog dometa.

Za izračunavanje dubine polja čitanja laserskog čitača potrebno je definisati sljedeće promjenjive:

1) prečnik struka laserskog zraka;
2) talasna dužina emitovane svjetlosti.

Tačka u kojoj prečnik laserkog zraka postaje veći od $\sqrt{2}d$ nazivaju se granica polja čitanja. Dubina
polja čitanja se izračunava kao

$$\frac{\pi\left(d^2\right)}{2\lambda}$$

gdje je :

π = 3.1415927……..
d= prečnik struka
λ = talasna dužina svjetlosti
633nm=crvena svjetlost
900nm=infracrvena svjetlost

Slika 2.1.51 Zrakovni struk i dubina polja čitanja laserskih čitača

Za laserske čitač kao i za ostale čitače sa pokretnim zrakom važna

veličina je *vidljivo polje* Ono se definiše kao dužina bar koda koja može biti skenirana sa određenog odstojanja od čitača. Putanja pokretnog zraka, odnosno dužina koju zrak može da prijeđe lijevo i desno od centralnog položaja, određena je dužinom zraka. Kako razmak između simbola i čitača raste, raste i vidljivo polje, ali se mora voditi računa da se ne izađe iz polja čitanja.

RUČNI ČITAČI SA POKRETNIM ZRAKOM

Oblik ručnog čitača sa pokretnim zrakom zavisi od načina na koji je realizovan izvor svjetlosti (sa užarenim vlaknom, helijum-neonski ili sa laserskim diodama). Primjer ručnog čitača sa laserskim diodama kao

izvorom svjetlosti dat je na Slici 2.1.52.

Slika 2.1.52 Laserski čitač sa laserskim diodama kao izvorom svjetlosti

Prvi ručni čitači sa pokretnim zrakom koristili su helijum-neonsku cijev za generisanje monohromatske koherentne svjetlosti. Takav način generisanja svjetlosti zahtijeva napajanje od približno 1000 volti . To nije problem ako se čitač napaja sa mreže. Međutim, ako se napajanje vrši baterijski, da bi se dobilo 1000 volti, potreban je specijalni transformator. Helijum-neonska cijev i napajanje takvog čitača činili su blizu 65% njegove ukupne cijene.

Zamjenom helijum-neonske cijevi laserskim diodama koje se napajaju naponom od 5 do 12 volti, došlo je do znatnog smanjenja cijene koštanja čitača. To je i uzrokovalo da danas čitači sa pokretnim zrakom, uglavnom, koriste laserske diode kao izvor svjetlosti. Kao i diode prvih svjetlosnih olovki, i prve laserske diode emitovale su infracrvenu svjetlost što je moguće aplikacije ograničavalo na trakaste kodove štampane mastilom na bazi ugljenika. Ali, ubrzo su se pojavile laserske diode koje emituju crvenu vidljivu svjetlost. Ove diode su proširile izbor mastila za štampanje koda.

Jedna od najčešćih primjena ručnih čitača sa pokretnim zrakom je skeniranje sa velike daljine u magacinima i skladištima (Slika 2.1.53). Tipičan opseg daljina koje treba pokriti ovim čitačima je od 50mm pa sve do 5m.

Postoje tri osnovna problema sa kojim sa susrijeću konstruktori čitača sa širokim poljem čitanja. Prvi problem je što je količina reflektovane svjetlosti od simbola veoma mala kada je simbol udaljen. Signal reflektovan od trakastog koda lociranog na 3m od operatera je 150 puta manji od signala koji se reflektuje kada je simbol na udaljenosti 30 cm. Ovako slabi reflektovani signal zahtijeva od čitača da posjeduje dovoljno snažan izvor svjetlosti, veliku efikasnost optike za fokusiranje svjetlosti kao i dovoljno veličinu optike za prijem svjetlosti.

Drugi zadatak je da se omogući široko polje fokusiranja. Simbol se može nalaziti bilo gdje u rasponu od 0.5 do 5m od operatera. Srećna okolnost je što se u magacinima i skladištima skeniraju simboli male gustine sa najužim elementom širine 1.4mm. Međutim, težnja u industriji je da se na što manjem prostoru smjesti što više informacija što povećava gustinu simbola. Da bi se ostvarilo isto polje fokusiranja potrebno je upotrijebiti nakonvencionalne optičke elemente ili jednostavne i brze zoom sisteme kao djelove laserskog sistema za fokusiranje.

Treći važan paramtar za čitače na daljinu je i vidljivost laserske svjetlosti. Potrebno je imati dovoljno svjetlosti da bi je operater vidio sa 5m udaljenosti. Vidljivost je najjednostavnije povećati upotrebom dioda koje emituju svjetlost manje talasne dužine. Postoje takve laserske diode (650 nm) ali je njihova cijena znatno veća. Drugi mogući način se naziva ″uoči pa čitaj″. Ta metoda koristi dvopoložajni prekidač. Kada je prekidač u prvom položaju čitač emituje mnogo kraći i mnogo vidljiviji svjetlosni zrak, operater tada uočava simbol, prebaci prekidač u drugi položaj izvrši čitanje simbola.

1990 Symbol Technologies su napravile 8500 Alr čitač sposoban da čita trake širine 0.38mm sa rastojanja od 2m. Isti čitač može čitati simbol sa najužim elementom od 1.3mm sa udaljenosti više 3m. Druga verzija čitača na daljinu može čitati simbole sa elementima širine 1.4mm sa udaljenosti od 5m. 1992 Scan-Tech je demonstrirao čitač koji može čitati simbole sa elementima širine 2.5mm sa udaljenosti od 30m.

Slika 2.1.53 Ručni laserski čitač očitava simbole trakastog koda u magacinu

Na slici 2.1.54 prikazan je ručni čitač serije MS900 proizvod Microscan-a. Karakteriše ga puna automatizovanost sa mogućnošću automatskog podešavanja na promjenu udaljenosti simbola. Koristi laserskie dioda koje emituju vidljivu svjetlost. Malih je dimenzija i niske cijene. Postiže izuzetnu tačnost skeniranja i može čitati sa različitih udaljenosti. Dubina polja čitanja mu iznosi 130mm. U mogućnoati je automatski raspoznati postojeće često korištene simbologije.

Slika 2.1.54 Ručni laserski čitač trakastog koda, serije MS900, proizvod Microscan-a.

MS900 serija ručnih laserskih čitača je donijela inovacije u dizajnu i mogućnost automatskog podešavanja za skeniranje sa različitih daljina. Inovirani dizajn omogućava operateru maksimalni komfor pri radu a mogućnost automatskog podešavanja donosi dvije značajne prednosti i to: čitač zahtijeva manji pokret ruke operatera i može se koristiti sa postolja čime se oslobađaju ruke operateru

STACIONARNI ČITAČI SA POKRETNIM ZRAKOM ZA TRANSPORTNE TRAKE

Stacionarni čitači sa pokretnim zrakom, kako samo ime kaže, su fiksirane pozicije i povezani su kablom sa izvorom napajanja i komunikacionim kanalom. Da bi stacionarni čitač pročitao simbol trakastog koda potrebno je predmet sa kodom donijeti u vidno polje čitača. Ovi uređaji mogu skenirati simbole koji se kreću njihovim vidnim poljem. Podaci dobijeni sa simbola se šalju nekom obliku kompjuterskog sistema. Na taj način može se upravljati procesima kao što su sortiranja i skaldištenja proizvoda sa proizvodne trake (Slika 2.1.55).

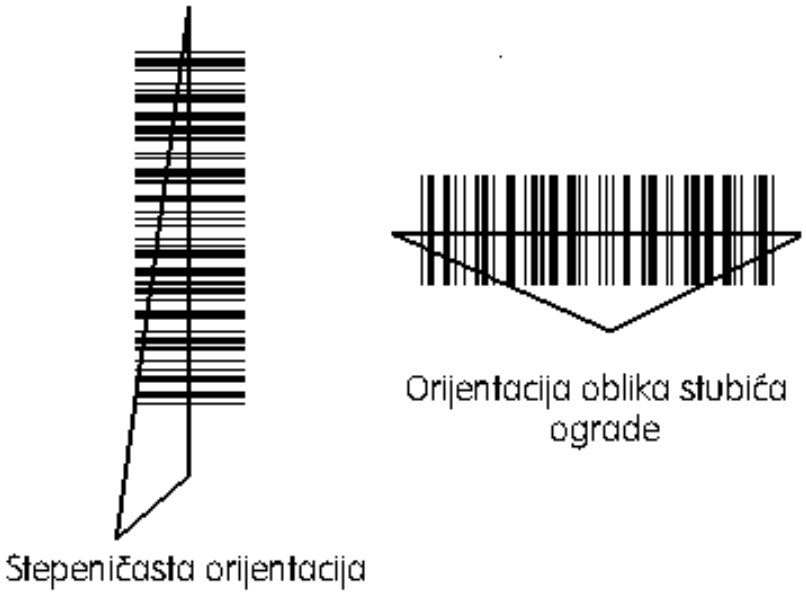
Slika 2.1.55 Primjene stacionarnih čitača sa pokretnim zrakom

Stacionarni čitači sa pokretnim zrakom obično se montiraju na stranama proizvodne trake. Simboli trakastog koda su na proizvodima štampani u obliku ″stubića ograde″ što predstavlja standardnu orijentaciju simbola. Standard je utvrđen još u vrijeme kada su postojali samo čitači sa fiksiranim zrakom i ne predstavlja optimalanu orijentaciju za čitače sa pokretnim zrakom. Pogodnija je stepeničasta orijentacija simbola (Slika 2.1.56). Na primjer, ako je brzina skeniranja 200 pokušaja u sekundi i oba simbola se kreću brzinom 55 metara u minuti, simbol stepeničaste orijentacije je 108 milisekunda u vidnom polju čitača (21 pokušaj), dok je simbol oblika ″stubića ograde″ u vidnom polju 60 milisekundi (11 pokušaja).

U zatvorenim aplikacijama, ukoliko se čitač montira sa strane proizvodne trake preporučuje se upotreba simbola ″stepeničaste″ orijentacije. Ako je čitač montiran iznad ili izpod proizvodne trake, može se koristiti orijentacija oblika ″stubića ograde″.

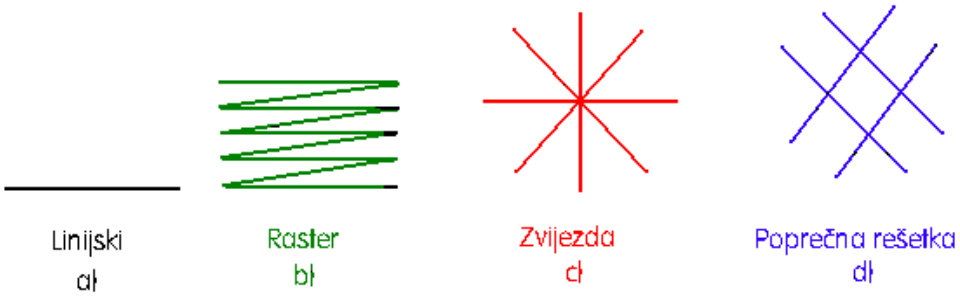
Skeneri sa pokretnim zrakom, uopšte, emituju pokretnu svjetlosnu mrlju. Brzina je 40 skeniranja u sekundi ili više. Zbog toga se dobija utisak da se radi o kontinualnoj svjetlosnoj liniji.

Da bi trakasti kod bio uspješno pročitan potrebno je da svaka traka i međuprostor budu presječni u jednom pokušaju skeniranja.



Slika 2.1.56 Stepeničasta i orjentacija ″stubića ograde″ simbola trakastog koda

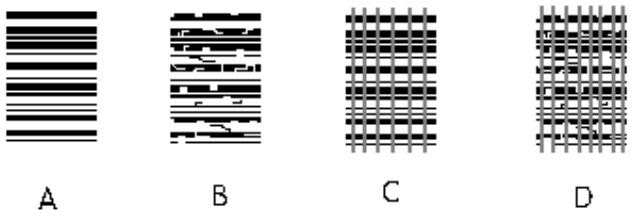
Da bi se obezbijedila veća tolerancija u orijentaciji simbola prema čitaču kreiraju se različiti obrasci skeniranja simbola. Neki od ovih obrazaca predstavljeni su slikom 2.1.57. Najbolji rezultati se postižu ako je obrazac skeniranja zvjezdastog oblika (Slika 2.1.57c). Ovakav obrazac omogućuje ma kakvu orjentaciju simbola ali je složen za realizaciju i poskupljuje čitač. Alternativa je u obezbjedjivanju da se simbol uvijek pojavljuje u istoj poziciji prema skeneru, tako da se u mnogim slučajevima simbol nalazi na istom odstojanju od dna proizvoda.



Slika 2.1.57 Različiti obrasci skeniranja trakastog koda

Čitači sa pokretnim zrakom, često, imaju kružni algoritam, sposoban da više puta skenira simbol koji se kreće ispred. Ovim postupkom se zahtijeva da svaki simbol bude nekoliko puta (dva, tri ili više) uzastopno ispravno pročitan, da bi se podaci dobijeni sa simbola prihvatili i proslijedili na dalju obradu. Ovime se umanjuje mogućnost dobijanja pogrešnih podataka kada se čita loše odštamapan simbol, što je ilustrovano Slikom 2.1.58. Na Slici

2.1.58a) prikazan je dobro odštampan simbol trakastog koda dok na Slici 2.1.58b) predstavljen je simbol sa bitno oštećenom štampom. Slika 2.1.583c) prikazuje dobro odštampan simbol stepeničasto orjentisan prema čitaču montiranom sa strane transportne trake dok Slika 2.1.58d) prikazuje loše odštamapan simbol u istoj poziciji.



Slika 2.1.58 Kružnim algoritam skeniranja pomaže u očitavanju loše oštampanih simbola

Bitno je napomenuti i zavisnost između brzine transportne trake, brzine skeniranja i visine simbola trakastog koda (Na slici 2.1.58 visinu simbola predstavlja horizontalna dimenzija).

Kao primjer stacionarnog čitača sa pokretnim zrakom na Slici 2.1.59 prikazan je čitač MS-710 proizvod Microscan-a. Čitač koristi poluprovodničke laserske diode koje emituju vidljivu svjetlost (670nm nominalno). Brzina skeniranja mu je između 300 i 550 skenova u sekundi (predefinisana vrijednost je 500 skenova u sekundi), a ugao skeniranja 60°. Potrebni kontrast u simbolu je minimalno 25%, širina traka se može kretati u opsegu od 0.127mm do 1.02mm a domet čitača je od 5.08cm –do 25.4cm.

Slika 2.1.59 MS-170 čitač sa pokretnim zrakom

MS-710 uspješno skenira simbole različitog kvaliteta štampe i različite gustine. Upotreba rotirajućeg ravnog ogledala omogogućuje mu emitovanje 10 linija skeniranja (raster) koje su pod uglom od 2°. Na taj način čitač omogućuje veliku fleksibilnost u pozicioniranju simbola trakastog koda. Trajni, brushless motor ne zahtijeva održavanje i precizno zakreće ogledalo bez obzira na brzinu skeniranja iz pomenutog opsega.

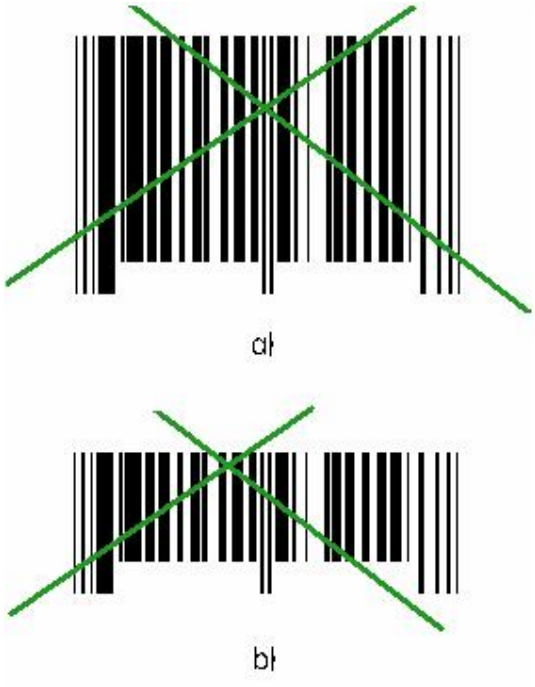
U slučaju pogrešnog očitavanja simbola, čitač pomoću ogledalnih

senzora može da odredi da li je to posljedica oštećenja simbola ili simbol nije u vidnom polju čitača (patemt Mocroscan-a).

Robusno kućište i zaštita elektronike od prašine i vlage čini MS-710 otpornim na štetne uticaje industrijskog okruženja.

ČITAČI NA PRODAJNIM MJESTIMA (POINT-OF-SALE)

Pregled čitača sa pokretnim zrakom ne bi bilo kompletan ako se ne bi spomenuli čitači na prodajnim mjestima (u supermarketima, na šalterima itd.). Ovi čitači su uglavnom isti kao i ostali sa pokretnim zrakom izuzev što posjeduju obrazac skeniranja namijenjen da olakša čitanje UPC simbola. Ovaj obrazac je obično zvjezdasti ili oblika rešetke, s tim što omogućava da lijeva strana simbola bude pročitana jednom svjetlosnom linijom a druga polovina simbola drugom svjetlosnom linijom. Ovo proširuje opseg položaja simbola prema čitaču. Za ilustraciju ovoga Slika 2.1.60a) pokazuje ortogonalni obrazac skeniranja gdje lijevu stranu U.P.C. simbola presijeca jedna linija a desnu stranu simbola druga linija. Slika 2.1.60b) pokazuje negativan efekat skraćivanja visine simbola. Sa slike se vidi da sada mora čitav simbol da presiječe jedna svjetlosna linija da bi bio ispravno pročitan.



Slika 2.1.60 Skraćivanje visine simbola trakastog koda otežava njegovo očitavanje

2.1.3.3.3 CCD čitači

Svi do sada razmatrani čitači koristili su izvor svjetlosti i jedan fotodetektor koji je davao električni signal proporcionalan reflektovanoj svjetlosti (zavisno od rasporeda traka i međuprostora u simbolu).

Slika 2.1.61 Uobičajeni izgled CCD čitača

CCD skeneri, čiji je primjer dat na Slici 2.1.61, funkcionišu slično običnom fotografskom aparatu ili kameri. Simbol se osvjetljava. Kao što kod fotografskih sistema reflektovana svjetlost pada na fotoosjetljivi film, CCD skeneri fokusiraju reflektovanu svjetlost na fotoosjetljive poluprovodničke komponente. Ove komponente predstavljaju fotodiode i raspoređene su u redovima. U jednom fotodiodnom redu ima između 1.024 i 4,096 tankih fotodioda, dimenzija manjih od 25 mikrona. Kada reflektovana svjetlost sa simbola trakastog koda padne na fotodiode, međuprostori izazivaju naelektrisanje dioda (označavajući prisustvo velike količine reflektovane svjetlosti), a trake izazivaju nedovoljno naelektrisanje fotodioda označavajući prisustvo male količine reflektovane svjetlosti. Uzorke sa piksela uzima mikroprocesor, određuje nivo zasićenja svake i proizvodi signal ekvivalentan simbolu koji je pročitan. Dalje, kao i kod drugih čitača trakastog koda, signal se digitalizuje i dekodira.

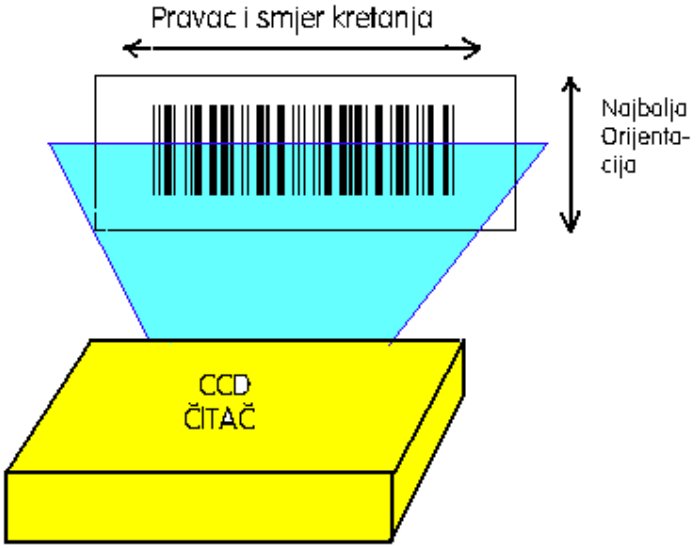
Za za razliku od laserskih čitača, polje čitanja CCD skenera je desetak cm. Vidljivo polje CCD skenera je ograničeno brojem pixela (malih fotodioda). Tendencija je da se izrađuju CCD čitači sa sve većiom dubinom polje čitanja i vidljivim poljem.

Broj pixela po jedinici dužine određuje rezoluciju čitača. Povećanjem broje pixela možemo čitati sve manje elemente u trakastom kodu odnosno kodove sve većih gustina.

Noviji CCD skeneri imaju detektor u obliku matrice sa više linija

fotodioda. Ovakvi skeneri su u stanju kompenzovati oštećenja u simbolu koja su posljedica loše štampe ili habanja a koja mogu uzrokovati grešku kada je prisutna samo jedna linija fotodioda.

CCD čitači skeniraju brzinom od oko 500 skenova u sekundi, tako da se mogu koristiti za skeniranje trakastih kodova na objektima koji se kreću velikim brzinama. CCD čitači mogu čitati kodove koji prolaze brzinom od oko 500cm/sec ili brže, što zavisi od karakteristika pojedinog trakastog koda. Da bi se podržala najveća brzina promicanja koda, on mora biti orjentisan prema čitaču tako da trake budu paralelne kretanju skenirajućeg svjetlosnog snopa, kao na slici 2.1.62. Ukoliko su obrnute orijentacije maksimalna brzina pomjeranja simbola trakastog koda je ograničena na oko 13cm/sec (opet zavisno od karakteristika pojedinog trakastog koda).



Slika 2.1.62 Optimalna orjentacija simbola trakastog koda prema CCD čitaču

CCD skeneri mogu biti ručni ili fiksno montirajući.

U primjenama na prodajnim mjestima, ručni CCD skeneri su se dugi niz godina utrkivali sa laserskim ručnim skenerima. Danas su uglavnom u prednosti jer imaju veću osjetljivost i rade na učestanosti 2MHz ili većoj.

U industrijskim aplikacijama postoji konkurencija između fiksno montirajućih laserskih skenera i fiksno montirajućih CCD skenera. U textu koji slijedi dato je poređenje ova dva tipa skenera.

Prednosti fiksno montirajućih CCD skenera su:

- CCD skeneri nemaju pokretnih djelova. Laserski skeneri imaju rotirajuća ili oscilirajuća ogledala a takav mehanizam je podložan oštećenjima.
- CCD skeneri koriste LED za osvjetljavanje simbola trakastog koda. LED imaju oko deset puta duži radni vijek od laserskih dioda. Njihova svjetlost je skrivena od direktnog pogleda, pa dodatne mjere

predostrožnosti nijesu nephodne.

- CCD skeneri su, generalno, manjih dimenzija i niže cijene od laserskih skenera.
- CCD skeneri se mogu postaviti vrlo blizu trakastog koda, neki gotovo do kontakta. Ovo omogućuje upotrebu ne mjestima gdje je prostor ograničen. Laserski skeneri trebaju veće rastojanje između skenera i koda i instalacija zauzima više prostora.

Prednosti laserskih fiksno montirajućih skenera su:

- Laserski skeneri mogu biti locirani mnogo dalje od simbola trakastog koda i imaju veću dubinu polja čitanja. CCD skeneri imaju optički domet od desetak cm, dok kod laserski skenera objekat sa simbolom trakastog koda može biti udaljen nekoliko stotina cm ili više.
- Laserski čitači mogu čitati duže trakaste kodaove nego li CCD čitači. Mnogi CCD čitači čitaju trakaste kodove maximalne dužine oko 8 cm.
- Laserski skeneri postižu veće brzine skeniranja koje dosežu i do 2000 skenova u sekundi.

Na Slici 2.1.63 dat je primjer CCD čitača. To je ABC 30X čitač proizvod Barcode store, USA.

Slika 2.1.63 ABC 30X CCD čitač, proizvod Barcode store, USA.

Ovaj čitač koristi linearni CCD senzor visoke rezolucije (2048 pixela). Kao izvor svjetlosti upotrebljava crvene LED koje emituju svjetlost talasne dužine 660nm. Brzina skeniranja mu je 100 očitavanja (skenova) u sekundi. Najuža traka koju je ABC 30X u stanju prepoznati je širine 0.127mm. Dubina polja čitanja (DoF) mu je 0-15mm a maximalna dužina koda 80mm. Može čitati sljedeće simbologije: Code 39, UPC/EAN, Interlaved 2 of 5, Code 128, Codebar, MSI/Plessey i Code 1.

Kao drugi primjer na slici 2.1.64 pokazan je novi Datalogic-ov čitač DLC7070-M koji može čitati sa otprilike 40cm udaljenosti od simbola trakastog koda. Baziran je na CCD tehnologiji koja omogućava čitanje na veće daljine slično laserskim čitačima. Datalogic-ova iskustva iz primjene čitača u maloprodajnim objektima, bankama, kancelarijama i sl. pokazuju da korisnici najčešće očitavaju simbole trakastog koda sa udaljenosti 3 do

18 cm, što je nazvano: INSTIKTIVNA daljina. DLC7070-M ima najbolje performanse baš u tom opsegu. Čitanje je pouzdano zahvajujući osjetljivom optičkom sistemu koji koncentriše svjetlosni zrak što olakšava orijentisanje simbola trakastog koda prema čitaču. Optički sistem je bez pokretnih dijelova što ga čini dugovječnim.

Maximlna rezolucija čitača je 0.13mm a kao izvor svjetlosti koristi crvene vidljive LED. Brzina čitanja mu je 100 očitavanja u sekundi. Minimalni kontrast u simbolu mora iznositi najmanje 15%

Slika 2.1.64 DLC7070-M Datalogic CCD čitač

DLC7070-M može čitati sljedeće simbologije: Interleaved 2 of 5, Code 39, Code 93, Code 128, Code 32, Code 39 CIP, EAN 128, EAN/UPC, Codebar. Polje čitanja čitača se se proteže do 200mm. Dubina polja čitanja iznosi 135mm za EAN 13 simbole i 280mm za Code 39 simbole.

2.2 OPTIČKE MEMORIJSKE KARTICE (LASERSKE KARTICE)

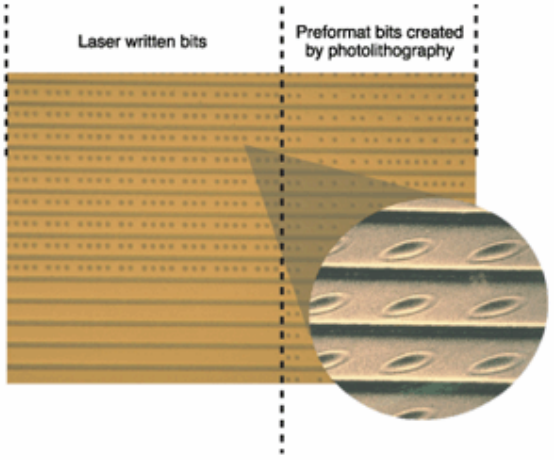
U najpoznatije optike memorijske uređaje spadaju optički diskovi. Iako se često srijeću u raznim primjenama, optičke memorijske kartice (laserske kartice) su ipak znatno manje poznate.

Optičke kartice imaju slične mogućnosti zapisivanja podataka kao i diskovi plus nekoliko značajnih specifičnih osobina. Oblik i gipkost kartice su slični kreditnim karticama (Slika 2.2.1).

Slika 2.2.1 Optička memorijska kartica, proizvod firme LaserCard

Optička kartica je izrađena na način da bude otporna na spoljašnje uticaje. Za razliku od optičkog diska, može se nositi u novčaniku bez bojazni od oštećenja. Siguran je nosilac nepromjenjivih podataka, koji mogu uključivati sliku ili tekst [28].

Za razliku od rotirajućih diskova, optičke kartice koriste pravolinijski format zapisivanja podataka. Trake su poređane upravo kao linije na išpartanom listu hartije. Svaka traka je numerisana (Slika 2.2.2).



Slika 2.2.2 Memorijske trake optičke kartice

Prilikom čitanja podataka, kartica se pomjera u pravcu trake u oba smjera. Prelaz sa trake na traku omogućen je pokretanjem optičke glave čitanja u pravcu normalnom na pravac prostiranja traka.

Slika 2.2.3 Optička kartica i njen čitač

Optičke kartice nalaze primjenu u mnogim sistemima gdje je potrebna prenosivost skladištenih podataka. Najznačajnija primjena im je u identifikaciji ljudi. The US Permanent Resident Card ("green card") i Italian national ID su neke od najžna čajnijih primjena optičkih memorijskih kartica [29], [30].

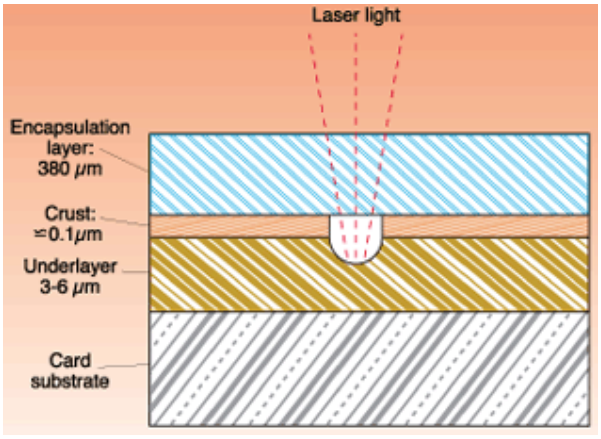
Optičke memorijske kartice imaju kapacitet do 2.9MB, što je znatno više nego što je raspoloživo na magnetnim karticama (270B) ili većini pametnih kartica (do 16KB). U cilju obezbjeđivanja kompatibilnosti sa postojećom infrastrukturom i proširenja spektra primjene, optičke kartice mogu sadržavati i magnetnu traku ili čip.

2.2.1 Memorijski medij

Memorijski medij upotrijebljen u optičkoj kartici ja zasnovan na silver-halid fotografskom filmu. Formatiranje medija se izvodi fotografskim postupkom prije enkapsulacije medija u kartici. Proces fotografskog formatiranja omogućava kreiranje u mediju vidljive slike visoke rezolucije (12000dpi), koja ne može biti ponovljena štampanjem. Pripremljeni optički medij ima karateristike WORM (wtite once read many) medija.

Na čeonoj strani tijela kartice nalaze se tri sloja: enkapsulacioni sloj, ljuska (engl. crust) i podsloj. Enkapsulacioni sloj je istanjeni 380μm-ski polikarbonatni film. Ljuska sadrži srebrna granulasta vlakna sferičnog oblika rasuta u organskom kolidu. Podsloj se satoji od istog organskog

kolida ali on ne sadrži srebrna zrnca. Podsloj termički izoluje refleksionu ljusku i povećava osjetljivost prilikom laserskog upisivanja podataka. Podaci se upisuju 780nm-skim poluprovodničkim laserom . Laserski zrak izaziva anglomeraciju srebrnih granula (čestica) redukujući pokrivenost njima a time i refleksivnost djelova medija. Sekundarno, termička deformacija koloidnog veziva rezultuje formiranjem rupa (Slika 2.2.4). Rupe su prečnika 2.5µm. To je prilično veliko u poređenju sa veličinom bita na optičkom disku, pa je optička kartica otporna na grubo rukovanje, kao što je nošenje u novčaniku, u dužem vremenskom periodu. Veća veličina bita i trake debljine 12µm obezbjeđuju robustnost koja se ne može postići sa geometrijom uobičajeno korištenom kod optičkih diskova [31].



Slika 2.2.4 Laserski zrak upisuje bitove kroz ljusku medija i podsloj.

Dalje povećanje pouzdanosti postiže se primjenom PPM-a (Pulse Position Modulation) prilikom upisivanja podataka. PPM se koristi radije nego PWM (Pulse Width Modulation) koja je u upotrebi kod optičkih diskova. Obzirom da se kartica može naći u širokom opsegu različitih spoljašnjih uslova, PPM šema upisivanja podataka čini karticu otpornijom na promjene u samom mediju i u laserskom zraku, izazvane ekstremnim uslovima sredine [32].

2.2.2 Čitači optičkih kartica

U pogledu napajanja, čitači optičkih kartica mogu biti predviđeni za napajanje iz spoljašnjeg izvora (fiksni čitači) ili mogu imati baterijsko napajanje (prenosivi).

Na Slici 2.2.5 prikazan je primjer fiksno montirajućeg čitača optičkih kartica, proizvod firme LaserCard.

Slika 2.2.5 LaserCard 600-Q Optical Card Drive

LaserCard 600-Q Optical Card Drive je standardi uređaj namijenjen za očitavanje i upisivanje podataka na optičku memorijsku karticu To je standardni SCSI II ili USB periferni uređaj, konstruisan da može da radi sa većnom optičkih kartica. Uređaj omogućava čitanje i upisivanje podataka na sve optičke kartice izrađene po ISO standardu [28]. Na Slici 2.2.6 date su osnovne karakteristike ovog uređaja.

Specifications:

Dimensions	5.5"W x 9.8"D x 2.5"H (139W x 254D x 64H mm)
Weight	5.5 lbs (2.6 Kg)
Card Type	ISO 11693, 11694 Parts 1-4 (Annex B) 2.86 MB & 1.1 MB
Sector Formats	ISO 11694 Part 4 Annex B, Formats 0-6
Read Speed	11.2 KB/sec throughput (bi-directional)
Write Speed	5.6 KB/sec throughput
Access Time	100 msec (overall width) 1.7 msec (track to track)
Corrected Error Rate	Less than 10^{-12}
Power	12VDC, 4.0 Amp continuous input
Power Consumption	Standby: 0.2 - 0.1A Operating: 0.8 - 0.4A Peak: 1.2 - 0.5A

Environmental Conditions:

Operation	5°C to 40°C, 20% to 80% RH (no condensation)
Storage	5°C to 55°C, 20% to 90% RH (no condensation)
Installation Conditions	Horizontally, indoor environment

Safety Regulations:

Agency Approvals	UL/CE/TUV/CSA/FCC/FDA

Interface Options:

Software Interface Options	LaserCard File System DLL for Windows XP/2000
Interface	SCSI-II or USB 1.1

Slika 2.2.6 Osnovne karakteristike LaserCard 600-Q Optical Card Drive

Dodatne opcije uključuju: kontaktni ili beskontaktni čitač IC čipa, onemogućavanje upisivanja podataka na karticu (read-only mode), i mogućnost izmjene firmware-a za primjene u kojima se zahtijeva specifično kodiranje podataka.

Slika 2.2.7 prikazuje prenosivi čitač optičkih kartica, takođe proiyvod LaserCard-a.

Slika 2.2.7 LaserCard Portable Optical Card Reader

Ovo je lagan uređaj, baterijski napajan, namijenjen za čitanje optičkih kartica u primjenama gdje je naophodna prenosivost čitača. Može se koristiti kao samostalan uređaj ili u kombinaciji sa PDA, laptop ili desktop kompjuterom. Veza sa kompjuterom ostvaruje se serisjskoj ili USB interfejsa. Po potrebi, Portable Reader se može povezati sa računarom i preko BlueTooth interfejsa I ostvariti wireless konekciju sa udaljenosti do 30 stopa.

Osnovne karakjteristike ovog uređaja date sun a slici 2.2.8.

Specification:

Dimension
2.6"W x 8.6"D x 1.8"H
(66W x 218D x 46H mm)

Weight
1.6 lb (.73 kg)

Card Type
ISO 11693, 11694 Parts 1-4 (Annex B)
2.86 MB & 1.1 MB

Sector Formats
ISO 11694 Part 4 Annex B, Formats 0-6

Read Speed
4.0 KB/sec throughput (bi-directional)

Access Time
1 sec (overall width)
9 msec (track to track)

Corrected Error Rate
Less than 10^{-12}

Power Source
5VDC, 1.4 Amp continuous input

Power Consumption
Standby: 0.3A
Sleep: .15A
Operating: 0.3 - 1.2A
Peak: 1.3A

Environmental Conditions:

Operation
5°C to 40°, 20% to 80% RH
(no condensation)

Storage
5°C to 55°, 20% to 90% RH
(no condensation)

Installation Conditions
Horizontally, indoor environment

Interface Options:

Software Interface Options
LaserCard File System DLL for
Windows XP/2000/NT/ME/98

Interface
USB, Bluetooth

Slika 2.2.8 Osnovne karakteristike LaserCard Portable Optical Card Reader

Čitači optičkih kartica razlikuju se od uobičajenih čitača optičkih diskova. Ralzika potiče otuda što se optičke kartica dizajniraju tako da budu izdržljivije u upotrebi. Čitači optičkih kartica koriste snažnije algoritme za korekciju greške, nego što su to Read-Solomon kodovi [27], uobičajeno korišteni kod optičkih diskova. Koristi se BEST (Burst Error for Satellite Transmission) kod, koji povećanje sigurnosti podataka ostvaruje umetanjem znatne veće količine redudantnih podataka. Tako na primjer za upisivanje 2.9MB podataka kodiranih BEST kodom potreban je memorijski prostor od 4.1MB [33]. Na ovaj način obezbijeđeno je da se podaci mogu pročitati i sa kartice koja je oštećena usljed dugotrajne upotrebe.

Činjenica da je svaka traka na kartici numerisana, otvara mogućnost uvođenja dodatnog nivoa sigurnosti. U pojedinim aplikacijama, u cilju povećanja sigurnosti, moguće je uvesti jedinstveno numerisanje traka, različito od onog specificiranog ISO standardom. Firmware čitača se tada modifikuje da omogući pristup nestandardno numerisanim trakama. Tako se dobija kombinacija kartica/čitač specifična za datu aplikaciju. U ovakvoj situaciji, falsifikator me može koristiti standardni čitač za pristup podacima na kartici.

Ostvarenje ovog nivaoa sigurnosti nije skupo. Zahtijeva jedino specifično numerisanje traka i modifikaciju firmwere-a čitača. Kao dodatno povećanje sigurnosti, korisnički firmware se može vezati za serijski broj čitača. Zahvaljujući tome, ako bi se čip sa koriničkim fimrware-om premjestio u drugi uređaj on ne bi funkcionisao.

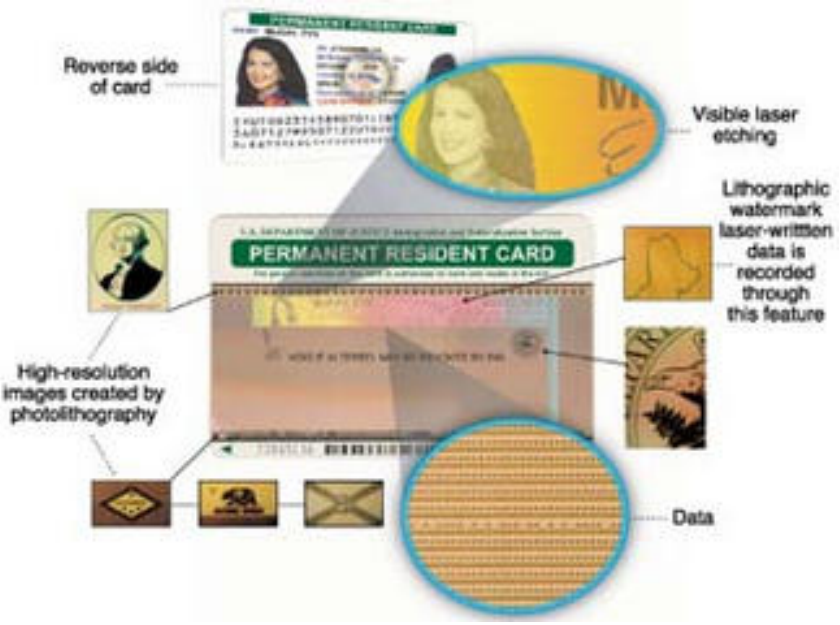
U cilju predupređivanja pokušaja falsifikovanja kartica, kao i neautorizovanoig pristupa podacima na originalnim karticama, u mnogim primjenama pod pokroviteljstvom države, koristi se neka šema specigičnog numerisanja traka.

Kao to se moglo zaključiti iz prikazanih primjera čitača optičkih kartica, oni se mogu praviti tako da omoguće samo čitanje ili i čitanje i upisivanje podataka na karticu. Na primjer, u pojedinim aplikacijama može se koristiti uređaj sposoban za upisivanje podataka na karticu, dok se u drugim može koristiti uređaj koji vrši samo verifikaciju postojećih podataka.

2.2.3 Primjena optikih memorijskih kartica

Optičke kartice se koriste u širokom opsegu aplikacija gdje se zahtijeva smještanje podataka na prenosivom mediju. Ipak, najveća primjena im je za sigurnu personalnu identifikaciju. U memorijskom mediju optičke kartice moguće je upisati slike i vodene žigove visoke rezolucije (do 12000dpi) koje se ne mogu duplirati tehnikama štampanja ili kopiranja. Veliki kapacitet podataka omogućava upisivanje više identifikacionih karakteristika korisnika, kao što su fotografija, fingerprint i potpis.

U mediju kartice moguće je laserski ugravirati vidljivu prepoznatljivu grafiku, čime se kartica nepovratno markira identitetom nosioca kartice (Slika 2.2.9). Obzirom da memorijski medij nije brisljiv, ovako kreirane slike ne mogu se mijenjati.



Slika 2.2.9 Optička memorijska kartica sadrži mnoge sigurnosne identifikacione karakteristike

Optičke memorisjke kartice našle su identifikacionu primjenu u brojnim sferama ljudske djelatnosti.

Zahvaljujući svojim karakteristikama primijenjene su u kontroli prelaska granice, kao i aplikacijama javne sigurnosti od strane vlada U.S.A., Italije, Kanade, Srednjeg-Istoka i država Latinske Amerike.

Jedna od najvećih primjena optičkih kartica desila se 1997 godine, od strane vlade U.S.A., kroz uvodjenje U.S. Permanent Resident Cards poznatih kao "green cards" (Slika 2.2.10) [29].

Slika 2.2.10 Oprička memorijska kartica kao U.S. Permanent Resident Card (Green Card)

Povedena dobrim iskustvom sa green card 1998 godine, U.S. vlada uvodi optičke kartice i za povećanje sigurnosti U.S/Mexico granice. Naime, u cilju olakšanja prelaska granice građanima Mexika iz graničnog područja, koji moraju često prelaziti granicu, vlada sjedinjenih država je izdala B1/B2 vize. Ove vize, nazvane Border Crossing Card (BCC) ili Laser Visa, su zapravo memorijske optičke kartice (Slika 2.2.10) [34].

Slika 2.2.10 Border Crossing Crad (BCC)

Optičke memorijske kartice koriste se i od strane agencija za registraciju automobila [35]. Na kartici je moguće upisati kompletnu istoriju automobila. Mogu se upisati podaci o prvoj prodaje, obnovi licance, polisi osiguranja, sabraćajnim nezgodama, preprodaji, itd. Kartica može sadržati i sliku vlasnika i, ako je potrebno, i njegove biometrijske karakteristike.

Slika 2.2.11 Optiča memoriska kartica kao registracioni dokument automobila

Kako sadržaj optičke memorije ne može biti naovlašteno mijenjan, podaci su vrlo pouzdani i mogu se koristiti od strane dežavnih organa u cilju suzbijanja falsifikovanja registracionih dokumenata, mijenjanja podataka o prodaji i slično.

U brodskom i kopnenom transportu optičke memorijske kartice sadrže informacije o sadržini tereta (Slika 2.2.12) [36].

Slika 2.2.12 Optiča memoriska kartica nalazi primjenu i u broskom transportu.

Zahvaljujuući pouzdanosti zapisa i mogućnosti brze obradee podataka primjena optičkih kartica u brodskojm i kopnenom transportu , donosi brojne dobitke:

- smanjuje se količina rada koji je potrebno uložiti za kontrolu tovara,
- smanjije se broj grešaka,
- omogućava se automatsko generisanje izvještaja,
- ...

Veoma interesantnu primjenu optičke memorijske kartice nalaze i u oblasti zdravstva. Mnoge zdravstvene ustanove imaju kompjuterizovani sistem za bilježenje elektroskih podataka o pacijentima. Ali i pored toga ostao je veliki broj izazova. Što uraditi u odsustvu komjuterske mreže? Što se receptima? Kako integrisati novootvorene klinike? Kako efikasno i jeftino prenositi podatke o pacijentu između raynorodnih zdravstvenih ustanova?

Primjena optičkih memorijskih kartica u ovoj oblasti može donijeti rješenja za pobrojana pitanja. Korištenjem optičke kartice, pacijent nosi sa sobom elektronke podatke i stavlja ih na raspolaganje bilo kojoj zdravstvenoj ustanovi kojoj pristupi (Slika 2.2.13) [36].

Slika 2.2.13 Optičke memorijke kartice u primjeni u zdravstvu mogu zamijeniti zdravstvene kartone i time ubrzati proces prikupljanja i obrade podataka o pacijentu

Pacijen može primijetiti sljedeća poboljšanja:

- mogućnost obavljanja nekih kontrola na osnovu njgovih ličnih zdrvstvenih zapisa;
- pacijent sam vodi brigu o svojim zdravstvanim podacima
- prilikom pregleda pacijent zna da liječnik raspolaže sa kompletnim i tačnim podacima o istoriji njegove bolijesti;
- pacijent se može zaštititi od neovlaštene izmjene podataka.

I pored brojnih primjena, optičke memorijske kartice, ipak prilično zaostaju u masovnosti upotebe iza trakastih kodova, magnetnih i pametnih kartica. Ovo je u prvom redu uslovljeno specifičnošću i visokom cijenom prateće opreme kao i visokom cijenom samih kartica.

GLAVA III

3. RFID TEHNOLOGIJA

3.1 UVOD

Radio frekvencijska identifikacija, ili RFID, je opšti naziv za tehnologije koje koriste radio talase za automatsku identifikaciju ljudi ili objekata. To je tehnologija koja se u poslednje vrijeme snažno razvija, i nalazi brojne primjene u svakodnevnom životu [22]. RFID tehnologija omogućava identifikaciju uz minimum napora korisnika. Korisnici se mogu identifikovati bez potrebe da pronalaze identifikator (karticu) u svojoj tašni ili novčaniku. Dovoljno je da se kartica nađe u polju čitača i indentifikacija je obavljena. Bezkontaktna razmjena podataka doprinosi da radni vijek RF čitača i RF identifikatora bude duži nego što je slučaj sa čitačima i identifikatorima drugih tehnologija.

U RFID sistemima:

- nema oštećenja kontakata kao kod sistema sa kontaktnim karticama,
- nema oštećenja glave čitača kao kod sistema sa magnetskim karticama,
- nema problema sa prljavštinom i ogrebotinama kao kod sistema sa bar kodom i magnetskim zapisom.
- RF čitač i RF identifikator su otporniji na sabotažu.

Zahvaljujući prenosu podataka putem radio frekvencija, nije potrebna direkna vidljivost između čitača i RF identifikatora. Ovakvu osobinu ne posjeduje ni jedna do sada razvijena identifikaciona tehnologija [37, 38].

Primjene RFID tehnologije su brojne. Na primjer, elektronska identifikacija, praćenje ljudi, stvari i životinja, označavanje proizvoda, magacinska poslovanja, maloprodajni objekti, bezbjedonosni sistemi, sistemi za potrebe vojske itd [39, 40, 41, 48].

U primjeni, za označavanje proizvoda u distribucionim i maloprodajnim objektima RFID tehnologija sve više potiskuje tehnologiju trakastih kodova [39, 41]. RF identifikatori imaju značajnih prednosti u odnosu na simbol trakastog koda. Neke od prednosti su:

- Za razliku od simbola trakastog koda koji zahtijevju direktnu vidljivost sa čitačem, RF identifiktori mogu se čitati kroz različite supstance, nezavisno od orjentacije prema čitaču. Ovo značajno ubrzava očitavanje identifikatora. U maloprodajnom objektu, RF identifikatori značajno ubrzavaju process naplate, na zadovoljstvo i prodavca i kupaca
- Više RF indentifikatora može biti pročitano odjednom.
- Simboli trakastog koda sadrže fiksnu količinu podataka, dok RF identifikatori osim postojećih podataka imaju i raspoloživi memorijski prostor za daljnju nadogradnju.

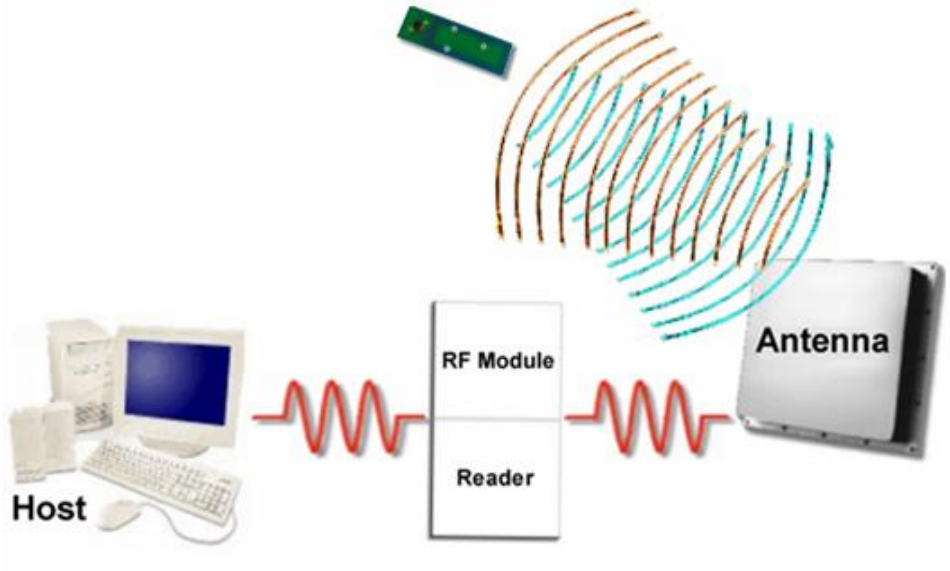
Osnovni sastavni djelovi RFID tehologije su: RF identifikator, RFID čitač i sistem za prikupljanje, distribuciju i upravljanje podacima (Slika 1.1.1) [37].

RF čitač i RF identifikator komuniciraju putem RF signala.

Kompletan RFID sistem, u najkraćem, funcioniše na sljedeći način:

- Čitač generiše elektromagnetni talas.
- Antena RFID taga podešena je da prima ove talase.
- Pasivni RFID tag crpi snagu iz polja čitača i koristi je za napajanje mikročipa.
- Čip moduliše talase, koje tag šalje nazad ka čitaču.
- Antena čitača prihvata modulisani signal.
- Čitač dekodira podatke.
- Izvještaj se šalje host-u.

RF identifikatori predstavljaju se čitaču jedinstvenom šifrom (jedintvenim identitetom).



Slika 3.1.1 Osnovni sastavni djelovi RFID sistema

RF čitač i RF identifikator komuniciraju putem RF signala.

Kompletan RFID sistem, u najkraćem, funcioniše na sljedeći način:

- Čitač generiše elektromagnetni talas.
- Antena RFID taga podešena je da prima ove talase.
- Pasivni RFID tag crpi snagu iz polja čitača i koristi je za napajanje mikročipa.
- Čip moduliše talase, koje tag šalje nazad ka čitaču.
- Antena čitača prihvata modulisani signal.
- Čitač dekodira podatke.
- Izvještaj se šalje host-u.

RF identifikatori predstavljaju se čitaču jedinstvenom šifrom (jedintvenim identitetom).

Da bi mogli komunicirati RFID tagovi i čitači moraju biti podešeni na istu frekvenciju. U različitim RFID sistemima korite više različitih frekvencijskih opsega. Postoje sistemi koji koriste:

- niske frekvencije (oko 125KHz),
- visoke frekvencije (oko 13.56MHz),
- ultra-visoke frekvencije (860-960MHz) i
- mikrotalasi (2.5GHz).

Radio talasi različitih frekvencija različito se ponašaju. Tako:

- radio talasi niskih frekvencija bolje se probijaju kroz nemetalne substance. Stoga se preporučuje korištenje niskofrekventnih RF tagova na objektima sa visokim sadržajem vode (voće, povrće, ...). Domet čitanja niskofrekventnih tagova je relativno mali, manji od 0.3m [38].

- RF identifikatori visokih frekvencija rade bolje na metalnim objektima a mogu raditi i na objektima sa visokim sadržajem vode. Maksimalni domet visokofrekventnih identifiktora je oko 1m [38].

- UHF frekvencije obezbjeđuju veći domet čitanja (4-7m) i brži prenos podataka. Loše osobine su im veća potrošnja i slabije probijanje kroz materijale. Zahtijevaju veću usmjerenost, odnosno, čistu putanju između identifikatora i čitača. Pogodni su za identifikaciju paketa proizvoda [38].

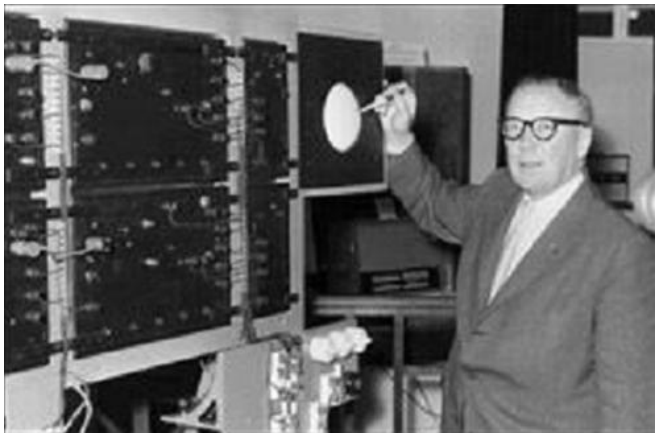
Za određenu aplikaciju potrebno je izabrati frekvenciju koja najviše odgovara konkretnoj primjeni.

3.2 ISTORIJAT RAZVOJA RFID TEHNOLOGIJE

Interesantno je osvrnuti se na istorijat razvoja RFID tehnologije. I pored toga što je ova tehnologija u poslednjoj dekadi dostigla svoj puni zamah, ona ipak nije sasvim nova. Prve primjene datiraju još iz vremena drugog svjetskog rata. Tada su se RF identifikatori koristili u avionima za prepoznavanje prijatelja - Foe sistemi (Slika 3.2.1). Foe sistemi su dali značajnu prednost savezničkoj floti [42].

Slika 3.2.1 Savezнички avion opremljen Foe sistemom

23-eg Januara 1973 registrovan je prvi američki patent za aktivni RF identifikator sa rewriteble-nom memorijom (Sliika 3.2.2). Sedamdesetih godina RFID sistemi nalaze primjenu i u telemetriji [43].



Slika 3.2.2 Prvi američki patent za aktivni RFID tag

Kasnijih 1970-ih RF identifikatori se u ograničenoj primjeni javljaju u sistemima za upravljanje inventarom. Sredinom 80-ih RFID tehnologija počinje da se ubrzano komercijalizuje. Razvijeni su pasivni RFID tagovi za praćenje stoke (Slika 3.2.3).

Slika 3.2.3 RFID tag upotrijebljen za praćenje stoke

Ranih 1990-ih IBM je razvio i patentirao ultra-high frequency (UHF) RFID sistem. Od 1999 do 2005 više od 100 velikih end-user komanija, U.S Department of Defense i mnogi trgovci prhvataju RFID tehnologiju. Na Slici 3.2.4 data su predviđanja koliko će RF identifikatora, u narednom periodu, trebati nekim od vodećih kompanija u SAD-u.

Kompanija	RFID (milijarde)
CHEP	0.2
Johnson & Johnson	3.0
Kimberly Clark	10.0
WestVaco	10.0
Gillette	11.0
YFY	15.0
Tesco	15.0
Proctor & Gamble	20.0
Unilever	25.0
Altria	30.0
Wal-Mart	53.0
International Paper	53.0
Coca-Cola	200.0
Pod suma	412.2
(Over-counting 15%)	-61.8
US Postal Service	200.0
Ukupno	555.4

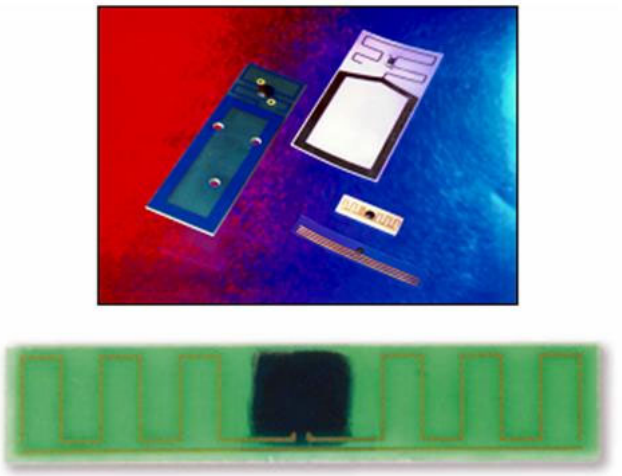
Slika 3.2.4 Predviđanje broja RF identifikatora potrebnih odabranim kompanijama

3.3 RF IDENTIFIKATORI

RF identifikatori su mali ili minijaturni čipovi koji sadrže podatke o objektu ili biću na koje se odnose. Mogu biti različitih oblika i dimenzija (Slika 3.3.1).

Slika 3.3.1 RFID identifikatori različitih oblika i dimenzija

Osnovni sastavni djelovi RF identifikatora su mikročip i antenna (Slika 3.3.2) [22].



Slika 3.3.2 Razni oblici antenna kod RF identifikatora

Prema tipu memorije koju sadrže, RF identifikatori mogu biti:
- Read-Only (fabrički programirni),
- WORM (write ones read multiple),
- Reprogrammable (field programmable),
- Read/Write (mogu se programirati u toku upotrebe) ili
- Chipless [44, 45, 46].

U Read/Write identifikatorima podaci se mogu upisivati više od 100000 puta. Read-Only identifikatori obično sadrže samo šifru na osnovu koje se u bazi podatka pronalaze informacije o onome na što se identifikator odnosi.

Prema načinu na koji se napajaju RF identifikatori se dijele na aktivne, polu-pasivne i pasivne (Tabela 3.3.1) [37, 44].

	Passive	Semi-Passive	Active
Power Source	Passive	Battery	Battery
Transmitter	Passive	Passive	Active
Max Range	10 M	100 M	1000 M

Tabela 3.3.1 Podjela RF tagova prema načinu napajanja

Aktivni identifikatori sadrže bateriju iz koje se napajaju. Oni mogu inicirati komunukaciju sa čitačem ili sa drugim identifikatorom. Glavna prednost im je u velikom komunikacionom dometu. Identifikacija se može obavljati sa udaljenosti do 100 metara ili više. Zahvajujući stalnom

napajanju, aktivni identifikatori, osim identifikacije mogu obavljati i druge funkcije kao što su telemetrijska mjerenja, prikupljanje podataka i slično. S druge strane, stalno napajanje donosi i mane i to prvenstveno u pogledu ograničenja radnog vijeka, odnosno potrebe za održavanjem identifikatora u smislu izmjene baterije. Aktivni identifikator je skuplji od dugih i većih gabarita, što značajno ograničava spektar njegova primjene (Slika 3.9).

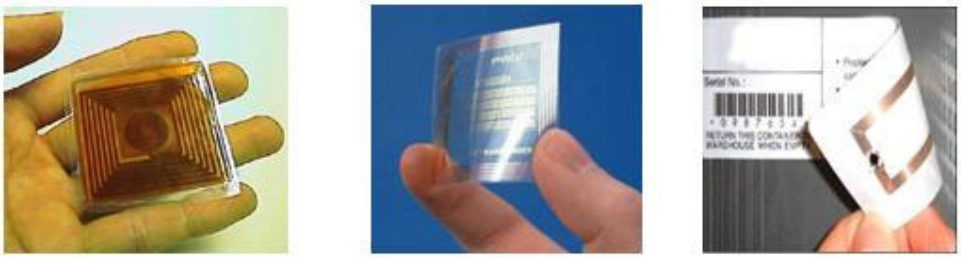
Polu-pasivni identifikatori imaju bateriju ali ne mogu inicirati komunikaciju već samo odgovarati na primljeni zahtjev. Drugim riječima, za komunikaciju sa čitačem koriste energiju iz polja čitača, dok im baterija obezbjeđuje napajanje mikročipa u odsustvu tog polja.

Pasivni identifiktori se u potpunosti napajaju iz polja čitača i naravno ne mogu inicirati nikakvu komunikaciju. RF čitači ″dozivaju″ pasivne RF identifikatore i zatim izvlače podatke iz rezultujućeg eha. Pasivni RF identifikatori su u potpunosti neaktivni u odsustvu polja čitača. Pasivni RF identifikatori imaju znatno kraći domet nego aktivni i polu-pasivni (ali i znatno duži vijek trajanja). Domet pasivnih tagova kreće se u opsegu do 5 metara [30,31] (Slika 3.3.3).

Slika 3.3.3 Primjeri aktivnih i pasivnih RF identifikatora

Posebnu grupu RF identifikatora predstavljaju Chipless identifikatori. Chipless RFID, odnosno RF identifikator bez čipa, kao što se iz naziva zaključuje, ne sadrži mikrokčip. Chiplees RFID koriste radio talase za komuniciranje ali se serijski broj ne čuva u silikonskom čipu RF identifikatora.

Chipless RFID čuva informaciju unutar elektromagnetskog materijala od kojeg je sačinjen. Chipless RFID je napravljen tako da reflektuje samo dio spektra radio talasa koji ga “pogađaju“. Kapacitet podataka obično manji od 32 bita. Šesto se koristi se za identifikaciju klase objekata pa mu veći ID niz nije ni potreban. Primjeri chipless kartica prikazani su na Slici 3.3.4

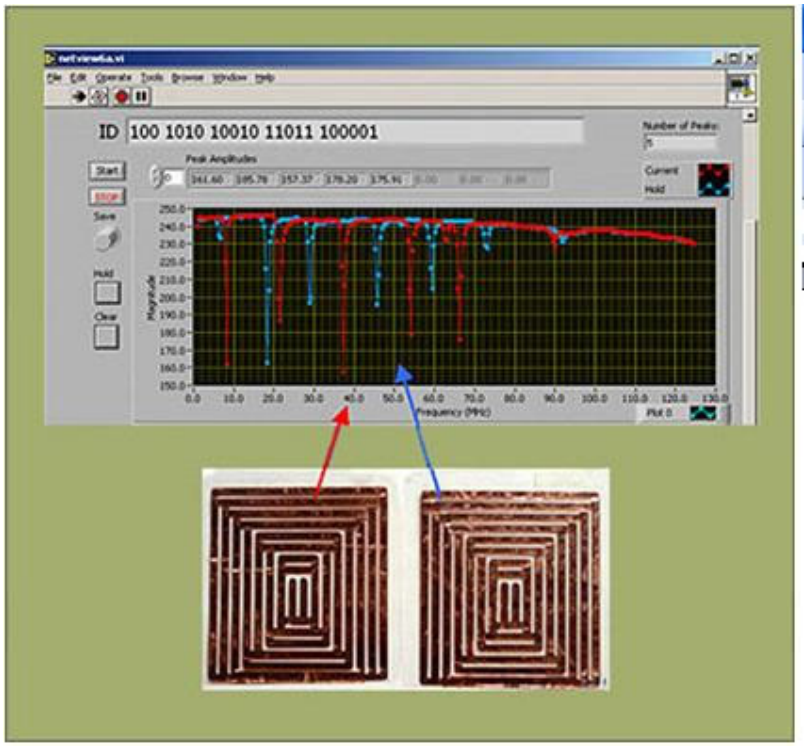


Slika 3.3.4 Chipless RFID tag

Čitači Chipless taga bilježi koji dio spektra je vraćen i prepoznaje identifikator (Slika 3.3.5).
Samo jedan chipless RF identifikator može biti u polju ćitača što predstavlja nedostatak za primjenu u lancima snadbijevanja.

Nake kompanije eksperimentišu sa ugrađivanjem RF reflektujućih fibera u papir u cilju zaštite od neovlaštenog fotokopiranja važnih dokumenata.

Postoje i LC rezonantni chipless tagovi koji se često srijeću na artiklima u trgovinama tekstila.



Slika 3.3.5 Očitavanje chipless rfid tag-a

RF identifikatori mogu biti zakačni na bilo koji objekat ili biće. Na primjer na:

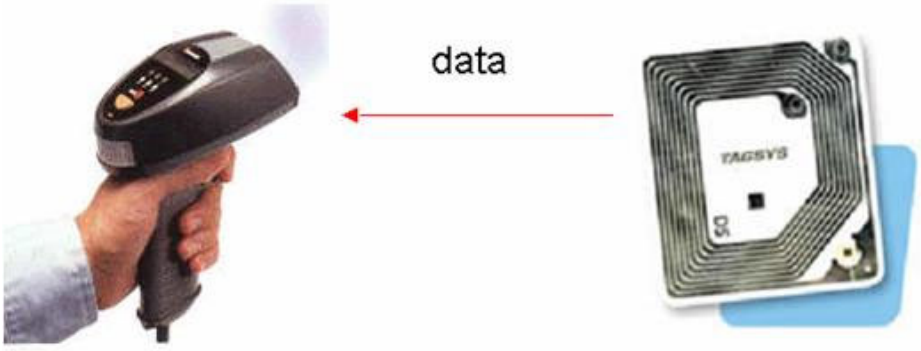
- paletama ili omotu proizvoda (Slika 3.3.6),
- automobilima,

- imovini preduzeća ili personalu,
- artiklima kao što su odjeća, prtljag, veš za pranje, …
- ljudima, stoci ili kućnim ljubincima,
- kompjuterima, televizorima, kamerama, …

Slika 3.3.6 RFID tag nalijepljen na omotu proizvoda

3.4 RF ČITAČI

RF čitači obavljaju sljedeće funkcije:
- slanjem upitnog signala aktiviraju RF identifikatore,
- napajaju pasivne identifikatore,
- kodiraju signale podataka koji idu ka identifikatorima i
- dekodiraju primljene podatke poslate od strane identifikatora (Slika 3.4.1) [37, 47].



Slika 3.4.1 RF čitač i RF identifikator

Da bi obezbijedili dodatnu funkcionalnost, RF čitači mogu sadržati internu memoriju za smještanje podataka, mogu imati mogućnost obrade podataka, a mogu se povezati i sa personalnim računarom odnosno softverom za prikupljanje, distribuiju i obradu podataka.

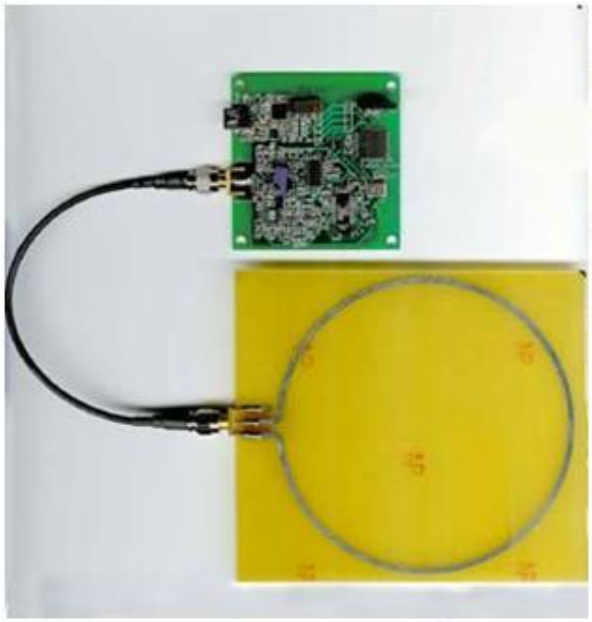
U praksi RF čitači mogu biti prenosivi uređaji ili postavljeni na fiksnu lokaciju (Slika 3.4.2).

Slika 3.4.2 Primjeri prenosivih RF čitača

Jedna od primjena nepokretnog čitača je ″pametna polica″. Pametna polica detektuje kada je koji predmet dodat ili oduzet. Pametna polica bi mogla imati ključnu ulogu u real-time sistemu za popis inventara.

U osnovi, RF čitači su sasvim jednostavni i mogu biti ugrađeni u mobilne uređeje kao što su telefoni. Troškovi izrade osnovnog RF čitača već su ispod 5 dolara.

Na slikama 3.4.3.i 3.4.4 prkazani su čitači LC-10 i LC-100 koji se koriste za detektovanje LC rezonantnih chipless RFID tagova, kao i chipless RFID tagova koji reflektuju dio spekta. Frekvencijski opseg čitača je za LC-10 2-50MHz i za LC-100 2-18MHz. Domet čitanja im je od 2 do 5cm.

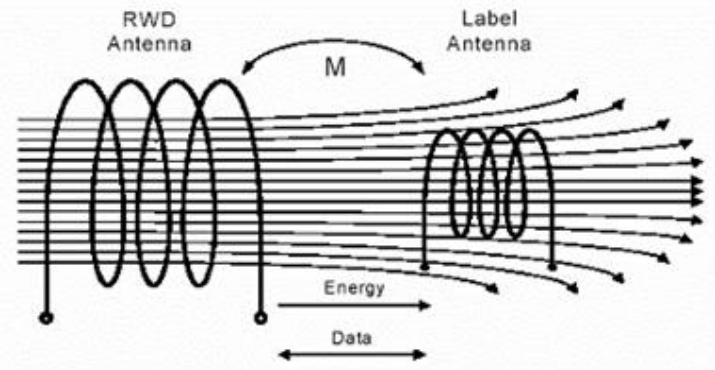


Slika 3.4.3 Chipless RFID reader LC 10

Slika 3.4.4 Chipless RFID reader LC 100

3.5 SPREZANJE (POVEZIVANJE) RF ČITAČA I RF IDENTIFIKATORA

Pasivni RF identifikatori se napajaju koristeći energiju iz elektromagnetskog polja čitača. Identifikatori moraju uzimati napajanje i komunicirati unutar uskog opsega radio frekvencija, specificiranog od strane regulatornih agencija poput FCC (Federal Communication Commision) i ERO (European Radiocommunication Office). U daljem tekstu centar frekvencijskog opsega će biti označen sa *f*.

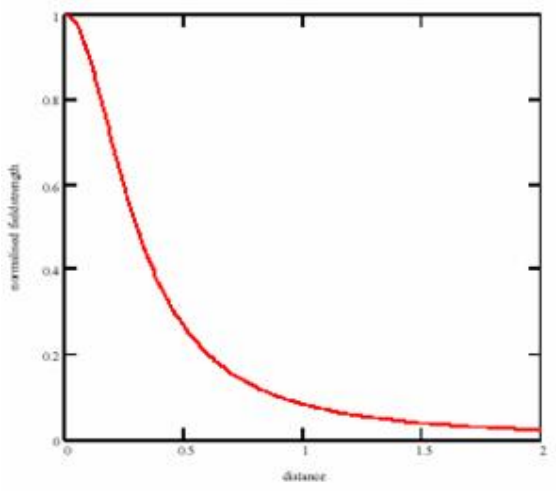


Slika 3.5.1 Induktivna sprega između RF čitača i RF identifikatora

Induktivna sprega između RF čitača i RF identifikatora radi ako transformator sa slabo spregnutim namotajima (Slika 3.5.1), s tim što je kod identifikatora, induktivni namotaj vezan sa kondenzatorom i formira

selektivno rezonantno kolo podešeno na učestanost nosioca. Na ovo kolo je dalje vezan diodni ispravljač koji obezbjeđuje napajanje ostatku identifikatora. Induktivna sprega je efikasna jedino u bliskom polju čitača, t.j. na rastojanjima do λ/10, gdje je λ - talasna dužina sinala.

Radni napon induktivno spregnutog identifikatora zavisi od gustine fluksa na datom rastojanju od čitača. (Slika 3.5.2).



Slika 3.5.2 Zavisnost jačine magnetskog polja od rastojanja identifikatora i čitača

Osim induktivnom spregom, RF identifikatori mogu se napajati i iz udaljenog polja. U oba slučaja, bilo da imamo napajanje iz bliskog ili udaljenog polja, snaga raspoloživa identifikatoru opada proporcionalno kvadratu rastojanju od čitača ($1/d^2$).

Pošto se ista učestanost koristi i za prenos snage i za prenos podataka, javljaju se određeni problemi. Prvi problem je taj što bilo kakva modulacija signala smanjuje snagu napajanja RF identifikatora. Drugi problem je što se modulisanjem sinusoide širi frekventni opseg signala. Širina frekventnog opsega (bočni opseg) i maksimalna snaga prenosa, obično su ograničeni propisima od strane regulatornih vlasti, čime se ograničava i količina informacija koja se može prenijeti od čitača prema identifikatoru i obrnuto.

3.6 KODIRANJE PODATAKA

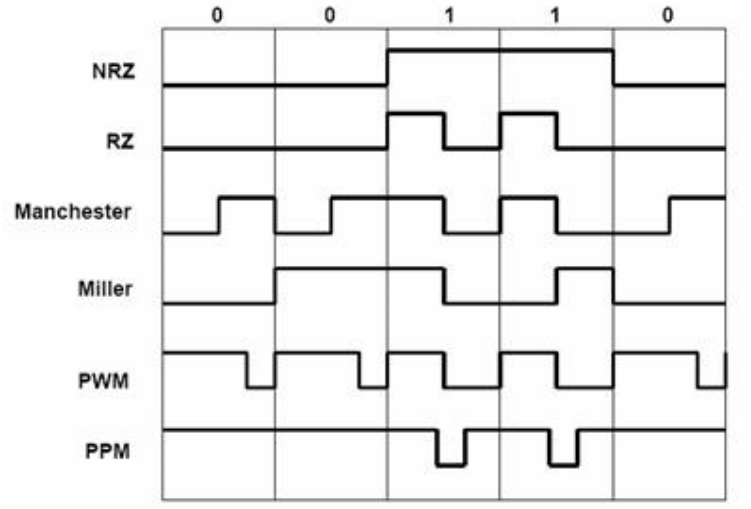
Podaci RF identifikatora moraju biti poslati čitaču na pouzdan način. Kodiranje ovih podataka i prenos preko modulisanog signala su dva ključna elementa pouzdnosti komunikacije. Izbor načina kodiranja podataka i modulisanja signala nosioca određuje širinu propusnog opsega, integritet podataka i potrošnju energije u komunikaciji između RF identifikatora i čitača.

Snaga kojom raspolažu i modulacione sposobnosti RF identifikatora određuju koje su metode kodiranja i modulacije prihatljive za RFID sisteme.

Dva široko upotrijebljena načina kodiranja u RFID sistemima su kodiranje nivoima (*level codes*) i kodiranje prelaskom (*transition codes*). Ranije šeme kodiranja pedstavljale su binarne vrijednosti određenim naponskim nivoom, dok su kasnije šeme bitove prestavljale promjenom naponskog nivoa. Kodovi prelaska su znatno robustniji od kodova nivoa. Nekoliko šema kodiranja prikazano je na slici 3.6.1.

Pulse Pause Modulation (PPM) je jednostavan kod u kojem vrijeme između dva impulsa reprezentuje vrijednost bita. PPM kod ima uzan spektar i jednostavan je za primjenu, ali ima malu brzinu prenosa.

Manchester kod predsatavlja 1-e i 0-e kao negativne i pozitivne prelaze između dva naponska nivoa, respektivno. Mančester kod ima veću brzinu prenosa podataka u odnosu na PPM kod ali i širi spektar.



Slika 3.6.1 Često korišteni načini kodiranja u RFID sistemima

Tehnika kodiranja podataka u RFID sistemima odabira se poštujući sljedeća tri kriterijuma:

1. Kodiranje mora trošiti sto je moguće manje snage RF identifikatora.
2. Kodiranje ne smije uzrokovati veliku širinu spektra signala
3. Kolizija mora biti detektovana.

Prvi kriterijum favorizuje PPM i PWM kodove, zbog njihovog relativno stabilog signala. PPM i PWM kodovi takođe zadovoljavaju i drugi kriterijum. Međutim detektovanje kolizije favorizuje Manchester kod.

Jedno rješenje je upotrijebiti PPM kodiranje u smjeru od čitača ka identifikatoru, a Manchester kodiranje u smjeru identifikator čitač. Ovo je pogodno zbog toga što PPM štedi snagu i ima uzan spektar, a kolizija može biti detektovana ako više identifikatora odgovore sa Manchester kodom. S druge strane, povratni kanal radi sa znatno manjim snagama, tako da širok

spektar Manchester koda ne predstavlja problem.

3.7 MODULACIJA

Dok kodiranje određuje predstavljanje podataka, modulacija upravlja načinom komuniciranja RF identifikatori i RF čitača. Karakteristično za RF komunikaciju je da se sastoji od nosećeg talasa modulisanog podacima. Postoje tri osnovna tipa digitalnih modulacija. To su amplitudska (ASK), frekencijska (FSK) i fazna modulcija (PSK). Svaki tip ima svoju vlastitu potrošnju, pouzdanost i širinu spektra.

Bitna razlika u snazi između RF identifikatora i RF čitača predstavlja poseban problem za RFID sisteme. U nekim prilikama, povratni signal prema čitaču može biti nadvladan signalom koji šalje čitač. Da bi se to izbjeglo, povratni signal je ponekad modulisan na različitoj frekvenciji (podnosilac). Na primjer, u ISO 15693 standardu za 13.56MHz RFID, upotrijebljen je podnosilac na učestanosi 13.56MHz/32 (=423.75 KHz) [49].

3.8 ANTI KOLIZIONE METODE KOD RF IDENTIFIKATORA

RF čitači često moraju pročitati jedan RF identifikator između mnogo prisutnih. Kada više RF identifikatora istovremeno odgovaraju na upit čitača, njihovi različiti signali mogu izazvati interferencu. Ova interferenca je nazvana kolizija i ona onemogućava komunikaciju.

Čitači i identifikatori moraju posjedovati metod za prevazilaženje kolizije, odnosno anti-kolizioni algoritam. Sličan kolizioni problem postoji u ćelijskoj telefonskoj mreži ili u Ethernet lokalnoj mreži i takođe se rješava anti-kolitionim algoritmom [50].

RFID sistemi imaju nekoliko specifičnih osobina u pogledu kolizije. RF identifikatori imaju ograničenu moć obrade signala i teške uslove rada (zbog promjenjive jačine signala) te teško mogu nadvladati problem kolizije. Dalje, pretpostavlja se da identifikatori nijesu u mogućnosti da međusobno komuniciraju. Ovo znači da punu odgovornost za detekciju kolizije snosi RF čitač.

Anti-kolizini algoritmi mogu biti probablistički ili deterministički. Poznati probablistički algoritam je Aloha scheme [51] upotrijebljen u Eternet lokalnim mrežama [52]. U kontekstu identifikator-čitač, identifikatori izbjegavaju koliziju sa drugim identifikatorima, slučajnim kašnjenjem njihovih odgovora. Ako se kolizija ipak pojavi, čitač će obavijestiti sve prisutne identifikatore i krivci će, prije nego nastave, sačekati još jedan, obično duži, slučajni vremenski interval. Veća gustina

identifikatora rezultiraće u većoj učestalosti kolizije i samim tim degradaciji performnsi sitema. ISO 15693 standard za RFID podržava Aloha način za anti-koliziju [53].

Jednostavan deterministički algoritam je šema binarnog šetanja (binary tree-walking). U ovom algoritmu, čitač od svakog identifikatora u svojoj blizini traži bit po bit njihovog ID-a. Ako su iz grupe identifikatora prenesene dvije različite vrijednosti bita, čitač će detektovati koliziju. Čitač dalje odlučuje da li će nastaviti komunikaciju sa identifikatorima koji su emitovali 0-bit ili identifikatorima koji su emitovali 1-bit. U stvari, čitač bira granu u binarnom stablu ID vrijednosti. Identifikator koji nije obuhvaćen čitačevim izborom prekinuće sa učešćem u komunikaciji. Tako će se sve više smanjivati broj identifikatora koji su još aktivni. Ako svi identifikatori imaju jedinstven ID, na kraju će samo jedan identifikator ostati u komunikaciji sa čitačem. Ovaj proces adresiranja i izdvajanja jednog identifikatora je poznat kao *singularizacija*. Na kraju singulatizacije, čitač zna cijeli ID identifikatora sa kojim komunicira.

Prilikom ocjene kvaliteta anti-kolizionog algoritma, prevladavaju sljedeći kriterijumi:

1. Performanse.
2. Domet (range).
3. Širina propusnog opsega (Bandwidth requirements).
4. Cijena primjene.
5. Otpornost na šum i greške.
6. Sigurnost.

Snaga binarnog šetanja je u efikasnosti i jednostavnoj primjeni u identifikatorima. Međutim, ova metoda sadrži bitan neostatak jer unosi prijetnju sigurnosti RFID sistema. U komunikaciji čitač-identifikator postoji nesimetrija u pogledu jačine signala kojeg emituje čitač i signala koji potiče od RF identifikatora. Svaki bit ID-a odabranog identifikatora emituje čitač. Signal čitača je jak i može biti uhvaćen od strane prisluškivača sa distance do 100m. Da bi se ovo preduprijedilo razvijene su sigurniji algoritmi u odnosu na normalno binarno šetanje. To su:

- Prekidno binarno šetanje (Blinded Tree-Walking) i
- Maskirano binarno šetanje (Randomized Tree-Walking)

U algoritmu Prekidnog binarnog šetanja čitač šalje ID bit identifikatora samo u slučaju kolizije. Ukoliko kolizije nema čitač samo traži sljedeći bit [54, 55]. Osnovna ideja u algoritmu Maskiranog binarnog šetanja sastoji se u tome da identifikatori privremeno, tokom procesa singularizacije, generišu slučajni pseudo-ID. Kada identifikator bude odabran, on će slati normalan ID prema čitaču. Medjutim, to će ići povratnim kanalom čija je snaga znatno manja pa prema tome udaljeni prisluškivač ga neće moći čuti [56].

Regulacija širine propusnog opsega je najvažniji parametar prilikom izbora anti-kolizionog algoritma. Kako probablistički algoritmi imaju uži propusni opseg, koriste ih identifikatori koji rade u strogo kontrolisanom

opsegu (13.56MHz). Identifikatori koji rade u manje kotrolisanom opsegu (915MHz), najčešće koriste determinističke algoritme.

3.9 FREKVENCIJE I REGULATIVA

Regulacija elektromagnetskog spektra od strane regulatornih vlasti utiče na karakteristike RFID sistema. Mnogi RFID sistemi rade u ISM (Indutrial-Scientific-Medical) opsezima koji su slobodni za sisteme male snage i kratkog dometa. Ovi opsezi su definisani od strane ITU (International Telecommunication Union) [57]. Pregled ove regulative može se naći i u [58].

U SAD-u, RFID sistemi najčešće koriste ISM propusne opsege 13.56MHz i 902-928 MHz. Nešto manje frekvencijskih licenci je raspoloživo za opseg od 9kHz – 135kHz. Uređaji koji rade u ovim osezima potpadaju pod različite regulative u odnosu na maksimalnu dozvoljenu snagu emitovanja i maksimalni propusni opseg.

Na primjer, direkni kanal sistema koji rade na frekvenciji 13.56MHz limitiran je propusnim opsegom od 14kHz. Povratni kanal može koristiti širi propusni opseg, jer je njegova snaga znatno manja.

Nasuprot tome, ISM opseg 915MHz nije tako strogo regulisan. Na raspolaganju je nekoliko opcija za komunikaciju od čitača prema identifikatoru. Opcija koja predviđa veći domet čitanja, zahtijeva od čitača da ″skače″ između 50 kanala svakih 0.4sec. Svaki kanal ima širinu propusnog opsega do 250kHz. ″Skokovi″ izazivaju prekide u komunikaciji čitač-identifikator jer identifikatori ne mogu imati neprekidnu komunikaciju u tim uslovima. Kontinuirana komunikacija čitač/identifikator mora biti ograničena na maksimalno 0.4sec. Transakcija mora biti kompletirana unutar tog perioda, inače će biti prekinuta frekvencijskim skokom.

3.10 MIFARE® 1 S50 (MF1ICS50) RFID KARTICA

Beskontaktna Mifare® 1 S50 bezkontaktna pametna pasivna kartica, veličine kreditne kartice, prvenstveno namijenjena da se koristi kao platna kartica. Kartica radi na učestanosti 13.56MHz. Podesna je za upotrebu u javnom transportu i sličnim aplikacijama, mada se može koristizi i za druge namjene, kao što je kontrola pristupa, evidencija radnog vremena, itd. (Slika 3.10.1).

Slika 3.10.1 Mifare® 1 S50 bezkontaktna pametna pasivna kartica

Mifare® 1 S50 je multi-aplikativna pametna kartica. Procesorska funkcionalnost kartice realizovana je kroz hardversku logiku.

Specijalni naglasak dat je na olakšavanje upotrebe korisniku, brzinu, pouzdanost, obezbjeđenje od prevara i nisku cijenu.

Razmjena podataka između kartice i čitača (transakcija) ostvaruje se kada korisnik karticu približi čitaču. Rastojanje između antene čitača i kartice mora biti u opsegu 100mm slobodnog prostora. RF komunikacioni interfejs omogućuje brzinu razmjene podataka od 106Kbaud-a. Ovako velika brzina onogućava da se transakcije izvršavaju brzo, najčešće za manje od 0.1sec. Usljed toga korisnik se ne mora zaustavljati kod čitača, već se potrebna transakcija može obaviti prolaskom njegove kartice kroz polje čitača. Ovakva osobina, na primjer, može značajno ubrzati proces naplate vožnje u javnom transportu, u odnosu na brzine koje se postižu tradicionalnim metodama izdavanja tiketa ili primjenom kontaktnih čip kartica.

Dodatna pogodnost koju ova kartica pruža korisniku je što se kartica ne mora vaditi iz novčanika da bi se transakcija izvršila, čak ni ako se u novčaniku nalazi sitan metalni novac.

Kartica posjeduje brzi ankolizioni algoritam. Ukoliko se više kartica istovremeno unese u polje čitača, ovaj algoritam sprečava da više njih istovremeno započne komunikaciju. Istovremena komunikacija nije poželna jer može dovesti do kolizije, kada ni jedna kartica ne bi obavila uspješno transakciju. Antikolizioni algoritam omogućava selekciju jedne kartice iz mnoštva. Kartice koje ostaju u polju čitača a nijesu selektovane ne remete komunikaciu selektovane kartice i čitača. Na primjer, ukoliko korisnik ima više MIFARE kartica u svom novčaniku, antikolizioni algoritam će omogućiti selekciju odgovarajuće kartice.

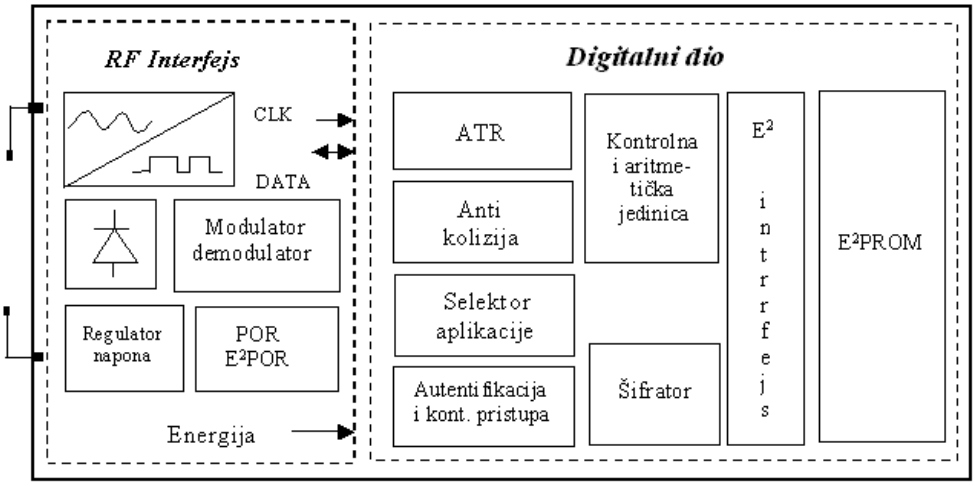
Više različitih nivoa autentifikacije i kodiranje podataka štite sistem od bilo koje vrste prevara i čine karticu interesantnom za primjenu u sistemima elektronskog plaćanja. Mehnizmi kontrole se izvršavaju brzo i neznatno produžavaju vrijeme transakcije. Jedinstveni serijski broj koji ne može biti promijenjen garantuje jedinstvenost kartice.

Multifunkcionalna memoriska struktura Mifare® 1 S50 kartice omogućava upotrebu iste kartice u različitim aplikacijama. Različite aplikacije su sigurno odvojene sa različitim ključem i uslovima pristupa koje može sefinisati korisnik.

Visoka pouzdanost sistema obezbijeđena je upotrebom poluprovodničkih komponenti, bez ijednog pokretnog mehaničkog dijela. Mifare® 1 S50 su pasivne kartice koje rade bez baretije. Pouzdanosti doprinosi i to što je kartice krajnje jednostavne strukture. Sastoji se od antene sačinjene od nekoliko navojaka žice i čipa, umetnutih u plastično tijelo kartice. Dodatno, beskontaktna tehnologija sprečava pojavu pohabanih kontakata i smanjuje rizik od vandalizma [58].

3.10.1 BLOK DIJAGRAM ELEKTRONSKE JEDINICE MF1ICS50 KARTICE

Na Slici 3.10.2 prikzan je blok dijagram elektronske jedinice Mifare® 1 S50 kartice.



Slika 3.10.2 Blok dijagram elektronske jedinice Mifare® 1 S50 kartice

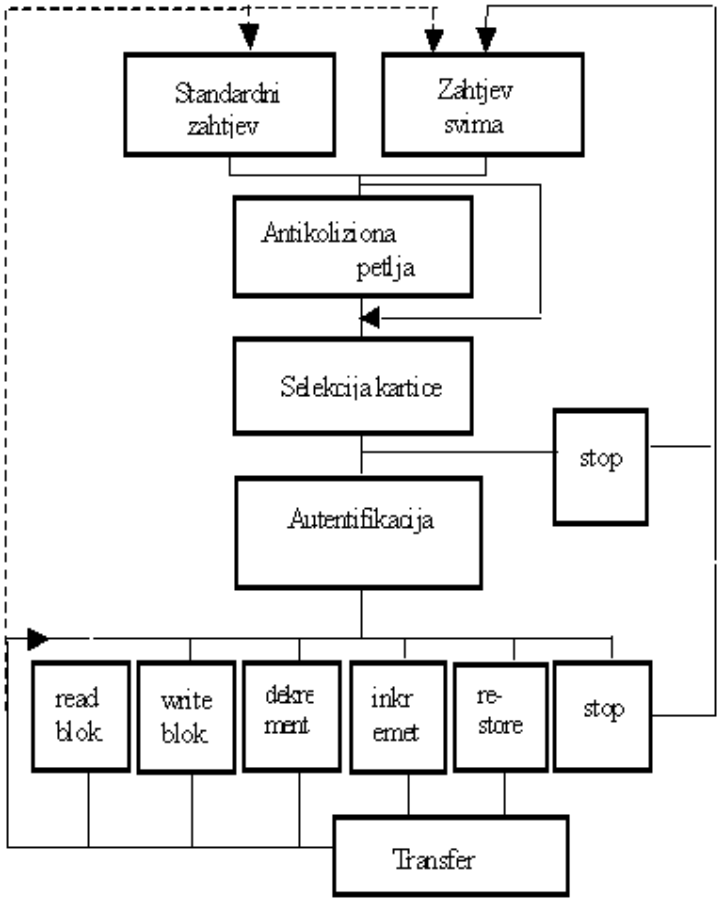
Osnovni djelovi su elektrmike kartice su: antena, RF interfejs i digitalni dio. Antena se sastoji od nekolika namotaja provodnika, pa je veoma podesna za integraciju unutar ISO kartice [5], [6]. RF interfejs konvertuje RF signal u digitalni oblik i prosljeđuje ga na dalju obradu, digitalnom dijelu. U digitalnom dijelu nalazi se kompletna logika potrebna za realizaciju trensakcije zahtijevane od strane čitača.

U okviru jedne transakcije najčešće je potrebno izvršiti:

- identifikaciju kartice,
- čitanje podataka iz memorije kartice i/ili
- upisivanje podataka u memoriju karticu.

3.10.2 KOMUNIKACIONA ŠEMA ČITAČ-KARTICA

Na Slici 3.10.3, u obliku dijagrama toka, dat je prikaz komunikacione šeme između čitača i kartice.



Slika 3.10.3 Dijagram toka komunikacionog protokola čitač-kartica.

Sekvencom ″zahtjev svima″ čitač proziva sve kartice koje su u njegovom polju. Ako se neka kartica odazove pozivu, čitač nastavlja komunikaciju prema datom protokolu.

U antikolizionoj petlji vrši se čitanje serijskog broja kartice. Ako ima nekoliko kartica u polju čitača one će biti razlikovane njihovim serijskim brojem i jedna će biti selektovana za dalje transakcije. Neselektovane kartice vraćaju se u ″stand by″ mod i čekaju za novi ″zahtjev svima ″ i novu antikolizionu petlju.

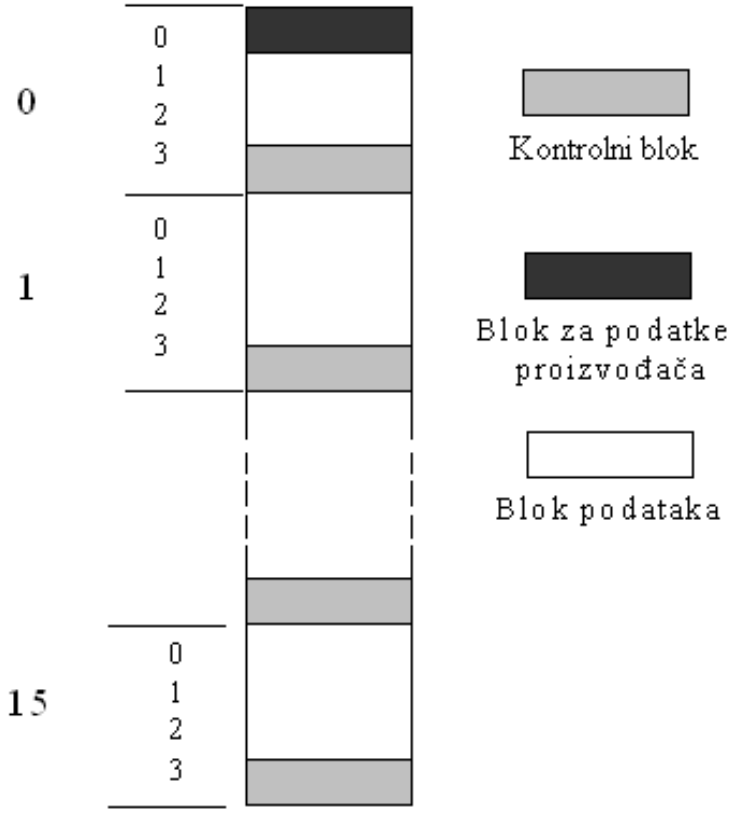
Čitač selektuje jednu od kartica komandom ″selekcija kartice″. Kartica odgovara sa ATS (Answer to Select) kodom [6].

Nakon identifikacije i selekcije čitač prelazi u fazu autentifikacije. Za autentifikovanje čitač koristi pristupni ključ kartice. Nakon autentifikacije, svaka razmjena podataka sa karticom je automatski šifrovana od strane pošiljaoca i dešifrovana od strane primaoca, .

Poslije uspješnog završetka faze identifikacije kartice čitač može pročitati podatke iz njenih memorijskih blokova, upisati podatke u memoriske blokove kartice kao i druge operacije ilustrovane slikom 3.10.3 [60, 61].

3.10.3 MEMORIJA MIFARE® 1 S50 KARTICE

Memoriju Mifare® 1 S50 kartice čini EEPROM veličine 1KB. Na slici 5. dat je blok dijagram EEPROM-a kartice.

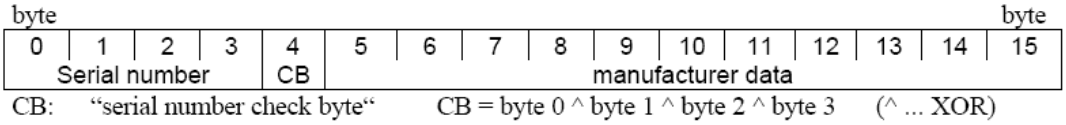


Slika 3.10.4 Blok dijagram EEPROM-a kartice

EEPROM kartice je podijeljen u 16 sektora. Svaki sektor sadrži 4 bloka od po 16 okteta.

BLOK ZA PODATKE PROIZVOĐAČA

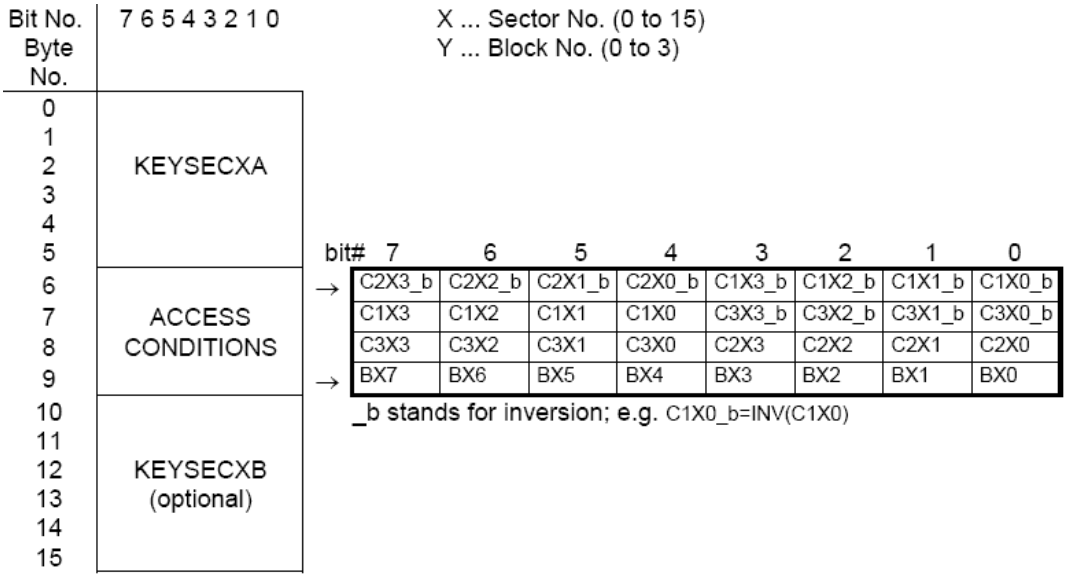
Prvi blok EEPROM-a kartice rezervisan je za podatke proizvožača, kao što je 32-bitni serijski broj. Ovaj blok EEPROM-a može se samo očitavati. U mnogim dokumentima označava se kao ″Block 0″. Memorijski sadržaj ovog bloka, nakon IC testa, prikazan je na Slici 3.10.5.



Slika 3.10.5 Struktura bloka za podatke proizvođača

KONTROLNI BLOK

Četvrti blok svakog sektora je tzv. ″kontrolni blok″. ″Kontrolni blok″ jednog sektora sadrži pristupni ključ A (KEYSECXA) i opcioni ključ B (KEYSECXB), kao i uslove pristupa, za četiri bloka tog sektora.



Slika 3.10.6 Struktura kontrolnog bloka

Ako ključ B nije neophodan, zadnjih 6 okteta kontrolnog bloka mogu se koristiti kao okteti podataka.

C1XY do C3XY (Y=0, 1, 2, 3) su bitovi kontrolnog bloka koji nezavisno definišu uslove pristupa za sva 4 bloka sektora. Iz razloga sigurnosti, ovi bitovi su zapisani 2 puta unutar kontronog bloka, prema šemi sa Slike 3.10.6. U ponovljenom zapisu bitovi imaju invertovanu vrijenost. Zadnji oktet uslova pristupa može se koristiti za smještanje nekog specifičnog aplikacionog podatka (npr. lokacija backup bloka).

Pregled mogućih uslova pristupa podacima kontrolnog bloka dat je na Slici 3.10.7. Key A|B znači ključ A ili ključ B. Ako se ključ B može pročitati (sve osijenčene linije sa slike 3.10.7) onda se on ne može koristiti za autentifikaciju. U ovim sličajevima, memorijski prostor rezervisan za ključ B koristi se za podatake. Obzirom da proizvodjač specificira uslove pristupa kontrolnom bloku kao (C1X3, C2X3, C3X3)=(0, 0, 1), nova kartica se ne može autetifikovati ključem B.

			KEYSECXA		ACCESS COND.		KEYSECXB	
C1X3	C2X3	C3X3	read	write	read	write	read	write
0	0	0	never	key A	key A	never	key A	key A
0	1	0	never	never	key A	never	key A	never
1	0	0	never	key B	key A|B	never	never	key B
1	1	0	never	never	key A|B	never	never	never
0	0	1	never	key A	key A	key A	key A	key A
0	1	1	never	key B	key A|B	key B	never	key B
1	0	1	never	never	key A|B	key B	never	never
1	1	1	never	never	key A|B	never	never	never

Slika 3.10.7 Pregled mogućih uslova pristupa podacima pratećeg sektora

Pregled mogućih uslova pristupa blokovima podataka sektora dat je na Slici 3.10.8.

C1XY	C2XY	C3XY	read	write	incr	decr, transfer, restore
0	0	0	keyA|B[1]	key A|B[1]	key A|B[1]	key A|B[1]
0	1	0	keyA|B[1]	never	never	never
1	0	0	keyA|B[1]	key B[1]	never	never
1	1	0	keyA|B[1]	key B[1]	key B[1]	key A|B[1]
0	0	1	keyA|B[1]	never	never	key A|B[1]
0	1	1	key B[1]	key B[1]	never	never
1	0	1	key B[1]	never	never	never
1	1	1	never	never	never	never

Slika 3.10.8 Pregled mogućih uslova pristupa blokovima podataka datog sektora.

Po proizvodnji kartice bitovi za kontolu pristupa blokovima podataka imaju vrijednosti 000, što odgovara prvoj vrsti tabela sa slike 3.10.8.

Redni brojevi kontrolnih bokovi u EEPROM-u kartice su 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59 i 63. Memorijski sadržaj kontrolnih bloka, nove, još ne upotrebljivane kartice, prikazan je na Slici 3.10.5.

byte										byte					
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
transport key A						FF	07	80	xx	transport key B					

Slika 3.10.9 Memorijski sadržaj kontrolnog bloka nove, neupotrbljivane, Mifare® 1 S50

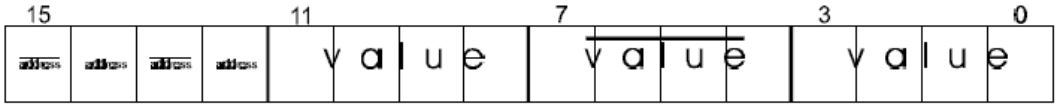
Vrijednost devetog okteta kontrolnih blokova nije precitno definisana od strane proizvođača kartica. Ova vrijednost kod novih kartica varira.

BLOKOVI PODATAKA

Blokovi podataka sadrže promjenjive podakte definisane od strane korisnika odnosno integratora sistema. Uslovi pristupa za Blokove podataka nalaze se u Kontrolnom bloku. Shodno ovim uslovima, podaci se mogu čitati, prepravljati, inkrementirati, dekrementirati, može se vršiti transfer podataka pomoću ključeva A ili B a može biti i zabranjen pristup podacima.

U Mifare® 1 S50 karticama koriste se dva tipa blokova podataka:

- Blokovi za čitanje/upisivanje podataka opšte namjene. U njima se upisuje 16 okteta podataka rezličitog značenja.
- Blokovi za promjenljive. Ovi blokovi se koriste da omoguće što efikasniju realizaciju funkcija elektronskog plaćanja (čitanje, inkrementiranje, dekrementiranje, transfer, ponovno memorisanje). I pored toga što se zauzima kompletan blok dužine 16 okteta, maksimalna veličina vrijednosne promjenljive iznosi 4 okteta uključujući i bit znaka. U cilju omogućavanja detekcije i korekcije greške, vrijednosna promjenjiva se tri puta zapisuje unutar jednog vrijednosnog bloka. Preostala četiri okteta mogu koristiti za pojačanje kontrole vrijednosne promjenjive, kao dodatni kontrolni podaci (Slika 3.10.10).



Slika 3.10.10 Struktura vrijednosnog bloka

MULTIFUNKCIONALNOST I STRUKTURA MEMORIJE

Organizacija EEPROM-a kartice omogućava korištenje različitih sektora za različite aplikacije. Svaka aplikacija može koristiti zaseban ključ. Ključeve može mijenjati jedino čitač koji poznaje ključ A ili ključ B (ukoliko je dozvoljen uslovima pristupa) za određeni sektor kartice.

Prije izvršenja komande čitača hardver kartice provjerava korektnost formata uslova pristupa u kontrolnom bloku sektora kojem se pristupa. Tako da, prilikom upisivanja nove vrijednosti u kontrolni blok treba voditi računa da se ne naruši korektnost ovog formata. Ukoliko bi se format narušio trajno bi se blokirao pristup podacima tog sektora.

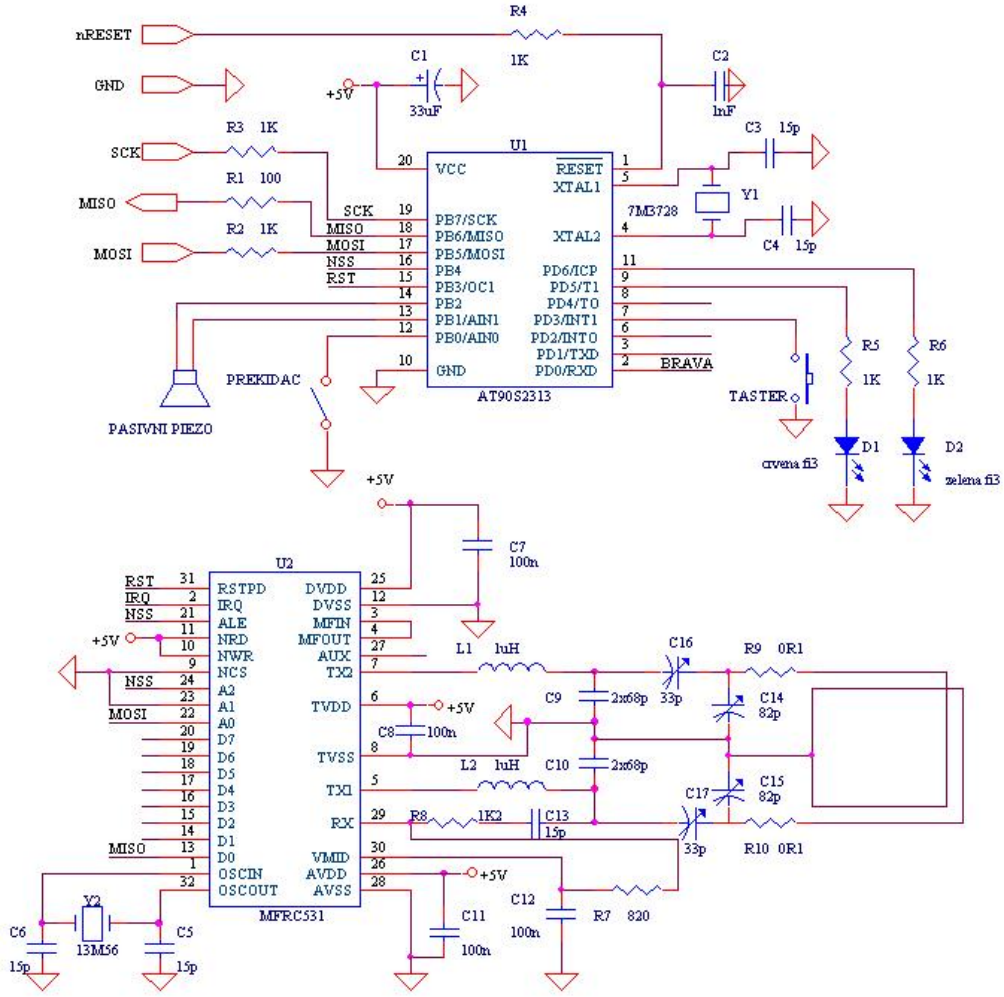
3.10.4 ČITAČ MIFARE® 1 S50 KARTICE

Na Slici 3.10.11 prikazana je električna šema jednog jednostavnog čitača Mifare® 1 S50 kartica.

Glavni djelovi čitača su mikrokontroler AT90S2313 i čip MFRC531.

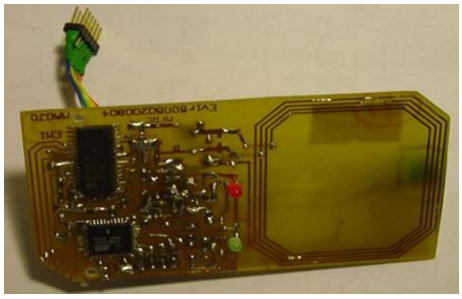
MFRC531 služi za beskontaktnu komunikaciju sa karticom. MFRC531 posjeduje kompletno integrisan modulator i demodulator za sve vrste pasivnih beskontaktnih komunikacionih metoda i protokola, na učestanosti 13.56MHz.

Na slici 3.10.13 dat je blok dijagram MFRC531 čipa. MFRC531 podržava sve nivoe ISO 14443 standarda, uključujući komunikacione šeme tipa A i tipa B [3]. Podržava beskontaktnu komunikaciju sa brzinama do 424kHz. Integrisani predajnik je u mogućnosti da, bez dodatnih aktivnih kola, pogoni antenu dizajniranu za blizinsko očitavanje do 100mm. Prijemnik obezbjeđuje robustno i efikasno demoduliranje i dekodiranje signala iz ISO 14443 kompatibilnih predajnika [60].

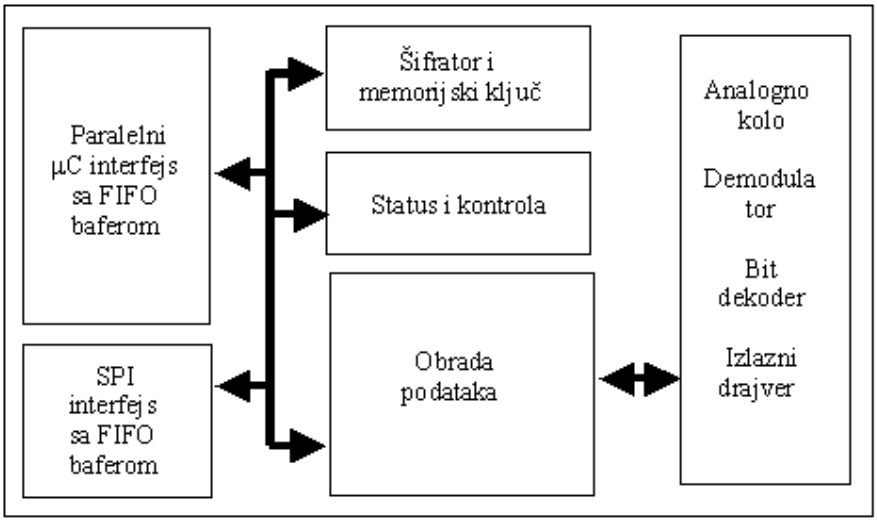


Slika 3.10.11 Električna šema čitača Mifare® 1 S50 kartica

Na slici 3.10.12 prikazan je izgled realizovanog čitača.



Slika 3.10.12 realizovani čitač Mifare® 1 S50 kartica



Slika 3.10.13 Blok dijagram MFRC531 čipa

Paralelni mikrokontrolerski interfejs automatski detektuje vrstu 8-bitnog paralelnog interfejsa koji je povezan na njega. Ovaj interfejs posjeduje komforni bidirekcioni FIFO bafer i podešljivi interapt izlaz.

MFRC531 posjeduje i SPI interfejs. Tokom SPI komunikacije MFRC531 radi kao ″slave″. SPI interfejs, takođe, uključuje bidirekcioni FIFO bafer.

Dio MFRC531 za obradu podataka vrši konverziju podataka iz paralelnih u serijske. Dio status i kontrola, pomaže da se MFRC531 prilagodi oktuženju i podesi da radi sa najboljim performansama [4].

Za komunikaciju sa Mifare Classic proizvodima, kao što je Mifare® 1 S50 kartica, koristi se brza kripto jedinica i sigurni, neuništivi, memorijski ključ.

Analogno kolo sadrži predajnik i prijemnik. Predajnik može da omogući očitavanja kartice koja je na rastojanju ne većem od 100mm. Prijemnik je sposoban da datektuje i dekodira čak veoma slabe odzive [59].

U mirkokotroleru se nalazi relativno jednostavan softver, čija ja glavna uloga da ostvari komunikaciju sa MFRC531 čipom, odgovarajuću signalizaciju i, po potrebi, komunikaciju čitača sa višom instancom (npr. PC-em).

3.11 PRIMJENE RFID TEHNOLOGIJE

Primjene RFID tehnologije su sve brojnije. Wal-Mart i ostali lideri u distribucionoj i maloprodajoj industriji SAD-a počeli su uvoditi RFID tehnologiju u njihov lanac snadbijevanja. Food and Drog administracija SAD-a dala je preporuku za masovnu upotrebu RFID tehnologije u farmaceutskoj industriji. Potencijalne koristi za ekonomiju i potrošače su ogromne. RFID tehnologija može dramatično smanjiti troškove u upravljenju lancima snadbijevanja, unaprijediti magacinsko poslovanje, automatizovati uvid u stanje zaliha, povećati tačnost i efikasnost popunjavanja zaliha robe, smanjiti krađu, poboljšati prevenciju od stavljanja u promet falsifikovanih proizvoda (ljekova na primjer), i još mnogo drugih prednosti.

Da bi se ilustrovale koristi koje RFID sistemi donose, posmatrajmo RFID sistem primijenjen u nekom magacinu, odnosno skladištu. Primjenom RFID sistema svaki artikl u magacinu dobija RF identifikator. RF identifikator sadrži identifikacione podatke kao što su kod proizvođača, kod za tip proizvoda, kao i jedinstveni serijski broj proizvoda. U magacinu, u kojem je apliciran RFID sistem, police, sredstva za pretovar robe i vrata opremljeni su RF čitačima. Zahvaljujući tome police ″znaju″ svoj sadržaj i mogu da prepoznaju kada je neki artikl dodat ili oduzet. Slično, sredstva za pretovar robe ″znaju″ što su prenijela a i vrata ″znaju″ koji artikli su unijeti ili iznijeti (Slike 3.11.1, 2, 3). Svaka od ovih akcija se bilježi u bazi podataka čime se dobija detaljan prikaz kompletne istorije svakog pojedinačnog artikla. Dodatni podaci kao što su informacije o proizvodu, računi i drugo takođe se mogu pratiti [62].

Slika 3.11.1 Sredstva za pretovar usklasištene robe opremljena RF čitačima

Slika 3.11.2 Vrata u biblioteci opremljena RF čitačima

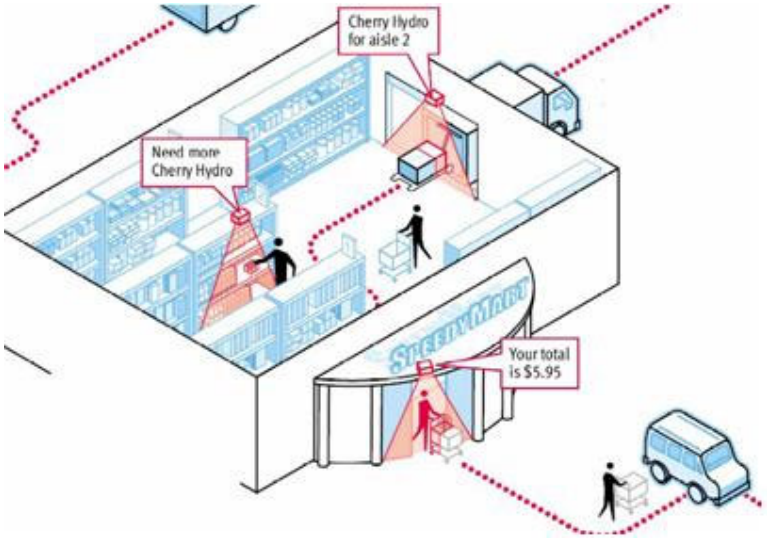
Slika 3.11.3 Pokretna traka opremljena RF čitačima

Na osnovu navedenog može se zaključiti da zahvaljujući mogućnostima RFID tehnologije stanje magacina, u kome je primijenjen RFID sistem, može biti ažurirano u realnom vremenu, t.j. u svakom trenutku, svaki artikl u magacinu može biti automatski lociran. Ovlašteno lice može pomjerati artikle po policama bez potrebe da bilježi gdje je nova pozicija artikla. Polica će to uraditi umjesto njega. Automatska analiza pomjeranja i razmještaja artikala pomože u optimizaciji organizacije magacina. Konačno, stalni nadzor inventara značajno redukuje kalo, što donosi značajne uštede proizvođačima [63].

RFID tehnologija omogućava najbolje premoštavanje jaza između digitalnog i realnog svijeta. U drugim identifikacionim sistemima nije moguće uspostaviti tako čvrstu vezu izmedju podataka o objektima i samih objekata. Unošenje u bazu podataka informacije o pristigloj robi i to da je određeni objekat smješten na određenoj lokaciji je, zapravo, ništa više od fotografije uzete u određenom trenutku. Ako se objekat pomjeri, informacije u bazi podataka više nijesu tačne. Neko je i dalje potreban da stvarno verifikuje prisutnost objekta. RFID tehnologija omogućava automatsku identifikaciju fizičkog objekta i omogućava da inventar jednom popisan bude dalje praćen automatski. Kontinulno ažuriranje baze podataka pruža bolji prikaz realnog svijeta. Drugim riječima, ″fotografija″ se zamijenjuje ″prenosom uživo″.

Zahvaljujući opisanim mogućnostima, RFID tehnologija nalazi i brojne

druge primjene. Veliki američki trgovinski lanac Wal Mart planira uvođenje tzv. ″brzih″ marketa. Radi se o prodavnicama u kojima nebi postojala kasa za naplatu. Umjesto da kupac kod kase čeka red za naplatu, on bi jednostavno izašao iz prodavnice. Pomoću RF čitača naplaćivanje bi se izršilo automatski, skidanjem odgovarajuće svote sa kreditnog RF identifikatora u džepu kupca (Slika 3.11.4). Nepostojanje potrebe za naplatnim kasama smanjuje prodajne troškove a samim tim utiče povoljno i na cijenu proizvoda. Osim automatizacije procesa naplate, ″brzi″ marketi donose brojne pogodnosti i u procesu snabdijevanja. Zahvaljujući postojanju RF čitača na svakoj polici, svakom ulazu u market, kao i u svakom transportnom sredstvu proces evidencije nabavke kao i kontrole snabdijevenosti je kompletno automatizovan. Štaviše, ″pametne″ police same dojavljuju da je određeni artikl gotovo rasprodat i da treba izvršiti dopunu. Više se vlasniku marketa ne može desiti da neblagovremeno sazna za nestašicu nekog od artikala.



Slika 3.11.4 Speedy Mart

Banke razmatraju ugrađivanje RF identifikatora u novčanice u cilju sprječavanja falsifikovanja. Jednostavno je provjeriti poklapa li se kod RF identifikatora sa oštampanim serijskim brojem na novčanici. Međutim, opasnost od narušavanja privatnosti čini neizvjesnom ovu primjenu RF identifikatora [57, 65].

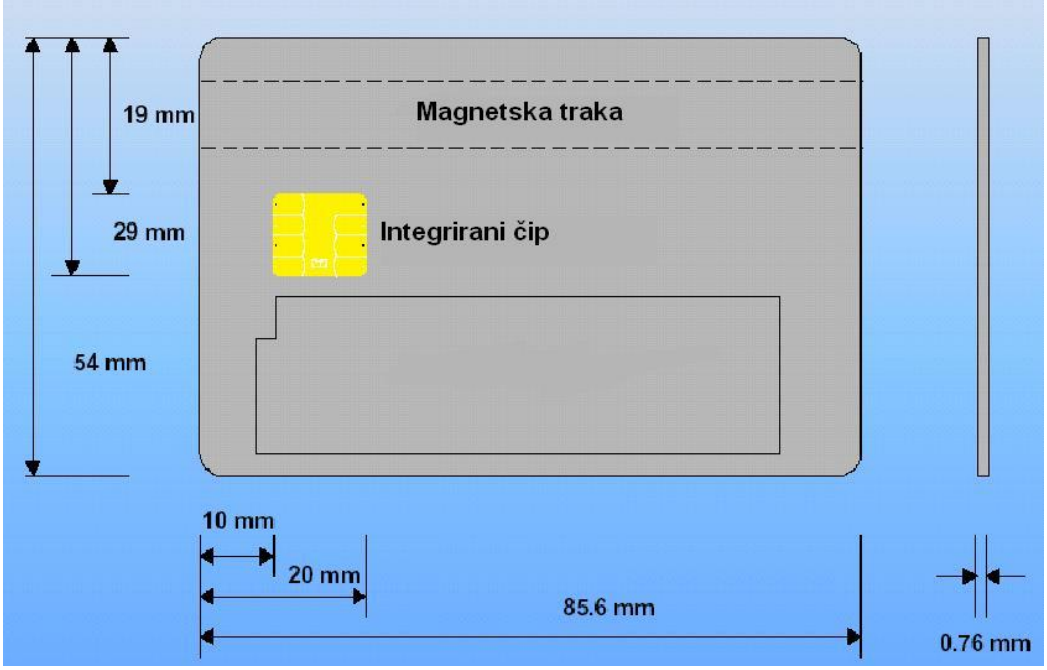
RFID sistemi se takođe koriste i za prećenje ljudi i životinja [64]. Koriste se u vojne svrhe. Na primjer prilikom spasavanja posade oborenih aviona i slično [66]. Upotrebljevaju se u sistemima kontrole pristupa, sistemima evidencije radnog vremena i mnogim drugim.

GLAVA IV

4. PAMETNE KARTICE

4.1 UVOD

Pametne kartice se definišu kao kartice standardne veličine koje imaju ugrađen čip i mogu obrađivati informacije (Slika 4.1.1) [67]. Time se podrazumijeva da katica može primati, memorisati, obrađivati i odašiljati podatke. Poseban naglasak stavlja se na sigurnost podataka i brzinu obrade kritpografskih funkcija.



Slika 4.1.1 Standardne dimenzije pametne kartice

Pametne kartice se još nazivaju i čip kartice ili ICC (Integrated Circuit Card).

"Pametne" kartice su prvi predložili njemečki naučnici Helmut Gröttrup i Jürgen Dethloff in 1968. Patent je prihvaćen 1982. Prva masovna upotreba pametnih kartica bila je 1983 godine u Francuskoj. Pametne kartice su upotrijebljene za bezgotovinsko plaćanje telefonckih razgovora.

1974. godine Roland Moreno predlaže svoj prvi koncept memorijske kartice. Prvu mikroprocesorsku pametnu karticu predlaže Michel Ugon iz Honezwell Bull-a, 1978 godine. Bull je patentirao SPOM (Self Programmable One-chip Microcomputer) koji definiše neophodnu

arhitekturu za auto-programiranje čipa. Tri godine kasnije, prvi "CP8" zasnovan na ovom patentu proizveden je od strane Motorole. Danas, Bull ima 1200 patenta vezanih za pametne kartice.

Druga velika primjena bila je 1992. godine, takođe u Francuskoj. Ovom primjenom je u sve debitne kartice u Francuskoj ugradjen je čip (Carte Bleue –Slika 4.1.2) [67].

Slika 4.1.2 Carte Bleue

Tokom 1990-ih širom Evrope pojavljuju se sistemi u kojima se ″pametne″ kartice koriste kao elektronski novac. U ovim sistemima podatak o količini novca čuva se na kartici a ne na nekom spoljašnjem računu.

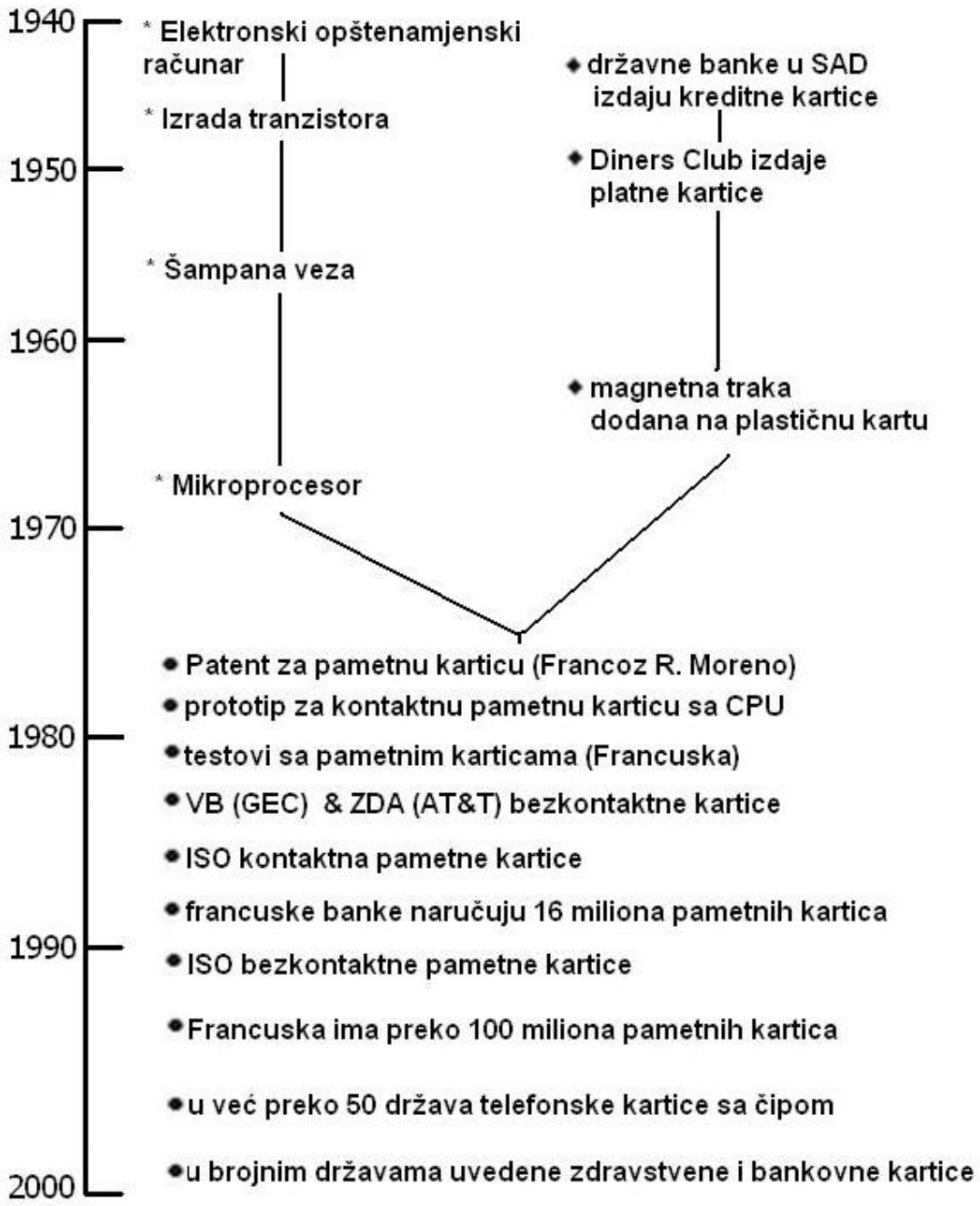
Glavnu primjenu ″pametne″ kartice dobijaju, tokom 1990-ih u mobilnoj telefoniji, kroz uvođenje SIM kartica.

1993. godine MasterCard i VISA prihvatili su uvođenje čipa u njihove kreditne i debitne kartice. Prva verzija EMV (Europay, MasterCard and VISA) sistema pojavlila se 1994. godine. Kanije su uslijedile novije savršenije verzije. Danas, EMV je standard za upotrebu IC kartice i IC kompatibilnih POS terminala [67].

Glavni interes banaka za uvođenje pametnih kartice je u smanjenju broja prevara, falsifikovanja i krađa. Količina novca koju banka, usljed toga, gubi na postojećim sistemima (npr. sistemi sa karticama sa megnetnim zapisom), je glavno mjerilo hoće li se upustiti u uvođenje novog sistema. Ukoliko su gubici znatno manji od novca koji treba uložiti za unapređenje, banke, često, zadržavaju postojeću tehnologiju. S druge strane, u današnjim uslovima ubrzanog razvoja pametnih kartica, neki korisnici se opredjeljuju sačekati sljedeću generaciju. Dobar primjer za to je USA payments industry koja se u većini opredijelila da sačeka sa primjenom postojećeg EMV, i

uvede EMV koji će biti zasnovan na tehnologiji beskontaktnih pametnih kartica [67].

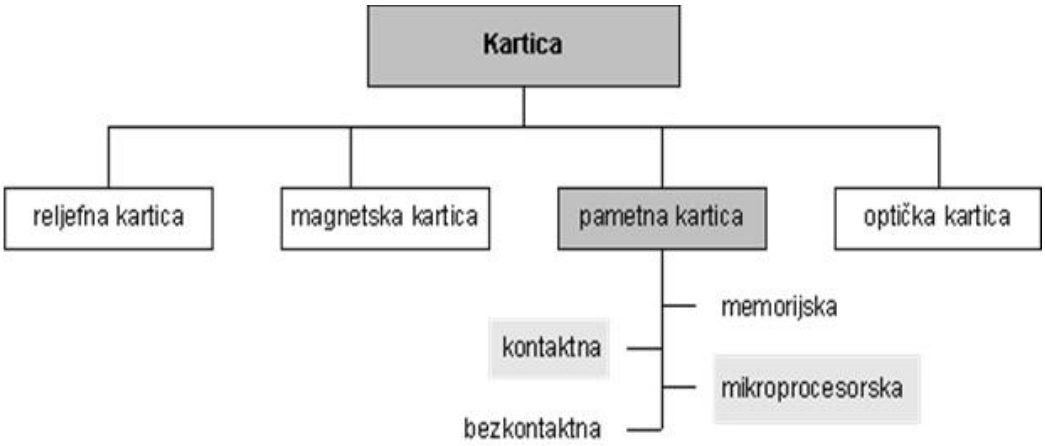
Na slici 4.1.3 dat je kratak preged istorijata razvoja pametnih kartica.



Slika 4.1.3 Istorijski pregled razvoja pametnih kartica

4.2 VRSTE PAMETNIH KARTICA

U dosadašnjem razvoju identifikacinih sistema pojavljivalo se više različitih tipova identifikacionih kartica (Slika 4.2.1) [68].



Slika 4.2.1 Postojeći tipovi identifikacionih kartica

U mnogim sistemima, u kojima se koriste identifikacione kartice, postoje dva nivoa provjere identiteta. Jedan nivo je - "ono što posjeduješ" a to je kartica, dok je drugi nivo - "ono što zanš", a to je, najčešće, PIN kod, odnosno lozinka.

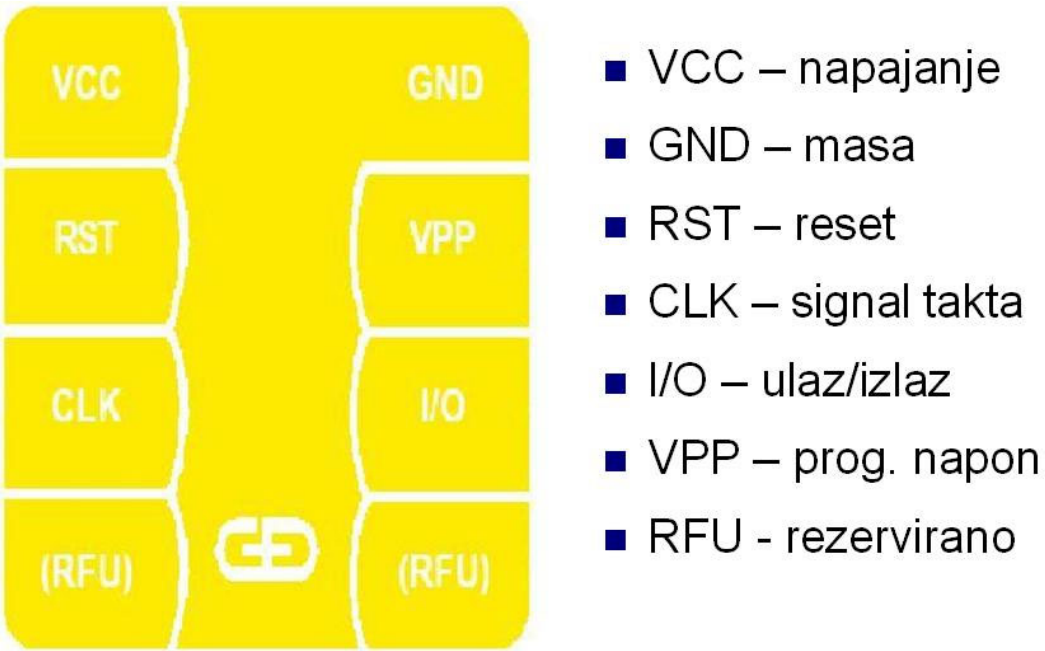
Od svih navedenih vrsta identifikacionih kartica, pametne kartice se izdvajaju, po sigurnosti podatka i fleksibilnosti primjene. Pametna kartice, jedine su u stanju primati, obrađivati i slati podatke. One omogućavaju i vrlo jednostava postupak izmjene i brisanja iz svoje memorije, postojećih podataka, daleko fleksibilnije nego bilo koje druge identifikacione kartice.

Sa stanovišta razmjene podataka sa okruženjem, pametne kartice se mogu podijeliti na:

- kontaktne,
- bezkontakne,
- hibridne i
- i kartice sa dvostrukim interfejsom (dual interfejs cards) (Slike 4.2.2).

Slike 4.2.2 Interfejsi za razmjenu podataka sa okruženjem kod pametnih kartica

Za razmjenu podataka sa okuženjem kontaktne pametne karice posjeduju izvedene kontakte na svojoj površini. Izgled i značenje pojadinog kontakta dati su na slici 4.2.3.



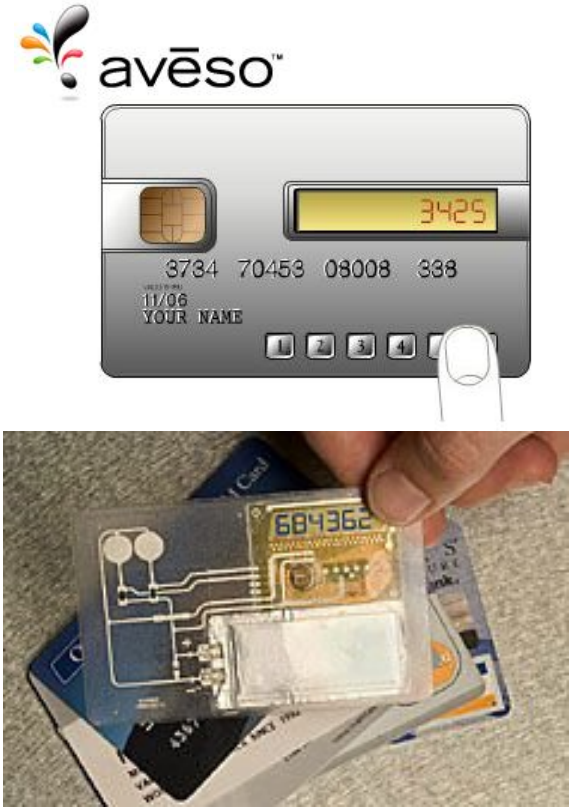
Slika 4.2.3 Izgled i značenje pojedinog kontaka

Bezkontaktna pametna kartice, za razmjenu podataka sa okuženjem koristi antenu ugrađenu u tijelo kartie (Slika 4.5).

Hibridna pametna kartica sadrži dva čipa. Razmjena podataka sa jednim čipom vrđi se preko izvedenih kontakata a sa srugim pomoću antene (Slika 4.5).

Kartice sa dvojnim interfejsom posjeduju jedan čip kome se može pristupiti i kontaktno i bezkontaktno (Slika 4.5).

Posebnu vrstu pametnih kartica predstavljaju kartica sa ugrađenim displejem i tasterima (Slika 4.2.4) [69].



Slika 4.2.4 Pametna kartica sa displejem i tastaturom.

Na Slici 4.7 prikazana je jedna ovakva kartica, proizvod firme Aveso Inc. U odnosu na uobičajene, krtica sa displejem i tasterima pruža viši nivo sigurnosti identifikacije. To se ogleda u mogućnosti primjene OTP (One Time Password) koncepta, odnosno dinamičkog PIN koda. Drugim riječima, za svaki pristup sistemu upotrebljava se drugačiji PIN kod. Statički PIN kod se unosi tasterima na samoj kartici a na displeju se dobija dinamički PIN kod za pristup sistemu. Osim toga, postojanje LCD dipleja omogućava jednostavnu provjeru stanja računa korisnika.

Prema vrsti ugrađenog čipa pametne kartice se mogu svrstati u dvije osnovne kategorije i to:

- Memorijske kartice i
- Mikroprocesorske kartice

Memorijske kartice sadrže samo postojanu memoriju (EEPROM) i moguće neku specifičnu sigurnosnu logiku. To je, najčešće, logika za kriptovanje i dekriptovanje komunikacionih podataka. Ne sadrži mikroprocesor i ne može se re-programirati nakon proizvodnje. Omogućava direktan pristup memoriji i podržava nekoliko naredbi koje se ne mogu mijenjati.

Na osnovu vrste ugrađene memorije razlikuju se sljedeći tipovi memorijskih kartica:

- Kartice sa običnom memorijom,
- Kartice sa zaštićenom memorijom
- Kartice sa brojačem

Kartice sa običnom memorijom namijenjene su uglavnom pohranjivanju podataka. Imaju najnižu cenu po bitu pohranjene informacije. Pojavljuju se kao kartice sa čipom i EEPROM memorijom ili kartice sa fleš memorijom.

Kartice sa zaštićenom memorijom imaju ugrađene jednostavnu logiku za kontrolu pristupa podacima. Često se rade sa dijeljenom memorijom u cilju obezbjeđivanja multiaplikativnosti. Pristup pojedinom dijelu memorije kontroliše sigurnosna logika i odgovarajući ključ. Za svaki pojedini dio može se zadati zaseban ključ i specifični uslovi pristupa. U jednoj primjeni kartice, koristi sa samo jedan dio memorije, sa ključem i uslovima pristupa specificiranim za taj dio. Drugi djelovi memorije nijesu dostupni toj aplikaciji. Kao primjer kartice sa dijeljenom memorijom može poslužiti Mifare MF1ICS50 kartica opisana u poglavlju 3.11 i prikazana na Slici 4.2.5.

Slika 4.2.5 Mifare MF1ICS50 kartica, primjer kartice sa dijeljenom memorijom.

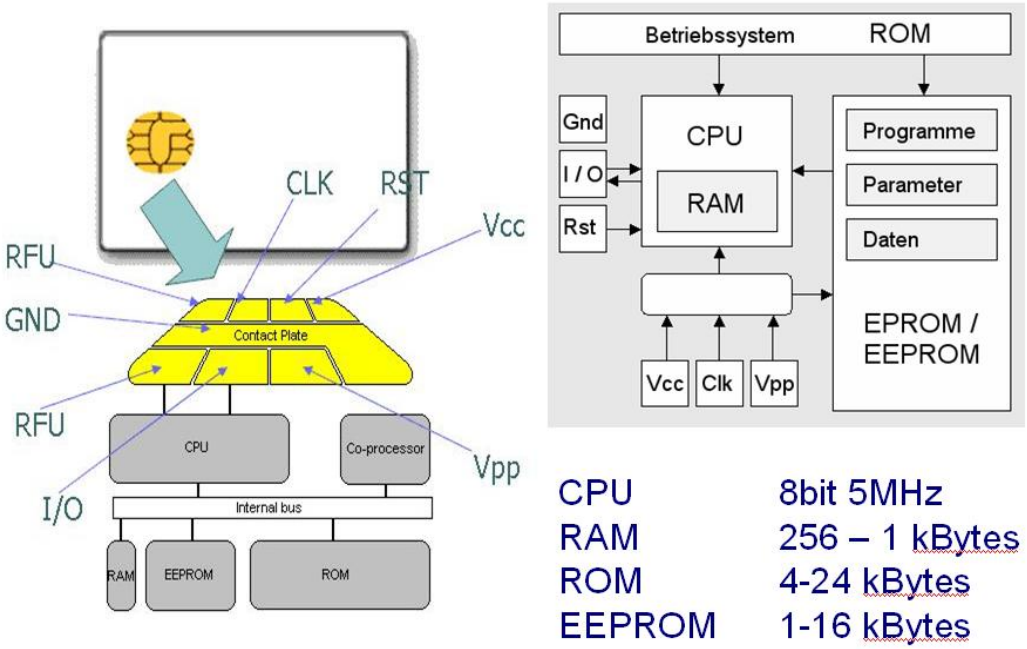
Kartice sa brojačem namenjene su držanju vrijednosti. Mogu biti za jednokratnu ili višekratnu upotrebu. Tipičan primer kartice sa brojačem je telefonska kartica (Slika 4.2.6).

Slike 4.2.6 Telefonska kartica, primjer kartice sa brojačem

Brojač, kartice sa brojačem, najčešće broji samo u jednom smjeru. Usljed toga karitica postaje neupotrebljiva nakon što se se odbroji predefinisana vrijednost. Na primjer, telefonska kartica postaje neupotrebljiva nakon što se potroši predefinisani kredit.

Kao što i sam naziv govori, mikroprocesorske kartice sadrže mikroprocesor. Postojanje mikroprocesora omogućuje zanatno bolju zaštitu podataka na kartici. Omogućena je ugradnja kriptografskih algoritama i primjena širokog skupa zaštitnih mehanizama. Mikroprocesorske kartice su u mogućnosti pamtiti, obrađivati podatke i donositi odluke u određenim granicama. Često se naziv pametna kartica vezuje samo za mikroprocesorske kartice.

Na slici 4.2.7 prikazani su sastavni djelovi jedne tipične pametne kartice.



Slika 4.2.7 Osnovni sastavni djelovi tipične mikroprocesorske kartice.

Kao što se sa slike uočava mikroprocesorska kartica predstavlja PC u malom. Sadrži:

- procesor (CPU) pomoću kog se vrši izračunavanje,
- ROM (Read-Only Memory), memorija na kojoj se nalazi operativni sistem i aplikativni program,
- RAM (Random Access Memory) memorija koja se koristi za privremeno skladištenje podataka tokom rada procesora,
- EEPROM (Electronically Erasable and Programmable Read-Only Memory), memorija u kojoj su smješteni podaci od interesa (broj tekućeg računa, sertifikati, ključevi i sl.),
- Takt i ulazno izlazni sklop preko koga se komunicira sa okolinom (čitačem).

Tipična smart kartica ima 8-bitni procesor koji radi na 5MHz, 256 do 1024 KB RAM-a, 6 do 24 KB ROM-a, 1 do 16 KB EEPROM-a.

Mikroprocesorska kartica posjeduje vlastiti operacioni sistem. Najčešće je to: Java Card, MultOS, OSCCA ili Smartcard.NET [70]. Omogućavaju pisanje vlastitih aplikacija koje se izvršavaju u sigurnom okruženju.

Specijalno su konstruisane za ispunjavanje visokih sigurnosnih standarda. Visok stepen sigurnosti postiže se ugrađivanjem procesora koji obavlja enkripciju/dekripciju podataka. Povjerljivi podaci nikada ne napuštaju karticu.

4.3 KRIPTOVANJE PODATAKA

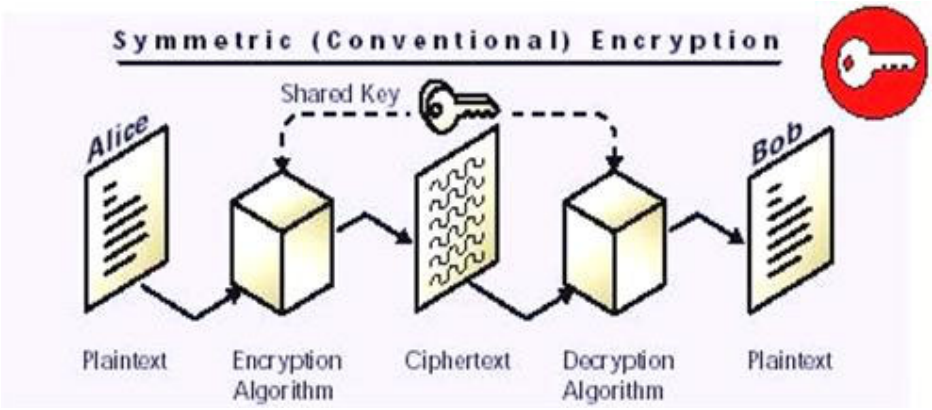
U cilju zaštite podataka, u komunikaciji sa pametnim karticama koriste se sljedeći algoritmi kriptovanja:

- Simetrični algoritmi kriptovanja,
- Asimetrični algoritmi kriptovanja i digitalni potpis [71, 79].

4.3.1 SIMETRIČNA KRIPTOGRAFIJA

Simetrični algoritmi kriptovanja za kriptovanje i za dekriptovanje upotrebljavaju jednostavno povezane, često identične, kriptografske ključeve. Ključevi su ili identični ili se jednostavnom transformacijom iz jednog izvodi drugi ključ. U ovom načinu šifrovanja ključevi predstavljaju dijeljenu tajnu između dvije ili više strana (Slika 4.3.1) [72].

Drugi nazivi za simetrično šifrovanje su sifrovanje sa tajnim-ključem (secret-key), jedinim-ključem (single-key), dijeljenim-ključem (shared-key), jednim-ključem (one-key) ili, eventualno, privatnim-ključem (private-key). Zadnji naziv ne preba miješati sa terminom privatni-ključ u asimetričnim algoritmima šifrovanja.



Slika 4.3.1 Simetrično šifrovanje

Algoritmi simetričnog šifrovanja se mogu podijeliti u dvije grupe i to:

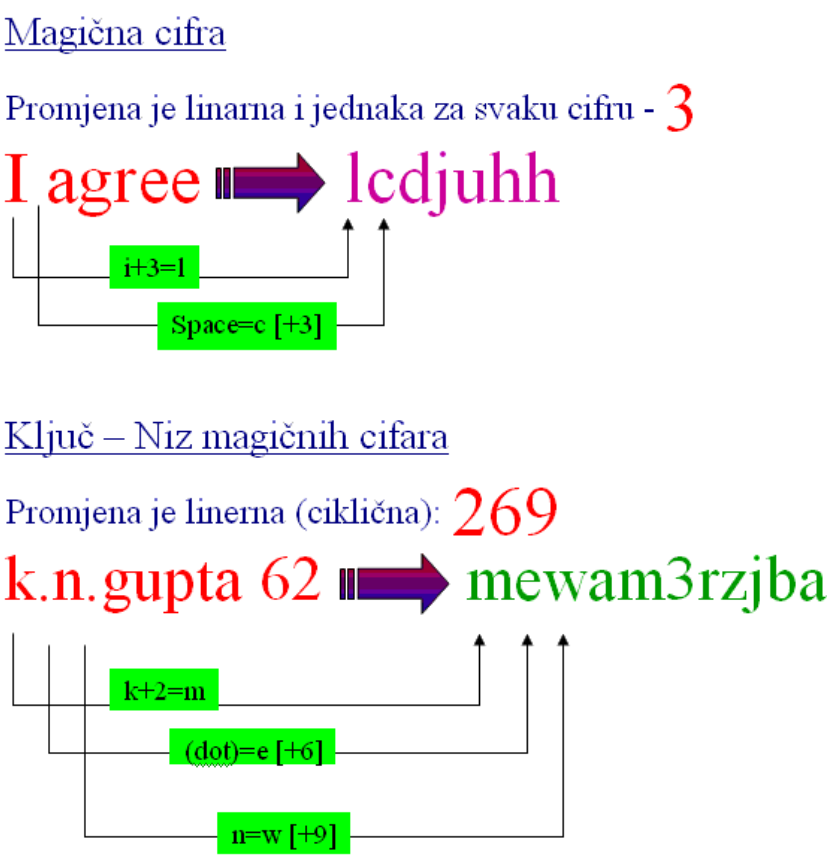
- *stream ciphers* i
- *block ciphers* algoritmi.

Stream ciphers algoritmi kodiraju bit po bit poruke, dok *block ciphers* algoritmi uzimaju blok bitova poruke i šifruju ga kao jednu cjelinu.

Block ciphers algoritmi najčešće uzimaju po 64 bitova. *Advanced Encryption Standard* algoritam, prihvaćen od *NIST*-a (National Institute of Standards and Technology) u Decembru 2001 godine ima 128 bitova u jednom bloku.

Neki od popularnih simetričnih algoritama šifrovanja su: *Twofish*, *Serpent*, *AES* (ili Rijndael), *Blowfish*, *CAST5*, *RC4*, *TDES*, and *IDEA* [72].

Kao primjer simetričnog šifrovanja na Slici 4.3.2 prikazani je najprostiji algoritmi poznati kao Magična cifra ili Niz magičnih cifara.



Slika 4.3.2 Simetrično ktiptovanje primjenom prostih algoritama poznatih kao Magična cifra i Niz magičnih cifara

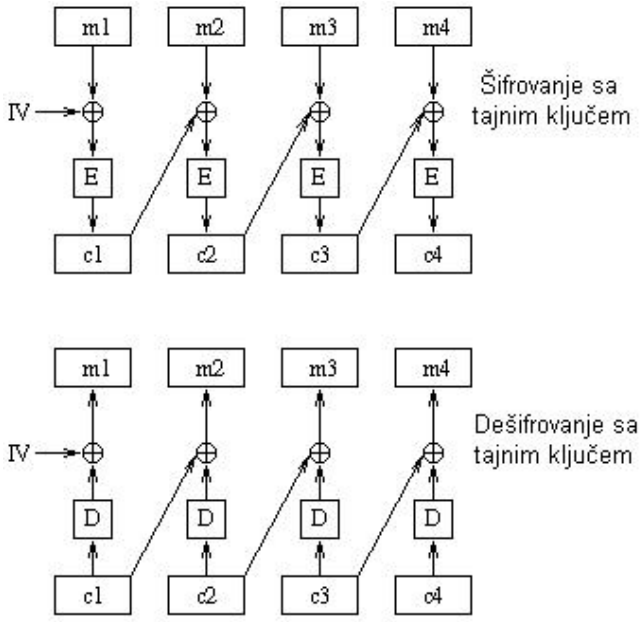
Kao što se sa Slike 4.3.2 vidi u algoritmu Magična cifra, kriptovana poruka se dobija tako što se na ASCII vrijednost svakog karaktera iz originalne poruke doda određena konstantna vrijednost tzv. magična cifra. Pri tome se vodi računa o graničnim uslovima, odnosno obezbjeđuje se da nakon dodavanja magične cifre novodobijeni ASCII kod bude iz domena slova, cifara ili znakova interpunkcije. Na Slici 4.3.3 prikazana je tabela kodiranja, prema kojoj je izvršeno kriptovanje poruka sa Slike 4.3.2.

Char	1	2	3	4	5	6	7	8	9
a	b	c	d	e	f	g	h	i	j
b	c	d	e	f	g	h	i	j	k
c	d	e	f	g	h	i	j	k	l
d	e	f	g	h	i	j	k	l	m
e	f	g	h	i	j	k	l	m	n
f	g	h	i	j	k	l	m	n	o
g	h	i	j	k	l	m	n	o	p
h	i	j	k	l	m	n	o	p	q
i	j	k	l	m	n	o	p	q	r
j	k	l	m	n	o	p	q	r	s
k	l	m	n	o	p	q	r	s	t
l	m	n	o	p	q	r	s	t	u
m	n	o	p	q	r	s	t	u	v
n	o	p	q	r	s	t	u	v	w
o	p	q	r	s	t	u	v	w	x
p	q	r	s	t	u	v	w	x	y
q	r	s	t	u	v	w	x	y	z
r	s	t	u	v	w	x	y	z	0
s	t	u	v	w	x	y	z	0	1
t	u	v	w	x	y	z	0	1	2
u	v	w	x	y	z	0	1	2	3
v	w	x	y	z	0	1	2	3	4
w	x	y	z	0	1	2	3	4	5
x	y	z	0	1	2	3	4	5	6
y	z	0	1	2	3	4	5	6	7
z	0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	.
2	3	4	5	6	7	8	9	.	
3	4	5	6	7	8	9	.		a
4	5	6	7	8	9	.		a	b
5	6	7	8	9	.		a	b	c
6	7	8	9	.		a	b	c	d
7	8	9	.		a	b	c	d	e
8	9	.		a	b	c	d	e	f
9	.		a	b	c	d	e	f	g
. (Dot)		a	b	c	d	e	f	g	h
Space	a	b	c	d	e	f	g	h	i

Slika 4.3.3 Tabela kodiranja

Algoritam - Niz magičnih cifara, slično algoritmu - Magična cifra, dodaje konstantnu vrijednost na karaktere originalne poruke, s tim što na svaki n-ti karakter dodaje istu vrijednost, pri čemi je n broj magičnih cifara u nizu.

Ako se *Stream ciphers* i *Block Ciphers* algoritmima, u njihovoj osnovnoj formi, šifriraju isti blokovi podataka, dobijaju se identični šifrirani blokovi. Kako mnoge poruke, koje treba prenijeti, sadrže deterministička zaglavlja, ovakva osobina *Stream ciphers* i *Block Ciphers* algoritama izlaže ih opasnosti "razbijanja". Drugim riječima, raste mogućnost da neovlašćena strana iz šifrovanih determinističkih podataka "izvuče" tajni ključ i dalje, neovlašteno prima podatke. Da bi se tako nešto spriječilo uveden je lančani mod kriptovanja (Chiper Block Chaining - CBC). U ovom načinu kriptovanja prethodni blok podataka utiče na kriptovanje tekućeg bloka podataka. Da bi se obezbijedilo da ni prvi blok podataka ne bude šifrovan samo na osnovu podataka sadržanih u njemu, uveden je tzv. inicijalni vektor (IV). Na šifrirani sadržaj prvog bloka, osim sadržaja bloka utiče i IV (Slika 4.3.4).



Slika 4.3.4 Blok dijagram šifrovanja primjenom Chiper Block Chaining – CBC algoritma

U slučaju CBC algoritama dijeljenu tajnu sačinjavaju tajni ključ i inicijalni vektor.

4.3.1.1 DES algoritam simetričnog šifrovanja

Krajem 60-tih i početkom 70-tih godina 20. vijeka, razvojem finansijskih transakcija, kriptografija postaje zanimljiva sve većem broju potencijalnih korisnika. Dotad je glavna primjena kriptografije bila u vojne i diplomatske svrhe, pa je bilo normalno da svaka država (ili čak svaka zainteresovana državna organizacija) koristi svoju šifru za koju je vjerovala da je najbolja. Međutim, tada se pojavila potreba za šifrom koju će moći koristiti korisnici širom svijeta, i u koju će svi oni moći imati povjerenje - dakle, pojavila se potreba uvođenja *standarda* u kriptografiji.

Godine 1972. američki National Bureau of Standards -NBS (sada se ova agencija zove National Institute of Standards and Technolog (NIST)) inicirao je program za zaštitu računarskih i komunikacijskih podataka. Jedan od ciljeva je bio razvijanje jednog standardnog kriptosistema. 1973. godine NSB je raspisao javni konkurs za takav kriptosistem [73]. Taj kriptosistem je trebao zadovoljiti sljedeće uslove:

- visoki stepen sigurnosti
- potpuna specifikacija i lako razumijevanje algoritma
- da sigurnost leži u ključu, a ne u tajnosti algoritma

- dostupnost svim korisnicima
- prilagodljivost upotrebi u različitim primjenama
- ekonomičnost implementacije u elektoničkim uređajima
- efikasnost
- mogućnost provjere
- mogućnost izvoza (zbog američkih zakona)

Na tom konkursu nijedan predlog nije zadovoljavao sve ove zahtjeve. Međutim, na ponovljenom konkursu iduće godine pristigao je predlog algoritma koji je razvio IBM-ov tim kriptografa. Algoritam je zasnovan na tzv. *Feistelovoj šifri*. Gotovo svi simetrični blokovni algoritmi koji su danas u upotrebi koriste ideju koju je uveo *Horst Feistel* 1973. godine [74]. Jedna od glavnih ideja je alternativna upotreba supstitucija i transpozicija kroz više iteracija (tzv. rundi).

Predloženi algoritam prihvaćen je kao standard 1976. godine i dobio je ime *Data Encryption Standard* (DES). U ovoj odluci učestvovala je i američka organizacija National Security Agency , NSA, koja se bavi dizajniranjem i analizom raznih vrsta šifarskih sistema.

OPIS DES ALGORITMA

Osnovni element zaštite je šifarski sitem. Svaki šifraski sistem obuhvata par transformacija podataka :

• Šifrovanje
• Dešifrovanje

Šifrovanje je procedura koja transformiše originalnu informaciju (otvoren tekst) u šifrovane podatke (šifrat). *Dešifrovanje* rekonstruiše otvoreni tekst na osnovu šifrata. U šifarskoj transformaciji, pored otvorenog teksta, takodje se koristi jedna nezavisna vrijednost, tzv. *ključ šifrovanja.* Transformacija dešifrovanja koristi *ključ dešifrovanaja.* Broj simbola koji predstavljaju ključ zavisi od šifarskog sitema.

U svom osnovnom obliku **DES** algoritam šifruje otvoreni tekst dužine 64 bita, koristeći ključ K dužine 56 bitova. 56 je efektivni broj bitova ključa, a on se zapravo sadrži 64 bita, pri čemu svaki osmi bit služi za provjeru parnosti. Šifrovanjem se dobijaju blokovi podataka koji ponovo imaju 64 bita.

Algoritam se sastoji iz 3 etape:

1. U prvoj etapi se od datog otvorenog teksta x, permutacijom pomoću fiksne **inicijalne permutacije IP** (Tabela 4.3.1) dobije tekst x_0. Ovo se obično zapisuje kao $x_0 = \mathrm{IP}(x)$, pri čemu je $x_0 = L_0R_0$, gdje L_0 predstavlja prva (lijeva) 32 bita, a R_0 zadnja (desna) 32 bita od x_0.

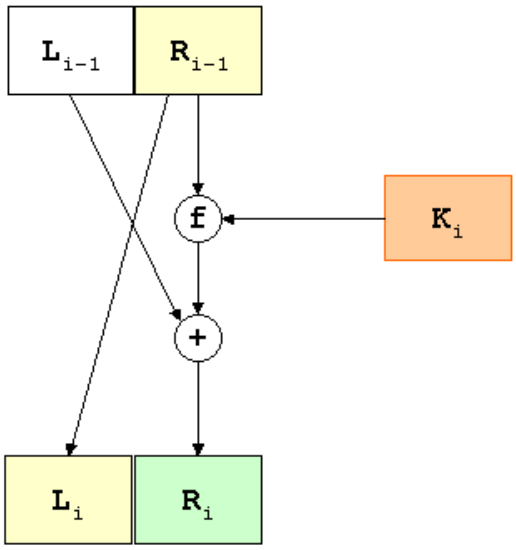
IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Tabela 4.3.1 Matrica fiksne inicijalne permutacije

2. U drugoj etapi Feistel-ova funkcija f se iterira 16 puta. L_i R_i, $1 \leq i \leq 16$, izračunavaju se po sljedećem pravilu:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i),$$

gdje $\oplus$ označava operaciju "ekskluzivno ili" - XOR (Slika 4.3.5). Feistel-*ova* funkcija f će biti opisana kasnije. $K_1, K_2, \ldots, K_{16}$ su nizovi bitova dužine 48, koji se dobijaju kao permutacije bitova ključa K.



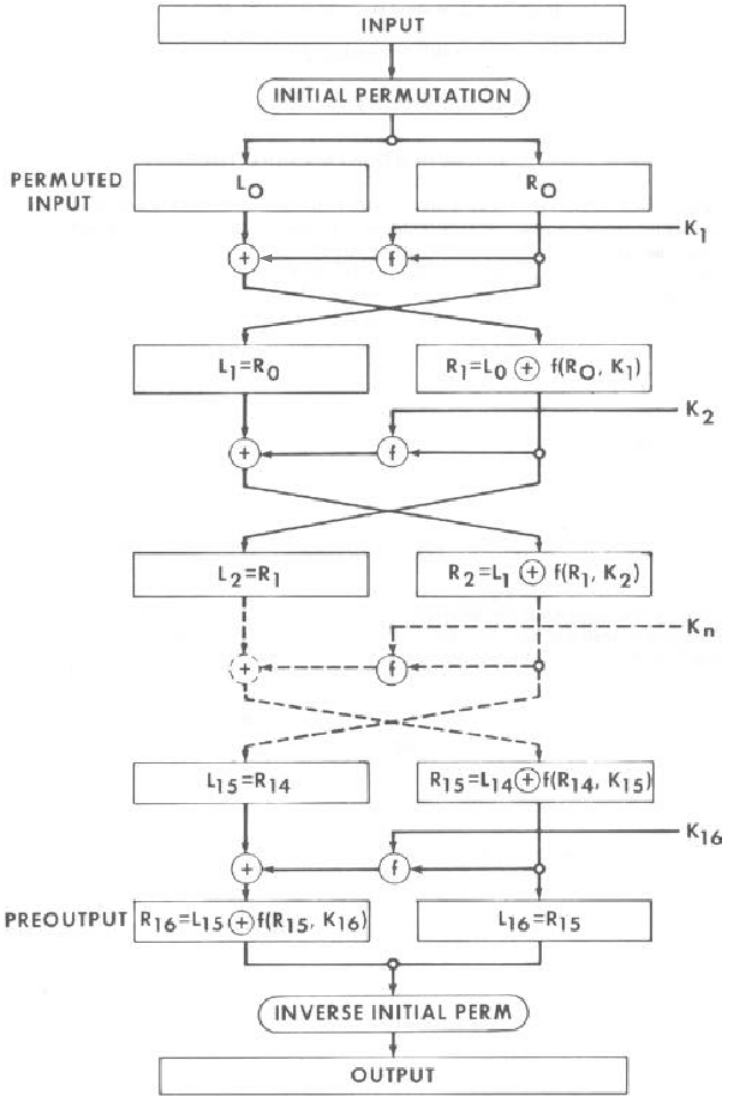
Slika 4.3.5 Blok dijagram izračunavanja nad L_i i R_i bitovima

3. U trećoj fazi primjenjuje se **IP^{-1}** (Tabela 4.3.2) na $R_{16}L_{16}$ i tako dobijamo šifrat y. Dakle, $y = \text{IP}^{-1}(R_{16}L_{16})$. Uočimo inverzni poredak od L_{16} i R_{16}.

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

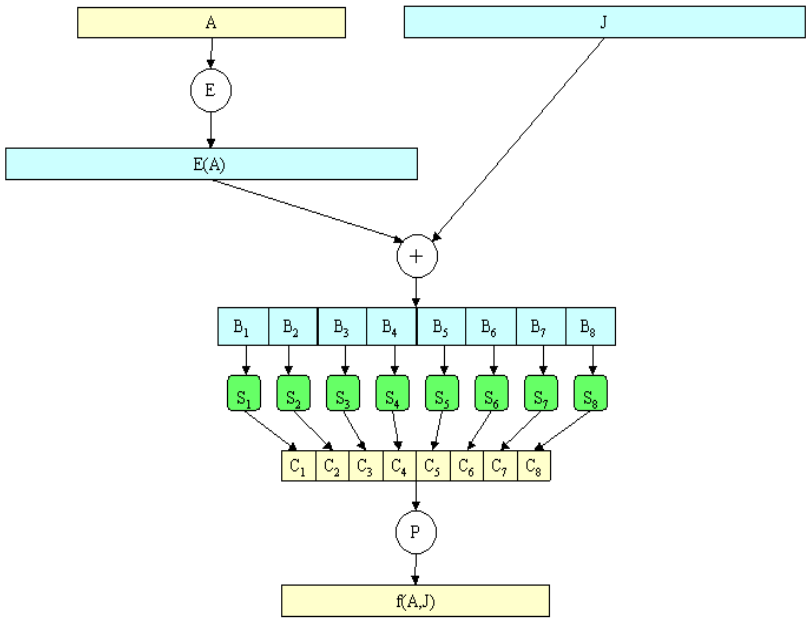
Tabela 4.3.2 Matrica prmutacije inverzne inicijalnoj

Na Slici 4.3.6 prikazan je dijagram toka sifrovanja DES algoritmom.



Slika 4.3.6 Dijagram toka šifrovanja DES algoritmom

Slika 4.3.7 daje šematski prikaz Feistel-ove funkcije DES algoritma.



Slika 4.3.7 Šematski prikaz *Feistel-ove funkcije DES algoritma*

Funkcija *f* za prvi argument ima niz bitova *A* dužine 32 (R_{i-1}), a za drugi argument ima niz bitova *J* dužine 48 (K_i). Kao rezultat se dobija niz bitova dužine 32.

Funkcija se računa u sljedeća 4 koraka:

1. U prvom koraku argument *A* se "proširi" do niza dužine 48 u skladu s fiksnom **funkcijom proširenja E** (Tabela 4.3.3). Niz E(*A*) se sastoji od 32 bita iz *A*, permutiranih na određeni način, s time da se 16 bitova pojavi dva puta.

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tabela 4.3.3 Matrica funkcije proširenja E.

2. U drugom koraku izračunva se E(A)$\oplus J$ i rezultat se zapisuje kao spoj od osam 6-bitnih nizova

$$B = B_1B_2B_3B_4B_5B_6B_7B_8.$$

3. Sljedeći korak koristi 8 supstitucionih matrica S_1, ... , S_8, tzv **S-kutija** (Slika 4.3.8). Svaka S_i matrica je fiksna 4 × 16 matrica čiji su elementi cijeli brojevi između 0 i 15. Za dati niz bitova dužine 6, recimo $B_j = b_1b_2b_3b_4b_5b_6$, računamo $S_j(B_j)$ na sljedeći način. Bitovi b_1b_6 određuju binarni zapis reda r od S_j(r= 0,1,2,3), a četiri bita $b_2b_3b_4b_5$ određuju binarni zapis kolone c od S_j (c=0,1,2,...,15). Sada je S_j (B_j) po definiciji jednako $S_j(r,c)$, zapisano kao binarni broj dužine 4. Na ovaj način izračunamo $C_j = S_j(B_j)$, j = 1,2,...,8.

i	S_i															
1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Slika 4.3.8 S kutije

4. Niz bitova $C_1C_2C_3C_4C_5C_6C_7C_8$ dužine 32 se permutira pomoću **fiksne završne permutacije P** (Tabela 4.3.4). Tako se dobije P(C), što je po definiciji upravo $f(A,J)$ [73].

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Tabela 4.3.4 Matrica završne permutacije P

Na kraju slijedi opis računanje ključeva K_1, K_2, ... , K_{16} iz ključa K. Ključ K se sastoji od 64 bita, od kojih 56 predstavlja ključ, a preostalih 8 bitova služe za testiranje parnosti. Bitovi na pozicijama 8, 16, ... , 64 su definisani tako da svaki bajt (8 bitova) sadrži neparan broj jedinica. Ovi bitovi se ignorišu kod računanja tablice ključeva. Postupk izračunavanja Ki može se podijeliti u dvije etape.

1. U prvoj etapi za dati 64-bitni ključ K, ignorišu se bitove parnosti, i vrši permutacija za preostale bitove pomoću **fiksne permutacije PC1** (Tabela 4.3.5). Ovo se obično zapisuje kao PC1(K)=C_0D_0, gdje C_0 sadrži prvih 28, a D_0 zadnjih 28 bitova od PC1(K).

PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Tabela 4.3.5 Matrica permutacije PC1

2. U drugoj fazi, za i = 1, 2, ... , 16 računamo:

$$C_i = \mathrm{LS}_i\,(C_{i-1}),$$
$$D_i = \mathrm{LS}_i\,(D_{i-1}),$$
$$K_i = \mathrm{PC2}(C_i\,D_i).$$

   LS_i predstavlja ciklični pomjeraj ulijevo za 1 ili 2 pozicije, u zavisnosti od i. Ako je i = 1, 2, 9 ili 16, onda je pomjeraj za jednu

poziciju, a inače je pomjeraj za dvije pozicije. **PC2** (Tabela 4.3.6) je još jedna fiksna permutacija.

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Tabela 4.3.6 Matrica permutacije PC2

Ovim je u potpunosti opisan postupak šifrovanja.

Za dešifrovanje se koristi isti algoritam. Krenće se od šifrata y, ali se koristi tablica ključeva u obrnutom redosljedu: K_{16}, K_{15}, ... , K_1. Kao rezultat dobijamo otvoreni tekst x.

Uvjerimo se da ovako definisana funkcija dešifrovanja d_K zaista ima traženo svojstvo da je $d_K(y) = x$. Treba se podsjetiti da se y dobila kao $y = \mathrm{IP}^{-1}(R_{16}L_{16})$. Stoga se primjenom inicijalne permutacije na y dobije $y_0 = R_{16}L_{16}$. Nakon prve runde dešifrovanja, lijeva polovina postaje $L_{16} = R_{15}$, a desna $R_{16} \oplus f(L_{16},K_{16})$. Ali, iz zadnje runde šifrovanja se uočava da je

$$R_{16} = L_{15} \oplus f(R_{15},K_{16}) = L_{15} \oplus f(L_{16},K_{16}).$$

Zato je $R_{16} \oplus f(L_{16},K_{16}) = L_{15}$. Znači, nakon jedne runde dešifrovanja dobijamo $R_{15}L_{15}$. Nastavljajući taj postupak, nakon svake sljedeće rudne dešifrovanja dobija se redom: $R_{14}L_{14}$, $R_{13}L_{13}$ ..., R_1L_1 i nakon zadnje runde R_0L_0. Preostaje nam da zamijenimo redosljed lijeve i desne polovine i da primijenimo IP^{-1}. Dakle, na kraju postupka dešifrovanja dobija se $\mathrm{IP}^{-1}(L_0R_0)$, a to je upravo otvoreni tekst x, što je i trebalo dokazati.

Sada se vidi da je razlog za zamjenu lijeve i desne polovine teksta x prije primjene permutacije IP^{-1} leži upravo u želji da se za dešifrovanje može koristiti isti algoritam kao za šifrovanje.

SVOJSTVA DES-A

Iz predhodne analize DES algoritma može se uočiti da su sve primijenjene operacije linearne ($\oplus$ je zapravo sabiranje u $\mathbf{Z}_2$), s izuzetkom S-kutija. S-kutije su veoma važne za sigurnost DES-a. Od objave algoritma, pa sve do danas, S-kutije su obavijene tajnošću. Kod nasljednika

DES algoritma S-kutije su generisane eksplicitno navedenim algoritmom. Kod DES algoritma poznati su tek neki kriterijumi korišćeni u dizajniranju S-kutija:

1. Svaki red u svakoj S-kutiji je permutacija brojeva od 0 do 15.
2. Nijedna S-kutija nije linearna funkcija ulaznih podataka.
3. Promjena jednog bita u ulaznom podatku kod primjene S-kutije ima za posljedicu promjenu barem 2 bita u izlaznom podatku.
4. Za svaku S-kutiju i svaki ulazni podatak x (niz bitova dužine 6), S(x) i S(x ⊕001100) razlikuju se za barem 2 bita.

Kriterijumi za dizajniranje permutacije P bili su sljedeći:

1. Četiri izlazna bita iz svake S-kutije utiču (čine ulazne podatke) na šest različitih S-kutija u idućoj rundi, a nijedan par bitova ne utiču na istu S-kutiju.
2. Četiri izlazna bita iz svake S-kutije u i-toj rundi su distribuirani tako da dva od njih utiču na središnje bitove u (i+1)-voj rundi, a dva na krajnje bitove.
3. Za dvije S-kutije S_j i S_k vrijedi da ako neki izlazni bit od S_j utiče na neki središnji bit od S_k u idućoj rundi, onda nijedan izlazni bit od S_k ne utiče na središnje bitove od S_j. Za $j = k$ ovo povlači da izlazni bitovi od S_j ne utiču na središnje bitove od S_j.

Ovi kriterijumi imaju zadatak da povećaju tzv. *difuziju* kriptosistema, tj. postići da na svaki bit šifrata utiče što više bitova otvorenog teksta. Oni, također, otežavaju i tzv. diferencijalnu kriptoanalizu o kojoj će biti više riječi nešto kasnije.

Poželjno svojstvo svakog kriptosistema jeste da mala promjena bilo otvorenog teksta bilo ključa dovodi do značajne promjene u šifratu. Posebno, promjena jednog bita otvorenog teksta ili jednog bita ključa trebala bi uticati na mnogo bitova šifrata. Ako je promjena mala, to može značajno smanjiti broj otvorenih tekstova ili ključeva koje treba ispitati.

Kriptosistem DES ima gore opisano svojstvo koje se ponekad naziva i "*efekat lavine*". Ilustrovaćemo to s dva primjera [75]:

Primjer 1: Otvoreni tekstovi (zapisani heksadecimalno)

0000000000000000 i 1000000000000000

šifrovani su pomoću ključa (također zapisanog heksadecimalno s uključenim bitovima parnosti)

029749C438313864.

Broj bitova u kojima se razlikuju odgovarajući šifrati nakon svake pojedine runde DES-a prikazan je u sljedećoj tablici:

runda	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
broj bitova koji se razlikuju	1	6	21	35	39	34	32	31	29	42	44	32	30	30	26	29	34

Primjer 2: Otvoreni tekst

68852E7A1376EBA4

šifrovan je pomoću ključeva

E5F7DF313B0862DC i 64F7DF313B0862DC

koji se razlikuju samo u jednom bitu (i jednom bitu parnosti: prvih 7 bitova su im 1110010 i 0110010). Broj bitova razlike kod šifrata, po rundama, prika
zan je u sljedećoj tablici:

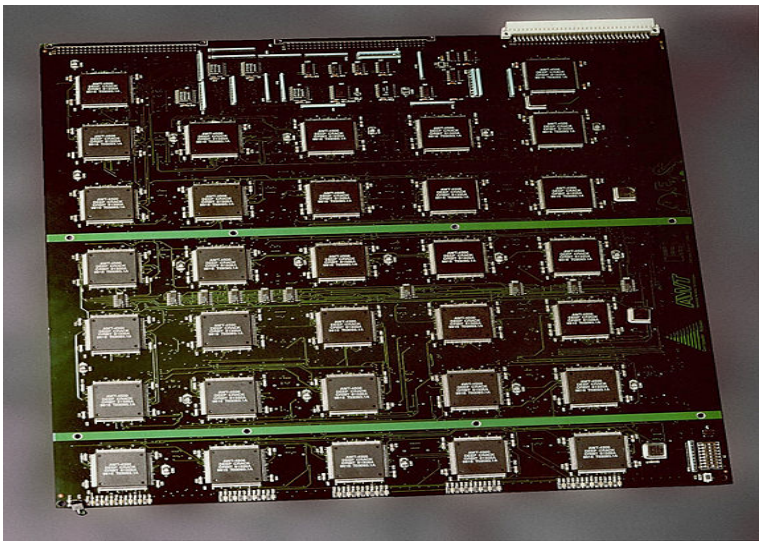
runda	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
broj bitova koji se razlikuju	0	2	14	28	32	30	32	35	34	40	38	31	33	28	26	34	35

Postavlja se pitanje zašto u DES-u imamo baš 16 rundi. Primjeri 1 i 2 sugerišu da već kod 3. runde efekat lavine dolazi do izražaja. Može se pokazati da nakon 5. runde svaki bit šifrata zavisi od svakog bita otvorenog teksta i svakog bita ključa, a nakon 8. runde šifrat je praktično slučajna funkcija bitova otvorenog teksta i ključa. Razlog što ipak imamo 16 rundi je u zahtjevu da poznati kriptoanalitički napadi (kao što je npr. diferencijalna kriptoanaliza) ne budu efikasniji od napada "grubom silom".

Originalna IBM-ova ponuda NBS-u je imala 112-bitni ključ. Prva IBM-ova realizacija Feistelove šifre - kriptosistem LUCIFER je imao 128-bitni ključ. Međutim, u verziji DES-a koja je prihvaćena kao standard dužina ključa je smanjena na 56 bitova (da bi ključ stao na tadašnje čipove, ali vjerovatno i pod uticajem NSA). Mnogi kriptografi su bili protiv tako

kratkog ključa jer su smatrali da ne pruža dovoljnu sigurnost protiv napada "grubom silom".

Uz 56-bitni ključ imamo $2^{56} \approx 7.2 \cdot 10^{16}$ mogućih ključeva, pa se na prvi pogled napad "grubom silom" može činiti sasvim nepraktičnim. Međutim, već 1977. godine Diffie i Hellman su utvrdili da tadašnja tehnologija omogućava konstrukciju računara koji bi otkrivao ključ za jedan dan, a troškove su procijenili na 20 miliona dolara. Na osnovu toga su zaključili da je tako nešto dostupno samo organizacijama kao što je NSA, ali da će oko 1990. godine DES postati sasvim nesiguran. Godine 1993. Weiner je procijenio da se za 100 000 dolara može konstruisati računar koji bi otkrio ključ za 35 sati, a za 10 miliona dolara onaj koji bi otkrio ključ za 20 minuta. Ipak sve su to bili hipotetski dizajni i konačno razbijanje DES-a se dogodilo tek 1998. godine. Tada je Electronic Frontier Foundation (EFF) za 250000 dolara zaista napravila mašinu "DES Cracker", koji je razbijao poruke šifrovane DES-om za 56 sati (Slika 4.3.9) [76].



Slika 4.3.9 "DES Cracker" sa 32 "Deep crack" čipa

Slika 4.3.10 "Deep crack" mikročip

Za fiksni ključ K pomoću DES-a definisana je permutacija skupa $\{0,1\}^{64}$. Dakle, skup od 2^{56} permutacija dobijenih pomoću DES-a je podskup grupe svih permutacija skupa $\{0,1\}^{64}$, čiji je red $2^{64}!$. Postavlja se pitanje da li je DES (tj. skup svih njegovih permutacija) podgrupa ove grupe. Odgovor na to pitanje je negativan. Naime, skup svih DES-permutacija nije zatvoren. Preciznije, poznato je da je red podgrupe generisane svim DES-permutacijama veći o 2^{2499}. Ova činjenica je jako važna jer pokazuje da se višestrukom upotrebom DES-a može postići veća sigurnost. Posebno je popularan tzv. Triple-DES koji koristi tri koraka običnog DES-a s različitim ključevima. Kad bi DES činio grupu, Triple-DES ne bi bio ništa sigurniji od običnog DES-a.

Neki DES-ključevi su znatno nesigurniji od ostalih, pa ih svakako treba izbjegavati. Prvi među njima su tzv. DES *slabi ključevi*. Kod njih su svi međuključevi K_1, ... , K_{16} jednaki. To znači da su postupak šifrovanja i dešifrovanja doslovno jednaki. Dakle, vrijedi $e_K(e_K(x)) = x$. Drugim riječima, DES sa slabim ključem je involucija. Poznato je da šifrovanje sa slabim ključem ostavlja 2^{32} otvorenih tekstova fiksnim. Postoje tačno 4 DES slaba ključa. To su oni kod kojih se fiksne permutacije PC1(K) = C_0D_0, lijeve i desne polovine C_0 i D_0 sastoje ili od samih nula ili od samih jedinica. Par ključeva (K,K') je par DES *polu-slabih ključeva* ako je kompozicija DES-ova s ključevima K i K' identiteta. Drugim riječima, šifrovanje s jednim je isto kao dešifrovanje s drugim. Kod DES-a s polu-slabim ključem, među 16 međuključeva K_1, ... , K_{16} postoje samo dva različita; svaki od njih se koristi po 8 rundi. Postoji tačno 6 parova DES polu-slabih ključeva. Konačno, neki ključevi generišu samo 4 različita međuključa. Takvi se ključevi zovu DES *potencijalno slabi ključevi* i ima ih tačno 48. Sve u svemu, između 2^{56} mogućih ključeva imamo samo 64 ključa koja treba izbjegavati, pa je to lako i učiniti [77].

KRIPTOGRAFSKI MODOVI KOD DES-A

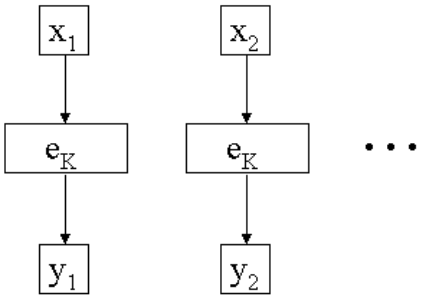
Iako je sam opis DES-a dosta dug, on se može vrlo efikasno implementirati, i hardverski i softverski. Do 1991. godine u NBS-u registrovano 45 hardverskih implementacija DES-a. Godine 1992. proizveden je čip s 50000 tranzistora koji može šifrovati 10^9 bita (tj. 16 miliona blokova) po sekundi (čip je koštao 300 dolara).

Jedna važna primjena DES-a je u bankarskim transakcijama. Tako se, između ostalog, DES koristio za šifrovanje PIN-ova (personal identification numbers), kao i transakcija preko bankomata. DES je takođe takođe našao primjenu i u civilnim satelitskim komunikacijama.

U ovom poglavlju do sada je opisano kako radi DES na jednom bloku od 64 bita. U realnim situacijama, u kojima su poruke znatno duže, poznata su 4 *načina djelovanja odnosno moda* (modes of operation) DES-a. Ti

modovi pokrivaju sve moguće primjene DES-a, a također su primjenjljivi na bilo koju simetričnu blokovnu šifru.

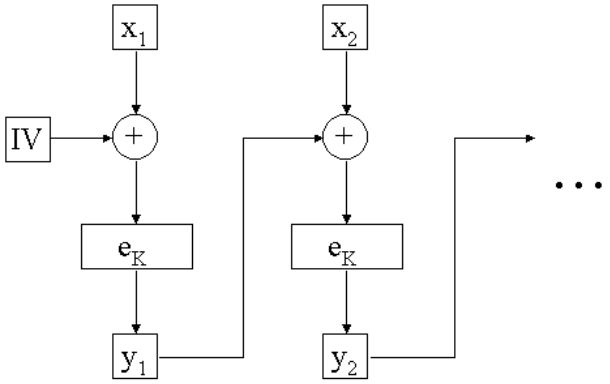
Najjednostavniji mod je **ECB (Electronic Codebook)** u kojem se svaki blok otvorenog teksta šifruje s istim ključem. Dakle, poruka se razbije na blokove od po 64 bita (zadnji blok se dopuni ako je potrebno), pa se šifrira jedan po jedan blok koristeći uvijek jedan isti ključ (Slika 4.3.11).



Slika 4.3.11 Grafički prikaz ECB moda

ECB mod je idealan za kratke poruke, pa se često koristi za razmjenu ključeva za šifovanje. Kod dugih poruka sigurnost ECB moda se smanjuje, budući da identični blokovi u otvorenom tekstu daju identične šifrate.

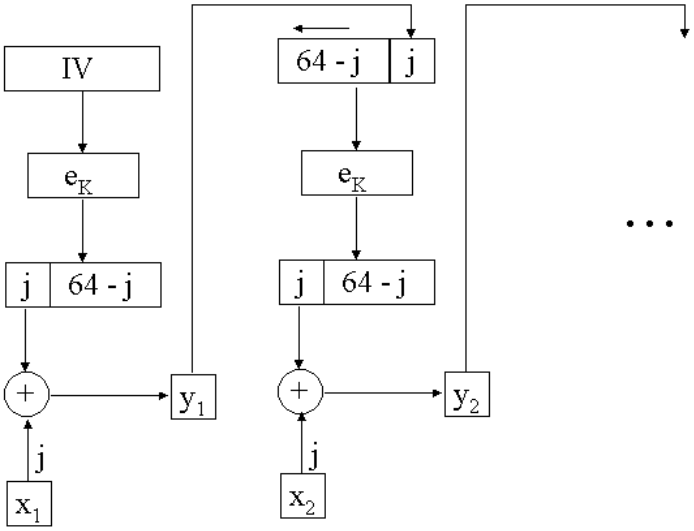
Da bi se povećala sigurnost, ideja je postići da identičnim blokovima u otvorenom tekstu odgovaraju različiti šifrati. Relativno jednostavan način da se to postigne je korišćenje **CBC (Cipher Block Chaining)** moda (Slika 4.3.12). Na trenutni blok otvorenog teksta se primjeni operacija XOR sa šifratom prethodnog bloka, a tek onda se šifruje pomoću ključa K. Dakle, $y_i = e_K(y_{i-1} \oplus x_i)$ za $i \geq 1$. Na startu uzimamo da je y_0 = IV, gdje je IV tzv. inicijalizirajući vektor, koji mora biti poznat i primaocu i pošiljaocu. To se može postići, npr., tako što se pošalje ECB modom. Za dešifrovanje koristimo relaciju $x_i = y_{i-1} \oplus d_K(y_i)$.



Slika 4.3.12 Grafički prikaz CBC moda

U prethodna dva moda DES funkcioniše kao blokovna šifra. Ali, od DES-a se može napraviti i protočna (stream) šifra. Prvi način je pomoću **CFB (Cipher Feedback) moda.** Kod protočnih šifri nema potrebe za proširivanjem poruke da bi se dobio cijeli broj blokova. To znači da će šifrat biti iste dužine kao otvoreni tekst. Obrađuje se odjednom j bitova ($1 \leq j \leq 64$). Najčešće je $j = 1$ ili $j = 8$ (Slika 4.3.13). Ako je $j = 8$, to znači da se šifruje slovo po slovo (jednom slovu odgovara 8 bitova po ASCII standardu).

U šifrovanje krećemo šifrovanjem 64 bitnog inicijalizivanog vektora IV. Na j zadnjih lijevih bitova izlaznog podatka primijenimo XOR sa x_1 i tako dobijemo y_1. Ulazni podatak za sljedeći korak šifrovanja se dobije tako što se prethodni ulazni podatak pomjeri za j mjesta ulijevo, a na desni kraj se stavi y_1. Postupak se nastavlja sve dok se sve jedinice otvorenog teksta ne šifruju.

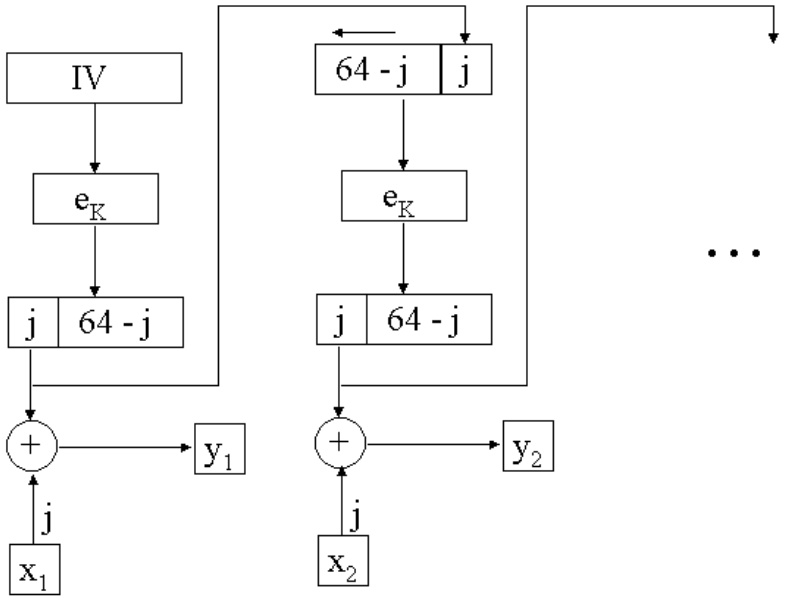


Slika 4.3.13 Grafički prikaz CFB moda

Kod dešifrovanja se koristi ista šema, osim što se na odgovarajući šifrat primjeni XOR s izlaznim podatkom funkcije šifrovanja e_K da bi se dobio otvoreni tekst. Uočimo da se ponovo koristi funkcija e_K, a ne d_K. Naime, ovdje je funkcija šifrovanja zapravo XOR, a on je sam sebi inverzan. Zapravo, ovaj mod možemo shvatiti kao svojevrsnu realizaciju "jednokratnog zapisa", u kojoj nam e_K ne služi za šifrovanje, već za generisanje "pseudoslučajnog" ključa za jednokratni zapis. Ovo pokazuje da inicijalni vektor IV mora biti "svjež", tj. ne bi se dva puta smio koristiti isti inicijalni vektor.

OFB (Output Feedback) mod je vrlo sličan kao CFB. Jedina razlika je što se ulazni podatak za funkciju e_K u idućem koraku šalje odmah nakon primjene e_K u prethodnom koraku (prije primjene XOR-a) (Slika 4.3.14).

Jedna od prednosti OFB moda je da se greške u transmisiji ne propagiraju. Npr. greška u y_1 utiče samo na x_1. Ovaj mod se često koristi kod šifrovanja poruka sa satelita. Ali, ovo svojstvo može biti i nedostatak. Zato se modovi CBC i CFB koriste za ustanovljavanje vjerodostojnosti poruke.



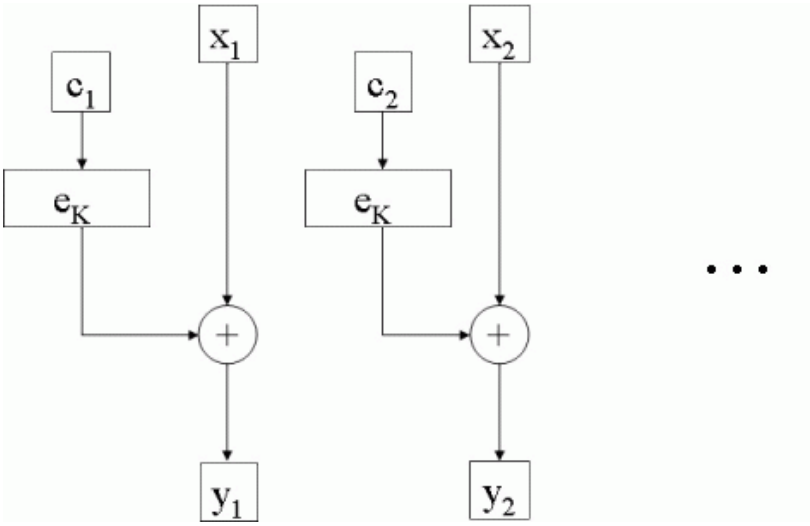
Slika 4.3.14 Grafički prikaz OFB moda

Pored ova četiri (klasična) načina djelovanja, u posljednje vrijeme je sve popularniji **CTR (Counter) mod.** U njemu se koristi niz brojača (countera) c_1, c_2, ... Niz blokova šifrata dobija se po sljedećem pravilu:

$$y_i = x_i \oplus e_K(c_i).$$

Brojači moraju biti u parovima različiti. Obično se to postiže tako što se brojaču c_1 pridruži neka inicijalna vrijednost, a potom se ostali brojači povećavaju za 1: $c_i = c_1 + (i - 1)$ (sabiranje je po modulu 2^b, gdje je b dužina bloka; kod DES-a je $b = 64$) (Slika 4.3.15).

Za razliku od prethodna tri "ulančana" (chaining) moda, u CTR modu se šifrovanje (i dešifrovanje) može lako dovesti u paralelu. Kod ulančanih modula je to bio problem, jer je algoritam morao završiti obradu jednog bloka, da bi prešao na naredni. To pokazuje još jednu prednost CTR moda, a to je mogućnost dešifrovanja samo jednog određenog bloka, što može biti interesanstno za neke aplikacije. Slično kao kod CFB i OFB, i ovdje se u dešifrovanju ponovo koristi funkcija e_K (a ne d_K). Ovo nije neka posebna prednost kod DES-a, ali može biti relevantno kod blokovnih kriptosistema kod kojih algoritam dešifrovanja nije doslovno isti kao algoritam šifrovanja (npr. AES).



Slika 4.3.15 Grafički prikaz CTR moda

KRIPTOANALIZA DES-A

U ovom poglavlju biće opisana tri najčešće načina napada na DES: *diferencijalnu kriptoanalizu*, *linearnu kriptoanalizu* i EFF-ov *DES Cracker*. Iako prva dva napada nisu dovela do razbijanja DES-a, njihova je važnost u tome što su primjenljivi na bilo koji simetrični blokovni kriptosistem. Tako su kod većine mogućih nasljednika DES-a operacije i broj rundi odabrani upravo tako da bi dobijeni kriptosistem bio što otporniji na diferencijalnu i linearnu kriptoanalizu.

Metodu *diferencijalne kriptoanalize* prvi su javno opisali izraelski kriptolozi *Eli Biham* i *Adi Shamir* 1990. godine. Ali, po svemu sudeći, ta metoda je bila poznata konstruktorima DES-a već 1974. godine, i imali su je u vidu kod dizajna S-kutija i permutacije P. Metoda spada u napade "odabrani otvoreni tekst". Biće pokazano kako ova metoda može biti primjenjena na DES s n rundi ($n \leqslant 16$) [75]. U tu svrhu može se ignorisati inicijalna permutacija IP i njen inverzni oblik. Oni nemaju nikakav efekt na kriptoanalizu. Zato se L_0R_0 uzima za otvoreni tekst, a L_nR_n za šifrat u DES-u s n rundi. Osnovna ideja diferencijane kriptoanalize jeste poređenje XOR-a od dva otvorena teksta sa XOR-om od odgovarajuća dva šifrata. Uopšteno, posmatraju se dva otvorena teksta L_0R_0 i $L^*_0R^*_0$ sa zadatom XOR vrijednošću $L'_0R'_0 = L_0R_0 \oplus L^*_0R^*_0$.

Definicija: Neka je S_j neka S-kutija ($1 \le j \le 8$) i neka je (B_j, B^*_j) uređeni par 6-bitnih nizova. Tada $B_j \oplus B^*_j$ zovemo *input XOR*, a $S_j(B_j) \oplus S_j(B^*_j)$ zovemo *output XOR*.
Za svaki $B'_j \in (\mathbf{Z}_2)^6$, sa $\Delta(B'_j)$ označavamo skup svih uređenih parova (B_j, B^*_j) čiji je input XOR jednak B'_j.

Sada slijedi da je:

$$\Delta(B'_j) = \{ (B_j, B_j \oplus B'_j) : B_j \in (\mathbf{Z}_2)^6 \},$$

pa skup $\Delta(B'_j)$ sadrži $2^6 = 64$ para. Za svaki par iz $\Delta(B'_j)$ možemo izračunati output XOR. Dobijamo 64 output XOR-a koji su distribuirani između $2^4 = 16$ mogućih vrijednosti za output XOR. Činjenica da ovih 64 output XOR-ova nije uniformno distribuirano predstavlja osnovu za kriptoanalitički napad.

Primjer 1: Posmatramo prvu S-kutiju S_1 i input XOR 110100. Sada je

$\Delta(110100)$ = {(000000,110100), (000001,110101), ... , (111111,001011)}.

Za svaki uređeni par iz $\Delta(110100)$ izračunava se output XOR. Npr. $S_1(000000) = 14_{10} = 1110$, $S_1(110100) = 9_{10} = 1001$, pa je output XOR para (000000,110100) jednak 0111. Nakon što izračunamo output XOR-ove za sva 64 para, dobija se distribuciju prikazana na Slici 4.3.16

0000	0001	0010	0011	0100	0101	0110	0111
0	8	16	6	2	0	0	12

1000	1001	1010	1011	1100	1101	1110	1111
6	0	0	0	0	8	0	6

Slika 4.3.16 Distribucija output XOR-ova

U Primjeru 1 pojavilo se samo 8 od mogućih 16 output XOR-ova i to s vrlo različitim frekvencijama. U prosjeku se pojavljuje 75-80% mogućih XOR-ova.

Definicija: Za $j \in \{1, 2, \ldots, 8\}$, 6-bitni niz B'_j i 4-bitni niz C'_j definišemo

$$IN_j(B'_j, C'_j) = \{ B_j \in (\mathbf{Z}_2)^6 : S_j(B_j) \oplus S_j(B_j \oplus B'_j) = C'_j \},$$
$$N_j(B'_j, C'_j) = | IN_j(B'_j, C'_j) |.$$

Dakle, $N_j(B'_j, C'_j)$ je broj parova čiji je input XOR jednak B'_j, a output XOR je jednak C'_j. Distribucije iz Primjera 4. su zapravo vrijednosti $N_1(110100, C'_1)$, $C'_1 \in (\mathbf{Z}_2)^4$, dok su skupovi $IN_1(110100, C'_1)$ prikazani u sljedećoj tabeli na Slici 4.3.17.

output XOR	mogući inputi
0000	
0001	000011, 001111, 011110, 011111, 101010, 101011, 110111, 111011
0010	000100, 000101, 001110, 010001, 010010, 010100, 011010, 011011, 100000, 100101, 010110, 101110, 101111, 110000, 110001, 111010
0011	000001, 000010, 010101, 100001, 110101, 110110
0100	010011, 100111
0101	
0110	
0111	000000, 001000, 001101, 010111, 011000, 011101, 100011, 101001, 101100, 110100, 111001, 111100
1000	001001, 001100, 011001, 101101, 111000, 111101
1001	
1010	
1011	
1100	
1101	000110, 010000, 010110, 011100, 100010, 100100, 101000, 110010
1110	
1111	000111, 001010, 001011, 110011, 111110, 111111

Slika 4.3.17 Skupovi $IN_1(110100, C'_1)$

Podsjetimo se da ulazni podatak za S-kutije u i-toj rundi ima oblik $B = E \oplus J$, gdje je $E = E(R_{i-1})$ proširenje od R_{i-1}, a $J = K_i$ je i-ti međuključ. Sada je

$$B \oplus B^* = (E \oplus J) \oplus (E^* \oplus J) = E \oplus E^*,$$

pa input XOR ne zavisi od međuključa J. Zapišimo B, E, J, B^* i E^* kao spoj od osam 6-bitnih nizova:

$$B = B_1\, B_2\, B_3\, B_4\, B_5\, B_6\, B_7\, B_8$$
$$E = E_1\, E_2\, E_3\, E_4\, E_5\, E_6\, E_7\, E_8$$
$$J = J_1\, J_2\, J_3\, J_4\, J_5\, J_6\, J_7\, J_8$$
$$B^* = B^*_1 B^*_2 B^*_3 B^*_4 B^*_5 B^*_6 B^*_7 B^*_8$$
$$E^* = E^*_1 E^*_2 E^*_3 E^*_4 E^*_5 E^*_6 E^*_7 E^*_8$$

Definicija: Neka su E_j i E^*_j 6-bitni nizovi, a C'_j 4-bitni niz. Definišemo $\text{test}_j\,(E_j, E^*_j, C'_j) = \{\, B_j \oplus E_j : B_j \in \text{IN}_j\,(E'_j, C'_j)\,\}$, gdje je $E'_j = E_j \oplus E^*_j$.

Primjer 2: Neka je $E_1 = 000001$, $E^*_1 = 110101$, $C'_1 = 1101$. Budući da je $\text{N}_1(110100, 1101) = 8$, skup $\text{test}_1(000001, 110101, 1101)$ će imati 8 elemenata. Sa Slike X.X se vidi da je

$$\text{IN}_1(110100, 1101) = \{\, 000110, 010000, 010110, 011100, 100010, 100100, 101000, 110010\,\},$$

pa je

$$\text{test}_1(000001, 110101, 1101) = \{\, 000111, 010001, 010111, 011101, 100011, 100101, 101001, 110011\,\}.$$

Pretpostavka 1: *Neka je* $C'_j = \text{S}_j\,(B_j) \oplus \text{S}_j\,(B^*_j)$. *Tada je* $J_j \in \text{test}_j\,(E_j, E^*_j, C'_j)$.

Dokaz: Po definiciji treba provjeriti da je $J_j \oplus E_j \in \text{IN}_j\,(E'_j, C'_j)$. No, $J_j \oplus E_j = B_j$ i $\text{S}_j\,(B_j) \oplus \text{S}_j\,(B_j \oplus B'_j) = \text{S}_j\,(B_j) \oplus \text{S}_j\,(B^*_j) = C'_j$, pa je $J_j \in \text{test}_j\,(E_j, E^*_j, C'_j)$.

Pretpostavka 1 daje nekoliko mogućnosti za J_j. Njenom primjenom na nekoliko različitih trojki E_j, E^*_j, C'_j, može se odrediti J_j. Jasno, ovdje je pretpostavka da su vrijednosti E_j, E^*_j, C'_j poznate. Veliko je pitanje koliko je ta pretpostavka realna.

Sad će se razmotriti kako se ove ideje mogu primijeniti u napadu "odabrani otvoreni tekst" na DES s 3 runde. Krećemo od parova otvorenih tekstova L_0R_0, $L^*_0R^*_0$ koje smo odabrali tako da je $R_0 = R^*_0$, tj. $R'_0 = 00...0$ i odgovarajućih šifrata L_3R_3, $L^*_3R^*_3$. Imamo da je:

$$R_3 = L_2 \oplus f(R_2,K_3) = R_1 \oplus f(R_2,K_3) = L_0 \oplus f(R_0,K_1) \oplus f(R_2,K_3),$$
$$R^*_3 = L^*_0 \oplus f(R^*_0,K_1) \oplus f(R^*_2,K_3),$$
$$R'_3 = L'_0 \oplus f(R_2,K_3) \oplus f(R^*_2,K_3).$$

Sada je $f(R_2,K_3) = \mathrm{P}(C)$ i $f(R^*_2,K_3) = \mathrm{P}(C^*)$, gdje su C i C^* outputi od S-kutija. Stoga je

$$\mathrm{P}(C) \oplus \mathrm{P}(C^*) = R'_3 \oplus L'_0,$$

pa je

$$C' = C \ominus C^* = \mathrm{P}^{-1}(R'_3 \oplus L'_0).$$

Konačno, $E = E(R_2) = E(L_3)$ i $E^* = E(R^*_2) = E(L^*_3)$. Dakle, E, E^* i C' su nam poznati.

ALGORITAM:

Ulazni podaci: L_0R_0, $L^*_0R^*_0$, L_3R_3 i $L^*_3R^*_3$, gdje je $R_0 = R^*_0$

1. Izračunamo: $C' = \mathrm{P}^{-1}(R'_3 \oplus L'_0)$
2. Izračunamo: $E = E(L_3)$ i $E^* = E(L^*_3)$
3. Za $j = 1, 2, \ldots, 8$
   računamo $\mathrm{test}_j\ (E_j, E^*_j, C'_j)$.

Primjenom ovog algoritma na nekoliko različitih inputa možemo odrediti međuključ K_3, što nam daje 48 bitova ključa K. Preostalih 8 bitova možemo pronaći tako što testiramo svih $2^8 = 256$ mogućnosti.

Primjer 3: Pretpostavimo da imamo sljedeća tri para otvorenih tekstova i šifrata (zapisanih heksadecimalno) šifrovanih istim ključem (otvoreni tekstovi su odabrani tako da zadovoljavaju uslov $R_0 = R^*_0$):

otvoreni tekst	šifrat
748502CD38451097	03C70306D8A09F10
3874756438451097	78560A0960E6D4CB
486911026ACDFF31	45FA285BE5ADC730
375BD31F6ACDFF31	134F7915AC253457

357418DA013FEC86	D8A31B2F28BBC5CF
12549847013FEC86	0F317AC2B23CB944

Primjenom algoritma na prvi par, dobija se:

E = 000000000111111000001110100000000110100000001100

E*= 101111110000001010101100000001010100000001010010

C'= 100101100101110101011011011001111

Za drugi par dobijamo

E = 101000001011111111110100000101010000001011110110

E*= 100010100110101001011110101111110010100010101010

C'= 100111001001110000011111010101110

a za treći

E = 111011110001010100000110100011111011010010101111111

E*= 000001011110100110100010101111110101011000000100

C'= 110101010111010111011011001010111

Sada za svaki J_j, j = 1, 2, ... , 8, konstruišemo brojač koji broji za koliko parova J_j zadovoljava uslov iz Pretposavke 1. Na primjer, u slučaju prvog para i brojača za J_1 imamo E'_1 = 101111, C'_1 = 1001. Zatim se ima da je

$$IN_1 (101111, 1001) = \{ 000000, 000111, 101000, 101111 \}.$$

Budući da je E_1 = 000000, konačno se dobija

$$J_1 \in test_1 (000000, 101111, 1001) = \{ 000000, 000111, 101000, 101111 \}.$$

To znači da se brojač povećava za 1 na pozicijama 0, 7, 40 i 47. Konačne vrijednosti svih 8 brojača, nakon što su obrađena sva tri para, prikazane su na Slici 4.3.18.

J_1															
1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
0	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0
0	1	0	0	0	1	0	0	1	0	0	0	0	0	0	3
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

J_2															
0	0	0	1	0	3	0	0	1	0	0	1	0	0	0	0
0	1	0	0	0	2	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	1	0	1	0	0	0	1	0
0	0	1	1	0	0	0	0	1	0	1	0	2	0	0	0

J_3															
0	0	0	0	1	1	0	0	0	0	0	0	0	0	1	0
0	0	0	3	0	0	0	0	0	0	0	0	0	0	1	1
0	2	0	0	0	0	0	0	0	0	0	0	1	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0

J_4															
3	1	0	0	0	0	0	0	0	0	2	2	0	0	0	0
0	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1
1	1	1	0	1	0	0	0	0	1	1	1	0	0	1	0
0	0	0	0	1	1	0	0	0	0	0	0	0	0	2	1

J_5															
0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0
0	0	0	0	2	0	0	0	3	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	2	0	0	0	0	0	0	1	0	0	0	0	2	0

J_6															
1	0	0	1	1	0	0	3	0	0	0	0	1	0	0	1
0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0
1	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0

J_7															
0	0	2	1	0	1	0	3	0	0	0	1	1	0	0	0
0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	1
0	0	2	0	0	0	2	0	0	0	0	1	2	1	1	0
0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1

J_8															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	1
0	3	0	0	0	0	1	0	0	0	0	0	0	0	0	0

Slika 4.3.18 Konačne vrijednosti svih 8 brojača, nakon što su obrađena sva tri para otvorenih tekstova

Vidimo da u svakom brojaču postoje jedinstvene pozicije sa brojem 3. Te pozicije određuju bitove od J_1, J_2, ... , J_8. Te pozicije su redom; 47, 5, 19, 0, 24, 7, 7, 49, odnosno binarno

$$J_1 = 101111$$
$$J_2 = 000101$$
$$J_3 = 010011$$
$$J_4 = 000000$$
$$J_5 = 011000$$
$$J_6 = 000111$$
$$J_7 = 000111$$
$$J_8 = 110001$$

Sada je interesantno pogledati kako izgleda raspored bitova ključa u međuključu K_3. Na osnovu toga rekonstruiše se 48 bitova ključa K:

0001101 0110001 01?01?0 1?00100
0101001 0000??0 111?11? ?100011

Upitnici postoje na onim mjestima koja se ne koriste u međuključu K_3. Sada testiranjem preostalih 256 mogućnosti dobijamo da je ključ (zapisan heksadecimalno, sa bitovima parnosti) jednak:

1A624C89520DEC46.

U našem napadu na DES sa 3 runde pošli smo od zahtjeva da je $R'_0 =$ 00...0. Ova ideja se može uopštiti.

Definicija 4: Neka je n prirodan broj. *n-rundna karakteristika* je niz oblika

$$L'_0, R'_0, L'_1, R'_1, p_1, \ldots, L'_n, R'_n, p_n$$

sa svojstvima:

(1) $L'_i = R'_{i-1}$ za $1 \le i \le n$,

(2) Neka je $1 \le i \le n$ i neka su L_{i-1}, R_{i-1}, L^*_{i-1}, R^*_{i-1} izabrani tako da je $L_{i-1} \oplus L^*_{i-1} = L'_{i-1}$ i $R_{i-1} \oplus R^*_{i-1} = R'_{i-1}$. Pretpostavlja se da su L_i, R_i, L^*_i, R^*_i dobijeni primjenom jedne rudne DES-a. Tada je vjerovatnoća da je $L_i \oplus L^*_i = L'_i$ i $R_i \oplus R^*_i = R'_i$ jednaka p_i.

U datom primjeru korištena je 1-rundna karakteristika

$$L'_0 = \text{prozvoljno}, R'_0 = 00000000_{16}, L'_1 = R'_0, R'_1 = L'_0, p_1 = 1.$$

Jedna druga 1-rundna karakteristika je

$$L'_0 = 00000000_{16}, R'_0 = 60000000_{16}, L'_1 = R'_0, R'_1 = 00808200_{16}, p_1 = 0.21875.$$

Biham i Shamir su pronašli 13-rundnu karakteristiku pomoću koje se može razbiti DES (pronaći 48 bitova ključa) uz poznavanje šifrata za 2^{47} odabranih otvorenih tekstova. Ukoliko e postoji mogućnost korištenja napada "odabrani otvoreni tekst" već samo "poznati otvoreni tekst", onda iz većeg broja parova otvoreni tekst-šifrat moraju se odabrati one korisne. Možda je zanimljivo napomenuti da je procijenjeno da time broj potrebnih DES operacija u napadu diferencijalnom kriptoanalizom postaje približno 2^{55}, što je sasvim uporedivo s brojem DES operacija u napadu "grubom silom" uz jedan poznati par otvoreni tekst-šifrat. Broj ključeva koje treba testirati je 2^{56}. Može se napomenuti da je za DES sa 8, 10, 12 i 14 rundi potrebno poznavanje šifrata za 2^{14}, 2^{24}, 2^{31}, odnosno 2^{39} odabranih tekstova. Dakle, ovo nam daje pravo objašnjenje zašto DES ima upravo 16 rundi.

Linearnu kriptoanalizu je uveo japanski kriptolog *Mitsuru Matsui* 1993. godine i čini se da ova metoda nije bila poznata tvorcima DES-a. Ideja se sastoji u tome da iako bitovi ključa nisu linearne funkcije otvorenog teksta i šifrata, neki se bitovi ključa mogu dobro aproksimirati linearnom funkcijom. Pomoću linearne kriptoanalize Matsui je opisao napad "poznati otvoreni tekst" koji za razbijanje DES-a treba u prosjeku 2^{43} otvorenih tekstova. Ovaj napad je implementiran pomoću 12 radnih ćelija i za otkrivanje ključa je trebalo 50 dana.

Međutim, ni diferencijalna ni linearna kriptoanaliza nisu razbile DES, već su tu učinili brzi i jeftini čipovi. Naime, pokazalo se da je u praksi lakše napraviti napad "grubom silom" sa 2^{55} DES operacija, nego primijeniti napad linearnom kriptoanalizom koji zahtjeva 2^{43} poznatih parova otvoreni tekst-šifrat. U julu 1998. god., Electronic Frontier Foundation je napravio "DES Cracker". Koštao je $250000, a za njegovu izradu je utrošeno godinu dana. DES Cracker je razbio poruku šifrovanu DES-om za 56 sati. Sagrađen je od 1536 čipova koji mogu testirati 88 milijardi ključeva po sekundi. Sličnih prijedloga bilo je i ranije, ali EFF je prvi to sproveo u djelo i tek nakon izrade DES Crackera moglo se definitivno utvrditi da DES nije siguran kriptosistem.

4.3.1.2 DES, IDEA, DES-X

U ovom poglavlju dat je kratak opis kriptosistema koji se koriste kao zamjena za DES. To su Trostruki DES (Triple DES, TDES, 3DES), IDEA i DES-X.

Prije nego što se pređe na opis Trostrukog DES algoritma, poželjno je osvrnuti se na pitanje zašto se ne koristi "Dvostruki DES". Kod Dvostrukog DES-a bi svaki blok bi bio šifrovan dva puta, sa dva različita ključa K i L:

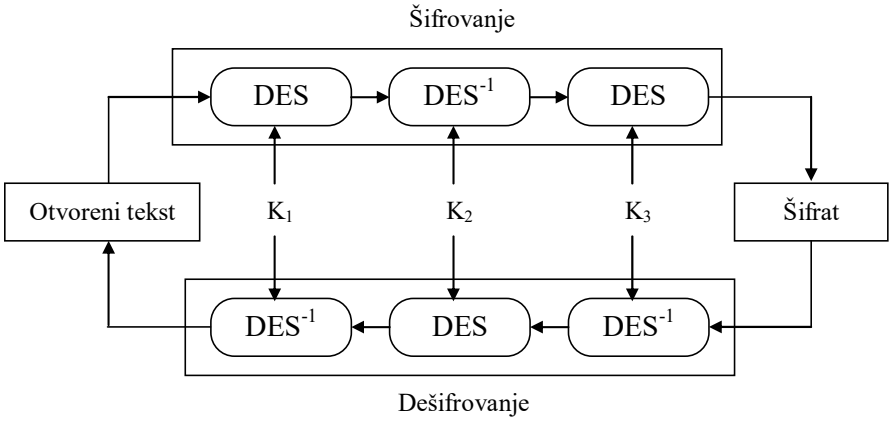
$$y = e_L(e_K(x)),\ \ x = d_K(d_L(y)).$$

Lako se pokazuje da Dvostruki DES, ne bi donio povećanje sigurnosti kodiranja. Naime, postoji nešto što se zove napad "*susret u sredini*", koji je opisao Diffie 1977. godine. Napad se izvodi na sljedeći način. Neka je poznat jedan par *otvoreni tekst-šifrat* (x,y). Orvoreni tekst x se šifruje sa svih 2^{56} mogućih ključeva K. Rezultati se upisuju u tablicu i sortiraju se po vrijednostima $z = e_K(x)$. Zatim se šifrat y dešifruje koristeći svih 2^{56} mogućih ključeva L. Nakon svakog dešifrovanja, potraži se rezultat u tablici (treba uzeti $z = d_L(y)$). Ako se pronađe, onda tako dobijeni par (K,L) se testira na sljedećem poznatom paru otvoreni tekst-šifrat. Ako test prođe, par (K,L) se prihvata za korektne ključeve. Vjerovatnoća da je napravljena greška je $2^{112\text{-}64\text{-}64} = 2^{-16}$. Na taj način je jasno da je za razbijanje Dvostrukog DES-a broj potrebnih operacija reda 2^{56}, što je neznatno više nego za obični DES.

Jedna od najpopularnijih zamjena za DES je ***Trostruki DES*** (koriste se još i nazivi Triple DES i 3DES):

$$y = e_M(d_L(e_K(x))),\ \ x = d_K(e_L(d_M(y))).$$

Ovdje je ključ dužine $56 \cdot 3=168$ bitova. Često se koristi i verzija u kojoj je $M = K$, pa je u njoj dužina ključa $56 \cdot 2=112$. Razlog za kombinaciju "*ede*" je kompatibilnost s običnim DES-om: dovoljno je staviti $L = M$ ili $K = L$. Za Trostruki DES broj operacija kod napada "susret u sredini" je reda $2^{112} \approx 5 \cdot 10^{33}$ dok je kod diferencijalne kriptoanalize procijenjen na 10^{52}. Možemo reći da je sigurnost kod trostrukog šifrovanja upravo onakva kakvu bismo možda naivno očekivali kod dvostrukog. U svakom slučaju, sigurnost 3DES-a je danas i više nego zadovoljavajuća.



Slika 4.3.19 Šema Triple DES-a

IDEA (*International Data Encryption Algorithm*) je kriptosistem koji su razvili švajcarski kriptografi *Xuejia Lai* i *James Massey* s ETH Zürich. Prvu verziju zvanu PES (*Proposed Encryption Standard*) su objavili 1990. Međutim, taj kriptosistem nije bio otporan na diferencijalnu kriptoanalizu (za 128-bitni ključ je trebalo 2^{64} operacija), pa su nakon Biham-Shamirovog otkrića, autori 1992. godine prepravili algoritam i nazvali ga IDEA.

IDEA koristi 128-bitni ključ za šifrovanje 64-bitnih blokova otvorenog teksta. Koristi tri operacije na 16-bitnim podblokovima:

- XOR (oznaka ⊕),
- sabiranje po modulu 2^{16} (oznaka ⊞),
- množenje po modulu $2^{16} + 1$ (oznaka ⊙).

Množenje se ovdje može smatrati analogono S-kutijama u DES-u. Moduo $2^{16}+1$ je odabran zbog efikasnije implementacije modularnog množenja. Ove tri operacije su inkompatibilne, u smislu da nikoje dvije ne zadovoljavaju zakone asocijativnosti i distributivnosti. IDEA ima 8 rundi i završnu transformaciju. U njima se koristi 52 16-bitnih međuključeva generisanih pomoću polaznog 128-bitnog ključa.

DES-X je još jedna od varijanti DES-a. Napravljen je u namjeri da se poveća sigurnost od "brute force attack"-a, odnosno od napada "grubom silom", koristeći tehniku "bijelog ključa" [78]. Zbog nedostatka koji je imao DES-male dužine ključa, 56 bita, odnosno 2^{56} mogućih kljuceva, i koji se mogao razbiti, NSA je zahtijevala da se poveća dužina ključa i usvojila novi algoritam. Nazvan je DES-X, a predlozio ga je američki kripograf Ronald Riverst, u maju 1984. god. Kod ovog kriposistema dužina ključa je sa 56 povećana na 184 bita. Ovim povećanjem je povećana i sigurnost od napada diferencijanom kripoanalizom i linearnom analizom. Kod diferencijalne kripoanalize za razbijanje DES-a je bilo potrebno 2^{47} otvorenih tekstova, a kod DES-X-a treba 2^{61}. Kod linearne analize za razbijanje DES-a je trebalo 2^{43} otvorenih tekstova, a kod DES-X-a 2^{60} .

4.3.1.3 Advanced Encryption Standard (AES)

Godine 1997. National Institute of Standards and Technology (NIST) objavio je konkurs za kriptosistem koji bi trebao kao opšte prihvaćeni standard da zamijeni DES. Pobjednik na konkursu dobio bi ime ***Advanced Encryption Standard*** **(AES).** NIST je postavio sljedeće zahtjeve na kriptosistem:

1. mora biti simetričan
2. mora biti blokovni
3. treba raditi sa 128-bitnim blokovima i ključevima s tri dužine: 128, 192 i 256 bitova.

Nekoliko je razloga zbog kojih NIST nije odabrao 3DES kao AES:

- 3DES koristi 48 rundi da bi postigao sigurnost za koju je vjerovatno dovoljno 32 runde.
- Softverske implementacije 3DES-a su prespore za neke primjene, posebno za digitalne video podatke.
- 64-bitni blokovi nisu najefikasniji u nekim primjenama.

Konkurs je završen 15.6.1998. Od 21 pristigle prijave, 15 ih je zadovoljilo NIST-ove kriterijume. U avgustu 1999. god. NIST je objavio 5 finalista: MARS, RC6, RIJNDAEL, SERPENT i TWOFISH.

MARS (IBM), RC6 (RSA Security Inc.) i TWOFISH (Counterpane Systems) spadaju u Feistelove šifre. Feistelova šifra je blokovna šifra u kojoj se u i-toj rundi koriste formule $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ (dakle, isto kao kod DES-a). Kod MARS kriptosistema blokovi ne dijele na 2, već na 4 dijela. MARS ima 32 runde, RC6 ima 20 rundi, dok TWOFISH ima 16 rundi. Specifičnost kriptosistema RC6 su korišćenje funkcije $f(x) = x(2x+1)$, kojom se orstvaruje difuzija i rotacija podataka. Ovo daje otpornost na diferencijalnu i linearnu kriptoanalizu. Specifičnost TWOFISH-a je da se S-kutije dinamički mijenjaju u zavisnosti od ključa, što komplikuje diferencijalnu i linearnu kriptoanalizu.

SERPENT su konstruisali kriptografi iz Engleske, Izraela i Danske. Spada u supstitucijsko-permutacijske šifre. Ima 32 runde i, što je za njega specifično, u svakoj rundi paralelno koristi 32 identične S-kutije.

RIJNDAEL su razvili belgijski kriptografi. Razlikuje se od ostalih po tome što se u konstrukciji S-kutija koriste operacije u konačnom polju $GF(2^8)$.

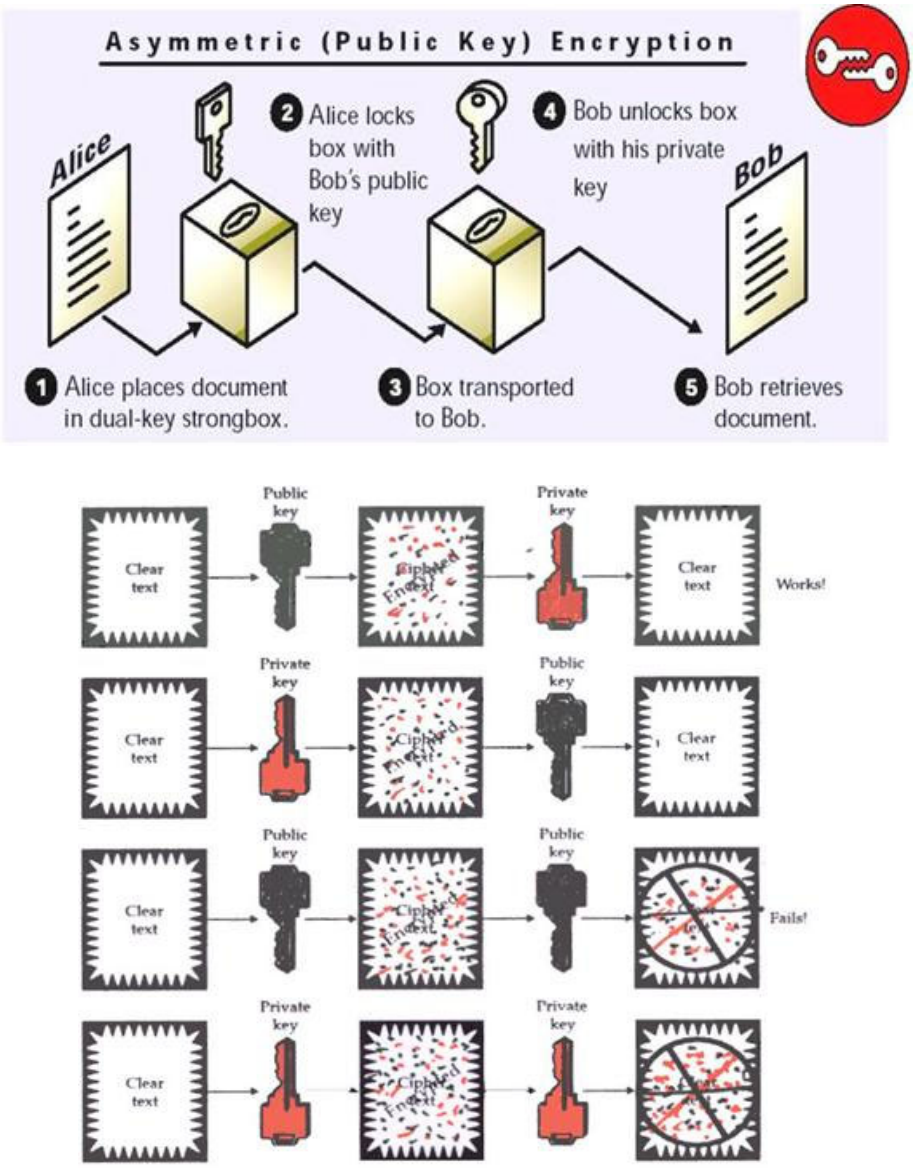
Konačno, 2.8.2000. objavljeno je da je pobjednik za AES-RIJNDAEL. RIJNDAEL su razvili belgijski kriptografi *Joan Daemen* i *Vincent Rijmen* s katoličkog sveučilišta Leuven, po kojima je i dobio ime.

Rijndael predstavlja blok šifarski algoritam koji podržava promjenljivu dužinu bloka informacije (128, 192 i 256 bita) kao i promjenljivu dužinu ključa (128, 192 i 256 bita). Naime, poruke šifrovane DES algoritmom su se, zbog nedostataka u samom algoritmu (bezbjedonosni nedostaci u supstitucionim s-kutijama), male dužine ključa (56-bita) i povećane procesne moći računara, mogle dešifrovati za samo par časova. Nakon selekcione procedure, za realizaciju AES standarda izabran je Rijndael algoritam. Rijndael algoritam je u odnosu na konkuretske algoritme (MARS, RC6, Serpent, Twofish) bio brži i zahtijevao je manje operativne memorije u procesu šifrovanja i dešifrovanja poruka. Rijndael algoritam sa 128-bitnom dužinom ključa je brži za oko 2.5 puta u odnosu na 3-DES algoritam.

4.3.2 ASIMETRIČNA KRIPTOGRAFIJA

Asimetrično kriptografija, takođe poznata i kao kriptografija javnim ključem, je vrsta kriptovanja u kojem se ključ za šifrovanje podataka razlikuje od ključa za dešifrovanje. Svaki korisnih upotrebljava par ključeva poznatih kao javni i privatni ključ. Privatni ključ se čuva u tajnosti dok je javni ključ poznat svima zainteresovanima. Važno je naglasiti da se poznavanjem javnog ključa ne može izračunati tajni ključ u nekom razumnom vremenu [80].

Pristigla poruka, koja je šifrovana primaočevim javnim ključem može biti dešifrovana samo njegovim tajnim ključem i obrnuto (Slika 4.3.20). Ključevi su matematički povezani, ali se privatni ključ praktično ne može izvesti iz javnog ključa.



Slika 4.3.20 Asimetrična kriptografija – osnovni princip

Dvije glavne grane asimetrične kriptografije su:

- **Šifrovanje javnim ključem** - poruka šifrovana primaočevim javnim ključem može biti dešifrovana jedino primaočevim tajnim ključem. Ovakav vid asimetričnog šifrovanja koristi se da obezbijedi povjerljivost (tajnost) poruke.
- **Digitalni potpis** - Poruka potpisana pošiljaočevim privatnim ključem, može biti verifikovana od strane bilo koga ko poznaje pošiljaočev javni ključ. Ovakav vid asimetričnog šifrovanja koristi se da obezbijedi potvrdu autentičnosti poruke.

Algoritmi asimetrične kriptografije mogu se svrstati u tri osnovne grupe:

1. algoritmi zasnovani na praktičnoj nemogućnosti faktoriziranja velikih prostih brojeva (RSA),
2. algoritmi zasnovani na praktičnoj nemogućnosti izračunavanja diskretnih logaritama (Diffie-Hellman protokol, DSA)
3. algoritmi zasnovani na eliptičnim krivuljama (praktične realizacije ove metode su tek u povojima)

Osnovni koncept rada asimetričnih kriptografskih sistema je vrlo jednostavan. Da bi se komunikacija mogla obavljati asimetričnim kriptovanjem potrebno je posjedovati:

Javni ključ – PK (Public Key) i

Tajni ključ – SK (Secret Key)

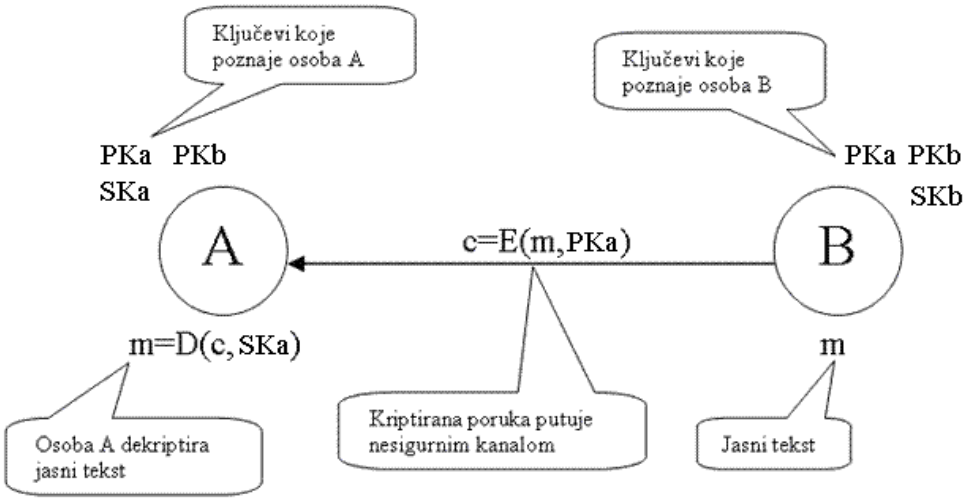
Ako osoba B želi osobi A poslati poruku sadržaja m, ona je kriptuje koristeći javni ključ osobe A - PKa:

$$c = E(m, PKa)$$

Osoba A dekriptuje poruku c koristeći svoj privatni ključ SKa:

$$m = D(c, SKa)$$

Ilustracija navedenog data je na Slici 4.3.21:



Slika 4.3.21 Šema rada asimetričnog kriptografskog sistema.

Glavni cilj ovoga načina kriptovanja je da pruži privatnost i pouzdanost. Međutim, pošto je javni ključ osobe A svima poznat, ovakav kriptografski sistem ne osigurava da se pouzdano zna odakle (od koga) je poruka stigla, a ne može se sa sigurnošću potvrditi niti integritet podataka. Da bi se obetbijedila autentičnost pošiljatelja potrebno je da poruka bude kodirana ili potpisana i privatnim ključem pošiljatelja [81]**.**

Asimetrični algoritmi daleko su sporiji od simetričnih algoritama kao npr. DES. Upravo zbog tog razloga kriptovanje asimetričnim algoritmima najčešće se koristi za:

- Izmjenu ključeva za poruke koje su kriptovane simetričnim algoritmima
- Zaštitu malih blokova podataka (primjer : PIN-ovi na pametnim karticama)

Najčešće korišteni algoritam asimetrične kriptografije je RSA algoritam, koji pripada prvoj grupi algoritama asimetrične kriptografije. RSA algoritam U daljem tekstu dat je detaljniji opis ovog algoritma.

4.3.2.1 RSA Algoritam

RSA kriptografski algoritam je najšire upotrebljavan algoritam asimetričnog kriptovanja. Moglo bi se reći da je RSA gotovo standard na području kriptovanja asimetričnim algoritmima [82].

Algoritam RSA je ime dobio po svojim tvorcima Ron Rivestu, Adi Shamiru i Len Adlemanu, koji su ga predložili 1977.

Četiri godine prije nego je RSA izumljen na M.I.T-u, 1973. godine britanski naučnik Clifford Cocks izumio je prethodnika RSA algoritma. Njegovo je otkriće odlukom britanske vlade proglašeno državnom tajnom, a javno je objavljeno tek 1997. godine.

Algoritam se može koristiti za kriptovanje i digitalne potpise. Sigurnost algoritma zasnovana je na teškom problemu faktoriziranja velikih cijelih brojeva (brojevi veći od 10^{100}) [75].

OSNOVNI KONCEPT ALGORITMA RSA

Da bi se određena poruka, odnosno tekst mogao kodirati RSA algoritmom, najprije preba generisati par ključeva, javni i tajni ključ. Postupak generisanja ključeva sastoji se iz sljedećih koraka:

1º Na startu se generišu dva velika prosta broja p i q. Brojevi trebaju biti približno jednako veliki.

2º U drugom koraku izračunava se:

n=p*q i
phi=(p-1)(q-1)

3º Odabire se broj ***e*** takav da je manji od phi, te da vrijedi da je najveći zajednički sadržilac ta dva broja jednak 1.

Nzs(phi,e)=1

4º Uz takav broj *e* izračuna se d tako da vrijedi:

e*d mod **phi =1**,

odnosno,

e*d=k*phi+1

5º Par (n, e) proglašava se javnim ključem, a par (n, d) tajnim ključem. Vrijednosti za phi, p i q također se moraju čuvati kao tajne.

Postupak kriptovanja sastoji se od pretvaranja poruke iz znakovnog niza u broj manji od n. Zatim se dobijeni broj M kriptuje formulom:

C = M*e mod **n**

Ako tekst, koji treba kodirati, ima više bitova nego broj n, tada se on dijeli u više blokova jednake dužine. Pri tome valja voditi računa da ti blokovi ne smiju biti duži od dužine broja n. Vrijednost znakovnog niza iz poruke čistog teksta pretvara se dakle u manje blokove jednake bitovne dužine. Blokovi se zatim predstavljaju kao cijeli brojevi i koriste se u algoritmu.

Ako je početna poruka čistog teksta bila M, možemo je podijeliti na niz cijelih brojeva jednake dužine:

M=M0M1M2M3…

Dekriptovanje se vrši analogno kriptovanju, ali se koristi privatni ključ. Izvorna informacija dobija se formulom:

$$\mathbf{M = C^{*}d} \bmod \mathbf{n.}$$

U slučaju da smo imali više poruka tada slijedi:

$$\mathbf{Ci}=\mathbf{Mi^{*}e} \bmod \mathbf{n} \text{ ili}$$
$$\mathbf{Mi = Ci^{*}d} \bmod \mathbf{n.}$$

JEDNOSTAVAN PRIMJER PRIMJENE RSA ALGORITMA

Osoba A bira proste brojeve:

$$p = 2357$$
$$q = 2551$$

Zatim izračunava:

$$n = pq = 6012707$$
$$phi = (p-1)(q-1) = 6007800.$$

Osoba A odabire:

$$e = 3674911$$

Pomoću izraza **e*d** mod **phi =1** pronalazi:

$$d = 422191.$$

Iz predhodnoh proizilazi da je javni ključ osobe A

$$(n = 6012707; e = 3674911),$$

a tajni

$$(n = 6012707; d= 422191).$$

Kriptovanje

Da bi kriptovala poruku m=5234673, osoba B koristi javni ključa (n,e) osobe A, i dobija:

$$C = (m*e) \bmod n = 52346733674911 \bmod 6012707 = 3650502$$

Kriptovanu poruku C osoba B i šalje osobi A.

Dekriptovanje

Da bi dekriptovala poruku C, osoba A koristi svoj privatni ključa (n,d), i dobija:

$$M = (C*d) \bmod n = 3650502422191 \bmod 6012707 = 5234673$$

MATEMATIČKA POZADINA ALGORITMA RSA

Da bi se bolje razumio način funkcionisanja algoritma RSA i shvatio njegov osnovni kvalitet ovdje će se kratko navesti neki dijelovi matematičke teorije brojeva koja je pozadina algoritma RSA.

Djeljivost

Kažemo da a dijeli b (b je djeljiv sa a) i pišemo $a|b$ ako i samo ako ($\exists k \in Z$, $b=ka$). Broj b nazivamo trivijalnim djeliteljem od a, za svaki $b \in \{1,a\}$. Faktorom nazivamo svaki b koji nije dio toga skupa. Primjer:

Broj a=24 ima slijedeće djelitelje:

1, 2, 3, 4, 6, 8, 12, 24

Trivijalni djelitelji su 1 i 24, a faktori su:

2, 3, 4, 6, 8, 12.

Prosti brojevi

Broj $p \in N$, $p>1$ je prost ako su mu 1 i p jedini djelitelji, tj. ako ima samo trivijalne djelitelje. Ako broj nije prost onda je složen. Broj 1 nije niti prost niti složen.

Osnovna teorema aritmetike:

$\forall n \in N$, n>1 postoji jedinstven rastav na proste faktore:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Gdje su $p_1 < p_2 < \ldots < p_k$ te su svi p_i prosti brojevi.

Euklidova teorema:
Skup svih prostih brojeva je beskonačan, tj. ne postoji najveći prosti broj.

Kongruencije

Piše se a≡b (mod m) (a i b su cijeli brojevi, m pozitivan), ako i samo ako je m|(a-b) tj. a i b daju isti ostatak pri dijeljenu sa m (a mod m = b mod m).

Relativno prosti brojevi

Brojevi a i b su relativno prosti ako je najveći zajednički djelitelj brojeva a i b jednak 1, tj. brojevi a i b nemaju zajedničkih faktora.

Eulerova phi finkcija

Eulerova funkcija Φ(m) se definiše kao broj brojeva ≤m koji su relativno prosti u odnosu na m.
Ako je p prost broj tada je:

$$\Phi(m) = p - 1$$

Ako su m i n relativno prosti tada je:

$$\Phi(mn) = \Phi(m)\Phi(n)$$

Ako se m može rastaviti na proste faktore

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

tada se Φ(m) može računati po slijedećoj formuli:

$$\Phi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

Eulerova teorema:
Ako su a i m relativno prosti tada vrijedi $a^{\Phi(m)}=1(\text{mod } m)$.
Posebno za proste brojeve vrijedi: $a^{m-1}=1(\text{mod } m)$

DUŽINA KLJUČEVA

Dužina ključeva za algoritam RSA uobičajeno je 1024 bita. Kriptovanje sa 512 bitova više se ne smatra sigurnim. Za potpunu sigurnost preporučuje se 2048 odnosno 4096 bitova. Na slici 4.3.22 prikazan je par ključeva, javni i privatni ključ, dužine 1024 bita. U prikazanim ključevima dodat je i identtifikator algoritma.

Privatni ključ

```
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2
0d83 463d e493 bab6 06d3 0d59 bd3e c1ce 4367 018a 21a8 efbc
ccd0 a2cc b055 9653 8466 0500 da44 4980 d854 0aa5 2586 94ed
6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1
463d 1ef0 b92c 345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7
8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd e6b7 a991
942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b2f0 1cd5 5ffb
6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16
6c89 2aca da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629
4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a
54fb ff78 41bc bd71 28f4 bb90 bcff 9634 04e3 459e a146 2840
8102 0301 0001
```

Javni ključ

```
3082 01e4 f267 0142 0f61 dd12 e089 5547 0f08 4ccb 0542 00e2
0d83 463d e493 bab6 0673 0d59 bf3e c1ce 4367 012a 11a8 efbc
ccd0 a2cc b055 9653 8466 0500 da44 4980 d8b4 0aa5 2586 94ed
6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1
463d 1df0 b92c 345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7
8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd e6b7 a991
942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b250 1cd5 5ffb
6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16
6c89 2aca da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629
4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a
54fb ff78 41bc bd71 28f4 bb90 bcff 9634 04de 45de af46 2240
8410 02f1 0001
```

Slika 4.3.22 Primjer javnog i tajnog ključa dužine 1024 bita + identifikator algoritma

Ključeve dužine 512 bitova nije moguće probiti na današnjim personalnim računarima. Postoje složeni računarski sistemi koji mogu probiti 512-bitni RSA u razumnom vremenu, međutim radi se o vrlo skupim i teško dostupnim sistemima.

Prilikom odabira dulžine ključa treba voditi računa o tome koliko nam je zapravo važna sigurnost informacije koju kriptujemo. Dužinu ključa biramo tako da naša poruka ostane tajna dovoljno dugo. Na primjer, ako želimo zaštiti neku običnu poruku od potpunog laika potpunu sigurnost možemo postići najprimitivnijim tehnikama kriptovanja. Ako pak želimo zaštiti neke vrlo važne podatke kao kreditne kartice, bankovne račune, …, državne tajne tada moramo koristiti najbolje i najsigurnije računarske metode. Prilikom izrade računarskih sistema i odabira dužine ključa potrebno je uvijek konsultovati i najnovije trendove na području računarske sigurnosti.

Preporučene dužine ključeva za asimetrične algoritme date su u Tabeli 4.3.7.

Minimalna Sigurna	Optimalna	Preporučena	US1*	US2**
1024	2048	4096	1024	512

Tabela 4.3.7 Preporučene dužine ključeva za asimetrične algoritme

(*) Zakonom dozvoljena dužina ključeva u SAD-u
(**) Zakonom dozvoljena dužina ključeva koju smije koristiti aplikacije koje se izvozi iz SAD-a

BRZINA ALGORITMA

U aplikacijama je često preporučljivo odabrati što manji eksponent (e), kao dio javnog ključa. Čak cijele grupe ljudi mogu koristiti isti e uz drugačiji modul (n). (Postoje određena ograničenja na faktore d i n kad je javni eksponent unaprijed odabran.) Ovaj način izbora ključeva ubrzava kriptovanje, a usporava dekriptovanje.

RSA je znatno sporiji od DES-a i ostalih simetričnih algoritama. DES je otprilike 100 puta brži u softverskim rješenjima i od 1,000 do 10,000 puta brži u raznim hardverskim rješenjima. U praksi, asimetrična kriptografija se često koristi u kombinaciji sa simetričnom kriptografijom. Tako, pošiljalac kriptuje poruku simetričnom kriptografijom, koristeći slučajno generisani tajni ključ, a taj tajni ključ kriptuje asimetričnom kriptografijom, koristeći javni ključ primaoca.

Postoje naznake da će u skoroj budućnosti razlika u brzini RSA i ostalih simetričnih algoritama smanjivati, ali takođe će doći i do ubrzanja svih algoritama uopšte.

SIGURNOST ALGORITMA

Sigurnost RSA algoritma se zasniva na tome što je faktorizacija proizvoda dva velika prosta broja težak matematički problem. Provođenje faktorizacije zahtijeva veliku procesorsku snagu i puno vremena.

"Sigurnost" ovdje ima čisto matamatičko značenje, i zavisi od konteksta u kojem se šema kriptovanja primjenjuje. Ne postoji šema asimetričnog kriptovanja koja se može oduprijeti napadaču sa neograničenom kompjuterskom snagom. Dokaz sigurnosti izvodi se uzimajući u obzir ograničene mogućnosti postojeće opreme za obradu podataka, i kaže se "šema ne može biti razbijena korišćenjem postojećeg desktop računara za recimo 1000 godina".

4.3.2.2 Digitalni potpis

Digitalni potpis je oblik alimetrične kriptografije koji se koristi kao zamjena za svojeručni potpis. Digitalni potpis obezbjeđuje autentičnost "poruke". Poruka može biti bilo što, od elektronskog pisma do ugovora [83, 84].

Šema digitalnog potpisa se sastoji od tri algoriutma:

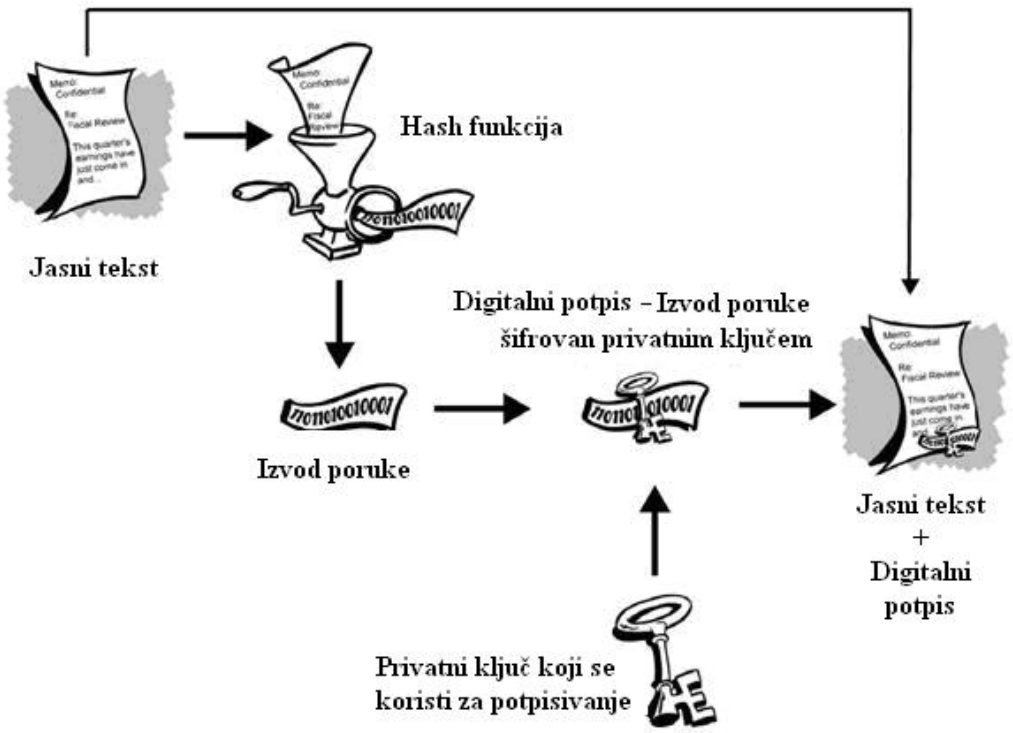
1. Algoritam za generisanje ključa – selektuje privatni ključ iz seta mogućih privatnih ključeva. Kao rezultat, ovaj algoritam vraća privatni i odgovarajući javni ključ.
2. Algoritam potpisivanja – iz date poruke i privatnog ključa generiše digitalni potpis.
3. Algoritam za verifikaciju potpisa – na osnovu potpisane poruke i javnog ključa obavlja verifikaciju digitalnog potpisa.

Digitalni potpis mora zadovoljiti dva osnovna zahtjeva. Prvi, potpis generisan iz fikne poruke i fiksnog privatnog ključa može se verifikovati jedino na toj poruci sa odgovarajućim javnim ključem. Drugi, treba biti računski neizvodljivo generisati validan potpis, od strane onog ko ne posjeduje privatni ključ.

POTPISIVANJE PORUKE

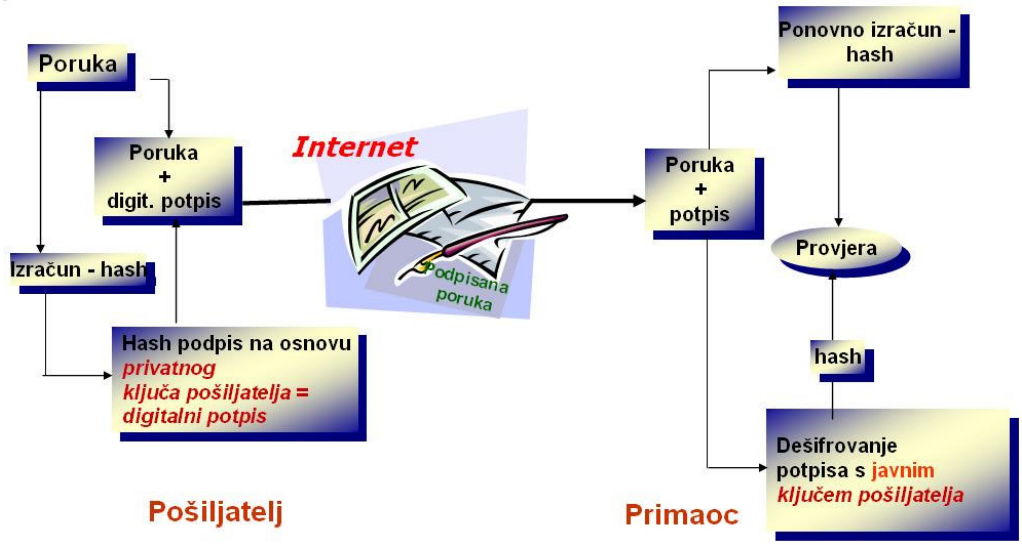
Na koji način se obavlja potpisivanje poruke digitalnim potpisom biće obješnjeno kroz primjer u kojem dvoje ljudi, A i B, žele razmijeniti potpisane poruke (podatke). Osobe A i B žele biti sigurne u identitet osobe od koje su poruku dobili. U sladu sa šemom digitalnog potpisa, obije osobe najprije kreiraju par komplementarnih ključeva, javni i tajni ključ. Nakon kreiranja ključeva, osobe A i B razmjenjuju svoje javne ključeve.

U cilju potpisivanja poruke, pošiljaoc (osoba A), koristi svoj tajni ključ za šifrovanje izvoda (sažetka) poruke. Sažetak poruke izračunat je nekom od «Hash» funkcija. Hash funkcija je funkcija koja iz zadane poruke (podataka) računa izvod (sažetak) fiksne dužine, obično od 128 do 256 bita (Slika 4.3.24).



Slika 4.3.24 Postupak potpisivanja poruke digitalnim potpisom

Kada primaoc (B) uspije dešifrovati sažetak poruke javnim ključem pošiljatelja (A), on računa i izvod primljene poruke. Izračunati izvod upoređuje sa dešifrovanim.



Slika 4.3.25 Ilustativni prikaz postupka slanja i prijema poruke sa digitalnim potpisom

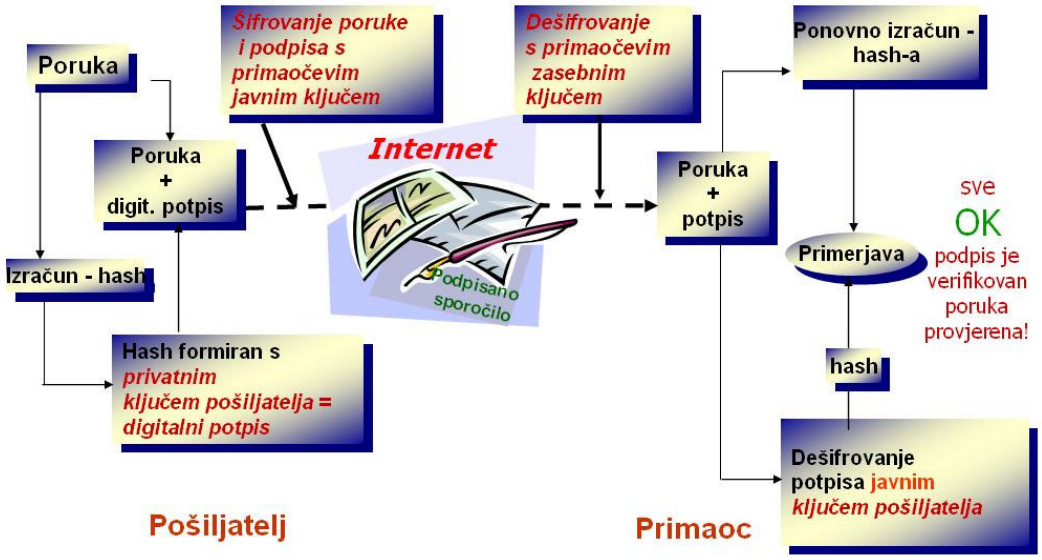
Ako je izračunati sažetak jednak onom dešifriranom, primaoc može biti siguran u porijeklo poruke (podataka). Ovo stoga jer je poruka mogla biti šifrovana jedino tajnim ključem pošiljaoca (A).

Osim autentičnosti primaoc može biti siguran i u integritet podataka u poruci. Ovo proističe iz toga što je izvod zavistan od sadržaja poruke. Svaka, i najmanja, izmjena poruke reflektuje se na vrijednoist izvoda. Prema tome, ukoliko bi poruka, od trenutka slanja do trenutka prijema, bila izmijenjena od stane trećeg lica izračunati i dešifrovani izvod se ne bi podudarili. Iz ovog proističe da je digitalni potpis različit od poruke do poruke i obezbjeđuje autentičnost svake riječi u dokumentu. Na Slici 4.3.26 prikazani su digitalni potpisi na različitim dokumentima dobijeni primjenom istog privatnog ključa (privatnog ključa iste osobe).

Slika 4.3.26 Digitalni potpisi na različitim dokumentima izvedeni primjenom istog privatnog ključa

TAJNOST POTPISANE PORUKE

Što uraditi ukoliko se osim autentičnosti poruke i integriteta podataka u poruci želi obezbijediti i tajnost poruke? U tom slučaju potrebno je da pošiljaoc potpisanu poruku šifruje primaočevim javnim ključem. S druge strane, primaoc, prije provjere potpisa, dešifruje pristiglu poruku svojim privatnim ključem (Skika 4.3.27).



Slika 4.3.27 Ilustativni prikaz postupka slanja i prijema šifrovane poruke sa digitalnim potpisom

RUČNI POTPIS – DIGITALNI POTPIS

Tabelom 4.3.8 dato je poređenje osobina ručnog i digitalnog potpisa.

Parametar	Papir	Electronika
Autentičnost	Može se krivotvoriti	Ne može se kopirati
Integritet	Potpis nezavistan od dokumenta	Potpis zavisi od sadržine dokumenta
Prihvatanje-odbacivanja	a. Potreban ekspert za rukopise b. Moguća greška	a. Svaki kompjuter b. Bez greške

Tabela 4.3.8 Poređenje osobina ručnog i digitalnog potpisa

4.3.2.3 Žaštita privatnog ključa

Kao što je već rečeno privatni ključ se mora čuvati u tajnosti. Najčešći načini čuvanja su:

- Na hard disku računara.
- Unutar pametne kartice.
- Unutar hardverskog modula (iKey) (Slika 4.3.28).

Slika 4.3.28 Uređaji koji se koriste za čuvanje privatnog ključa

Na hard disku računara šifrovani ključ se čuva u fajlu koji je zaštićen lozinkom. Ovo se smatra najnesigurnijim načinom čuvanja privatnog ključa. Ovo stoga što samim tim što se nalazi na hard diku, ključ dostupan a lozinka se može saznati ili razbiti.

Ukoliko se privatni ključ čuva u pametnoj kartici to podrazumijeva da se on generiše u kripto modulu kartice i ostaje u kartici. Ključ se čuva u memoriji kartice i veoma je bezbjedan jer je nikad ne napušta. Izvod poruke se šalje kartici na potis i potpis napušta karticu. Kartica obezbjeđuje prenosivost ključu, pa se potpisivanje može vršiti bilo gdje, gdje postoji čitač kartica.

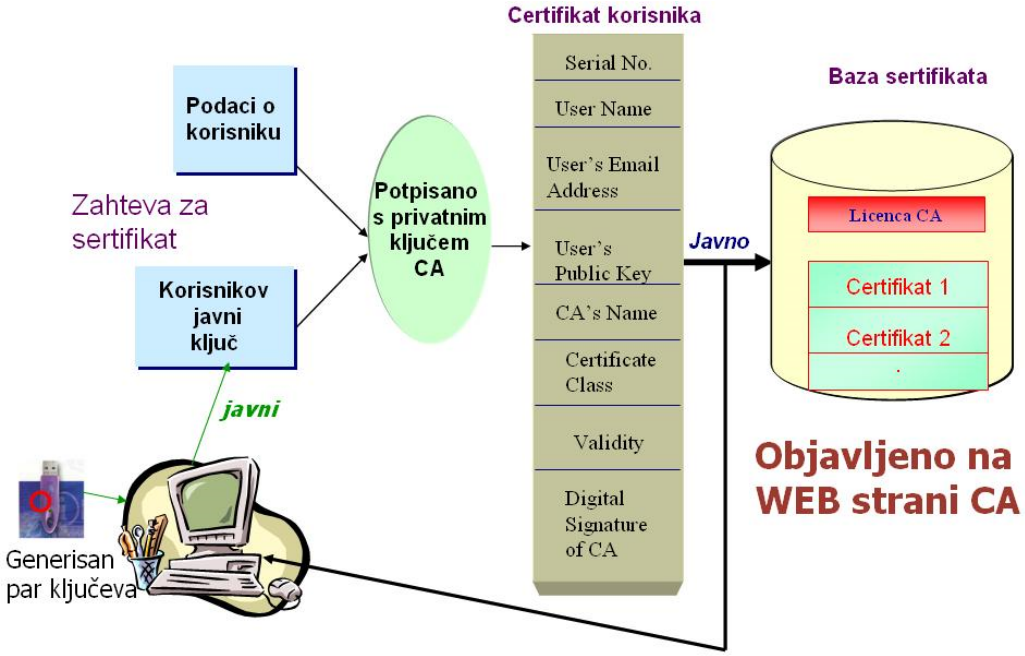
Čuvanjem privatnog ključa unutar hardverskog modula (iKey-a) postiže se funkcionalnost i zaštita slična pametnoj kartici. Kao prednost iKey-a može se navesti to on ne zahtijeva specijalni čitač već se može priključiti nas USB port računara.

4.3.2.4 Infrastruktura javnih ključeva

Unutar strukture asimetričnog kriptovanja postoji slaba karika na koju se mora ukazati. Ona se ogleda u nepostajanju sigurnosti da javni ključ za koji se smatra da pripada pošiljaocu (A) zaista i pripada njemu. Naime, ukoliko primaoc (B) ima javni ključ pošiljaoca (C), a vjeruje da ključ pripada pošiljaocu (A), tad je pošiljaoc (C) u mogućnosti zloupotrijebiti podatke pošiljaoca (A).

U cilju obezbjeđivanja apsolutne sigurnosti da javni ključ zaista pripada osobi za koju se smatra, uvodi se zastupna organizacija koja potvrđuje vezu između korisnika i njegovog javnog ključa. Ova organizacija se često

naziva CA (engl. "certifying authority"). Pretpostavka je da CA sve ostale stranke vjeruju, i da svoje javne ključeve lično donose na potpisivanje. Tom prilikom PS im uzima uobičajene lične dokumente. CA koristi svoj tajni ključ (javni ključ CA svima je poznat) za potpisivanje preuzetih podataka stranke. Na ovaj način CA garantuje svima ostalima zaiteresovanim strankama ispravnost potpisanog javnog ključa (Slika 4.3.29).



Slika 4.3.29 Postupak ovjeravanja javnog ključa stranke od strane CA

Postoji i druga mogućnost, a to je da CA svima generiše par ključeva, te uz prethodnu fizičku autentifikaciju, dodjeljuje ključeve. U tom slučaju svako ko bi htio provjeriti ispravnost potpisa osobe morao bi u bazi javnih ključeva (koju čuva CA) pronaći javni ključ te osobe i potom tim ključem pokušati dešifrovati primljene podatke. Nedostatak ovog drugog modela je taj što u tom slučaju CA posjeduje i tajne ključeve što predstavlja znatan sigurnosni problem.

Da bi mogla da obavlja sertifikaciju javnih ključeva svaka CA mora da zadovoljava sljedeće uslove:

- Mora biti javna i povjerljiva
- Mora imati precizno definisan postupak za izdavanje sertifikata.
- Stalan pristup izdatim sertifikatima.
- Stalan pristup ukinutim sertifikatima.
- Stalan pristup licenci dobijenoj od strane nadzornog organa (kontrolera)
- Izvještaj o procesu ovjeravanja (CPS) stalno dostupan na Web-u.
- Striktno poštovanje propisane regulative i uputstava.

Kao logičan izbor za CA nameću se državne ustanove, sudovi i javni bilježnici.

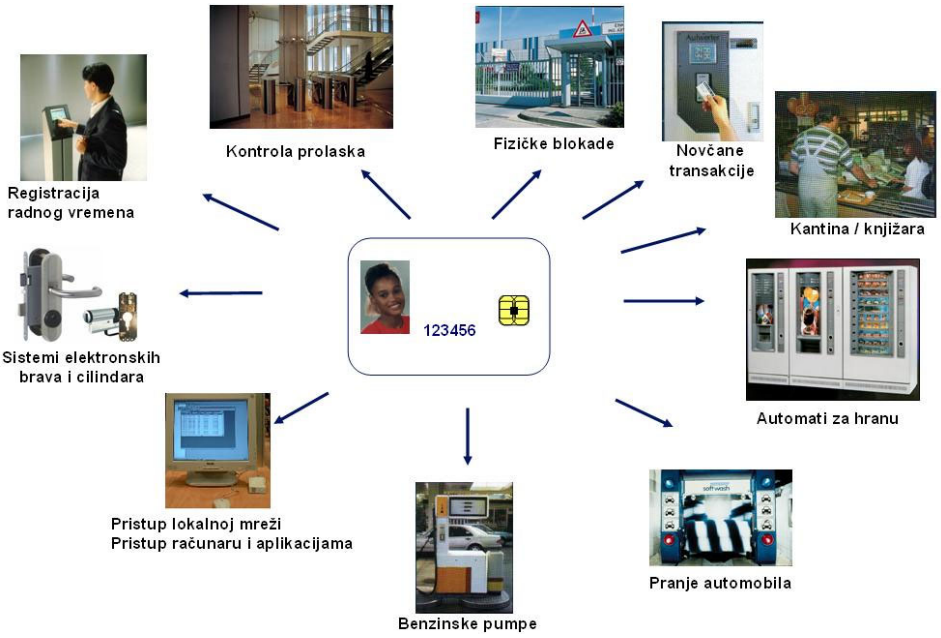
Privatni ključ od CA zahtijeva vrlo visok nivo sigurnosti. Za čuvanje privatnog ključa najčešće se koristi HSM (Hardware Security Module). HSM je smješten u strogo čuvanoj prostoriji sa video nadzorom 24 sati dnevno, 7 dana nedjeljno. Za pristup ovoj prostoriji kao HSM modulu potrebno je više od jedne osobe.

Za rad CA odgovoran je nadzorni odran, engl Controller. Nadzorni organ potvrđuje povezanost CA sa njenim javnim ključem. Nadzorni organ je jezgro sistema i on ovjerava tehnologiju, infrastrukturu i djelovanje CA. Nadzornik sam ovjerava svoj javni ključ.

4.4 PRIMJENE PAMETNIH KARTICA

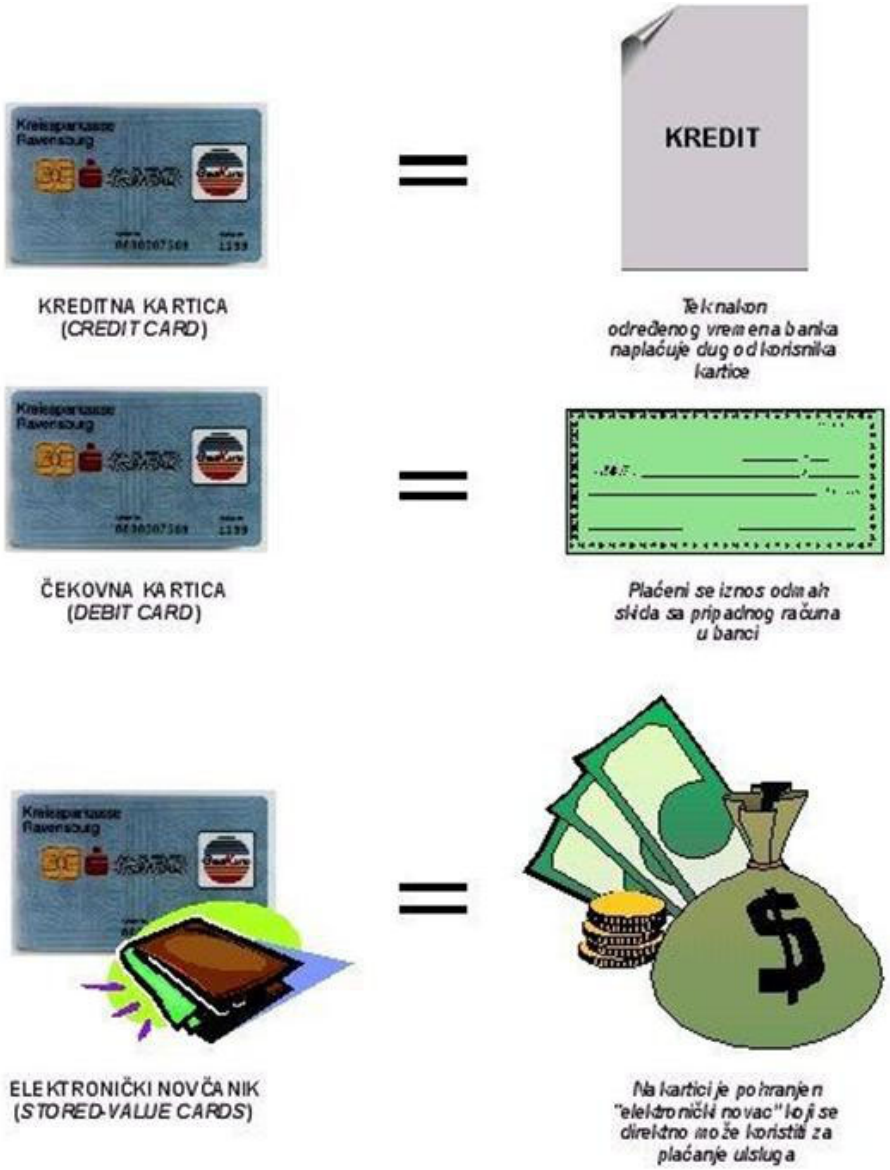
Primjene pametnih kartica su brojne (Slika 4.4.1). Mogu se koristiti:

- za novčane transakcije,
- kao zdavstvena knjižica,
- kao lična karta ili pasoš,
- za kontrolu pristupa,
- za evidenciju radnog vremena,
- za pristup lokalnoj računarskoj mreži, računaru ili aplikacijama,
- za automate za hranu,
- na parkinzima,
- na benzinskim pumpama,
- itd…



Slika 4.4.1 Primjene pametnih kartica

U novčanim transakcijama pametne kartice mogu biti:
- kreditne kartice (Credit Card),
- čekovne kartice (Debit Card) ili
- elektronski novčanik (Stored-Value Card) (Slika 4.4.2)



Slika 4.4.2 Pametne kartice kao finansijcke kartice

U primjeni kao zdravstvena kartica, pametna kartica donosi brojne prednosti u odnosu na tradicionalnu zdravstvenu knjižicu. Neke od njih su: Pomoću ličnog računara ljekar može pregledati i modifikovati podatke sa kartice.

- Pomoću personalnog računara ljekar može pregledati i modifikovati podatke sa kartice (Slika 4.4.3).

- Ljekar je u mogućnosti upoznati se sa istorijom pacijentove bolijesti, odnosno razlogom svake posjete ljekaru.
- Pametne kartice omogućavaju sigurno pohranivanje i brzo pretarživanje podataka.
- Izbjegava se upotreba velike količine papira.
- Eventualno oštećeni ili izgubljeni podaci se lako nadoknađuju kopijama na računarima.

Slika 4.4.3 Ljekar očitava pametnu karticu u cilju pregleda, modifikovanja ili dodavanja podataka.

Na slici 4.4.4 prikazana je francuska pametna zdravstvena kartica.

Slika 4.4.4 Pametna zdravstvena kartica u Francuskoj

Zamjena tradicionalnih ličnih karti pametnim karticama sve više uzima maha. U većini evropskih zemalja ovaj postupak je u toku ili je već završen. Na slici 4.4.5 prikazane su pametne lične karte u Beligiji i Španiji. Pametne lične karte su veličine bankovne kartice. Često se nazivaju i elektronske lične karte.

Slika 4.4.5 Pametne lične karte u Belgiji i Španiji

Na kartici su dati podaci kao:

- fotografija korisnika,
- ime i prezime, pol, ručni potpis,
- nacionalnost,
- mjesto i datum rođenja,
- broj lične karte i matični broj,
- datum izdavanja i datum isticanja roka važenja, ...

U cilju obezbjeđivanja od prostog kopiranja na tijelu pametne kartice umetnute su brojne zaštite, kao:

- reljefna stampa,
- tanke linije koje se teško kopiraju,
- promjenjiva laserska slika,
- optički promjenjivo mastilo,
- alphagram,
- laserska štampa,
- mikro slova,
- UV object,
- itd.

Pametna lična karta može sadržati kontaktni ili beskontaktni čip. U čipu se mogu smjestiti razni podaci vezani za korisnika kartice. U cilju identifikacije tu su biometrijski podaci (najčešće fingerprint). Osim njih kartica sadži i ključeve za asimetrično kriptovanje podataka. Komunikacija sa karticom je kriptovana. Privatni ključ korisniku obezbjeđivanje mogućnost digitalnog potpisivanja poruka, dokumenata, računa i sl..

Pametne kartice omogućavaju niz primjena koje nijesu bile moguće sa tradicionalnim ličnim kartama. Na primjer, zahvaljujući pametnim karticama, zvanični dokumenti kao što su izvod iz matične kljige rođenih, potvrda o državljanstvu, bračno stanje, materijalni status, itd. mogu se dobiti on-line bez potrebe za odlaskom u za to predviđenu ustanovu. Postoje i brojne druge primjene, među kojime su:

- siguran digitalni potpis,
- elektronsko glasanje,
- elektronsko slanje sudskih rješenja,
- on-line otvaranje bankovnog računa,
- on-line zahtjev za kredit,
- on-line registracija auta,
- autentifikovana pošta,
- autentifikacije za Web servise (siguran chat,...)
- kontrola pristupa objektima,
- elektronsko prikupljanje podataka,
- ...

Porast kriminala u svijetu kao i ilegalni ulasci u države korištenjem lažnih dokumenata, stvarju potrebu za unapređenje sigurnosti granica. Uvođenje elektronskog pasoša je jedna od mjera kojom se nastoje suzbiti ove pojave.

Elektronski pasoš je rješenje koje kombinuje tahnologiju pametnih kartica sa biometrijskom tehnologijom. U pasoš se ugrađuje bezkontaktni čip koji sadrži i biometrijske podatke korisnika. Na graničnom prelazu ovi podaci se očitavaju i porede sa biometrijskim podacima nosioca pasoša (Slika 4.4.6).

Osim povećanja sigurnosti granica, elektronski pasoš donosi i povećanje efikasnosti i ekonomičnosti u upravljanju velikom količinom podataka o

putnicima. Samim tim, elektroski pasoši doprinose ubrzanju procesa prelaska granice.

Slika 4.4.6 Elektronski pasoš i čitač elektronskog pasoša

GLAVA V

5. BIOMETRIJSKE IDENTIFIKACIONE TEHNIKE

5.1 UVOD

U biometrijskim identifikacionim sistemima prepoznavanje korisnika vrši se na bazi njegovih fizičkih i/ili karakteristika ponašanja. Samo ime biometrija potiče od grčkih riječi "bios", što znači - život i "metron", što znači - mjeriti.

Biometrijski sistemi se mogu podijeliti u dvije osnovne kategorije i to:

- sistemi zasnovani na prepoznavanju fizičkih karakteristika i
- sistemi zasnovani na prepoznavanju karakteristika ponašanja.

Trenutno ima preko 10 različitih biometrijskih identifikacionih tehnika (Tabela 5.1.1).

Biometrija	
Fizičke karakteristike	**Ponašanje**
Otisak prsta	**Prepoznavanje glasa**
Prepoznavanje lica	Potpis
Geomatrija šake	Način hodanja
Skenir. dužice oka	
Skeniranje mrežnjače	
DNA	
Vaskularni obrasci	

Tabela 5.1.1 Pregled osnovnih biometrijskih tehnika

Biometrijske identifikacione tehnike koje su u tabeli 5.1 ispisane tamnijom bojom, danas se najviše koriste i u njihov razvoj ulažu se najveći napori [85].

Jedna od najstarijih i najpoznatijih biometrijskih tehnologija je prepoznavanje otiska prsta [86]. Prvi identifikacioni sistemi ovog tipa razvijeni su još ranih šesdesetih godina prošlog vijeka. Do nedavno, ovi sistemi su dominantno korišteni u kriminalistici. Razvoj računarske tehnologije omogućio je proširenje spektra aplikacija. Danas su identifikacioni sistemi zasnovani na prepoznavanju otiska postali dobra alternativa tradicionalnim identifikacionim sistemima u mnogim državnim i

komercijalnim aplikacijama [87]. Pravilno korištena, tehnologija prepoznavanja otiska omogućuje visoku pouzdanost. Čitači otiska prsta mogu biti veoma mali, relativno niske cijene i lako se integrišu u tradicionalne identifikacione sisteme. Ipak, postoje i problemi. Jedan vid problema posljedica je velike izloženosti prstiju djejstvu spolješnje sredine. Posjekotine ili prljavština često otežavaju proces prepoznavanja. Drugi vid problema poljedica je mogućnosti relativno jednostavnog falsifikovanja otiska. Čitači otiska prsta, često, osim samog skeniranja otiska, raznim metodama pokušavaju prepoznati falsifikat (temperaturni test, test pulsa, test provodljivodti, itd.) [88, 89].

Prepoznavanje lica je jedna od najnovijih biometrijskih identifikacionih metoda. Njene osnovne prednosti su jednostavnost korištenja, nepostojanje potrebe za fizičkim kontaktom sa čitačem i mogućnost relizacije sistema na bazi korištenja postojeće tehnike široke namjene (u prvom redu web kamera) [90]. Međutim, postoje brojne poteškoće u procesu prepoznavanja lica. U odnosu na otisak prsta i dužicu oka, lice posjeduje manje detalja na osnovu kojih je moguće vršiti identifikaciju. Dodatan problem predstavlja velika vremenska promjenjivost karakteristika lica [91]. Ova tehnologija u poslednje vrijeme bilježi napredak, ali ipak do sada ima ograničenog uspjeha u praktičnim aplikacijama [92].

U tehnologiji geometrije šake prepoznaju se fizičke karakteristike šake i prstiju. Geometrija šake pruža dobar balans između mogućnosti i jednostavnosti upotrebe. Identifikacioni sistemi zasnovani na geometriji šake najšešće se koriste za kontrolu pristupa i u time/attendance sistemima [93]. Velika dimenzija skenera šake ograničava primjenu ove tehnologije. Tako, na primjer, tehnologija prepoznavanja geometrije šake najčešće se ne primjenjuje u kontroli pristupa kompjuterima ili kompjuterskim mrežama [94].

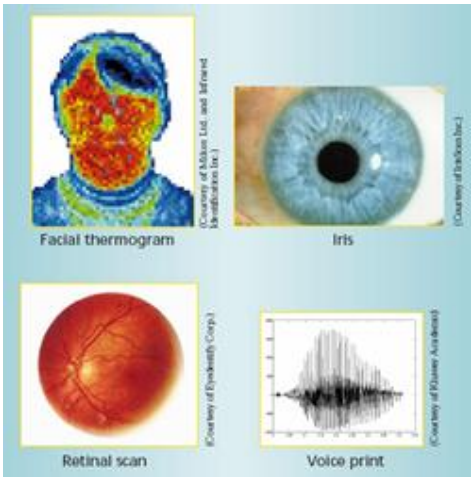
Tehnologijom skeniranja mrežnjače može se ostvarite visoka tačnost identifikacije. Međutim, prihvatanje od strane korisnika može predstavljati problem. Jedna od reakcija korisnika može biti - ″Ne dozvoljavam da laserski zrak usmjeravate u moje oko!″. U stvarnosti, u skeniranju mrežnjače ne koristi se laserski zrak, već vrlo nizak intezitet svjetla koji se smatra sasvim bezbjednim. Osnovna mana ove tehnologije je u potrebi za direktnim kontaktom korisnika sa čitačem. Ovo je prilično nepogodno za ljude koji nose naočari. Takođe, u javnim aplikacijama, postoji mogućnost prenošenja raznih infekcija među korisnicima. Drugi problem je što se korisnik mora fokusirati na datu tačku, jer svaka neoptimalnost u tom pogledu značajno smanjuje tačnost prepoznavanja [93, 95].

Tehnologija skeniranja irisa prevazilazi mnoge probleme koji postoje u tehnologiji skeniranja mrežnjače. Kako je iris vidljiv i sa odstojanja ne zahtijeva se dirktni kontakt sa čitačem a nije neophodno ni skidanje naočala. Tehnologija je zasnovana na prepoznavanju jedinstvenog obrasca irisa. Interesantno je da metod ne zavisi od boje irisa. Ovo je važno, zbog široko rasprostranjenog korištenja obojenih kontaktnih sočiva. Neki

proizvođači tvrde da će njihov sistem raditi čak i u prisustvu tamnih sučanih naočala [93, 96].

Zbog jednostavnosti upotrebe prepoznavanje glasa je, moguće, najpoželjniji metod od strane korisnika [97]. Međutim, implementacija je ekstrenmo teška. Iako se, u poslednje vrijeme, tehnologija prepoznavanja glasa značajno unaprijedila i dalje obiluje problemima [98]. Lokalna akustičnost, pozadinski šum, kvalitet mikrofona, nazeb, zabrinutost, užurbanost, ljutnja, svi ovi faktori mogu do te mjere izmijeniti čovječiji glas da njegovo prepoznavanje bude gotovo nemoguće. Osim toga, sistemi za prepoznavanje glasa su najzahtjevniji u pogledu vremena potrebnog za upis i prepoznavanje korisnika, kao i u pogledu potrebnog memorijskog prostora za smještanje profila glasa [99].

Na slici 5.1.1 dati su primjeri različitih biometrijskih karakteristika.



Slika 5.1.1 Primjeri različitih biometrijskih karakteristika

Korištenje bilo kojeg tipa biometrijskih identifikacionih sistema sadrži dvije etape. Prva etapa je proces upisivanja korisnika a druga etapa je proces prepoznavanja korisnika [94, 100].

U etapi upisivanja korisnika sistem se podučava da identifikuje datu osobu. Tokom ove faze biometrijski senzori skeniraju fizionomiju osobe i kreiraju njenu digitalnu reprezentaciju. Iz dobijene digitalne reprezentacije izdvajaju se najbitnije, najkompaktnije, najizražajnije karakteristike koje se nazivaju profil. Profil svakog korisnika se smješta u bazu podataka i dalje koristi za prepoznavanja. Baza podataka biometrijskog sistema može biti centralizovana ili distribuirana. Čest slučaj distribuirane baze podatka je kada se profil korisnika nalazi na njegovoj ″pametnoj″ ID kartici.

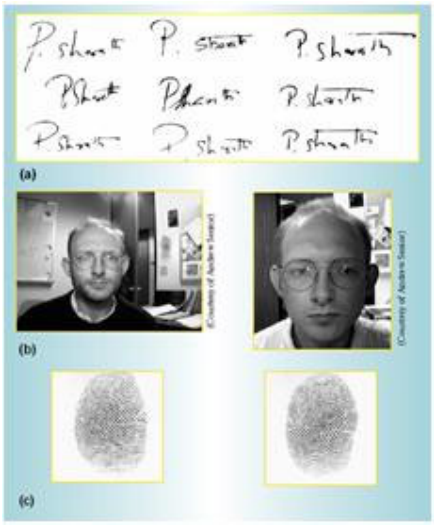
Da bi profil bolje odgovarao realnosti, biometrijske karakteristike se skeniraju više puta. Kada je riječ o prepoznavanju otiska prsta, da bi se dobio profil koji je u znatnoj mjeri nezavistan od položaja prsta prema skeneru, skeniranje se vrši tri do četiri puta za različite orijentacije prsta prema skeneru [89].

Obzirom, da je memorijski prostor za smještanje informacija o profilu, u ovim sistemima često ograničen (npr. u sistemima u kojima se informacije o profilu smještaju u ″pametnu″ karticu), uobičajeno je da se podaci profila kompresuju prije upisivanja [101].

U identifikacionoj fazi vrši se prepoznavanja korisnika. U toku identifikacije profil trenutno skenirane osobe se poredi sa profilima iz baze podataka. U slučaju poklapanja karakteristika sa nekim od snimljenih profila zaključuje se da je osoba prepoznata i dozvoljava joj se zahtijevana akcija. U nekim slučajevima, umjesto poređenja sa snimljenim profilima, vrši se samo verifikacija je li se osoba tačno predstavila [100].

I pored prednosti koje biometrijski identifikacioni sistemi imaju u odnosu na klasične identifikacione sisteme potrebno je uložiti još puno napora za njihovo unapređenje. To se u prvom redu odnosi na pouzdanost, brzinu rada, cijenu kao i jednostavnost upotrebe [102].

U klasičnom identifikacionom sistemu sa lozinkom, unošenje tačne lozinke uvijek rezultira prihvatanjem od strane sistema. Međutim, u biometrijskim identifikacionim sistemima ne može se garantovati da će identifikacija uvijek biti uspješno obavljena. Ovo zavisi od puno faktora, među kojima su, šum kod biometrijskih senzora, ograničenja primijenjene metode za obradu podataka, i možda i najviše, varijacije u biometrijskim karakteristikama [94]. Na Slici 5.1.2 ilustrovane su moguće varijacije u potpisu, licu i otisku prsta jedne te iste osobe.

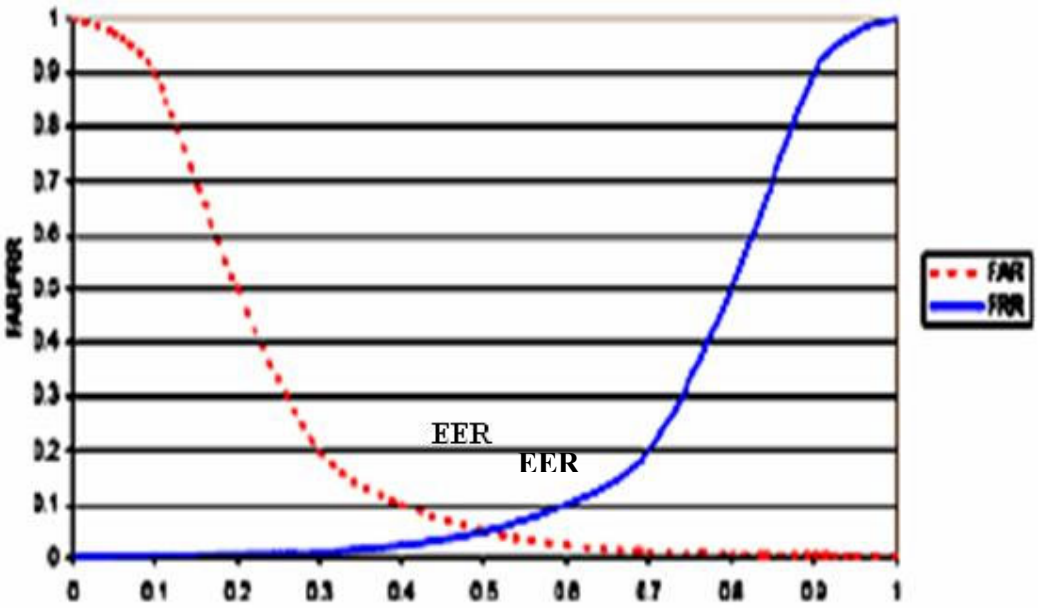


Slika 5.1.2 Promjenjivost je nerazdvojivo vezana sa svim tipovima biometrijskih karakteristika

Varijacije biometrijskih karakteristika čine neophodnim definisanje određene margine greške između posmatranih i snimljenih karakteristika iste osobe. Uvođenje margine greške povećava mogućnost obmanjivanja sistema. Drugim riječima, može se desiti da sistem prihvati osobu koja nema to pravo. Definisanje optimalne margine nije jednostavan posao. Ako

se predvidi premala margina greške, sistem će često odbacivati i osobe koje treba prihvatiti, dok u slučaju dopuštanja prevelike margine greške, osobe bez prava će biti prihvatane. Procenat odbacivanje osoba koja imaju pravo na datom sistemu naziva se FRR (False Reject Rate). Procenat prihvatanja osoba bez prava naziva se FAR (False Accept Rate). Prilikom realizacije biometrijskog sistema, cilj je minimizirati kako FRR tako i FAR. Nažalost ova dva odnosa nijesu nezavisna (Slika 5.1.3).

Sistemi za prepoznavanje treba da zadovolje uslov da mogućnost pojave ovih grešaka bude svedena na minimum.

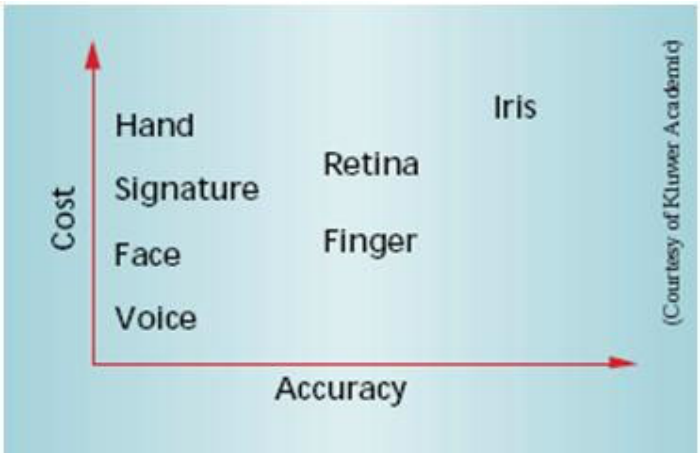


Slika 5.1.3 FAR/FRR i njihova presječna tačka EER (CER)

Vrijednost od FAR i FRR na mjestu u kojem se krive sijeku zove se jednaki udio grešaka – EER (engl. Equal Error Rate) ili prelazni odnos greške – CER (Cross-over error rate). Ova karakteristika predstavlja jednu od najustaljenih mjera kvaliteta biometrijskog sistema. Preciznost sistema je veća što je EER (CER) manji.

Optimalna margina greške se mora tražiti uzimajući u obzir specifičnosti same aplikacije. Odluka o iznosu margine greške zavisi od svrhe biometrijskog sistema i predstavlja kompromis između upotrebljivosti i sigurnosti. Niža margina greške znači da će sistem rigoroznije obavljati poređenje trenutno unešenih podataka što će smanjiti broj pogrešnih prihvaćanja i vrijednost FAR-a, ali će povećati broj pogrešnih odbijanja i proporcionalno FRR. Što znači da u praksi uvijek postoji raskorak između ovih grešaka i smanjenje FAR-a ujedno znači povećanje FRR-a [103, 104].

Poređenje cijene implementacije i pouzdanosti različitih tipova identifikacionih sistema dato je na Slici 5.1.4.



Slika 5.1.4 Poređenje cijene primjene i tačnosti rada pojedinih biometrijskih identifikacionih metoda

U praksi, biometrijski identifikacioni sistem se često kombinuje sa nekim klasičnim identifikacionim sistemom. Na primjer, u kontroli pristupa, često se istovremeno koriste RF identifikator i otisak prsta (fingerprint) ili nek drugi biometrijski identifikacioni mehanizam. Za autentifikaciju korisnika kompjutera često se osim korisničkog imena i lozinke zahtijeva i provjera otiska prsta korisnika. U slučaju identifikacije putem telefonske linije često se uz čovjekovo znanje (lozinka i lične informacije) vrši i prepoznavanje čovjekovog glasa. Korištenjem dva identifikaciona faktora - ″nešto što znaš″ (″nešto što posjeduješ″) i ″nešto što si″ omogućuje dobijanje optimalnog stepena sigurnosti. Sadjejstvom klasičnih i biometrijskih identifikacionih sistema umnogome se prevazilaze mnogi nedostaci kako jednih tako i drugih. Klasični identifikacioni sistem potpomognut biometrijskim sistemom oslobađa se nedostatka jednostavne kompromitacije koja se ogleda u povjeravanju neovlaštenom licu tuđeg korisničkog imena i lozinke ili ustupanjem tuđe ID kartice. S druge strane biometrijski identifikacioni sistemi potpomodnuti klasičnim ID sistemom lakše prevazilaze nedostatak nesigurnog prepoznavanja korisnika uzrokovanog varijaciom biometrijskih karakteristika [105].

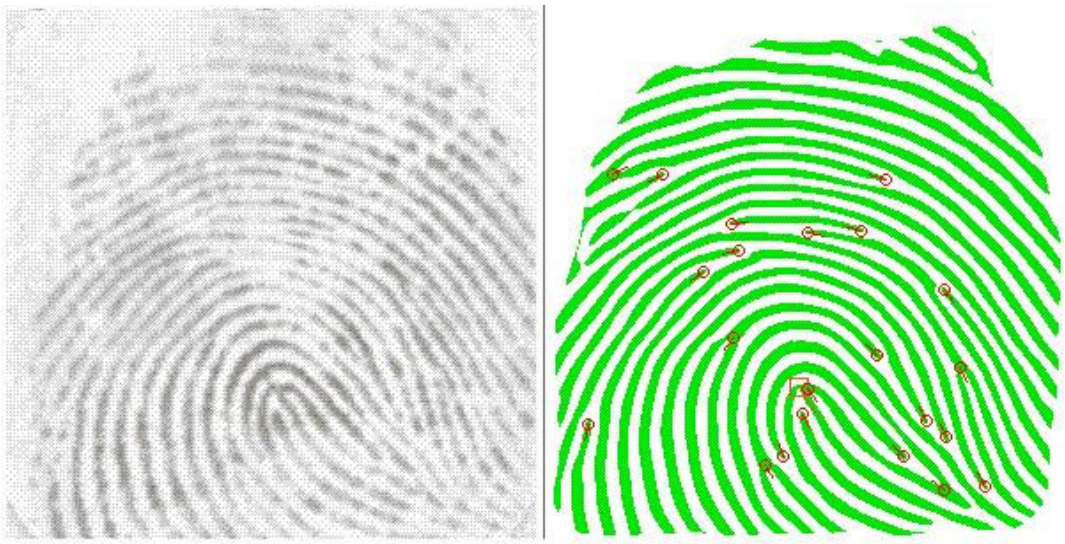
Osim sistema dobijenih kombinacijom klasičnog i biometrijskog načina identifikacije, postoje i multibiometrijski sistemi. U ovim sistemima identifikacija se vrši na osnovu prepoznavanja više biometrijskih karakteristika [106].

U daljem tekstu, ovog poglavlja, biće više riječi o biometrijskim identifikacionim metodama prepoznavanja oriska prsta, prepoznavanja dužice oka, prepoznavanja karakteristika lice i prepoznavanja karakteristika glasa.

5.2 PREPOZNAVANJE OTISKA PRSTA

Otisak prsta je jedinstven za svakog čovjeka i može se upotrijebiti za provjeru njegovog identiteta [107]. U prošlosti se otisak prsta najčešće koristio u kriminalistici. Danas, automatsko prepoznavanje otiska prsta postaje sve popularnije. Uređaji za prepoznavanje otiska koriste se u sistemima za kontrolu pristupa fizičkim lokacijama, kompjuterskim mrežama, bankovnim računima, ili registraciju prisustva radnika u preduzećima [89, 108].

Prepoznavanje otiska prsta prostim poređenjem sa drugim, već poznatim otiscima, nije preporučljivo jer često ne daje tačan rezultat. Razlozi za pojavu greški su smetnje prilikom uzimanja otiska, ogrebotine i druga oštećenja kože u dijelu sa kojeg se uzima otisak, zatim različita pozicija prsta prema skeneru, kao i deformacija otiska tokom procedure skeniranja. Mnogo bolji način prepoznavanja otiska je izdvajanje detalja, takozvanih karakterističnih tačaka sa slike otiska prsta. Karakteristične tačke su tačke gdje se linije otiska granaju ili završavaju (Slika 5.2.1). Prepoznavanje otiska se vrši upoređivanjem skupa karakterističnih tačaka trenutno uzetog otiska sa skupovima karakterističnih tačaka već poznatih otisaka.



Slika 5.2.1 Karakteristične tačke sa otiska prsta

Uopšte uzevši otisak prsta sadrži oko 100 karakterističnih tačaka, dok dio otiska koji se obuhvata skenerom ima između 30 i 40 karakterističnih tačaka. Već preko 100 godina pravosudni organi kao i kriminalističke službe čitavog svijeta koriste karakteristične tačke na otisku prsta za identifikaciju osoba. U evropskim sudovima identifikacija se smatra vjerodostojnom ukoliko se najmanje 12 karakterističnih tačaka identifikuje u otisku. Izbor 12 karakterističnih tačaka često se naziva ″pravilo 12 tačaka″ [109]. Pravilo 12 tačaka je ekperimentalno definisano, na bazi

činjenice da u uzorku od čak 10 miliona ljudi nije bilo dva čovjeka sa istih 12 karakterističnih tačaka [110]. Najveći broj trenutno komercijalno raspoloživih skenera prepoznaje otisak prsta na osnovu 8 karakterističnih tačaka. Sa ovim brojem karakterističnih tačaka proizvođači garantuju FAR odnos 1:1000000.

Obrada slike otiska prsta zahtijeva sofisticirane algoritme za, eliminisanje šuma, izdvajanje karakterističnih tačaka i obezbjeđenje rotacione i translacione tolerancije. Istovremeno, algoritmi moraju biti što je moguće brži da bi se mogli uspješno primijeniti u aplikacijama sa velikim brojem korisnika. U slučaju kada se algoritmi za prepoznavanje otiska žele primijeniti u mikročipu, kompaktnost algoritma i mali utošak memorije takođe postaju važni [89].

5.2.1 ISTORIJAT

Čovjek je još od najranih vremena postao svjestan otiska svog prsta. O tome nam najbolje svjedoče arheološke iskopine još iz neolita, gdje su pronađeni predmeti na kojima se nalaze otisci prstiju (Slika 5.2.2).

Slika 5.2.2 Neolitsko doba

Do prve praktične primjene otiska prsta došlo se u starom Vavilonu. Naime, otisak prsta na glinenim tablicama korišćen je prilikom poslovnih transakcija.

Značajniji pomak u proučavanju otiska prsta dolazi tek krajem XVIII vijeka, kada je Njemački ljekar i anatom Mayer detaljno opisao karakteristike papilarnih linija (ispupčenja koja se nalaze na čovjekovom prstu) . Na Slici 5.2.3 prikazan je crtež koji je napravio Mayer, na kome se vidi detaljna struktura reljefa prsta.

Slika 5.2.3 Mayer-ov crtež

Prvu klasifikaciju otisaka prsta dao je Češki anatom *Jan Purkinje* (1823. godine), tako što ih je podijelio u 9 klasa, saglasno konfiguraciji ispupčenja i udubljenja na prstu (Slika 5.2.4) .

Slika 5.2.4 Purkinje-ova klasifikacija

Naredni korak napravio je škotski naučnik *Henry Faulds* koji je prvi uočio mogućnost primjene otiska prsta pri identifikaciji osoba (1880. godine). On je, takođe, sugerisao individualnost otiska prsta.

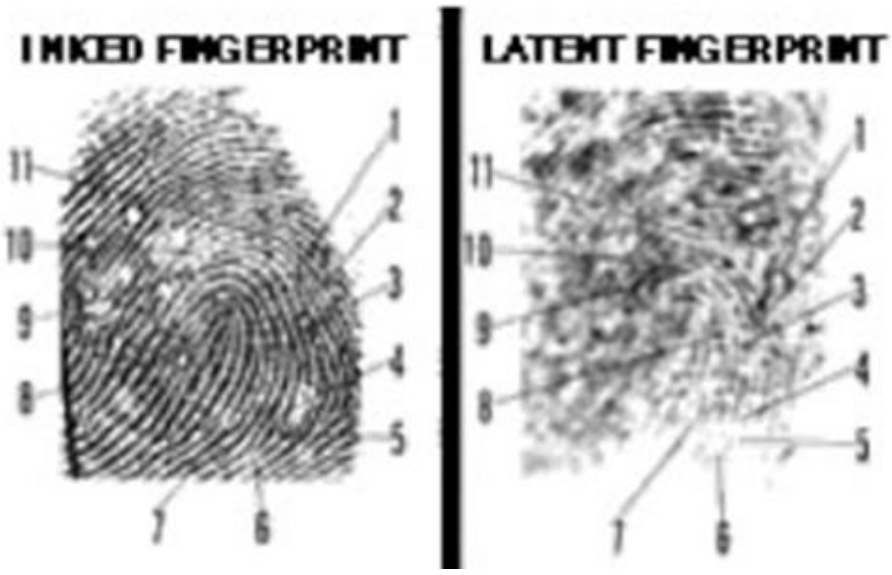
1888. godine, engleski naučnik *Sir Francis Galton* ustanovio je individualnost i stalnost otiska prsta. On je takođe uključio i karakteristike minucija (minutiae) prilikom poređenja otisaka. Municija predstavlja skup svih detalja koji se odnose na razne oblike pojavljivanja papilarnih linija.

Argentinski antropolog i policijski inspektor *Juan Vucetich* (rođen na Hvaru) prvi je praktično počeo da primjenjuje rezultate *Galton*-ovih

istraživanja i zaključaka. 1891. godine on je oformio prvu kartoteku otisaka prstiju.

Slika 5.2.5 Detalj iz Vicetich-eve kartoteke

Godine 1897. počela je primjena otiska prsta u kriminalistici. Početkom XX vijeka, tačnije 1901. godine u okviru Scotland Yard-a formiran je prvi biro za otiske prstiju. Francuski ljekar i pravnik, Edmond Locard, je 1918. godine utvrdio i predložio 12 identičnih tačaka na otisku prsta, kao dovoljan uslov za uspješnu identifikaciju (Slika 5.2.6). On je, između ostalog, definisao i princip forenzičke nauke, koji glasi: "Svaki kontakt ostavlja trag" (Every Contact Leaves a Trace). Škotski detektiv Bertie Hammond je 1931. godine osnovao u Škotskoj (Glazgov) prvo odjeljenje za otiske prstiju.



Slika 5.2.6 12 karakterističnih tačaka

Konačno, 1991. godine počinje primjena računara u oblasti prepoznavanja otisaka prstiju. Te godine je u SAD-u uveden prvi

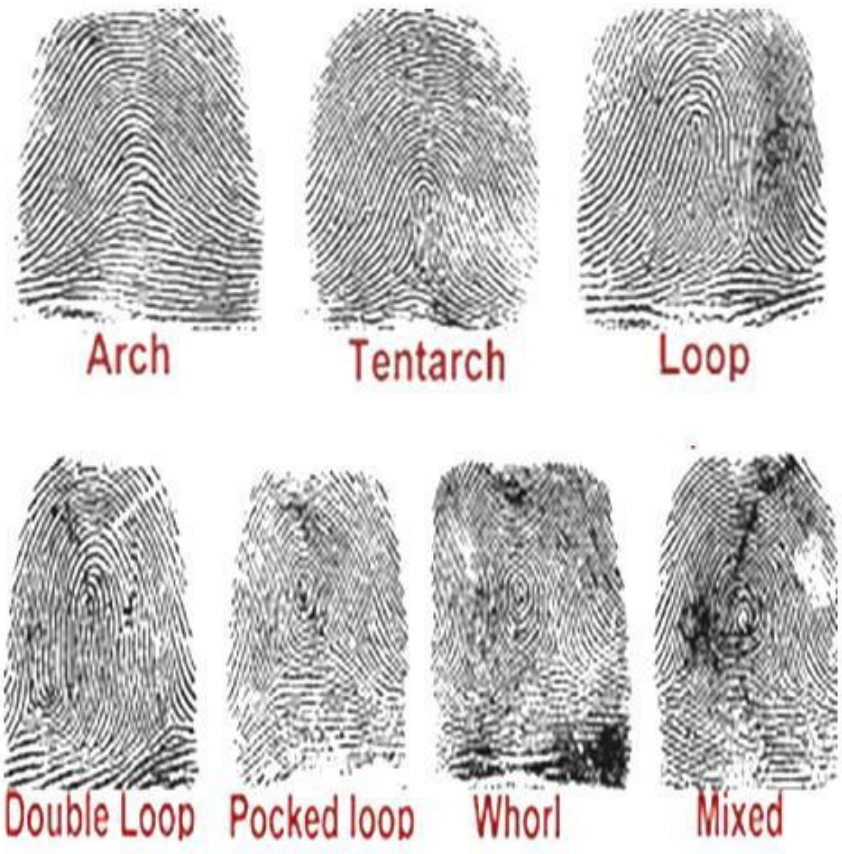
ralunarski sistem za prepoznavanje otiska prsta – *Automatic Fingerprint Recognition System* (AFIS).

Danas postoje brojni računarski sistemi za prepoznavanje otiska prsta. Za postupak verifikacije i identifikacije postoji više standarda. Najpoznatiji je onaj koji je propisao američki NIST (National Institute of Standards and Technology). Ovaj postupak identifikacije je široko rasprostranjen.

5.2.2 KARAKTERISTIKE OTISKA PRSTA

Kao sto je već rečeno,otisak prsta sa fiziološkog aspekta predstavlja konfiguraciju ispupčenja i udubljenja. Linije koje formiraju ispupčenja nazivaju se papilarne linije. Njihova nepromenljivost i individualna varijantnost čini da se otisak prsta može koristiti za identifikaciju. Papilarne linije se čak i kod monozigotnih blizanaca razlikuju.

Jedna od osnovnih klasifikacija otiska prsta jeste ona na osnovu morfološkog rasporeda papilarnih linija. Prema ovoj klasifikaciji razlikujemo sedam osnovnih tipova otiska prsta, i to: luk (*arch*), jeloviti luk (*tentarch*), petlja (*loop*), dvostruka petlja (*double loop*), jamičasta petlja (*pocked loop*), spirala (*whorl*) i mješoviti (*mixed*) (Slika 5.2.7).



Slika 5.2.7 Tipovi otiska prsta

Procentualna zastupljenost pojedinih tipova otiska prsta u ljudskoj populaciji je sledeća:

- petljasti tipovi (petlja, dvostruka petlja i jamičasta petlja) oko 60%,
- spiralni tip oko 30%,
- lučni tipovi (luk i jeloviti luk) oko 5% i
- miksovani tip oko 5%.

Tip otiska prsta predstavlja globalnu karakteristiku otiska prsta. U pravilu 12 karakterističnih detalja, jedan detalj je tip otiska.

Osim tipa otisaka, kao globalne karakteristike, otisak prsta sadrži mnoge specifične detalje. Ovi detalji su lokalne karakteristike i veoma su bitne za klasifikaciju i prepoznavanje. Detalji se često nazivaju terminusi ili singularne tačke. Singularne tačke daju preostalih 11 detalja u pravilu 12 karakterističnih detalja.

Singularne tačke su mjesta na otisku prsta gdje dolazi do promjene u papilarnim linijama. Na Slici 5.2.8 istaknute su neke singularne tačke.

Slika 5.2.8 Najčešće singularne tačke na otisku prsta

Značenje pojmova sa slike 5. je sledeće: *crossover* – ukrštanje, *core* – središte, *bifurcation* – račva,
ridge ending – kraj linije, *island* – ostrvo, *delta* – delta i *pore* – pora.

Postupak identifikacije otiska prsta može se podijeliti u dvije etape:

- svrstavanje u određeni tip otiska na osnovu tipa otiska,
- identifikacija na osnovu lokalnih karakteristika (singularnih tačaka).

Do sada je prepoznato oko 150 različitih singularnih tačaka na otisku prsta. To su često sitni detalji na brazdama otiska koje često nije moguće

lako i pouzdano izdvojiti. Dvije najčešće singularne tačke, koje se najlakše detektuju prikazane su na Slici 5.2.9. To su:

- završetak brazde i
- račva ili grananje brazde.

Slika 5.2.9 Najčešće i najuočljivije singularne tačke

Osobine koje papilarne linije čine veoma pogodnim i sigurnim pri identifikaciji su sljedeće:

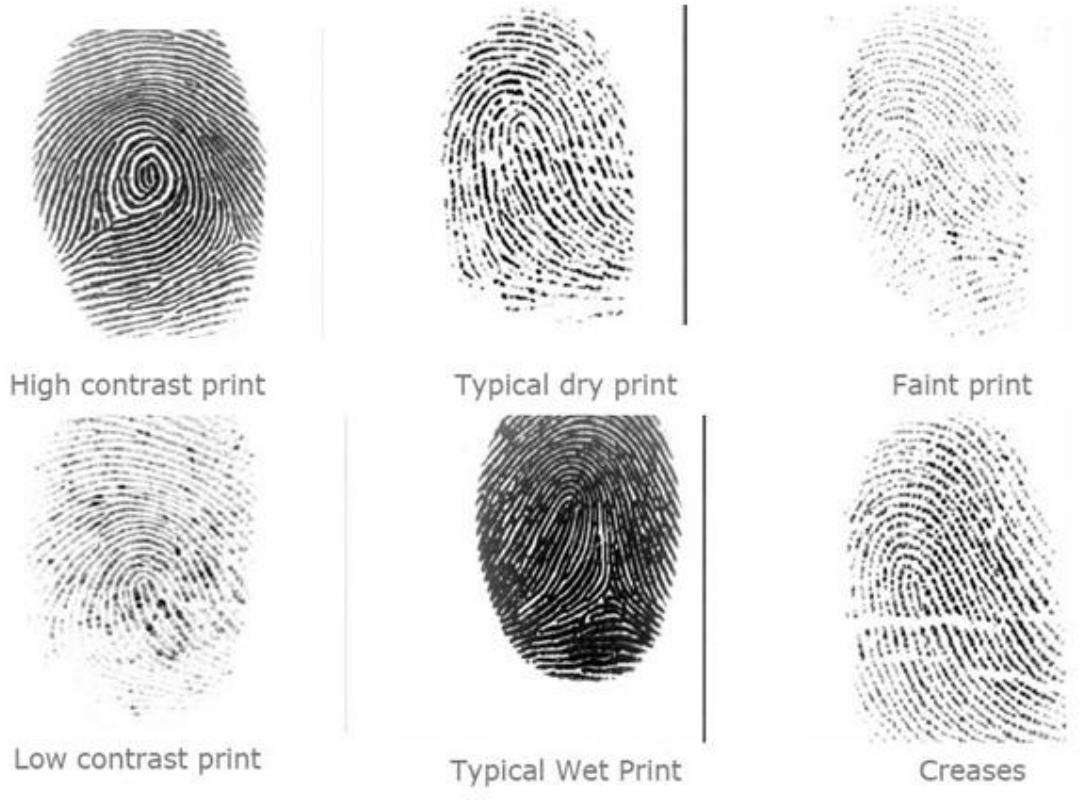
1. Nepromjenljivost broja i rasporeda minucija. Niko ne može svojevoljno izmijeniti izgled papilarnih linija već ih samo trajno uništiti;
2. Neponovljivost – Postoji veliki broj detalja (minucija). Ne postoji mogućnost da se dva otiska podudaraju. Francuski matematičar *Baltasar* je matematičkim putem dokazao da je takva vjerovatnoća praktično jednaka nuli;
3. Grupisanje – Vrlo važna osobina otisaka prstiju koja omogućava njihovu klasifikaciju na osnovu opštih (globalnih) sličnosti, što dovodi do znatnog smanjenja vremena potrebnog za identifikaciju.

5.2.3 POSTUPAK ANALIZE OTISKA PRSTA

Postupak prepoznavanja otiska prsta može se podijeliti u nekoliko faza i to:

- Skeniranje prsta.
- Obrada rezultata skeniranje – poboljšanje kvaliteta snimka (redukcija šuma), binarizacija, istanjivanje.
- Izdvajanje karakteristika (obrazac, karakteristični detalji, uklanjanje lažnih detalja).
- Upoređivanje.

U fazi skeniranja prsta dobija se snimak otiska prsta. Snimak može biti različitog kvaliteta (Slika 5.2.10) i potrebno je izvršiti njegovu obradu.

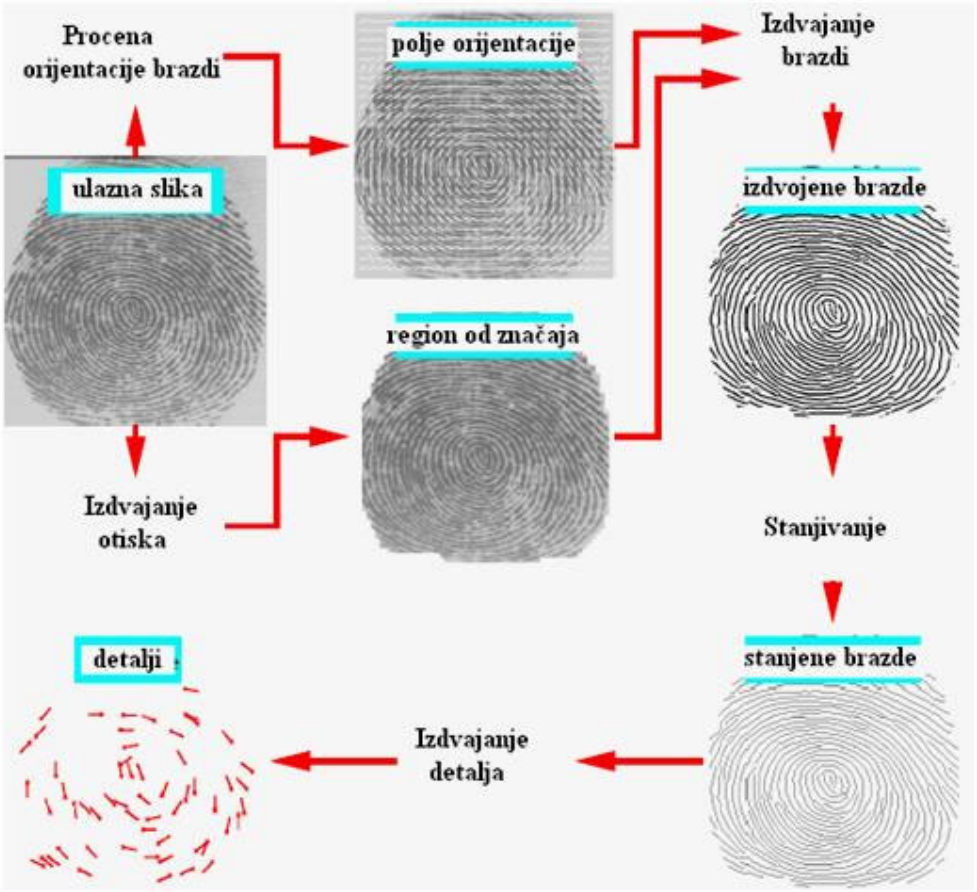


Slika 5.2.10 Snimci otiska prsta mogu biti različitog kvaliteta

Obrada snimka se vrši u sljedećim fazama:

- izdvajanje regiona otiska,
- proračun polja orijentacije i
- izdvajanje i istanjivanje brazdi

Po dobijanju istanjenih brazdi vrši se izdvajanje karakterističnih detalja (Slika 5.2.11).



Slika 5.2.11 Šematski prikaz postupka analize otiska prsta

IZDVAJANJE REGIONA OTISKA

Izdvajanje regiona otiska predstavlja segmentaciju ulazne slike kojom se region od značaja (foreground) odvaja od pozadinskog dijela slike koji ne nosi informacije značajne za dalju obradu.

Sastoji se od nekoliko koraka. Prvo se na osnovu standardne devijacije slike grubo procijeni region koji sadrži otisak prsta. Intenzitet slike normalizuje se koristeći srednju vrijednost i standardnu devijaciju ove oblasti. Zatim se cijela slika binarizuje uzevši za prag polovinu srednje vrednosti normalizovane slike. Prije formiranja maske za izdvojeni region otiska, koristi se median filtar da bi se uklonili nepoželjni so i biber šum koji može biti prisutan u binarizovanoj slici. Vrijednost koju daje ovaj filtar je srednja vrijednost unutar odabranog prozora

Dobar metod za segmentaciju slike treba da ispuni sledeće karakteristike:

- da je neosjetljiv na kontrast slike
- da otkrije zaprljane ili zone sa šumom i
- da rezultati segmentacije ne zavise od kvaliteta slike.

PRORAČUN POLJA ORIJENTACIJE

Orijentisanost brazdi otiska prsta predstavlja jednu od najvažnijih osobina slike otiska prsta. Određivanje polja orijentacije odnosno uglova kojima se brazde prostiru duž slike otiska veoma je važno za dalju obradu slike. Sliku najprije dijelimo na blokove. Rezultat dobijamo u jednom prolazu, bez iteracija.

Najvažniji koraci proračuna polja orjentacije brazdi u otisku prsta su sljedeći:

1. Izračunavanje gradijenta slike. Određivanje ivica preko gradijenta svodi se na traženje amplituda gradijenta. Procedure koje se koriste su Sobelov gradijentni operator ili filtriranje gradijentom Gausovog filtra. Oba filtra rade dijeljenje u jednom i glačanje u ortogonalnom smjeru. Detaljnije informacije o ovim filtrima mogu se naći u -knjizi "The Image Processing Handbook" od John C. Russ ili na adresi http://dsp.etfbl.net/dip/predavanja/5asegmentacija.pdf . Na ovaj način se dobiju dvije matrice koje sadrže gradijent slike duž x i y ose, δx i δy respektivno.

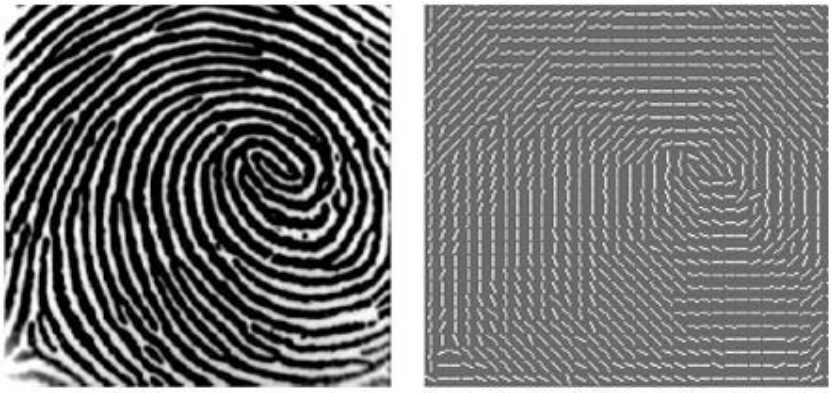
2. Pomoću sljedećih formula dobija se procjena polja orijentacije:

$$V_x(i,j) = \sum_{u=1}^{w}\sum_{v=1}^{w} 2 \cdot \partial_x(u,v) \cdot \partial_y(u,v)$$

$$V_y(i,j) = \sum_{u=1}^{w}\sum_{v=1}^{w} \left(\partial_x^2(u,v) - \partial_y^2(u,v) \right)$$

$$\theta(i,j) = \frac{1}{2} \cdot \tan^{-1}\left(\frac{V_x(i,j)}{Vy(i,j)} \right)$$

gde θ predstavlja aproksimaciju orijentacije brazdi metodom najmanjih kvadrata, dok (i,j) predstavlja označeni pixel a w predstavlja dužinu bloka.



Slika 5.2.12 Ulazna slika i njeno polje orijentacije

Procijenjene orijentacije brazdi prikazane na Slici 5.2.12. Usljed prisustva šuma, oštećenja brazdi i sličnog prikazane orijentacije mogu sadržati i grešku. Kako se orijentacije brazdi sporo mijenjaju u okolini jedne tačke, možemo primijeniti NF filtriranje kojim se ublažavaju postojeće nepravilnosti i nagle promjene u lokalnom polju orijentacije.

Da bismo izvršili NF filtriranje, polje orijentacije prvo pretvaramo u kontinualno vektorsko polje, definisano formulama :

$$\phi_x = \cos(\ 2 * \theta\ )$$
$$\phi_y = \sin(\ 2 * \theta\ )$$

Zatim na ϕ_x i ϕ_y primenjujemo Gausov NF filtar i dobijamo filtrirane komponente ϕ'_x i ϕ'_y.

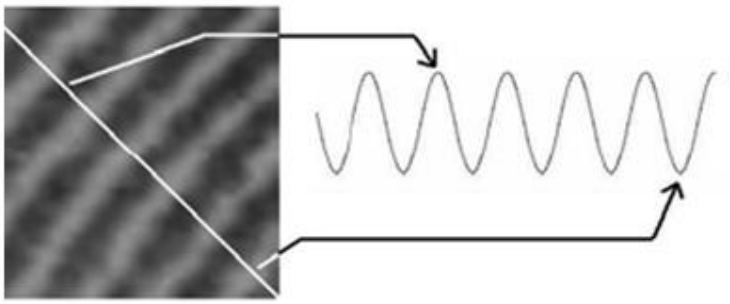
Zatim računamo orijentaciju brazdi *O* pomoću filtriranih x i y komponenti vektorskog polja ϕ'_x i ϕ'_y.

$$O = \frac{1}{2} \cdot \tan^{(-1)}\left(\frac{\phi'_x}{\phi'_y}\right)$$

IZDVAJANJE I ISTANJIVANJE BRAZDI

U malom, izdvojenom dijelu slike otiska prsta naizmjenično se prostiru svjetlije i tamnije pruge. One odgovaraju udubljenjima i ispupčenjima na koži prsta i formiraju približno dvodimenzionalnu sinusoidu predstavljenu na Slici 5.2.13. Brazde unutar manjeg regiona imaju izraženu lokalnu

frekvenciju i lokalnu orijentaciju, što omogućava lakše detektovanje piksela koji opisuju brazdu.



Slika 5.2.13 Udubljenja i ispupčenja formiraju sinusoidu

Izdvajanje teksture[1] brazdi vršimo primjenom Gaborovog filtra. Primjenom ovog filtra snižava se FRR ispod 2% a FAR ispod 0.01% (vidi poglavlje 6). Više o Gaborovom filtru može se naći u [6].

Parno simetričan Gaborov filtar u prostornom domenu ima sljedeći oblik :

$$G(x,y) = \exp\left[-\frac{1}{2}\cdot\left(\frac{x^2}{\partial_x^2}+\frac{y^2}{\partial_y^2}\right)\right]\cdot\cos(2\cdot\pi\cdot u_0\cdot x)$$

gdje je u_0 frekvencija sinusnog talasa duž x ose, a ∂x i ∂y su standardne devijacije Gausove anvelope duž x i y ose respektivno. ∂x i ∂y su empirijski utvrđene [112].

Gaborov filtar proizvoljne orijentacije dobija se rotacijom filtra datog prethodnim izrazom u x-y koordinatnom sistemu. Gaborovi filtri su i frekvencijski selektivni i selektivni za orijentaciju u teksturi. Ove filtre propusnike opsega koristimo za izdvajanje brazdi služeći se svojstvom da Gaborov filtar orijentacije θ izdvaja brazde koje se prostiru duž pravca θ + π/2 .

Prije filtriranja određujemo frekvenciju slike unutar blokova 32 x 32 piksela, jer kao što je već pomenuto, unutar manjih oblasti izražena je lokalna frekvencija brazdi. Eksperimenti su pokazali da je za dalju obradu najefikasnije da se usvoji frekvencija koja je median (srednja) vrijednost frekvencija određenih po blokovima slike.

Određeni region slike filtrira se filtrom čija orijentacija najbolje odgovara lokalnoj orijentaciji tog regiona. Filtriranjem slike postiže se jasnija struktura brazdi i povećava se robusnost algoritma za izdvajanje detalja u odnosu na kvalitet ulazne slike (Slika 5.2.14).

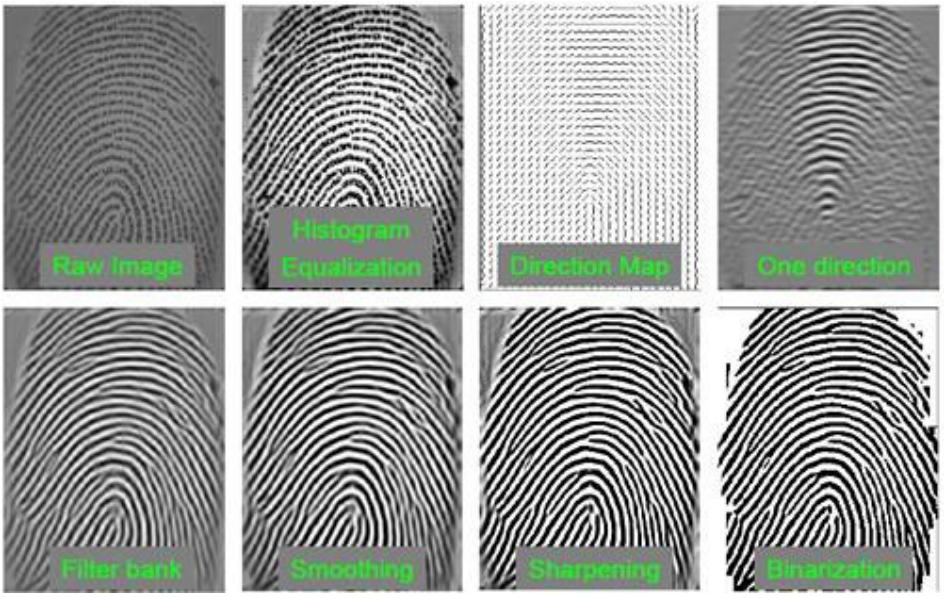
[1] prostorno organizovani pikseli koji se ne mogu opisati bojom ili lokalnim intenzitetom

Nakon postupka izdvajanja brazdi dobijena slika otiska prsta obrađuje se primjenom jednog od sljedeća dva metoda:

- metod baziran na binarizaciji ili
- metod baziran na skali sivog.

Kod metode binarizacije može doći do gubitka nekih informacija (singularnih tačaka) jer se u binarizaciji prilično grubom aproksimacijom dodjeljuju vrijednosti pikselima. Često se najtamniji piksel konvertuje u jedinicu dok ostali prelaze u nulu.

Drugom metodom se u znatnoj mjeri prevazilazi ovaj problem ali je metoda komplikovanija za implementaciju i troši više vremena pri izvršenju.

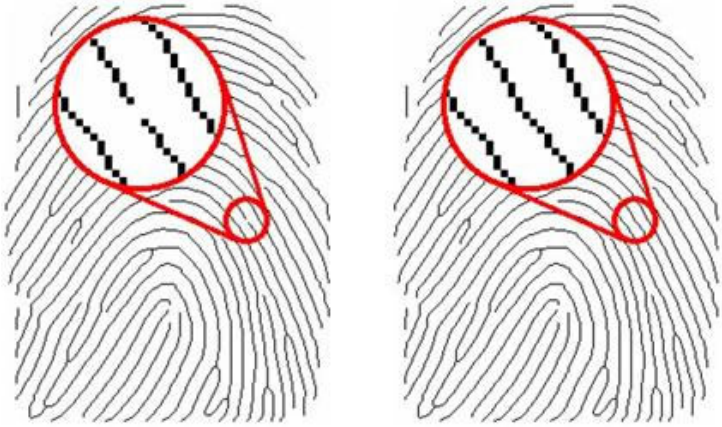


Slika 5.2.14 Faze prilikom obrade otiska prsta

Nakon binarizacije vrši se istanjivanje brazdi (Slika 5.2.15). Na kraju dobijamo sliku otiska sa stanjenim brazdama, čija je širina jedan piksel.

Slika 5.2.15 Stanjivanje brazdi u binarizovanoj slici otiska prsta

Poslednji korak podrazumijeva analizu slike u smislu detekcije i popunjavanja praznina u istanjenim papilarnim linijama (Slika 5.2.16).



Slika 5.2.16 Detekcija i popunjavanje praznina u istanjenim brazdama (papilarnim linijama)

IZDVAJANJE DETALJA

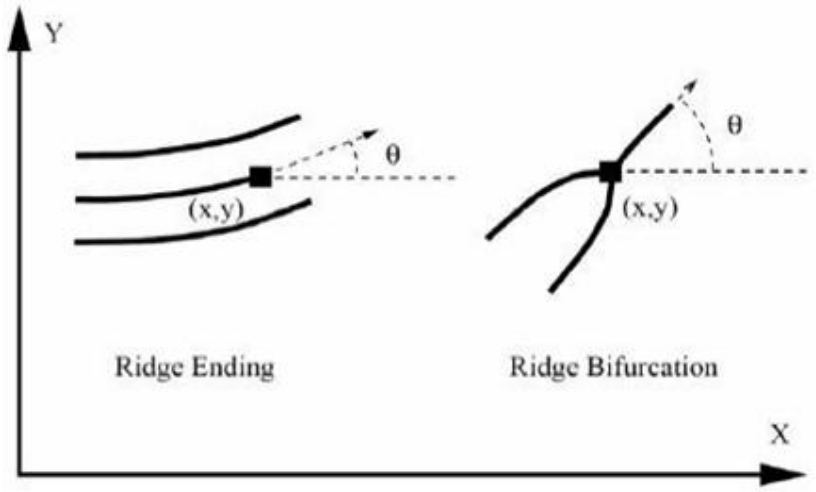
Kada su papilarni linije (brazde) široke svega 1 pixel prepoznavanje singularnih tačaka vrši se jednostavnim izračunavanjem na malom broju pixela, prema formuli:

$$sum = \sum_{u=-1}^{1} \sum_{v=-1}^{1} SB\,(i+u,\ j+v)$$

SB je matrica u koja sadrži vrijednost svakog piksela sa obrađene slike otiska prsta stanjenih brazdi. Ako je SB(i,j)=1 ukoliko je riječ o pikselu brazde (papilarne linije), dok ako je SB(i,j)=0 radi se o pikelu udubljenja. Ukoliko je dobijena suma sum=2 onda pixel(i,j) predstavlja završetak brazde, a ako je sum>3 onda pixel(i,j) označava grananje brazde (Slika 5.2.17).

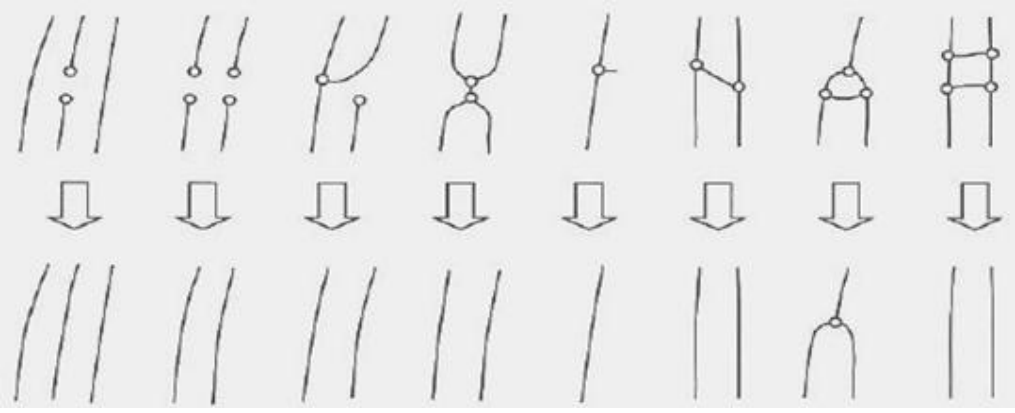
Slika 5.2.17 Detalji sa obrađene slike otiska prsta stanjenih brazdi

Svaki izdvojeni detalj, svaka singularna tačka, u digitalnoj prezentaciji otiska prsta (fingerprintu) opisuje se tipom, pozicijom (njegovim x i y koordinatama) i orijentacijom koja odgovara orijentaciji brazde na kojoj je detalj detektovan – ugao θ. (Slika 5.2.18).



Slika 5.2.18 Parametri kojima se opisuje singularna tačka

Dobar algoritam za izdvajanje detalja treba da precizno određuje poziciju i orijentaciju detalja kao i da ne unosi lažne detalje, a izostavlja prave. Takođe, dobar algoritam će lažne detalje unesene oštećenjem otiska prsta (posjekotine) registrovati i rekonstruisati ih na osnovu osobina brazdi. Na primjer, nemoguće je da se na kraju brazde identičnom putanjom nastavlja druga. U ovom slučaju algoritam treba da nadoveže datu brazdu. Veoma je bitno da algoritam uoči i eliminiše lažne karakteristične (Slika 5.2.19). Ispunjenje ovih zahtjeva zavisi od kvaliteta ulazne slike. Slike otiska lošeg kvaliteta će, zavisno od stepena oštećenja, biti ili poboljšane dodatnom obradom prije izdvajanja detalja, ili u najgorem slučaju biti odbačene.



Slika 5.2.19 Uklanjanje lažnih detalja

KLASIFIKACIJA

Klasifikacija otiska predstavlja proces svrstavanja posmatranog otiska u neki od osnovnih tipova (arch, loop, whorl, itd.). Pravilno klasifikovanje može u mnogome ubrzati prepoznavanje (uparivanje) otiska. Ovo se uglavnom odnosi na fazu poredjenja fingerprinta uzetog otiska sa fingerprintovima otisaka iz baze podataka.

5.2.4 UPARIVANJE

U fazi prepoznavanja fingerprinta ulaznog otiska prsta, on se poredi sa postojećim fingerprintovima iz baze podataka. Ovaj proces je poznat pod nazivom uparivanje fingerprintova. Poređenje fingerpreintova se vrši korištenjem prostorne distance *sd*. Ovaj parametar mora biti manja od partikularnog praga za dva fingerprinta koji su deklarisani kao upareni.

$$sd(m_j^{'}, m_i) = \sqrt{\left(x_j^{'} - x_i\right)^2 + \left(y_j^{'} - y_i\right)^2}$$

gdje $m_i = \{x_i, y_i, \theta_i\}$ predstavlja karakterističnu tačku i koja sadrži x-y kordinatu i ugao θ sklopljen sa x-osom pri čemu i = 1...m i $m_j^{'} = \{x_j, y_j, \theta_j\}$ koji predstavlja karakterističnu tačku j takođe sadrži x-y kordinatu i ugao θ sklopljen sa x-osom pri čemu j = 1...n .

Drugi prametar koji se računa je razlika smjera dd . *dd* se izračunava po formuli:

$$dd\ (m_j^{'}, m_i) = \min(|\ \theta_j^{'} - \theta_i\ |, 360\ ^{\circ} - |\ \theta_j^{'} - \theta_i\ |)$$

I *dd*, kao i *sd*, mora biti manji od praga odlučivanja.

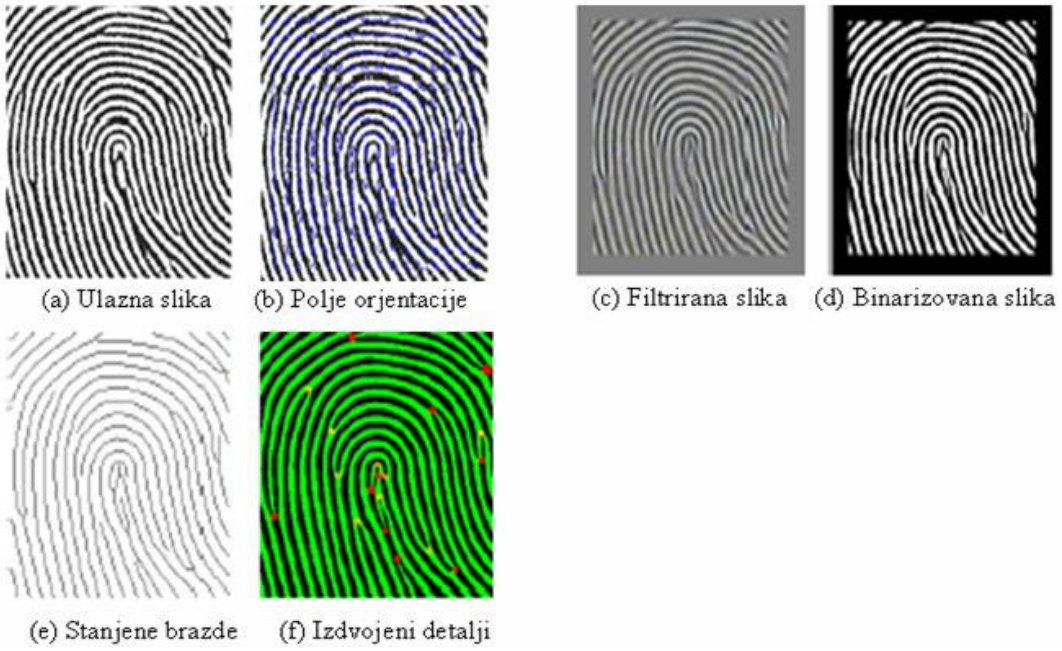
Ukoliko postoji određenena korelacija izmedju figerptintova, tada se transformacijama skaliranja i rotacije *sd* i *dd* mogu minimizirati.

5.2.5 TESTIRANJE ALGORITMA

Za testiranje algoritma koriste se dvije grupe otisaka prstiju. Prvu grupu čine otisci dobijeni pomoću demo programa Fingerprint Creator kompanije Optel. Ovaj program kompjuterski generiše slike otiska prsta, sa mogućnošću podešavanja više parametara kao što su kategorija otiska (četiri mogućnosti), broj detalja u slici, ugao rotiranosti slike i dr. Slike su binarne, veličine 256x256 piksela. [112]

Rezultati eksperimenata pokazuju da ovaj algoritam uspješno izdvaja prosečno 85% detalja koji postoje u ulaznoj slici. Ovaj dobar rezultat postiže se zahvaljujući činjenici da su brazde u ulaznoj slici bez oštećenja, jasno izražene kao i da je cijela slika bez šuma. Na Slici 20(a-f) prikazane su slike koje algoritam za izdvajanje detalja generiše kada se primijeni na sliku dobijenu pomoću Fingerprint Creator-a.

U ovom primjeru otisak prsta na ulaznoj slici po kategoriji pripada petlji u desno i generisan je sa 20 detalja. Algoritam je izdvojio ukupno 19 detalja koji su prikazani kao crvene tačke na Slici 5.2.20(f).



Slika 5.2.20 Prikaz slike otiska, generisanog demo programom Fingerprint Creator kompanije Optel, nakon rezličitih faza obrade

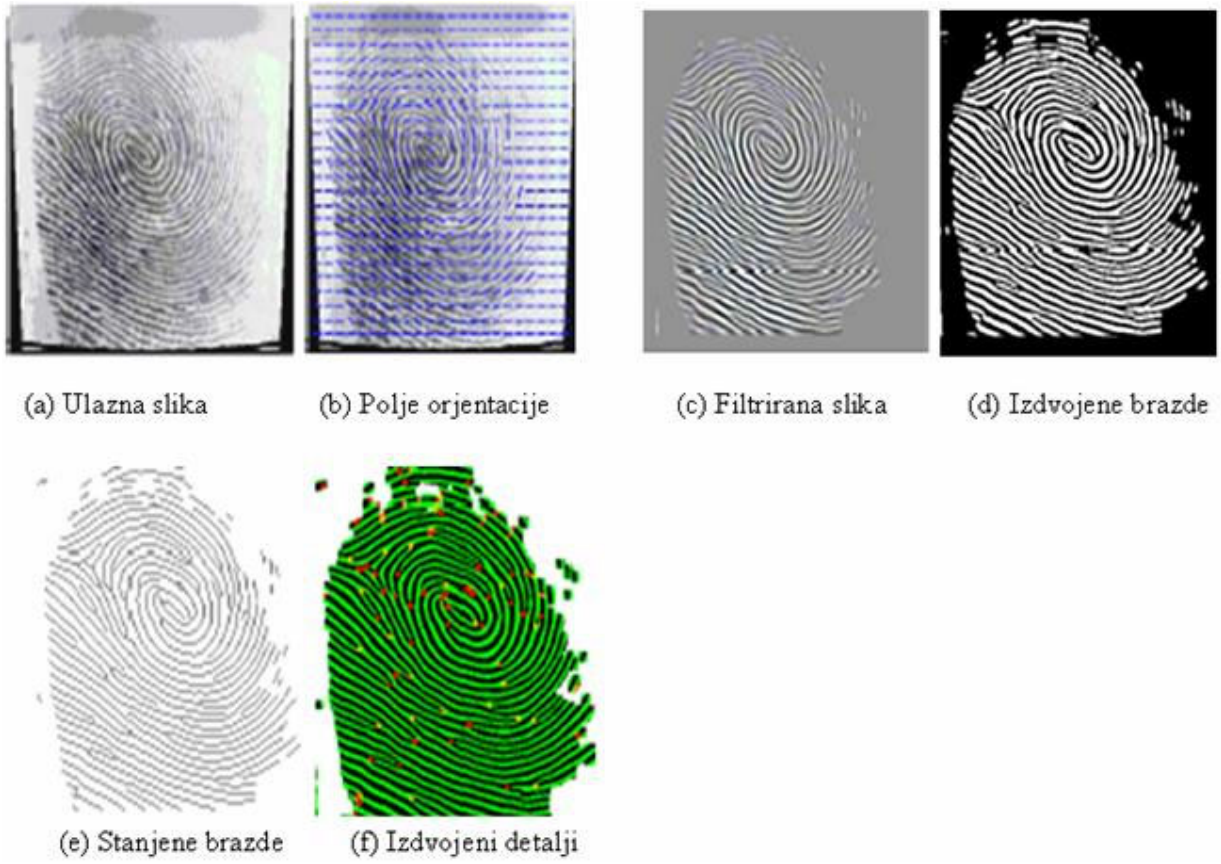
Drugu grupu čine otisci u VeriFinger bazi otisaka prstiju . Ova baza sadrži slike otisaka 40 prstiju tako što je za svaki prst uzeto po pet slika otisaka, ukupno 200 slika. Slike su veličine 360x364 piksela, sa rezolucijom 500 ppi (pixels per inch).

Za razliku od kompjuterski generisanih otisaka, ove autentične slike pokazuju sve teškoće preciznog izdvajanja brazdi i detalja iz slike otiska: slabo izražene brazde u pojedinim djelovima slike ili u cjelini, oštećene, prekinute i deformisane brazde, slika slabog kontrasta, slika oštećena šumom itd.

Filtriranjem bankom Gaborovih filtara čiji se parametri podešavaju prema ulaznoj slici, težimo da istaknemo pravu strukturu brazdi i interpolacijom rekonstruišemo brazde tamo gdje su oštećene.

Na sledećim slikama prikazane su slike koje algoritam za izdvajanje detalja generiše kad se primijeni na sliku otiska iz VeriFinger baze otisaka. Kao što se vidi na Slici 5.2.21(d) izdvojeni region otiska nije pravilnog

oblika i na njegovim granicama algoritam pravi greške generišući detalje koji odgovaraju lažnim završecima brazdi. Uprkos tome algoritam je u ovom primjeru izdvojio 29 detalja koji su karakteristika datog otiska prsta.



Slika 5.2.21 Prikaz slike otiska iz VeriFinger beze otisaka, nakon rezličitih faza obrade

5.2.6 TEHNIKE SKENIRANJA OTISKA PRSTA

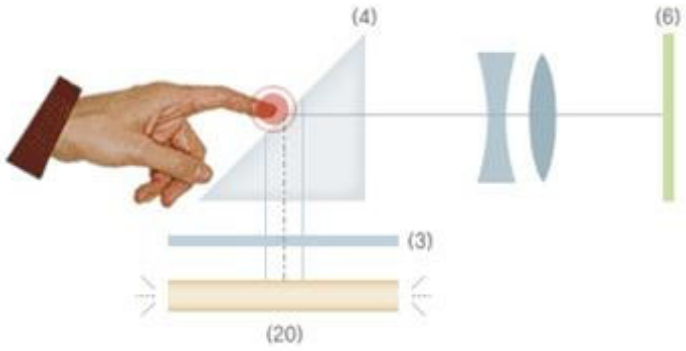
Čitači otiska prsta pojavili su se sredinom osamdesetih godina. Prva generacija čitača bila je zasnovana na upotrebi optičke tehnike za skeniranje prsta. Danas postoji više različitih tehnika skeniranja [89, 113].

Najčešće se srijeću sljedeći tipovi senzora:

- optički senzori sa CCD ili CMOS kamerama,
- ultarasonični senzori,
- poluprovodnički senzori električnog polja,
- poluprovodnički kapacitivni senzori,
- poluprovodnički temperaturni senzori.

Kada se koristi optički senzor, prst se pristisne na, za to predviđenu, pločicu. Nakon toga prst se osvijetli sa LED izvorom svjetlosti. Kroz

prizmu i sistem sočiva slika se projektuje na kameru (Slika 5.2.22). Kamera može biti CCD ili modernija CMOS. Upotrebom frame-grabber tehnike slika se snimi i spremna je za dalju analizu.



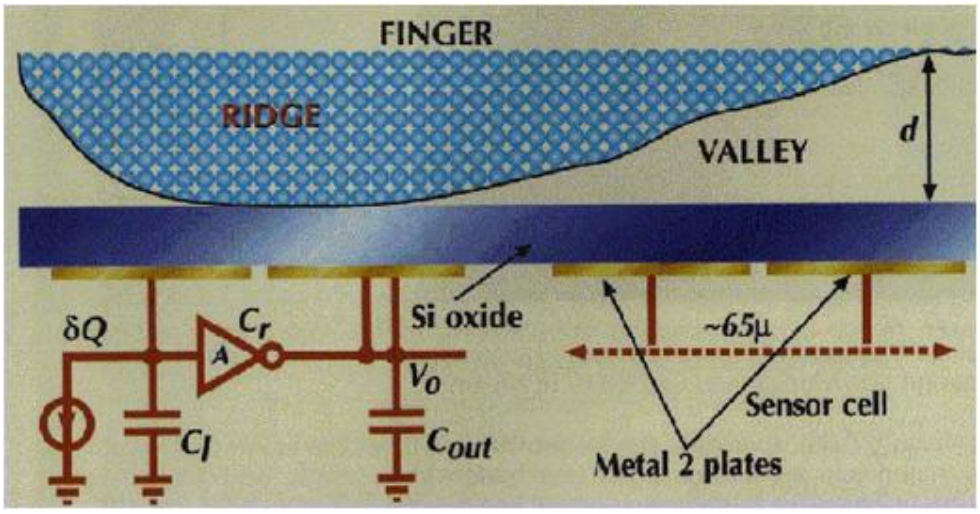
Slika 5.2.22 Sistem sočiva kod optičkih fingerprint senzora

Ultrasonična tehnika je zasnovana na postojanju razlike u akustičnoj impedansi na koži prsta. Senzori koji se koriste u ovoj tehnici nijesu novi. Već se dugi niz godina koriste u medicini za pravljenje eho-snimka. Frekventni opseg koji ovi senzori upotrebljavaju je od 20KHz pa do nekolika GHz. Vršne frekvencije moraju biti u mogućnosti da skeniraju kožu prsta sa rezolucijom od oko 500dpi (oko 200 tačaka po cm). Ova rezolucija je neophodna da bi se mogle prepoznavati karakteristične tačke na koži prsta.

Poluprovodnički senzori su dovoljno malih dimenzija da se mogu ugraditi u gotovo svaki uređaj. Mogu čak biti toliko tanki da se mogu smjestiti i u plastičnu karticu kao npr. kreditnu karticu i sl..

Senzori električnog polja su poluprovodnički senzori veličine pečata. Ovi senzori stvaraju električno polje i pomoću niza piksela mjere varijacije u polju. Varijacije su poljedica naboranosti kože prsta. Zavisno od proizvođača varijacije električnog polja se detektuju u provodnom sloju kože, ispod površine kože ili u epidermu.

Kapacitivni senzori su, kao i senzori elektičnog polja, veličine pečata. Kada se prst postavi na senzor, niz piksela mjeri varijacije u kapacitivnosti između senzora i prsta. Varijacije su posljedica postojanja brazdi na koži prsta, odnosno razlike u kapacitivnosti između kože i senzora (Slika 5.2.23).



Slika 5.2.23 Principijelna šema kapacitivnog senzora

Kao primjer primjene kapacitivnog čitača otiska prsta, na Slici 5.2.24 prikazan je uređaj LM-520 FSC, proizvod firme iGUARD.

Slika 5.2.24 Kapacitivni čitač otiska prsta

Senzori koji mjere temperaturu prsta mogu biti manji od samog prsta (Slika 5.2.25).

Slika 5.2.25 Termički čitač otiska prsta

Skeniranje otiska vrši se prelaskom prsta preko senzora. Senzor sadrži niz tačaka kojima se može detektovati razlika temperature kože (bore na koži prsta) i vazduha (udubljenja na koži prsta).

5.2.7 FALSIFIKOVANJE OTISKA PRSTA

Najveći problem tehnologije prepoznavanja otiska prsta jeste mogućnost falsifikovanja otiska. Nijedan od trenutno raspoloživih čitača nije u mogućnosti da pouzdano razlikuje stvarni prst od dobro urađene kopije. Kopija otiska može se uraditi uz saradnju vlasnika ili bez nje. Tehnologija prepoznavanja otiska, je u poređenju sa drugim biometrijskim tehnologijama, najpodložnija mogućnosti dobijanja kopije otiska bez znanja vlasnika [89, 113, 114].

Na slici 5.2.26 prikazana je tanka silikonska oblanda koja predstavlja kopiju otiska prsta. Ovakav falsifikat moguće je napraviti bez puno opreme za nekoliko sati. Prilično se lako može nalijepiti na prst, i veoma ga je teško detektovati [115].

Slika 5.2.26 Tanka silikonska oblanda kao kopija otiska prsta

Glavni izazov koji se postavlja pred proizvođače čitača je razlikovanje vještačkog materijala od prirodnog epidermisa prsta. Rade se mnoga istraživanja sa ciljem da se obezbijedi da samo prst bez ikakvih dodatnih vještačkih dijelova može biti identifikovan. Pažnja se usredsređuje na osobine kao što su temperatura, provodljivost, puls, krvni pritisak, itd..

U sobnom okruženju temperatura epiderma prsta je oko 8-10 stepeni veća od spoljašnje temperature (18-20 stepeni). Upotrebom silikonskog omotača teperatura prsta koju detektuje senzor je za oko 2 stepena niža. Međutim, senzori koji su namijenjeni da rade i na vanjskim temperaturama najčešće imaju širi opseg prihvatljivih temperatura prsta. Čak i u slučaju kada je izvršena kompenzacija senzora, sama činjenica da je upotrijebljen u vanjskim uslovima, može usloviti da silikonska oblanda na prstu ne bude detektovana.

U cilju detektovanja falsifikata, u mnogim čitačima otiska prsta, dodati su senzori koji mjere provodljivost prsta. Provodljivost prirodnog prsta je veoma zavistna od tipa kože (normalna ili suva). Normalna provodljivost je oko 200KΩ. Međutim, isti prst će imati provodljivost od nekoliko MΩ tokom suvog i hladnog zimskog vremena, kao i svega nekoliko KΩ tokom ljeta, kada je oznojen. Granice senzora moraju biti veoma široke. Stavljenje malo pljuvačke na silikonsku oblandu može da navede čitač da povjeruje da je riječ o prirodnom prstu.

Neki proizvođači čitača tvrde da uspijevaju detektovati prirodni prst na bazi mjerenja pulsa. Ovo je prilično moguće, ali ipak postoje problemi. Ljudska aktivnost, naročito sportska, uzrokuje prilično velike promjene pulsa. Da bi mogao vršiti detekciju u svim tim uslovima čitač bi morao imati široke granice prihvatljivog srčanog ritma, što bi u znatnoj mjeri umanjilo njegovu sposobnost detektovanja falsifikata. Druga mogućnost je da korisnik sačeka uspostavljanje normalnog pulsa prije nego pokuša da se identifikuje. Međutim, kod mnogih osoba prisutna su povremena odstupanja u srčanom ritmu. U ovim slučajevima čekanje na uspostavljanje noralnog ritma može da potraje nepredvidivo dugo.

Neki proizvođači izrađuju čitače koji detektuju razliku relativne dielektrične konstante (RDC) ljudske kože i vještačkih materijala. Međutim, slično kao i na provodljivost na relativnu dielektričnu konstantu kože utiče vlažnost. Da bi se izbjegao veliki FRR, granice prihvatljivosti RDC moraju biti prilično široke. Stavljenjem nešto špirita na silikonsku oblandu, prije nego što će se prinijeti skeneru može se zavarati dielektrični senzor. Špirit se sastoji od 90% alkohola i 10% vode. Relativne dielktrične konstante alkohola i vode su 24 i 80 respektivno, dok je relativne dielektrična konstanta prsta negdje između ove dvije vrijednosti. Kako alkohol brže isparava od vode, RDC silikonske oblande će rasti dok ne upadne u opseg koji skener prihvata. Tada će i silikonska odlanda će biti prihvaćena kao normalni prst.

Postoje senzori kojima se na osnovu dodira sa dvije različite tačke ljudskog tijela može mjeriti krvni pritisak. Ovaj senzor, u primjeni za prepoznavanje prirodnog prsta, ima iste nedostatke kao i senzor pulsa. Neki senzori detektuju oblik linija ispod epiderma prsta. Linije u ovom sloju su identične kao i linije na otisku. Neke metode koriste činjenicu da je sloj ispod epiderma savitljiviji (ultrasonični senzori), dok druge metode se fokusiraju na veću provodljivost ovog sloja. Ipak, kada postane poznato koju osobinu senzor koristi, moguće je silikonsku oblandu prilagoditi tome. Ima slučajeva kada proizvođači razvijene metode drže kao poslovnu tajnu i na taj način pokušavaju otežeti ″razbijanje″ sistema.

Kao zaključak se može kazati da i pored postojanja brojnih metoda razvijenih u cilju razlikovanja vještačkog i stvarnog prsta, mogućnost falsifikovanja nije eliminisana. Usljed potrebe da čitač ispravno radi za prilično široke granice svih opisanih parametara, prst na koji je nalijepljana tanka silikonska oblanda, ipak može zavarati dodatne testove. Prema tome, za dobijanje višeg stepena sigurnosti identifikacije, poželjno je biometrijski identifikacioni sistem zasnovan na prepoznavanju otiska kombinovati sa nekim klasičnim identifikacionim sistemom (korisničko/lozinka, ″pametna″ kartica, itd.) [89, 113].

5.2.8 PRIMJENE TEHNOLOGIJE PREPOZNAVANJA OTISKA PRSTA

Biometrijska identifikaciona tehnologija zasnovana na prepoznavanja otiska prsta ima brojne primjene. Čitači otiska koriste se:

- kao sastavni dio brave,
- u sistemima za kontrolu pristupa,
- u sistemima za evidenciju prisutnosti,
- u sefovima,
- na PC miševima i USB fleš diskovima,
- akt tašnama itd.

Na slici 5.2.27 prikazana je brava (Fingerprint Door Lock 6600-92 – [116]

) koja kao jedan od ključeva koristi i čitač otiska prsta. Čitač može sadržati do 78 profila otiska prsta, visokog kvaliteta. FAR čitača je manji od 0.0001% dok je FRR manji od 1%.

Slika 5.2.27 Fingerprint Door Lock 6600-92

Osim čitača otiska brava ima i mogućnost unošenja lozinke, kontaktni identifikator kao i mehanički ključ (Slika 5.2.28).

Slika 5.2.28 Ključevi Fingerprint Door Lock 6600-92 brave

Kontrola pristupa se ostvaruje kombinacijom raspoloživih načina identifikovanja. Ova brava se može primijeniti za osiguraje vila, kancelarija, vojnih ojekata itd.

Na slici 5.2.29 prikazan je uređaj za evidenciju prisustva i kontrolu

pristupa REXECU-5100 [117]. Uređaj za identifikaciju koristi čitač otiska prsta. U cilju povećanja pouzdanosti identifikacije, REXECU-5100 se može integrisati sa klasičnim identifikacionim čitačima kao što su čitači trakastog koda, proksimiti čitači, čitači kontaktnih čip kartica i drugi.

Slika 5.2.29 Uređaj za evideciju prisustva i kontrolu pristupa REXECU-5100

Uređaj može sadržati do 6000 profila, veličine 256 okteta. FRR mu je manji od 0.01% a FAR manji od 0.00001%. Može se koristiti za evidenciju i kontrolu prisustva u prostorijama za sastanke, kompjuterskim salama, depozitnim prostorijama, evidenciju prisustva radnika u preduzećima itd..

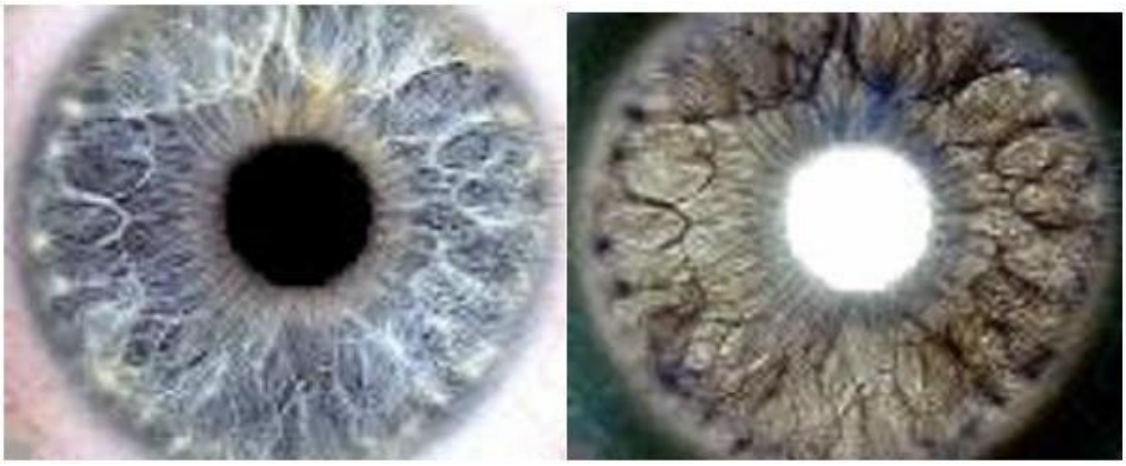
Biometrijsku tehnologiju prepoznavanja otiska počinju da koriste i proizvođači mobilnih telefona. Japanska firma *DoCoMo* predstavila je telefon s oznakom F505i, koji vlasnika prepoznaje po otisku prsta, a ne po PIN kodu.

Na slici 5.2.30 prikazane su još neke primjene čitača otiska prsta (na USB fleš disku, PC mišu i akt tašni).

Slike 5.2.30 Još neke primjene tehnologije identifikacije otiska prsta.

5.3 PREPOZNAVANJE DUŽICE OKA

Dužica oka ili (engl. iris) je obojeno tkivo koje okružuje zjenicu (Slika 5.11). Dužica posjeduje preko 200 detalja koji se mogu upotrijebiti za poređenje [94, 118].



Slika 5.3.1 Dužica oka slikana sa malog odstojanja i njen negativ

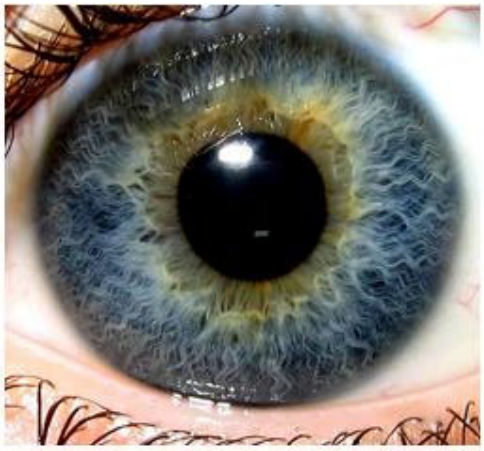
Čitači dužice koriste običnu video kameru. Ne zahtijeveju kontakt sa korisnikom. Skeniranje se može obaviti sa odstojanja i do 1m.

Mogućnost da dužica oka bude upotrijebljena za identifikaciju, najprije je sugerisana od strane oftamologa [119, 120]. Oni su kroz klinički praksu uočili da dužica ima veliki broj detalja koji su jednistveni i ostaju nepromijenjeni tokom vremena. 1936 godine oftamolog Frank Burch prvi sugeriše upotrebu dužice za personalnu identifikaciju. Ova ideja se tokom osamdesetih godina pojavljuje u filmovima Džemsa Bonda. 1987 godina, dva oftamologa, Aran Safir i Leonard Flom, daju njenu javnu prezentaciju. Dvije godine kasnije Dr. John Daugman, profesor na Harvard Universitetu, počinje sa razvojem algoritama za prepoznavanja dužice. 1994, Dr. Daugman patentirao je ove algoritme [121, 122, 123]. Patenti su danas vlasništvo Iridian Tecnhnologies, Inc.

5.3.1 ANATOMIJA OKA I DUŽICE

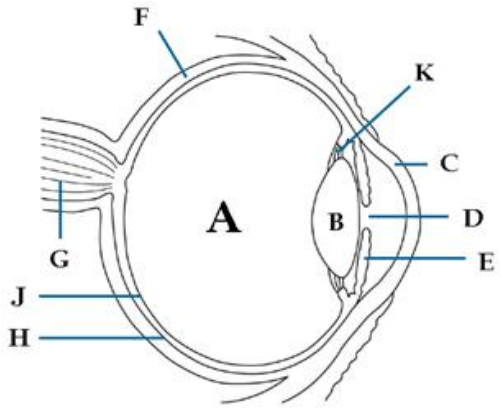
Za bolje shvatanje bogatstva dužice kao karakteristike za identifikaciju korisnika, dobro je razmotriti njenu strukturu. Sa stajališta anatomije, dužica (iris) je najvidljiviji dio oka. Dužica je jedini unutrašnji organ čovjeka koji se vidi spolja. Dužica se kod čovjeka počinje formirati oko tri mjeseca nakon začeća. Struktura linija i šara koje joj daju prepoznatljivost se formiraju do osmog mjeseca, ali se pigmenti koji joj daju boju stvaraju

tokom prve godine nakon rođenja. Izgled dužice se ne mijenja tokom ljudskog života. Sama dužica se sastoji od mišića za kontrolu širine zjenice, hromatofora, melanocita i pigmenta. Rezultat svega toga je niz linija i detalja koje svakoj dužici daju jedinstven izgled (Slika 5.3.2).



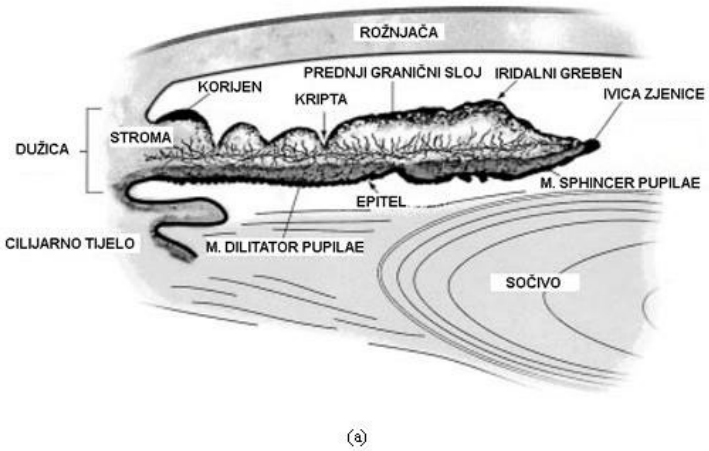
Slika 5.3.2 Oko sa karakterističnim šarama dužice

Dužica se nalazi između rožnjače i sočiva. Ona igra ulogu dijafragme oka, jer posebnim mišićnim mehanizmom reguliše količinu svjetlosti koja upada u oko. Obično je debljine između 0.3 i 0.4 mm, pri čemu je najtanja uz cilijarnu ivicu (Slika 5.3.3). Na dužici, koja se sastoji od nekoliko slojeva, nalazi se otvor, zjenica. Od količine pigmenta u pojedinim slojevima dužice zavisi boja dužice (Boja oka). Kod crnih ili kestenastih očiju dolazi do izražaja samo pigment prednjeg graničnog sloja, koji može biti izražen u većoj ili manjoj mjeri. Kod plavih očiju stroma dužice ne sadrži pigmente, nego reflektuje svijetlost kraće talasne dužine (plavi dio spektra). Naime, svijetlost veće talasne dužine prolazi kroz stromu i dospijeva do crnog sloja na prednjoj strani dužice, gdje se absorbuje (crveni dio spektra). Zato se iz takve dužice vraćaju samo plavi zraci, pa se čini da je oko plavo, iako u njemu nema ni traga plave boje. Zbog iste pojave i vene na koži izgledaju plave. Ako u stromi dužice ima nešto pigmenta oči će biti zelene, jer se plavi dio spektra koji se reflektuje miješa sa smeđom bojom pigmenta u stromi. Kod albina nedostaje pigment potpuno, čak i u zadnjem retinalnom sloju irisa, usljed čega im oči imaju crvenu boju [124].

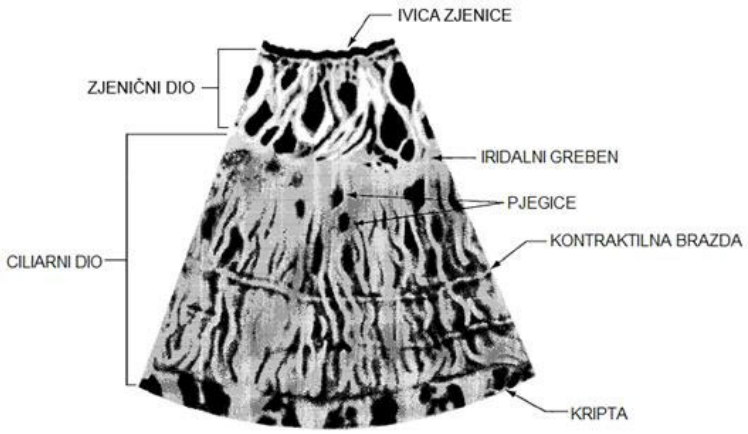


Slika 5.3.3 Dijagramski presjek ljudskog oka: A - staklasto tijelo, B - sočivo, C - rožnjača, D - zjenica, E - dužica, F -beonjača, G – očni nerv, H – sudovnjača, J - mrežnjača, K - cilijarno tijelo

U cilju jasnijeg uočavanja strukture dužice na Slici 5.3.4 prikazan je njen vertikalni i horizontalni presjek.



(a)



Slika 5.3.4 (a) vertikalni presjek dužice, (b) horizontalnii presjek dužice

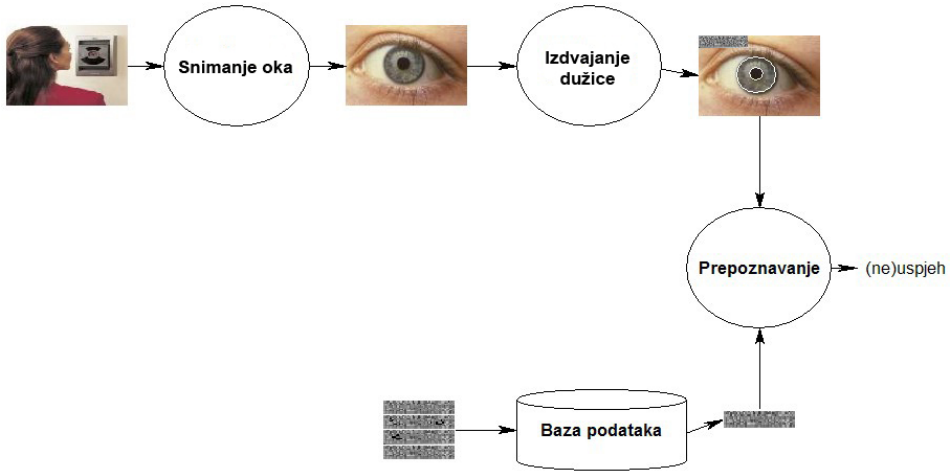
5.3.2 POSTUPAK PREPOZNAVANJA DUŽICE OKA

Postupak prepoznavanje dužice oka se može podijeliti u nekoliko faza, a to su:

• Slikanje oka
• Segmentacija
• Normalizacija
• Dobijanje koda
• Uspoređivanje kodova

Prva faza je slikanje oka. Tom prilikom korisnik se postavlja ispred biometrijskog senzora (koji je u ovom slučaju video kamera), slika 3.1. Dobijenu sliku određeni algoritmi analiziraju u cilju određivanja položaja dužice (ili da li na slici uopšte postoji dužica). Zatim se iz dobijenog područja lokalizuje struktura dužice. Lokalizovana struktura je svojevrsni jedinstveni kod na temelju kojeg se vrši prepoznavanje (IrisCode). Kod se uspoređuje sa ostalim kodovima iz baze podataka.

Najpoznatiji algoritmi za prepoznavanje dužice su Daugmanov [123] i Wildes-ov [124].



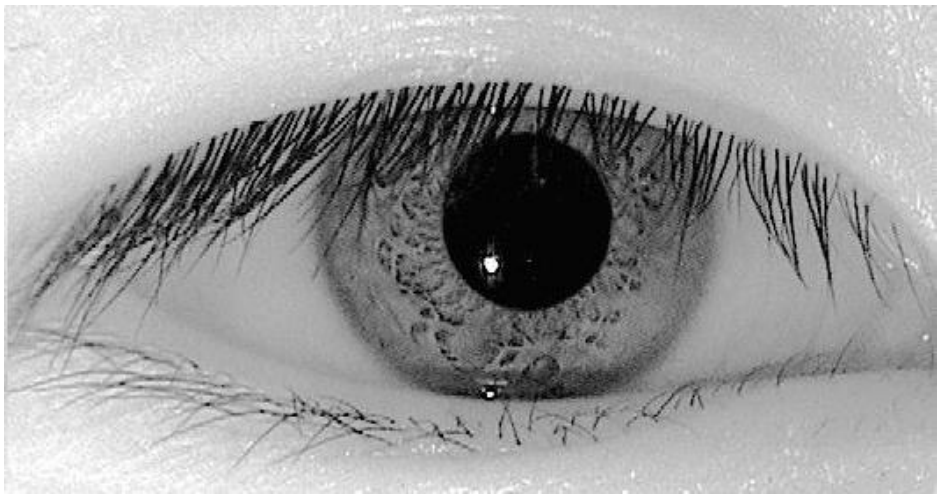
Slika 5.3.5 Sistem za prepoznavanje dužice oka

5.3.2.1 Dobijanje slike oka

Jedan od najvećih izazova identifikacije na osnovu prepoznavanja dužice jeste pravljenje visoko kvalitetnih slika oka. Pri tome se mora voditi računa da se zadrži dovoljno rastojanje kamere od čovječijeg oka. Dužica je relativno malena (u prosjeku veličine oko 1 cm). a ljudi po pravilu vrlo osjetljivi što se tiče njihovih očiju. To upućuje na zaključak da ovaj problem zahtijeva pažljivo razmatranje. Nekoliko pojedinosti treba uzeti u

obzir. Prvo, potrebno je slikati dužicu s dovoljno visokom rezolucijom i oštrinom kako bi prepoznavanje uopšte bilo moguće. Drugo, potrebno je imati dovoljno osvjetljenje, ali da to osvjetljenje ne smeta korisniku (optimalan intenzitet izvora svijetlosti). Treće, potrebno je da slike budu dovoljno dobro centrirane, ali da se time ne opterećuje korisnik. Koliko je to moguće, iz slike je potrebno je eliminisati nepotrebne detalje.

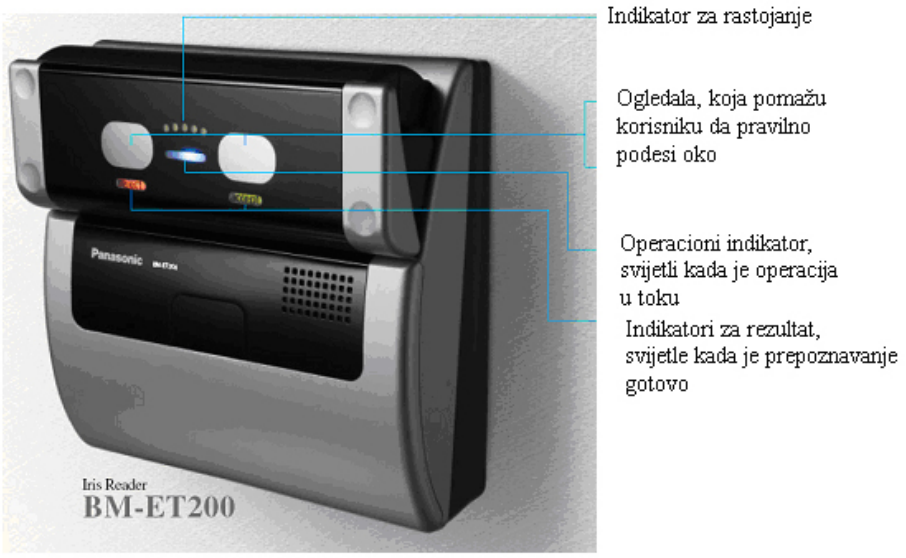
Za skeniranje dužice najčešće se koristi infracrvena svjetlost [125]. Vidljiva svjetlost se rjeđe koristi jer izaziva dilataciju zjenice oka i otežava identifikaciju. Čitač uključuje vidljivu svjetlost i varira njen intezitet da bi ustanovio da li dolazi do dilatacije zjenice. Ukoliko dilatacija zjenice postoji čitač sa sigurnošću konstatuje da se radi o prirodnom oku. Pod infracrvenom svjetlošću, čak i tamno obojene dužice otkrivaju svoje bogate i kompleksne osobine što je prikazano na slici 5.3.6.



Slika 5.3.6 Tamno braon dužica osvijetljena infracrvenim svijetlom.

Da bi se uhvatili bogati detalji dužice, sistem za snimanje bi trebao da postigne minimalno 50 piksela u radijusu dužice. Najtipičniji kvalitet je 100 do 140 piksela u radijusu dužice. Da slikanje nebi bilo vidljivo za ljude potrebna je iluminacija u opsegu 700nm-900nm. Usljed toga najčešće se koriste monohromatske CCD kamere (480x640). Neki sistemi za snimanje koriste širokopojasnu kameru za grubo lokalizovanje očiju na licima. One zatim upravljaju optikom uskopojasne pan/tilt kamere koja snima slike očiju u većoj rezoluciji [123].

U većini slučajeva koristi se tehnika ogledala, koje pomaže učesnicima da sami podese položaj svog oka, slika 5.3.7.



Slika 5.3.7 Panasonic-ov BM-ET200 iris čitač

5.3.2.2 Izdvajanje dužice sa slike oka (Segmentacija)

Nakon dobijanja slike oka, potrebno je izdvojiti region dužice. Region dužice se može aproksimirati jednim kružnim prstenom, čija unutrašnja granica je granica između zjenice i dužice, a spoljašnja između dužice i beonjače oka. U procesu segmentacije osim izdvajanja dužice uklanjaju se i smetnje, kao što su trepavice, očni kapci i odsjaj. Svijetla tačka na slici 3.1.1 u gornjem predjelu zjenice oka je primjer odsjaja. Za pronalaženje granica dužice, najpoznatije su dvije metode:

• Hough transformacija i
• Daugmanov itegralno-diferencijalni operator

HOUGH TRANSFORMACIJA

Hough transformacija je standardni algoritam koji se koristi za određivanje parametara jednostavnih geometrijskih oblika, kao sto su linije i krugovi [126]. U cilju prenalaženja radijusa, kao i koordinata centra zjenice i dužice koristi se kružna Hough transformacija. Segmentacioni algoritam baziran na Hough transformaciji koriste Wildes, Kong and Zhang [127], kao i Tisse [126]. Izdvajanje regiona dužice podrazumijeva dva koraka. Prvo se dobije mapa ivica korišćenjem Gauss-ovog filtra [128]. Zatim se dobijeni podaci analiziraju u kružnom Hough prostoru kako bi se našli parametri dužice i zjenice [129]. Hough prostor je difinisan kao :

$$H\,(x_o, y_o, r) = \sum_i h\,(x_i, y_i, x_o, y_o, r)$$

gdje je (x_i , y_i) piksel koji se nalazi na ivici, a

$$h\,(x_i , y_i , x_o , y_o , r) = \begin{cases} 1, & ako\ se(x_i, y_i)\ nalazi\ na\ krugu(x_o, y_o, r) \\ 0 & u\ ostalim\ slucajevima \end{cases}$$

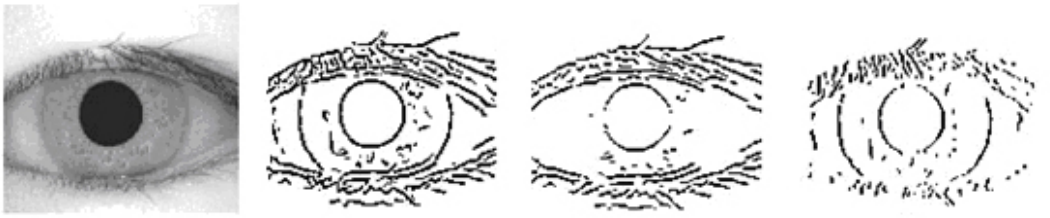
Parametri sa maksimalnom vrijednošću $H\,(x_o , y_o , r)$ će biti parametri kruga koji najbolje definiše ivicu, gdje su (x_o , y_o) koordinate centra tog kruga, r je njegov radijus.

Wildes, Kong i Zhang koriste parabolnu Hough transformaciju za detekciju očnih kapaka, aproksimirajući gornje i donje kapke sa paraboličnim lukom, čija je formula data kao :

$$(- (x - h_j) \sin\theta_j + (y - k_j) \cos\theta_j)^2 = a_j ((x - h_j) \cos\theta_j + (y - k_j) \sin\theta_j)$$

gdje a_j kontroliše nagib luka, (h_j , k_j) je vrh parabole, a θ_j je ugao relativne rotacije po x-osi.

Za pronalaženje ivica Wildes traži izvode po horizontalnom pravcu za detekciju očnih kapaka i po vertikalnom pravcu za detekciju spoljašnje granice dužice (slika 5.3.8). To je zato što su kapci obično horizonatlno raspoređeni, a vertikalno traženje gradijenta kapaka bi dovelo do smetnje pri traženju granice dužice. Traženje samo vertikalnog gradijenta za pronalaženje spoljašnje granice dužice je i dovoljno, jer za uspješnu lokalizaciju nisu potrebni svi pikseli koji definišu krug.



5.3.8 Izdvajanje ivica korišćenjem Hough transformacije

Međutim, postoji nekoliko problema sa Hough transformacijom. Kao prvo, ona zahtijeva da se izabere prag vrijednosti koji se koristi pri detekciji ivica. Drugo, njeno računanje je veoma zahtijevno da bi se primjenjivala u realnom vremenu.

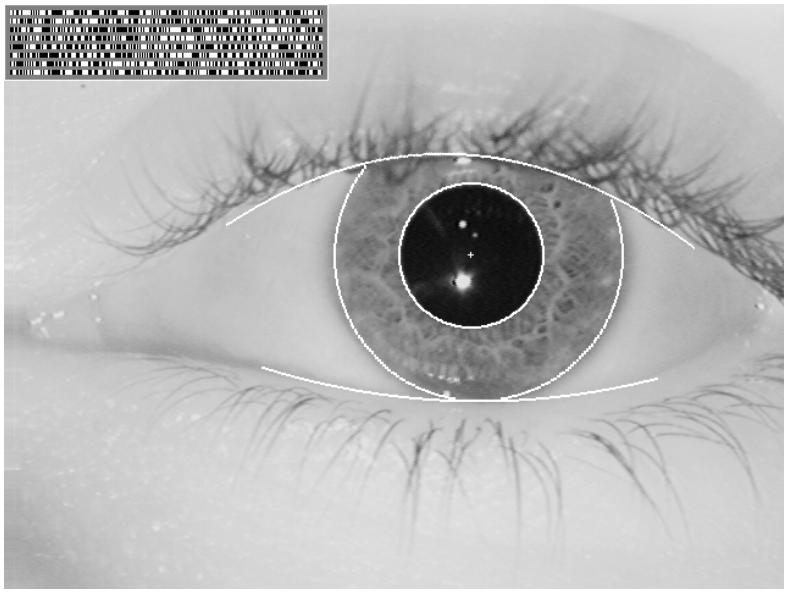
DAUGMANOV INTEGRALNO-DIFERENCIJALNI OPERATOR

Za pronalaženje spoljašnje i unutrašnje granice dužice, kao i granica očnih kapaka, Daugman koristi sljedeći integralno-diferencijalni operator :

$$\max_{(r,\,x,\,y)} \left| G(r) * \frac{\partial}{\partial r} \oint_{r,x_o,y_o} \frac{I(x,y)}{2\pi r} ds \right|$$

Gdje je *I(x,y)* slika koja sadrži oko (slika 1.3.2), *r* je radijus koji se traži, *G(r)* je Gaussova smoothing funkcija [130] , a *s* je kontura kruga definisana sa (r, x_o ,y_o). Simbol * označava konvoluciju. Operator traži po domenu čitave slike maksimum u parcijalnom izvodu po rastućem radijusu *r,* normalnog konturnog integrala *I(x,y)*. Odnosno, operator traži dio kruga gdje se dešava maksimalna promjena vrijednosti piksela, promjenom vrijednosti radijusa *r* i položaja koordinata centra *(x,y)*. Čitav operator se ponaša kao kružni detektor ivice, sa finoćom koja se podešava Gaussovom funkcijom [123].

Kada pretraga za ovim ivicama dodje do preciznosti od jednog piksela, tada se koristi sličan pristup za detektovanje granica gornjeg i donjeg očnog kapka. Razlika je samo što se putanja konturne integracije mijenja sa kružne na lučnu. Rezultat svih ovih lokalizacija je izolacija tkiva dužice od ostalih djelova slike, kao što je ilustrovano na slici 5.3.9.

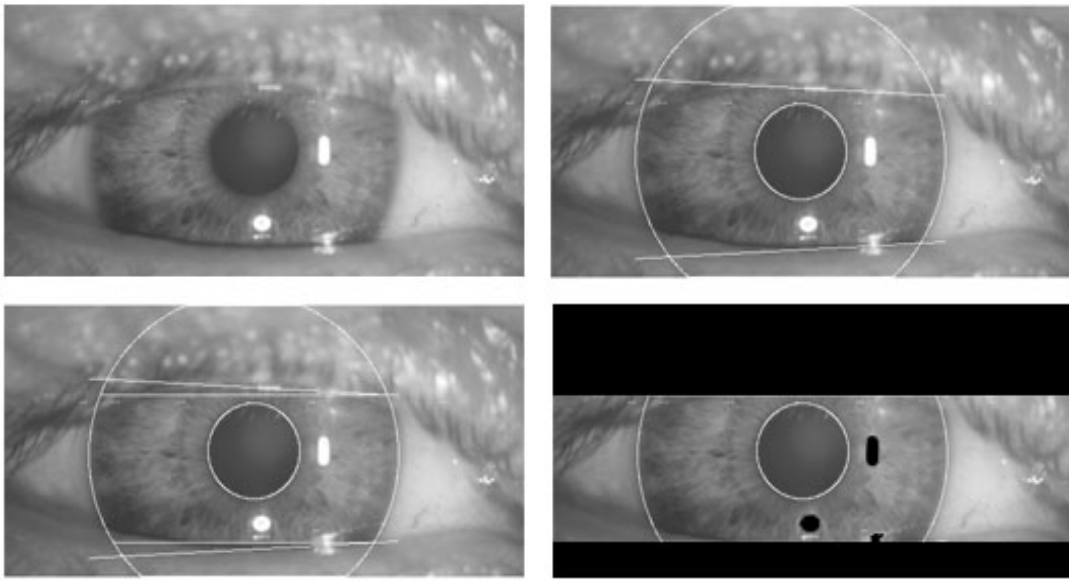


Slika 5.3.9 Slika dužice, snimljene monohromatski sa NIR iluminacijom u 700nm-900nm opsegu na udaljenosti od oko 35 cm. Bijela linija daje lokalizaciju dužice i zjenice i detekciju očnih kapaka. Niz bita u gornjem lijevom uglu je rezultat demodulacije sa kompleksnim 2D Gabor waveletima, o kojima će biti riječi.

5.3.2.3 Detekcija trepavica i smetnji

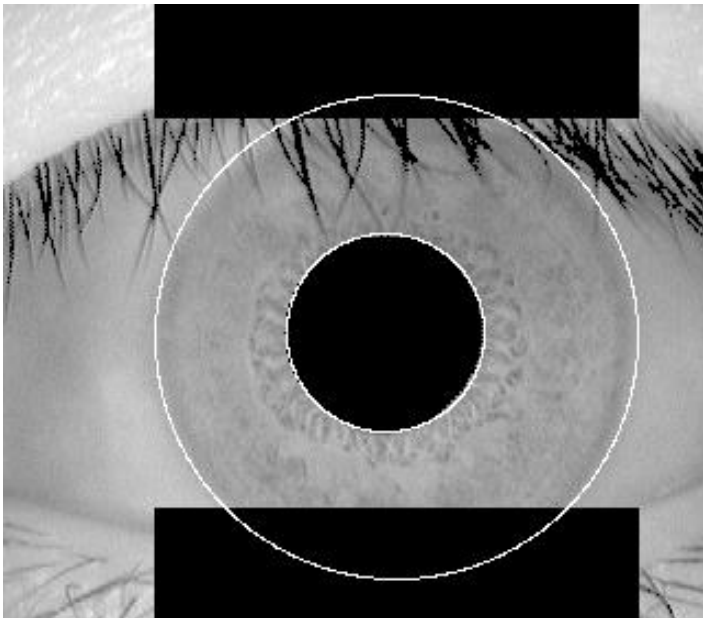
Kineski profesori, Kong i Zhang, trepavice tretiraju na dva načina: kao posebne trepavice (koje su izolovane na slici) i kao grupu trepavica (koje su u snopu na slici). Pomoću određenih filtara vrši se njihova detekcija [127]. Odsjaj se detektuje pomoću metode praga (u literaturi poznata kao tresholding). Jer će vrijednosti piksela ovog regiona biti veće od bilo kojeg dijela na slici [126].

Na slici 5.3.10 prikazan je postupak segmentacije. Za detekciju ivica zjenice i dužice korišćena je kružna Hough transformacija. Za detekciju očnih kapaka u ovom primjeru umjesto parabolne koristi se linearna Hough transformacija. Prednost linearne Hough transformacije u odnosu na parabolnu je to što je potebno manje parametara odrediti, što ovaj je proces čini dosta bržim. Nakon detekcija ivica, smetnje kao što su trepavice, kapci i spekularna refleksija se zatamnjuju.



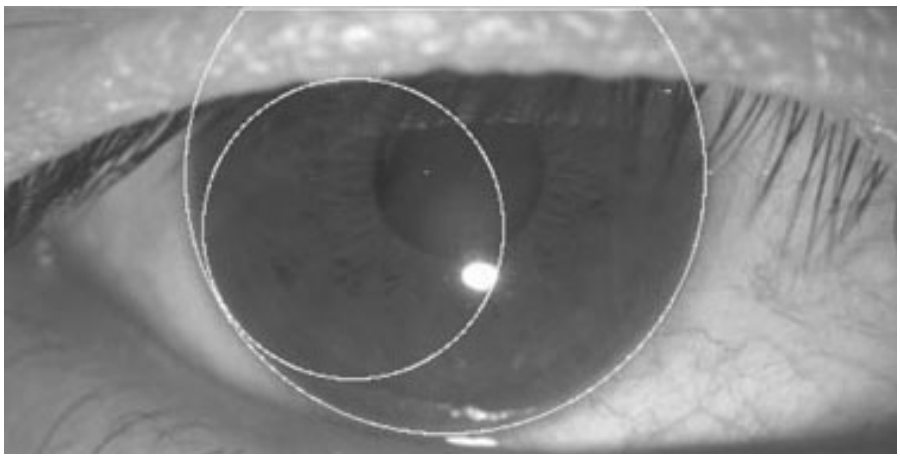
Slika 5.3.10 Detekcija ivica dužice, kao i smetnji-kapaka, trepavica i refleksija. Na donjoj desnoj slici sve ove smetnje su zatamnjene.

Prilikom detekcije ponekad se javlja problem sa svijetlim trepavicama. Može se desiti da neke od njih ne budu detektovane, kao na slici 5.3.11. Međutim, ovi nedetektovani djelovi su veoma mali u odnosu na region dužice, tako da neće uticati na prosec segmentacije.



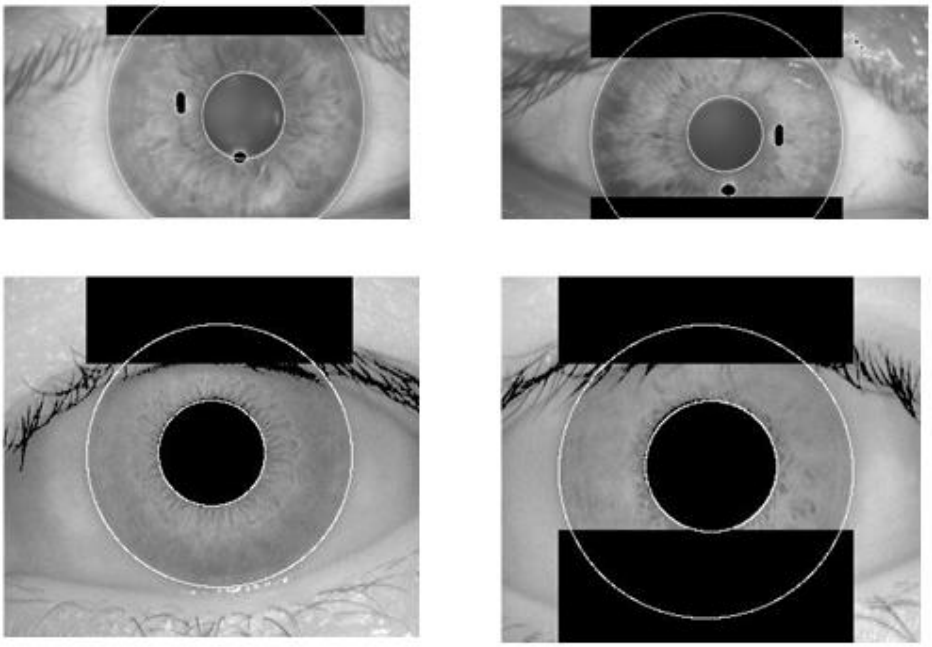
Slika 5.3.11 Zatamnjivanje detektovanih trepavica. U gornjem dijelu slike svjetlije trepavice nisu detektovane.

Ukoliko između regiona dužice i regiona zjenice postoji jako mali kontrast može se desiti da segmentacija bude neuspješna kao što je pokazano na slici 5.3.12.



Slika 5.3.12 Neuspješna detekcija zjenice

Na slici 5.3.13 dati su neki primjeri uspješne detekcije dužice i izolacije nepotrebnih djelova.



Slika 5.3.13 Primjeri uspješne segmentacije

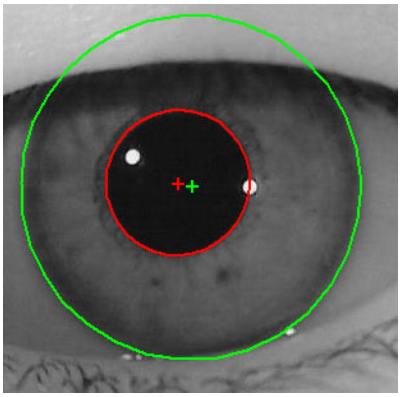
5.3.2.4 Normalizacija

Nakon što se sa slike uspješno izdvoji region dužice, sljedeće šta treba uraditi je transformisati taj region tako da ima stalne dimenzije. Odnosno, na prepoznavanje ne smiju uticati promjene u veličini, poziciji i orjentaciji dužice. Ovo znači da moramo da napravimo reprezentaciju koja je neosjetljiva na:

• optičku veličinu dužice na slici
• veličinu zjenice unutar dužice (stalno se mijenja usljed promjene osvjetljenja)
• lokaciju dužice unutar slike
• i orjentaciju dužice.

Optička veličina dužice zavisi od rastojanja oka od kamere, kao i faktora povećanja kamere. Orjentacija dužice zavisi od nagiba glave, uglova kamere, rotacije oka, pozicije kamere i ugla ogledala. Neosjetljivost na sve ove faktore može biti postignuta [123]. Isto tako, treba imati u vidu da region zjenice nije koncentričan u odnosu na dužicu, nego uvijek malo pomjeren (slika 5.3.14).

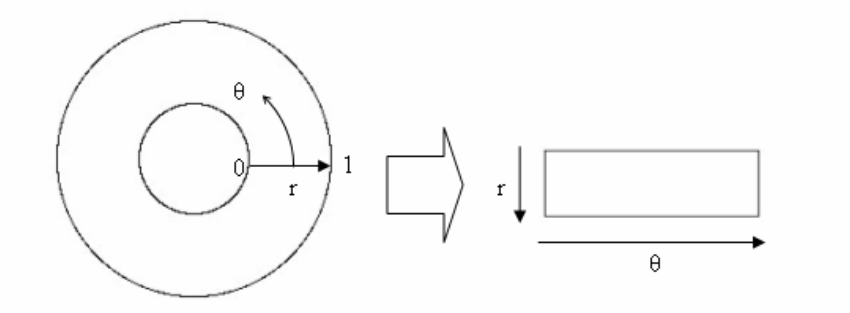
Nakon procesa normalizacije dobiće se region dužice koji će imati konstantne dimenzije, tako da dvije fotografije iste dužice pod različitim uslovima će imati iste karakteristike.



Slika 5.3.14 Centar zjenice i dužice se obično ne nalaze na istom mjestu

DAUGMANOV RUBBER SHEET MODEL

Poznati model koji se koristi za normalizaciju je Daugmanov rubber sheet model [123]. Ovim modelom vrši se transformacija slike u polarni koordinatni sistem (Slika 5.3.15). Mreža polarnih koordinata nije potrebno da bude koncentrična, pošto se centri zjenice i dužice obično ne poklapaju, čak nije neobično da nazalni pomjeraj bude i do 15 %. Ovaj koordinatni sitem možemo opisati kao dvostruko-bezdimenzionalan: polarna promjenljiva, ugao, je svojstveno bezdimenziona, ali u ovom slučaju i radijalna promjenljiva je takođe bezdimenziona, zato što uzima opseg od granica zjenice do limbusa uvijek kao jedinični interval [0,1]. Širenje i skupljanje dužice usljed promjene veličine zjenice modelovano je ovim koordinatnim sistemom kao istezanje homogene gumene trake.



Slika 5.3.15 Daugmanov rubber sheet model

Model homogene gumene trake dodjeljuje svakoj tački dužice (bez obzira na njenu veličinu i istezanje zjenice) par realnih koordinata (r,θ) gdje r leži na jediničnom intervalu [0, 1] , a θ je ugao [0, 2π]. Transformacija slike dužice $I(x, y)$ iz Cartesian koordinata (x,y) u bezdimenzioni ne-koncentrični polarni koordinatni sistem (r,θ) može biti predstavljena kao:

$$I\,(x(r,\theta),\, y(r,\theta)) \rightarrow I\,(r,\theta)$$

Gdje su $x(r, \theta)$ i $y(r, \theta)$ definisani kao linearna kombinacija graničih tačaka zjenice $(x_p(\theta), y_p(\theta))$ i graničnih tačaka spoljašnje granice dužice $(x_s(\theta), y_s(\theta))$. Pa je :

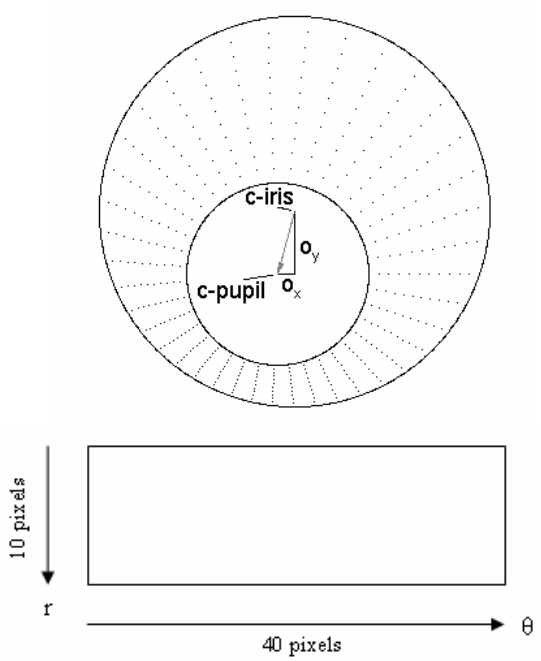
$$x(r,\theta) = (1 - r)x_p(\theta) + rx_s(\theta)$$

$$y(r,\theta) = (1 - r)y_p(\theta) + ry_s(\theta)$$

Iako ovaj model rješava problem dilatacije zjenice, pozicije i veličine dužice, on ne rješava pitanje orjentacije dužice u okviru slike. U Daugmanovom sistemu ovaj problem se rješava u dijelu gdje se porede kodovi dužice. To se radi tako što se kod koji se poredi šiftuje u smjeru θ.

PRIMJER NORMALIZACIJE CENTRA ZJENICE I CENTRA DUŽICE

Proces normalizacije regiona dužice postignut je pomoću Daugmanovog rubber sheet modela. Za referentnu tačku izabran je centar zjenice. Na slici 5.3.16 su prikazani i radijalni vektori po cijelom regionu dužice. Duž svake radijalne linije selektovan je određen broj tačaka. One definišu radijalnu rezoluciju. Broj radijalnih linija koje okružuju region dužice definišu ugaonu rezoluciju.



Slika 5.3.16 Normalizovani region dužice sa radijalnom rezolucijom od 10 piksela i ugaonom od 40 piksela

Kako centar zjenice nije koncentričan u odnosu na dužicu potrebna je formula koja će da reskalira te tačke, koje zavise od ugla. To je postignuto formulom:

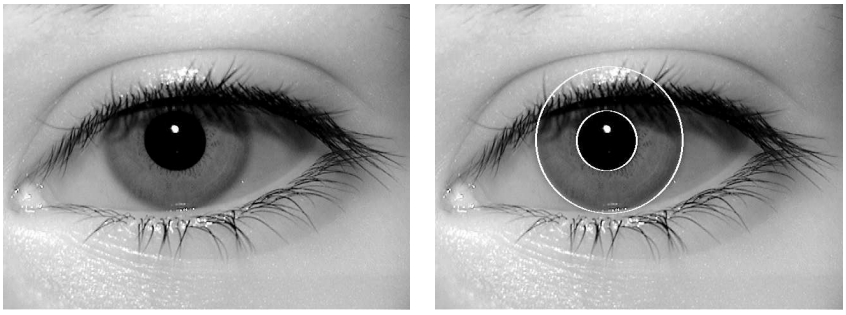
$$r' = \sqrt{\alpha}\,\beta \pm \sqrt{\alpha\beta^2 - \alpha - r_i^2}$$

gdje je :

$$\alpha = o_x^2 + o_y^2$$

$$\beta = \cos\left(\pi - \arctan\left(\frac{o_y}{o_x}\right) - \theta\right),$$

pri čemu o_x i o_y predstavlju relativni pomjeraj centra zjenice u odnosu na centar dužice, r' je rastojanje između ivice zjenice i ivice dužice u zavisnosti od ugla θ, a r_i je radijus dužice.
Duž svake radijalne linije izabran je konstantan broj tačaka bez obzira na to koliki je radijus u određenom uglu. Iz takozvanog "doughnut" oblika normalizacijom smo dobili 2D polje. Horizontalna dimenzija ovog polja predstavlja ugaonu rezoluciju, a vertikalna radijalnu rezoluciju. Drugo polje služi da se obilježe refleksije, trepavice i kapci, koji su detektovani u procesu segmentacije (Slika 5.3.17). Tačke koje se nalaze na granici zjenice i dužice se ne uzimaju u obzir, da ne bi region koji ne sadrži dužicu oštetio potrebna područja [126].



a) Slika oka b)Lokalizacija dužice

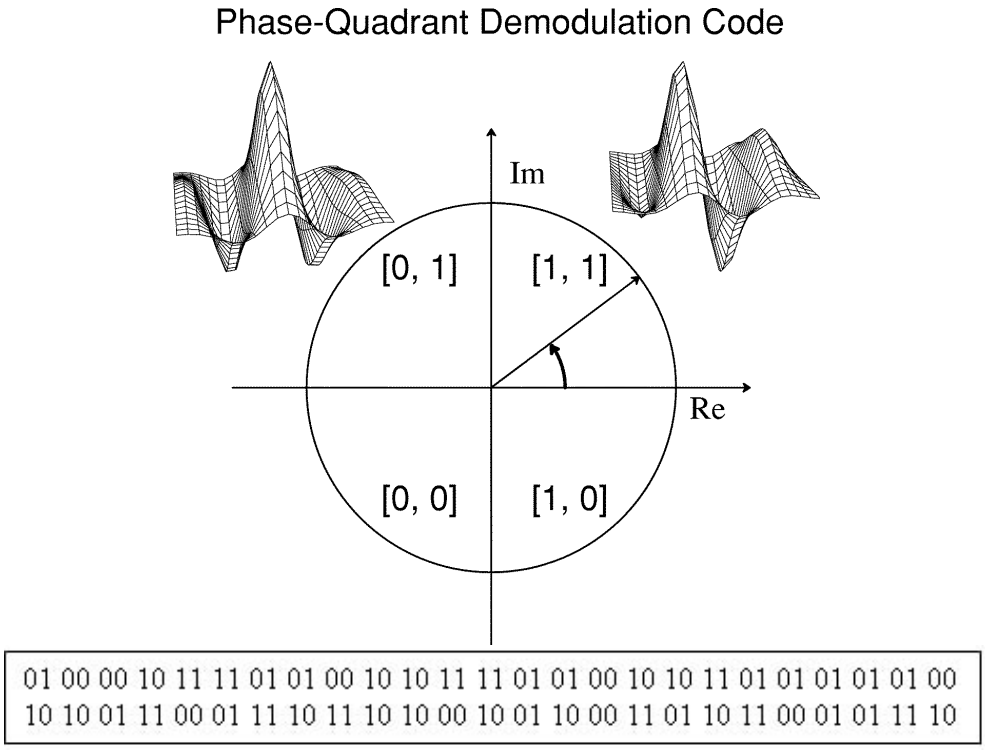
c) Slika dužice nakon normalizacije

d) Maska za ukljanjajnje smetnji

Slika 5.3.17 Proces normalizacije

5.3.2.5 Dobijanja koda dužice demodulacijom sa 2D Gabor wavelet-ima

Za dobijanje koda dužice koriste se dvodimenzionalni *Gabor wavelet*-i [131]. Pomoću njih se struktura dužice prikazuje kao niz vektora u kompleksnoj ravni. 2D Gabor wavelet predstavlja složenu matematičku funkciju, koja ima svoju realnu i imaginarnu komponentu. Komponente su dobijene modulacijom sinosnog/kosinusnog talasa sa Gaussovom funkcijom [132]. Nakon normalizacije slike vrši se konvolucija svakog piksela sa 2D Gabor waveletom. Funkcija Gabor filtra ima kompleksnu vrijednost, pa će i rezultat mati realni i imaginarni dio. Djelovi se posmatraju odvojeno. Svi upotrijebljeni Gabor wavelet filtri čine banku wavelet-a.



Slika 5.3.18 Dobijanje koda pomoću fazne demodulacije

Daugman koristi proces fazne demodulacije za kodiranje teksture dužice, (Slika 5.3.18) [123]. Lokalni regioni dužice su projektovani na kvadraturne 2D Gabor wavelete, generišući kompleksne projekcione koeficijente čiji realni i imaginarni djelovi daju koordinate fazora u kompleksnoj ravni. Ugao svakog fazora je kvantiziran na jedan od četiri kvadranta, dajući dva bita informacije o fazi. Ovaj se proces ponavlja čitavom površinom dužice sa mnogo veličina waveleta, frekvencija i orjentacija, da bi se na kraju izdvojilo 2048 bita.

Za prepoznavanje dužice koristi se samo fazna informacija. Amplitudna informacija nije pogodna za računanje jer zavisi od mnogo faktora kao što su: kontrast slike, iluminacija i pojačanje kamere.

Koristeći 2D Gabor wavelete, svaka izolovana šara dužice se demoduliše i izdvaja se njena fazna informacija. Ovaj proces kodiranja jednak je faznoj kvantizaciji teksture dužice. Proces se odvija tako što se data oblast projektuje na kompleksne 2D Gabor wavelete i određuje u kojem kvadrantu kompleksne ravni leži svaki rezultantni fazor:

$$h\{Re,Im\} = sgn\{Re,Im\} \int_\rho \int_\phi e^{-i\omega(\theta o-\phi)} e^{-(r_o-\rho)^2/\alpha^2} e^{-(\theta_o-\phi)^2/\beta^2} I(\rho,\varphi)\rho d\rho\, d\varphi$$

h(Re,Im) se posmatra kao bit koji ima realni i imaginarni dio, $h=h_{\mathrm{Re}}+ih_{\mathrm{Im}}$. Vrijednosti h_{Re} i h_{Im} su 1 ili 0 (sgn) zavisno od znaka 2D integrala :

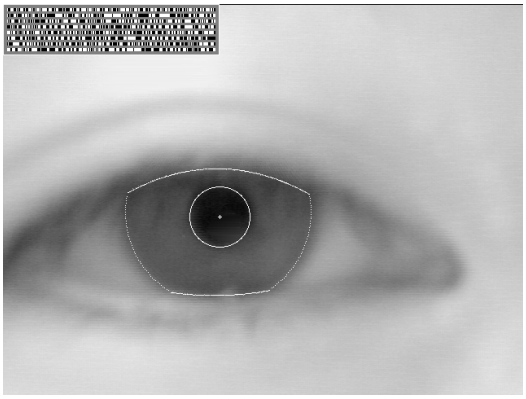
$h_{\mathrm{Re}}=1$ ako je $\mathrm{Re}\int_\rho\int_\phi e^{-i\omega(\theta o-\phi)} e^{-(r_o-\rho)^2/\alpha^2} e^{-(\theta_o-\phi)^2/\beta^2} I(\rho,\varphi)\rho d\rho\, d\varphi \geq 0$

$h_{\mathrm{Re}}=0$ ako je $\mathrm{Re}\int_\rho\int_\phi e^{-i\omega(\theta o-\phi)} e^{-(r_o-\rho)^2/\alpha^2} e^{-(\theta_o-\phi)^2/\beta^2} I(\rho,\varphi)\rho d\rho\, d\varphi < 0$

$h_{\mathrm{Im}}=1$ ako je $\mathrm{Im}\int_\rho\int_\phi e^{-i\omega(\theta o-\phi)} e^{-(r_o-\rho)^2/\alpha^2} e^{-(\theta_o-\phi)^2/\beta^2} I(\rho,\varphi)\rho d\rho\, d\varphi \geq 0$

$h_{\mathrm{Im}}=0$ ako je $\mathrm{Im}\int_\rho\int_\phi e^{-i\omega(\theta o-\phi)} e^{-(r_o-\rho)^2/\alpha^2} e^{-(\theta_o-\phi)^2/\beta^2} I(\rho,\varphi)\rho d\rho\, d\varphi < 0$

I(ρ,φ) je čista slika dužice u bezdimenzionom polarnom koordinatnom sistemu koji je neosjetljiv na veličinu i translaciju. α i β su parametri 2D waveleta, ω je frekvencija waveleta, a (ρ_o, θ_o) su polarne koordinate svake oblasti na dužici za koju se računaju koordinate *h(Re,Im)* fazora. Takva fazno kvadratna sekvenca kodiranja je grafički prikazana u gornjem lijevom uglu slike 5.3.9. Poželjna osobina faznog koda je da bude cikličan (npr. Gray-ov kod) [133]. Ukupno 2048 takvih faznih bita (256 bajtova) je izračunato za svaku dužicu. Velika prednost u odnosu na prethodne algoritme (Daugman 1993, Daugman 1994) je ta što se sada isti broj maskirnih bita računa da naznači da li je bilo koji dio dužice prekriven kapcima, sadrži li trepavice, ima li refleksija, itd.



Slika 5.3.19 Loše fokusirana slika dužice i njeh kod

Ekstrakcija faze ima još jednu prednost. Prednost se ogleda u tome da se fazni uglovi mogu naći bez obzira koliko je loš kontrast slike (Slika 5.3.19). Niz bita sa ove slike ima statističke osobine slične nizu bita sa slike 5.3.18 koja je pravilno fokusirana. Činjenica da fazni bitovi postoje i kod loše fokusirane slike je velika prednost sistema za prepoznavanje dužice. Različite loše fokusirane slike se ne mogu pomiješati kada se uporede njihovi fazni kodovi.

LOG-GABOR FILTAR

Nedostatak Gabor fitra je to što ima DC komponentu kad god širina propusnog opsega pređe oktavu [126]. Poništavanje DC komponente, za bilo koji propusni opseg filtra, se može postići korišćenjem Gabor filtra sa logaritamskom skalom, što je poznato kao Log-Gabor filtar. Frekvencija odziva ovog filtra je data sa :

$$G(f) = \exp(\frac{-(\log(f/f_o))^2}{2(\log(\sigma/f_o))^2})$$

gdje je f_o centralna frekvencija, a σ širina propusnog opsega filtra. Više o ovome filtru je dato u [134].

LAPLASIAN-GAUSOV FILTAR

Za dekompoziciju regiona dužice, Wildesov sisitem koristi Laplasian-Gausov filtar koji čija funkcija je data sa:

$$\nabla G = -\frac{1}{\pi\sigma^4}\left(1-\frac{\rho^2}{2\sigma^2}\right)e^{-\rho^2/2\sigma^2}$$

gdje je σ gausova standardna devijacija, a ρ je radijalno rastojanje tačke do centra filtra. Filtrirana slika je predstavljena Laplasianovom piramidom [124] koja je u stanju da kompresuje izdvojene podatke. Detaljnije o ovom filtru može se naći u [135].

5.3.2.6 Test statističke nezavisnosti

Kada je dobijen kod dužice, treba ga uporediti sa kodovima u bazi podataka. To se radi testom statističke nezavisnosti. Ključ u prepoznavanju dužice je da ne prođe test statističke nezavisnosti, odnosno da rezultat testa bude jednak 0. Test statističke nezavisnosti uključuje toliko mnogo stepena

slobode tako da je garantovano da će imati veliku vrijednost kad god se fazni kodovi različitih očiju porede, a malu kada se fazni kod nekog oka poredi sa drugom verzijom istog oka [123].

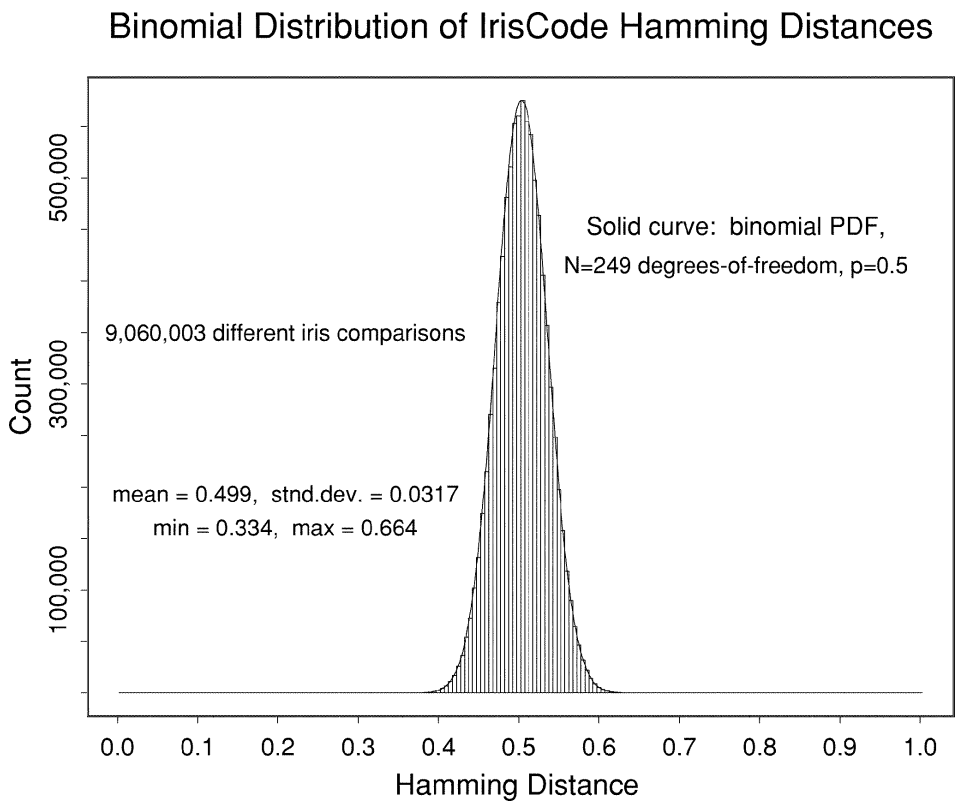
Test statističke nezavisnosti se implementira pomoću prostog Boolean Ekskluzivnog ILI operatora (XOR). Operator se primjenjuje na 2048-bitne fazne vektore koji kodiraju bilo koje dvije dužice. Rezultat se maskira pomoću I (AND) operatora. XOR operator $\otimes$, detektuje neslaganje između odgovarajućih parova bita, dok AND operator $\cap$, potvrđuje da poređeni bitovi nisu oštećeni kao posledica trepavica, kapaka, ili nekog drugog šuma.

Kao mjera nepoklapanja između kodiva dvije dužice, čiji su fazno kodirani bit vektori dati (*cadeA*, *codeB*) i čiji su maskirni vektori takođe dati (*maskA*, *maskB*), računa se Hamming-ova distanca po sljedećoj relaciji:

$$\mathrm{HD}=\frac{\left\| (code\,A \otimes code\,B) \cap mask\,A \cap mask\,B \right\|}{\left\| mask\,A \cap mask\,B \right\|}$$

Imenilac označava ukupan broj faznih bita koji su važni u poređenju dužica nakon što se uklone trepavice i refleksije. Rezultat HD=0 bi predstavljao savršeno poklapanje. Bollean operatori $\otimes$ i $\cap$ se primjenjuju u vektorskoj formi na binarne stringove. Stringovi mogu biti dužine kao i dužina riječi u CPU i mogu se izvršavati kao jedna mašinska instrukcija. Na primjer obične 32-bitne mašine, bilo koja dva cijela broja između 0 i 4 milijarde mogu XOR-ovati u jednoj instrukciji. Bitovi rezultantnog cijelog broja su u dobijeni kao rezultat XOR operacija odgovarajućih parova bita u prvobitnim cijelim brojevima. Implementacija ove formule u paralelnim 32-bitnim djelovima omogućuje brzo poređenje kodova dužice kada. Na 300MHz CPU, na ovaj način je moguće porediti 100,000 dužica u sekundi.

Za bilo koji bit u faznom kodu dužice jednako je vjerovatano da bude 1 ili 0. Usljed toga kada dužice nisu u korelaciji, očekivana vrijednost Hamingove distence je HD=0.500. Histogram na slici daje distribuciju HD-ova prikupljenih iz preko 9 miliona poređenja između različitih parova dužica prikupljenih od strane algoritama iz UK, USA i Japana [123].



Slika 5.3.20 Distribucija Hammingove distance za preko 9 miliona poređenja različith parova dužice

VJEROVATNOĆA GREŠKE U ZAVISNOSTI OD HAMMINGOVE DISTANCE

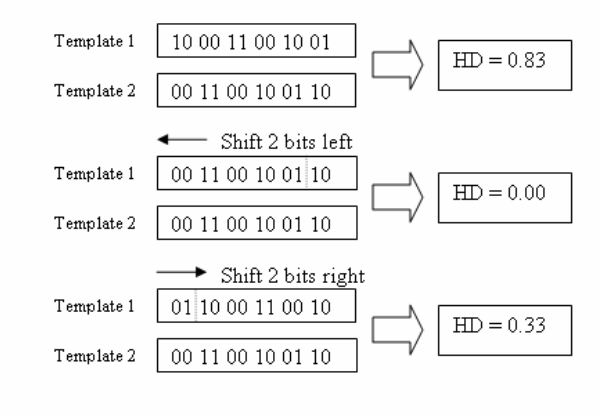
U sljedećoj tablici prikazano je kolika je vjerovatnoća greške u zavisnosti od vrijednosti Hammingove distance. Za vrijednosti Hammingove distance koje su manje od 0.26 smatra se da je vjerovatnoća greške jednaka 0, tj. da se radi o istim dužicama.

Vrijednost HD	Vjerovatnoća greške
0.26	$1 : 10^{13}$
0.27	$1: 10^{12}$
0.28	1: 84 biliona
0.29	1: 8.6 bilona
0.30	1: 1 bilion
0.31	1: 127 miliona
0.32	1: 18 miliona
0.33	1: 2.9 miliona
0.34	1: 527 000
0.35	1: 105 000

Tabela 5.3.1. Prikaz vjerovatnoće greške usljed različitih vrijednosti Hammingove distance

ŠIFTOVANJE KODA

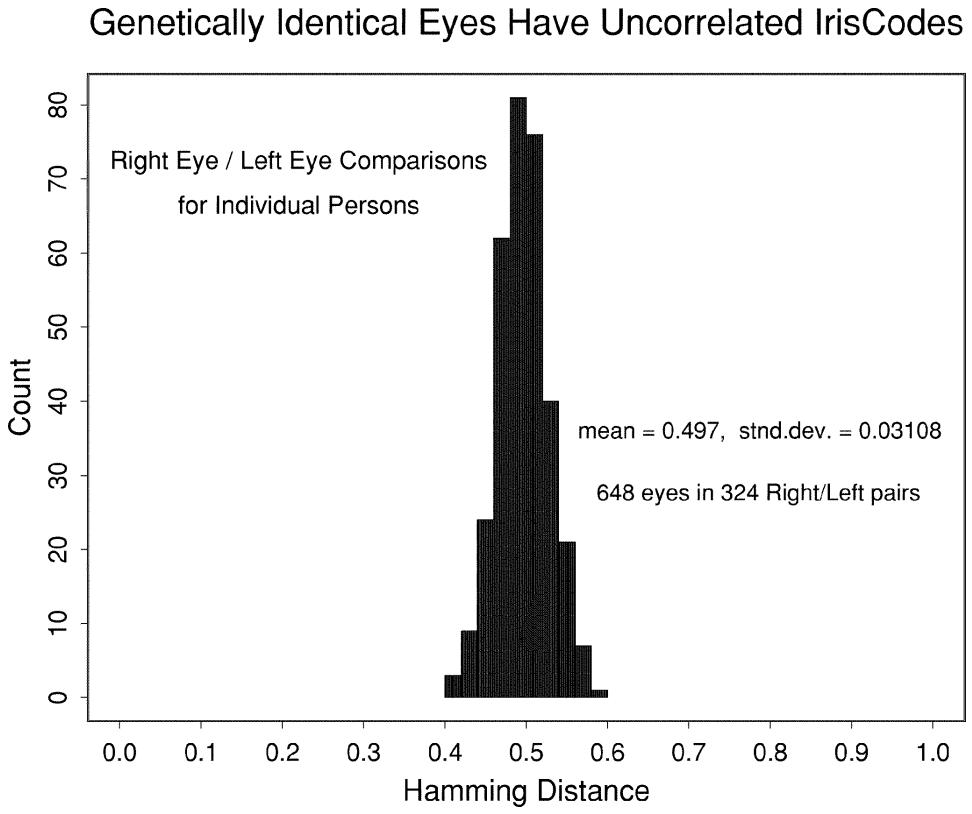
Da bi se uklonile nepravilnosti usljed rotacije slike Daugman je predložio proces šiftovanja nakon što se izračuna Hammingova distanca dva koda [126]. Svako šiftovanje je definisano kao šiftovanje dva bita u lijevu stranu i šiftovanje dva bita u desnu stranu. Zatim se za obe vrijednosti računa Hammingova distanca i uzima se najmanja vrijednost jer se ti kodovi najbolje podudaraju. Šiftovanje se vrši u horizontalnom smjeru, odnosno u θ smjeru, jer odgovara ugaonoj rotaciji regiona dužice. Na sljedećoj slici prikazano šiftovanje koda, jedno u desnu i jedno u lijevu stranu, kao i dobijene vrijednosti Hammingovih distanci.



Slika 5.3.21 Ilustracija procesa šiftovanja koda i dobijanje najmanje Hammingove distance,u ovom slučaju 0.

5.3.3 DUŽICE ISTOG GENOTIPA

Često postavljano pitanje je: Šta je sa dužicama blizanaca? U kakvoj su vezi i da li se na taj način može "prevariti" sistem? Međutim, upoređivanjem velikog broja dužica lijevog i desnog oka iste osobe, dokazano je da čak i genetički identične dužice imaju različite kodove, odnosno potpuno drugačije teksture. Kao ilustracija, na slici 5.3.22, date su vrijednosti Hammingovih distanci nakon poređenja dužica lijevog i desnog oka iste osobe [123]. Vidi se da su vrijednosti iste kao da se radi o paru dužica različitih osoba. Isto tako je i sa dužicama blizanaca. Tekstura dužice nije genotip, nije nasljedna kao što je to slučaj sa bojom dužice. Tekstura zavisi od početnih uslova u mezodermu embriona i jedinstvena je za svaku dužicu [136].



Slika 5.3.22 Distribucija Hammingove distance za poređenje dužica lijevog i desnog oka iste osobe

5.3.4 PERFORMANSE U POGLEDU BRZINE

Test je rađen na računaru čiji je takt procesora 300MHz.

Operacija	Vrijeme koje je potrebno za izvršenje operacije u milisekundama
Podešavanje fokusa slike	15 ms
Uklanjanje odsjaja	56 ms
Lokalizacija oka i dužice	90 ms
Pronalaženje zjenične granice	12 ms
Detektovanje i uklanjanje kapaka sa slike	93 ms
Uklanjanje trepavica i linija od kontaknih sočiva	78 ms
Demodulacija i kreiranje koda dužice	102 ms
XOR komparacija između dva koda dužice	10 ms

Tabela 5.3.2. Vrijeme izvršavanja operacija

5.3.5 PREDNOSTI I NEDOSTACI TEHNOLOGIJE PREPOZNAVANJA DUŽICE

U odnosu na ostale biometrijske identifikacione tehnologije, tehnologija skeniranja dužice ima bitnih, prednosti.

Jedna od prednosti je izolovanost i zaštićenost dužice od spoljašnje sredine. Ova osobina donosi prednost u odnosu na, recimo, tehnologiju prepoznavanja otiska prsta.

Šara irisa posjeduje visok stepen slučajnosti:

- 244 stepena slobode.
- 3.2 bita podataka po kvadratnom milimetru [122, 123].

Šara dužice je nezavisna od genetskog porijekla. Šare dvije dužice koje potiču od istog genotipa razlikuju se.

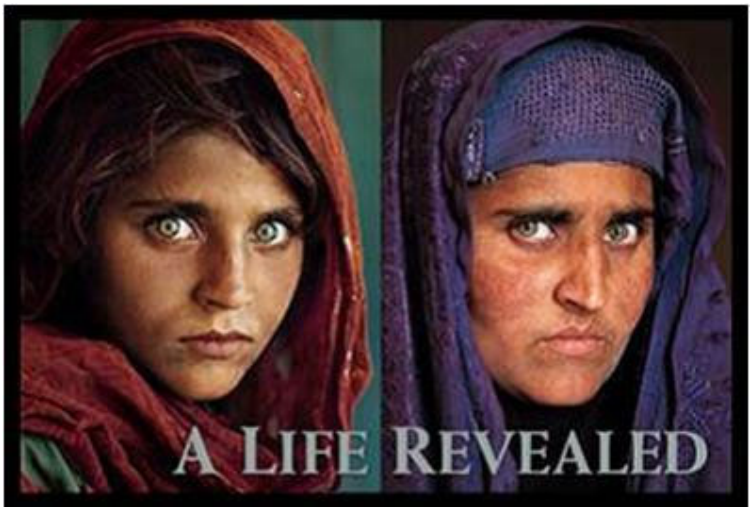
Fiziološka reakcija dužice na svjetlo predstavlja prirodni test za detekciju falsifikata. Slična povoljnost ne postoji kod drugih dijelova čovječijeg tijela, koji se koriste za identifikaciju. Ova osobina čini da je identifikacija na osnovu prepoznavanja dužice jedna od najpouzdanijih biometrijska identifikacija danas.

Falsifikovanje, dužice, hirurškom intervencijom je veoma komplikovano i nose neprihvatljiv rizik za gubljenje vida. S druge strane, hirurške intervencije sa ciljem falsifikovanja znatno su izvodljivije, na prstu ili čovječijem licu .

Karakteristike dužice se ne mijenju sa protokom vremena [118, 119]. U ovom pogledu dužici može parirati jedino glas. Na slici 5.3.23 može se uočiti koliko se protokom vremena mijenja lice osobe, dok dužica ostaje nepromijenjena.

Šara dužice je vidljiva i sa rastojanja što donosi prednost u odnosu na tehnologiju identifikacije mrežnjače [94].

Enkodiranje i prepoznavanje dužice se može prilično lako realizovati. Vrijeme koje je potrebno za analizu slike može se svesti i na oko jednu sekundu, dok brzina pretraživanja, uz upotrebu procesora 300MHz je oko 100,000 IrisCode profila u sekundi.



Slika 5.3.23 Slike iste osobe iz različitih perioda života

Kao nedostatak, može se navesti to što je veličina dužice svega 1cm pa njeno skeniranje zahtijeva striktnu saradnju korisnika. Za vrijeme skeniranja korisnik mora stajati mirno u propisanom položaju.

Sekeniranje dužice, dalje, otežava njena pokretljivost. Povremeno spuštanje očnih kapaka takođe ometa proces skeniranja.

Promjene veličine zjenice izazivaju neelestične deformacije dužice [123]. Usljed toga prilikom skeniranja najčešće se koristi infracrvena svjetlost.

Još uvijek postoji neskad između tvrdnji o tačnosti i pouzdanosti tehnologije skeniranja dužice i onoga što je ova tehnologija, danas, u stanju da pruži.

5.3.6 PRIMJENE TEHNOLOGIJE PREPOZNAVANJA DUŽICE

Brojne su primjene tehnologije skeniranja dužice. Primjenjuje se:

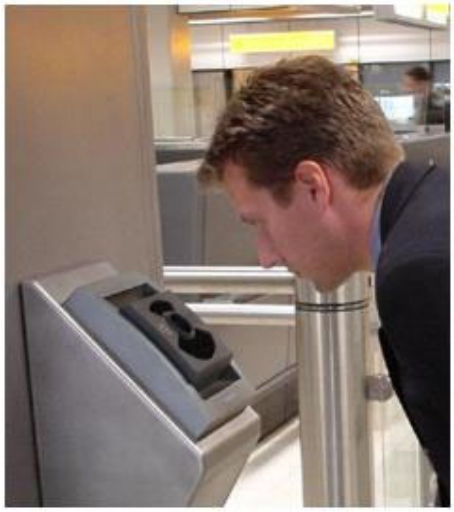
- kao zamjena za pasoše i identifikacione kartice,

- za obezbjeđenje sigurnosti u vazduhoplovstvu,
- za kontrolu pristupa određenim prostorima na aerodromu,
- za kontrolu pristupa bazama podataka i prijavljivanje na kompjuterske mreže,
- za kontrolu pristupa zgradama i kućama,
- za evidencije i kontrole pristupa u bolnicama,
- za provjeru identiteta na graničnim prelazima,
- itd..

Jedna od najvećih primjena tehnologije skeniranja dužice realizovana je od strane Ministarstva unutrašnjih poslova Ujedinjenih Arapskih Emirata (UAE). Na svih 17 zračnih, zemaljskih i morskih luka u UAE vrši se prepoznavanje dužice oka svih putnika koji ulaze u zemlju. IrisCode profil svakog putnika poredi se sa više od pola milliona IrisCode profila ljudi protjeranih iz UAE. IrisCode protjeranih uzet je prilikom protjerivanja i smješten u centralnu bazu podataka. Vrijeme koje je potrebno da bi se izvršila pretraga baze je oko jedna sekunda. Prosječno se dnevno izvrši provjera dužice za oko 7000 putnika. Na slici 5.3.24 prikazan jedan od kontrolnih punktova u UAE [139].

Slika 5.3.24 Jedan od kontrolnih punktova u UAE za identifikaciju na osnovu prepoznavanje dužice oka

Više aerodroma širom svijeta imaju instalisane identifikacione sisteme zasnovane na prepoznavanju dužice. Ovi sistemi služe, za provjeru putnika u cilju kontrole imigracije. Neki od aerodroma u kojima postoje ovi sistemi su London Heathrow, Amsterdam Schiphol, Frankfurt, Athens i nekoliko kanadskih aerodroma (Toronto, Vancouver, ...). Na slici 5.3.25 prikazan je uređaj za prepoznavanje dužice na amsterdamskom aerodromu Schiphol [140].



Slika 5.3.25 Uređaj za prepoznavanje dužice na amsterdamskom aerodromu Schiphol

Komisija Ujedinjenih Nacija za izbjeglice, poslije pada Talibanskog režima, kontroliše, i novčano potpomaže, povratak Afganistanskih izbjeglica iz susjednih zemalja. Umjesto dokumentacije kao što su lična karta, pasoš i sl., za identifikaciju i evidenciju izbjeglica koriste se sistemi za prepoznavanja dužice oka. Kroz ovaj program prošlo je više od 450.000 hiljada ljudi i dobijeno je isto toliko IrisCode profila. Na slici 5.3.26 prikazana je prostorija za skeniranje dužice u Takhtabaig Voluntery Repatriation centru, na Pakistansko-Avganistanskoj granici. Sistem koji je ovdje primijenjen je Bio-ID, a prikazana kamera je LG IrisAccess-2000 [140].

Slika 5.3.26 Prostorija za skeniranje dužice u Takhtabaig Voluntery Repatriation centru, na Pakistansko-Avganistanskoj granici.

U Velikoj Britaniji, u srednjoj školi u mjestu Sanderlend, postavljen je čitač koji može da prepozna osobu na osnovu snimka dužice oka. Čitač je

postavljen u školskoj kantini s ciljem da se učenicima omogući dobijanje obroka bez plaćanja gotovim novcem. Za prepoznavanje učenika dovoljno je nekoliko sekundi snimanja oka i još nekoliko trenutaka za uspoređivanje rezultata s bazom podataka učenika škole. Po istom principu, uređaj će biti postavljen i u školskoj biblioteci (Slika 5.3.27) [142].

Slika 5.3.27 Skener za identifikaciju na osnovu prepoznavanja dužice, postavljen u školskoj kantini u srednjoj školi u Sanderland-u

5.4 PREPOZNAVANJE LICA

Lice je dio čovjekove spoljašnjosti na osnovu kojeg se ljudi međusobno prepoznaju. Ljudi imaju urođenu sposobnost prepoznavanja lica. U poslednjih desetak godina čine se intezivni napori da se takva sposobnost razvije i kod kompjutera [143, 144].

Osim u slučaju identičnih blizanaca, svako lice posjeduje skup jedinstvenih fizičkih karakteristika, koje je moguće mjeriti i međusobno porediti [145].

U procesu prepoznavanja lica ne zahtijeva se fizički kontakt sa skenerom (kamarom). Prilikom implementacije sistema za prepoznavanje lica koristi se postojeća oprema kao što je web kamera, sigurnosna kamera itd. [146].

Lice nije u toj mjeri jedinstveno kao što je to slučaj sa otiskom prsta ili dužicom oka, pa je i njegova pouzdanost prepoznavanja nešto niža. Međutim, uzevši u obzir jednostavnost korištenja ova tehnologija ipak nalazi brojne primjene. Često se koristi u kombinaciji sa tehnologijom identifikacije otiska prsta ili drugom biometrijskom tehnologijom koja pruža veći nivo sigurnosti identifikacije [96].

Multi-biometrijski koncept identifikacionih sistema predstavlja dobro rješenje za obezbjeđenje visoke pouzdanosti identifikacije. Poznato je da u biometrijskim sistemima, usljed potrebe postojanja margine greške, sa porastom broja korisnika dolazi do povećanja FAR-a. Ovaj procenat može postati neprihvatljivo velik u aplikacijama sa velikom bazom podataka. U ovim situacijama često se pribjegava multi-biometrijskom sistemu u kojem se kao dopuna osnovnoj metodi često koristi tehnologija prepoznavanja lica.

Danas se u svijetu veliki broj kompanija i naučnih ustanova bavi razvojem tehnologije preoznavanja lica. Razvijeno je više algoritama [146, 147, 148, 149].

Na primjer, kompanija Visionics iz New Jersey-a je razvila softver za prepoznavanje lica, nazvan FaceIt, dok je kompanija Biometrix nudi softver BioFace. Ovi softveri su u stanju da izaberu lice iz svjetine, izdvoje to lice iz ostatka scene, izmjere njegove karakteristike i porede ih sa karakteristikama drugih lica iz baze podataka (Slika 5.4.1) [150, 151].

Slika 5.4.1 Slika ustupljena od od strane Visionics-a

Od naučnih ustanova, može se naglasiti, Colorado State University, gdje je razvijeno više algoritma za prepoznavanje lica [152, 153].

Tokom 90-tih godina prošlog vijeka, tačnije od 1993 do 1997 godine, organizovano je više skupova za procjenu mogućnosti i trenutnog razvoja tehnologije prepoznavanja lica (tzv FERET Evaluations) [154]. Od 2000 godine periodično se vrši procjena dostignuća u ovoj oblasti, kroz organizovanje Face Recognition Vendor Test-ova (FRVT). U ovom testiranju učestvuje više komercijalnih firmi koje se nezavisno bave razvojem tehnologije prepoznavanja lica. Testiranje omogućuje procjenu kvaliteta i nedostataka pojedinih rješenja iz ovog domena kao i određivanje smjernica daljeg razvoja. Do sada je ovakvo testiranje održano 2000, 2002 i 2005 godine [155, 156, 157, 158].

Kao rezultat povećanog angažovanja tehnologija prepoznavanja lica bilježi stalni napredak.

5.4.1 POSTUPAK PREPOZNAVANJA LICA

Kao što je već rečeno, svako lice ima svoje osobene karakteristike koje mu daju prepoznatljivost. Karakteristike lice koje se mogu mjeriti i koristiti za kasniju identifikaciju u daljem tekstu će se nazivati ključni detalji. Postoji oko 80 ključnih detalja na ljudskom licu. Neki od tih detalja su:

- Rastojanje između očiju,
- Širina nosa,
- Dubina očnih udubljenja,
- Jagodice,

- Vilična linija,
- Brada,
- …

Ključni detalji se mjere i formira se numerički kod, odnosno niz brojeva, koji predstavlja lice u bazi podataka -″faceprint″ (Slika 5.21). Obično algoritmi za prepoznavanja lice ne koriste svih osamdeset ključnih detalja. Na primjer, Visionics-ov FaceIt softver koristi svega 14 do 22 ključna detalja [150].

Kao i kod drugih biometrijskih identifikacionih sistema i ovdje razlikujemo proces upisivanja i proces identifikacije.

Faza upisivanja obično traje nekih 20 do 30 sekundi, tokom kojih se uzima nekoliko fotografija istog lica. Idealno je da se fotografije uzimaju sa blago različitim uglovima lica prema kameri. Nakon uzimanja fotografija, izdvajaju se karateristične osobine lica i kreira faceprint [145].

Postoje različiti algoritmi za prepoznavanja lica ali, uglavnom, svi oni sadrže sljedeće faze:

1. Fazu detekcije
2. Fazu podešavanja
3. Fazu normalizacije
4. Fazu kodiranja i
5. Fazu komparacije.

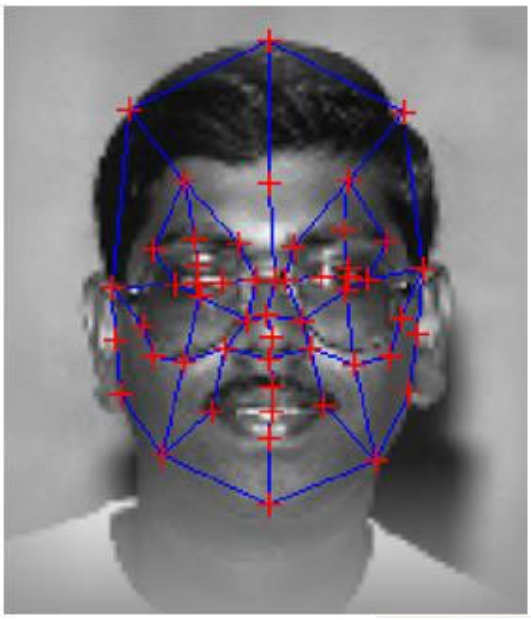
U fazi detekcije softver za prepoznavanje lica, trazi lice u polju vidljivosti kamere. Ova pretraga se vrši sa niskom rezolucijom slike. Tek kada se detektuje oblik koji podsjeća na ljudsku glavu, softver prebacuje kameru u režim rada sa visokom rezolucijom. Pouzdanost identifikacije veoma zavisi od kvaliteta fotografije.

Nakon faze detekcije prelazi se na fazu podešavanja. U ovoj fazi određuje se pozicija, veličina i orijentacija glave. Zatim se vrši prevođenje trodimenzionalnog prikaza glave u dvodimnenzionalnu nefrontalnu sliku. Na kraju, dvodimenzionala nefrontalna slika se prevodi u dvodimenzionalnu frontalnu sliku.

Najveći broj sistema za prepoznavanje lica vrši prepoznavanje iz tzv. ″mirne slike″. Pod ″mirnom slikom″ se podrazumijeva frontalna slika, sa uobičajenim izrazom čovječijeg lica. U odnosu na korištenje ″žive slike″, ovo, u prvom redu, značajno smanjuje veličinu numeričkog koda kojim se slika predstavlja u bazi podataka [142]. Da bi se dobila ″mirna slika″ nakon faze podešavanje potrebno je normalizovati frontalnu sliku. Pod normalizacijom se podrazumijeva statistička tehnika kojom se vrši korekcija razlika u licu istog čovjeka na različitim slikama. Normalizacione korekcije donekle umanjuju razlike i između različitih lica. Ipak, dosadašnja ispitivanja su pokazala da sistemi koji za identifikaciju koriste tzv. ″živu sliku″ ne postižu značajno bolje rezultate [158].

Nakon faze normalizacije pristupa se fazi kodiranja, koja je i ključna faza u procesu prepoznavanja lica. U fazi kodiranja vrši se mjerenje,

odnosno prevođenje ključnih detalja sa normalizovane dvodimenzione frontalne slike glave u jedinstveni digitalni kod (Slika 5.4.2) [145].



Slika 5.4.2 Faza kodiranja – mjerenje ključnih detalja lica

Dobijeni digitalni kod (faceprint), se u fazi komparacije koristi za poređenje sa drugim raspoloživim kodovima iz baze podataka.

Pouzdanost sistema za prepoznavanja lica je funkcija kvaliteta slika, kao i demografskih karakteristika populacija koja koristi sistem. Experimenti su pokazali da je lakše prepoznati muškarce nego žene, kao i da je lakše prepoznati starije nego mlađe ljude. Rezultati takođe pokazuju da razlike u lakoći prepoznavanja, muškaraca i žena, opadaju sa njihovim starenjem [156, 158].

Poznato je da protok vremena uslovljava stalne promjene na licu. Usljed toga, od trenutka upisivanja faceprinta u bazu podataka, pouzdanost prepoznavanja lica opada [142, 145, 155]. U ovom pogledu tehnologija prepoznavanja lica zaostaje u odnosu na tehnologiju prepoznavanja dužica i tehnologiju prepoznavanja otiska prsta.

Kao i u slučaju tehnologije prepoznavanja otiska prsta i tehnologija prepoznavanja lica je prilično ugrožena mogućnošću falsifikovanja [158].

5.4.2 NEKE PRIMJENE TEHNOLOGIJE PREPOZNAVANJA LICA

Prvi korisnici sistema za prepoznavanje lica bile su organizacije za sprovođenje zakona kao što su policija, sudovi itd.. Policija ove sisteme često koristi za nadzor određenih prostora. Nadzor se sastoji u provjeri identiteta slučajno odabranog lica iz svjetine. Na slici 5.4.3, prikazana jedna policijska kontrolna soba, iz koje se, može uzeti fotografija slučajno odabranog lica [159]. Fotografija se zatim prevodi u feceprint koji se poredi sa faceprint-ovima iz baze podataka. Baza podataka sadrži faceprint-ove ljudi koji su povezanai sa raznim kriminalnim aktivnostima.

Slika 5.4.3 Upotreba Visionics FaceIt softvera za prepoznavanje lica u policijskoj kontrolnoj sobi

Poznatiji sistemi za sigurnosni nadzor koji koriste tenologiju prepoznavanja lica su Virginia Beach Surveillance, City of Brentwood Police Department, Zurich Airport Face, Manchester NH Viisage, itd. [160].

Osim za sigurnosni nadzor sistemi za prepoznavanje lica se koriste i za druge namjene kao što su:

- sprečavanje lažnog glasanja na izborima,
- provjera identiteta prilikom upotrebe automata za keširanje novca,
- umjesto lozinke za pristup kompjuteru.

Jedan od prvih, značajnijih, primjena sistema za prepoznavanje lica u cilju sprečavanja lažnog glasanja na izborima, bila je od strane Meksičke vlade, za predsjedničke izbore 2000. godine. Da bi se što više uticalio na ishod izbora mnogi ljudi su bili registrovani pod različitim imenima i mogli su glasati više puta. Konvencionalni metodi za sprečavanje ovakvih

postupaka nijesu davali željene rezultate. Upotrebom tehnologije prepoznavanja lica, u trenutku glasanja, mogla se vršiti pretraga za duplikatima po glasačkoj bazi podataka. Novi faceprint se upoređivao sa već zabilježenim i tako se otkrivao onaj koji je pokušao glasati pod lažnim imenom.

Provjera identiteta, korištenjem tehnologija prepoznavanja, lica mogla bi povećati sigurnost korištenja aparata za keširanje novca. Ukoliko bi pored identifikacione kartice i PIN koda bila vršena i provjera faceprint-a korisnika, mogućnost krađe i neovlaštenih transakcija bila bi znatno smanjena (Slika 5.4.4) [160].

Slika 5.4.4 Uređaj za keširanje opremljen sistemom za prepoznavanje lica

Biometrijska tehnologija prepoznavanja lica može se upotrijebiti i za kontrolu pristupa kompjuteru. Montiranjem web kamere na kompjuter i instalacijom softvera, korisnikovo lice može zamijeniti lozinku za pristup kompjuteru (Slika 5.4.5). IBM je ugradio ovu tehnologiju unutar screensaver-a za A, T i X serija Thinkpad laptop-ova [161].

Slika 5.4.5 Softver za prepoznavanje lica može biti upotrijebljen za kontrolu pristupa kompjuteru

5.5 PREPOZNAVANJE GLASA

Od biometrijskih identifikacionih tehnologija zasnovanih na karakteristikama ponašanja, najveći se napori ulažu u razvoj tehnologije prepoznavanja glasa.

Upotreba sistema za prepoznavanje glasa je veoma jednostavna i jeftina. Intefejs između korisnika i sistema, može biti bilo koji audio uređaj, uključujući mobilne/fiksne telefone, PC mikrofone itd..

Prepoznavanje glasa se najčešće koristi u okruženju u kojem je glas jedini raspoloživi biometrijski identifikator. To su situacije kada je korisnik udaljen od identifikacionog centra.

Sistemi za prepoznavanje glasa nailaze na dobro prihvatanje od strane korisnika jer je glas najprirodniji način komunikacije za čovjeka.

Prepoznavanje glasa se često pogrešno poistovjećuje sa prepoznavanjem govora. U stvari, tehnologija prepoznavanja govora prevodi što je korisnik rekao, dok tehnologija prepoznavanja glasa, verifikuje identitet individue koja govori. Ipak, ove dvije tehnologije su često povezane. Na primjer, u nekom sistemu, prepoznavanje govora se može koristiti da se izgovorene riječi transformišu u, recimo, broj računa, a prepoznavanje glasa da se verifikuju vokalne karakteristike onoga ko je izgovorio te riječi [97].

5.5.1 POSTUPAK PREPOZNAVANJA GLASA

Osobine glasa dominantno su zavistne od oblika vokalnog trakta. Osijenčenim površinama na Slici 5.5.1 prikazan je prostor u ljuskom tijelu koji se naziva vokalni trakt [2].

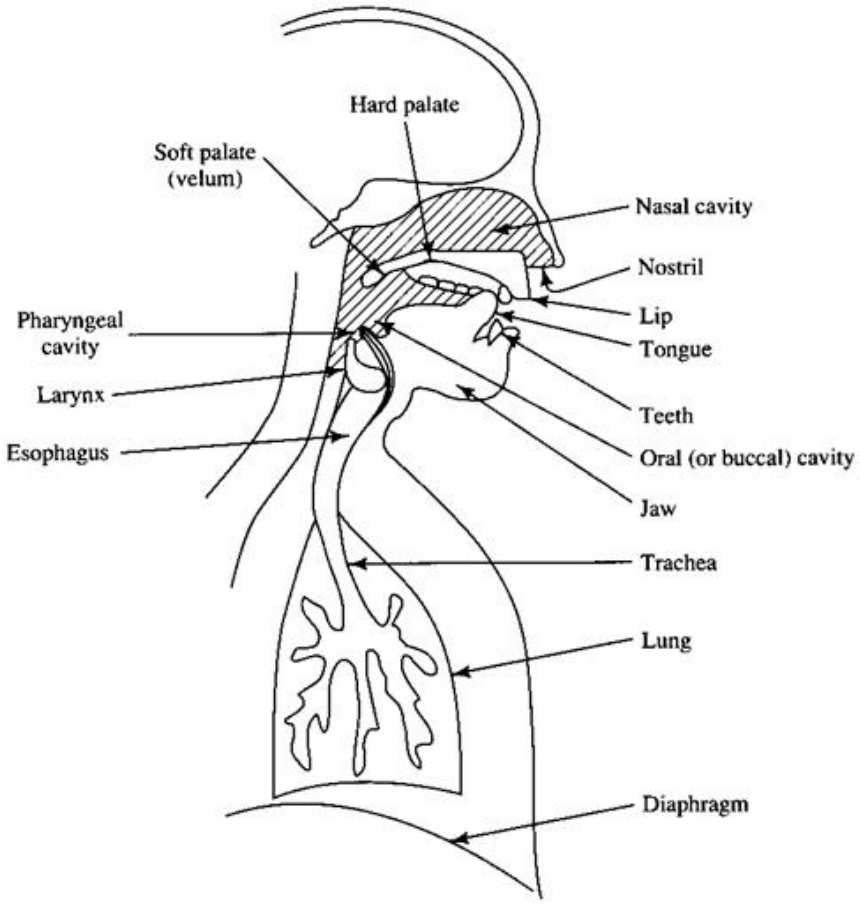
Generisanje glasa započinje na glasnim žicama. Između glasnih žica postoje prorezi. Kada započnemo sa govorom, mišići koji kontrolišu glasne žice, zatežu se. Kao rezultat toga, glasne žice se sužavaju. Prolazak našeg daha kroz proreze između između glasnih žica proizvodi glas. Jedinstvene karakteristike glasa oblikuju se prolaskom akustičnog talasa kroz vokalni trakt. Vokalni trakt modifikuje spektrani sadržaj glasa na način što neke harmonike pojačava dok druge prigušuje [162].

Prepoznavanje glasa vrši se digitalizacijom karakteristika ljudskog glasa i stvoranjem niza digitalnih podataka koji opisuju glas (″voice print″ ili ″profil glasa″). Digitalizacijaom se svaka izgovorena riječ svodi na segmente sastavljene od dominantnih frekvencija (formanta). Svaki segment ima nekoliko formanta. Svi formanti zajedno predstavljaju jedinstveni profil glasa [97, 163].

[2] Vokalni trakt se sastoji od: grkljana (ispod epiglotisa), grla (iza jezika, između epiglotisa i jednjaka, iza jednjaka, zadnji kraj nosne šupljine), usne šupljine (ispred jednjaka, ograničena usnama) i nosne šupljina (iznad nepca, produžena od pharynx-a do nozdrva).

Kao i kod drugih biometrijskih identifikacionih sistema i kod sistema za prepoznavanje glasa razlikuju se faza upisivanja i faza identifikacije.

U fazi upisivanja od osobe se zahtijeva da izgovori neku rečenicu i/ili niz brojeva. Korisnik, obično, ne govori duže od nekoliko sekundi. Odabir prekratke rečenice može rezultirati nemogućnošću prikupljanja dovoljne količine podataka o vokalnim karakteristikama glasa, dok preduga rečenica može donijeti obrnut efekat. U toku izgovaranja rečenice vrši se izdvajanje i digitalizacija glasovnih formanata i kreira profil glasa. Dobijeni profil se upisuje u bazu podataka i kasnije koristiti u identifikacijama. Da bi se dobio što bolji profil glasa, od korisnika se zahtijeva da više puta ponovi rečenicu. Potreba za višestrukim ponavljanjem čini da process upisivanja duže traje nego kod drugih biometrijskih identifikacionih sistema.



Slika 5.5.1 Vokalni trak - osijenčene površine na slici

Sistemi za prepoznavanje glasa mogu biti tekst zavisni, tekst nezavisni ili kombinacija ove dvije vrste [163, 164].

U tekst zavisnim sistemima, prilikom identifikacije, korisnik izgovara unaprijed definisane riječi ili rečenice. Ove rečenice, poznate kao ″pristupne rečenice″, mogu biti sastavljene od informacija kao što su ime, grad rođenja, omiljene boje, niz brojeva itd.. Glasovni profil dobijen iz

pristupnih rečenica na mjestu identifikacije, poredi sa glasovnim profilom istih tih rečenica dobijenim u procesu upisivanja.

U tekst nezevisnim sistemima ne koriste se unaprijed definisane pristupne rečenice. U ovim sitemima prepoznavanje se vrši na bazi signala govora dužeg trajanja. Veća dužina govora omogućuje sistemu da prepozna specifične glasovne karakterisike kao što su jačina, takt, tonalitet itd. [164].

Profil ljudskog glasa veoma je zavistan od zdravlja i emocionalnog stanja čovjeka. Da bi korisnik mogao biti prepoznat, on mora govoriti normalnim glasom, koji je koristio i prilikom kreiranja profila. Ako korisnik ima zdravstveni problem, kao što je nazeb ili je neuobičajeno uzbuđen ili depresivan, njegov glasovni profil se neće moći prepoznati.

Postoje i drugi faktori koji mogu uticati na rezultat prepoznavanja glasa. Pozadinski šum i loš kvalitet ulaznog uređaja (mikrofona) mogu stvoriti preobleme. Ukoliko se identifikacija vrši putem telefona, razlika u kvaltetu zvuka između mobilne i fikstne telefonije može uticati na uspješnost prepoznavanja.

Sistemi za prepoznavanje glasa ugroženi su i od pokušaja lažne identifikacije. Lažna identifikacija, na osnovu snimljenog glasa regularnog korisnika, je jedan on najčešćih slučajeva. U cilju sprečavanja ove mogućnosti razvijeni su mnogi sofisticirani algoritmi kojima se nastoji što pouzdanije provjeriti da li se radi o živom glasu ili snimku [97].

5.5.2 PRIMJENE TEHNOLOGIJE PREPOZNAVANJA GLASA

Tehnologija prepoznavanja glasa se danas najčešće koristi u sitemima u kojima se zahtijeva identifikacija na daljinu. Kao primjer se mogu navesti automatizovani pozivni centri i sistemi za obradu transakcija putem telefona ili kompjutera. Popularne aplikacije iz ove oblasti su finansijske transakcije (pristup računu, transver sredstava, plaćanje mjenica) i podrška sigurnosti u poslovanju kreditnim karticama [165, 166].

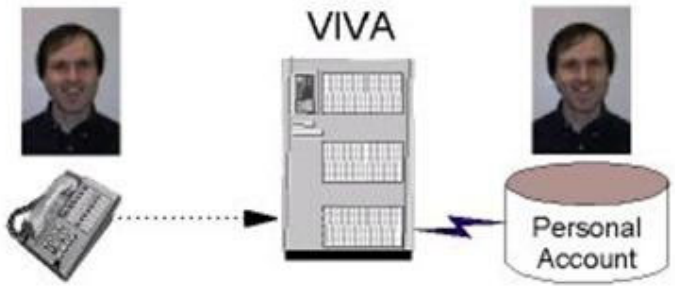
Kao primjer primjene tehnologije prepoznavanje glasa, može poslužiti Voice Identification and Verification Agent (VIVA), proizvod IBM-ovog istraživačkog tima [167]. VIVA omogućuje verifikaciju korisnika putem telefona. Verifikacija se vrši kombinovanjem dva izvora informacija:

1) Karakteristika glasa korisnika (″voice print″) i
2) Znanja korisnika (na primjer, lozinka i lične informacije)

Kombinacijom ova dva izvora, povećava se pouzdanost verifikacije. Proces verifikovanja sastoji se iz jedne ili nekoliko kratkih konverzacija. Tokom konverzacije VIVA korisniku postavlja slučajna pitanja, provjerava dobijene odgovore kao i ″voice-print″ korisnika.

Trajanje identifikacije zavisi od tačnosti odgovora i procjene ″voice-print″-a korisnika. U sučaju kada je na telefonskoj liniji regularani korisnik

konverzacija obično kratko traje i sastoji se od svega jednog pitanja. Usljed dobrog poklapanja glasovnih profila VIVA odmah zaključuje da je riječ o pravom korisniku (Slika 5.5.2).



Slika 5.5.2 Voice Identification and Verification Agent (VIVA)

U slučaju pokušaja lažnog predstavljanja konverzacija traje znatno duže. Usljed nepoklapanja glasovnih profila VIVA postavlja više pitanja sve dok prevarant ne da pogrešan odgovor ili VIVA ne zaključi da su glasovni profili definitivno različiti.

Eksperimentalno je utvrđeno da VIVA ima FAR manji od 0.00001% i FRR oko 3%.

GLAVA VI

IDENTIFIKACIONI SISTEMI

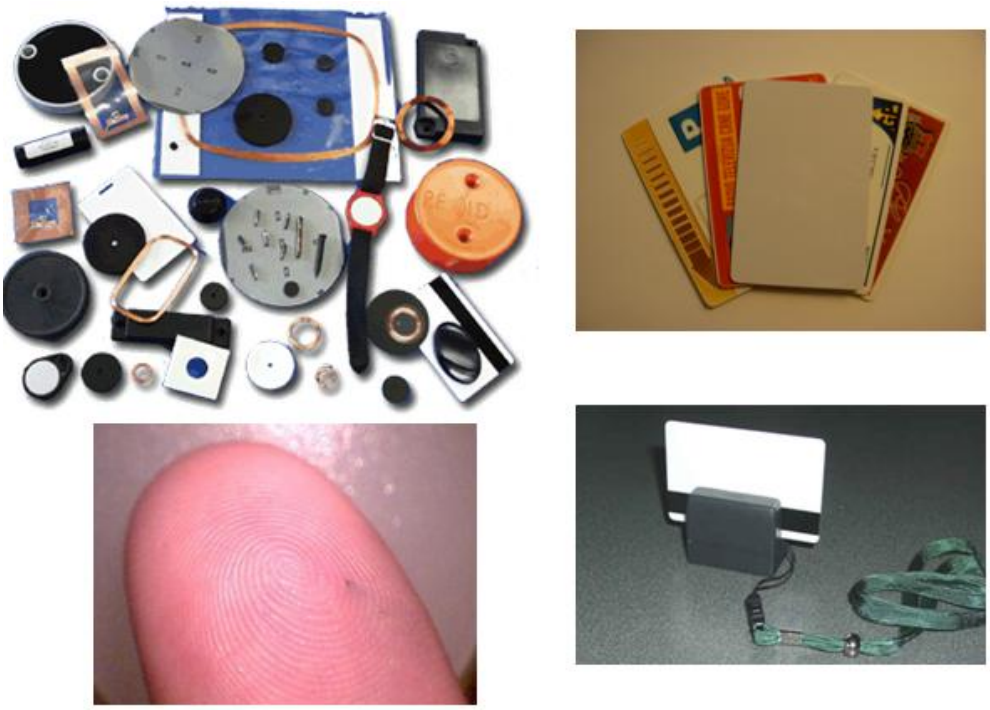
U pretodnim poglavljima dat je opis najčešće korištenih identifikacionih tehnika. Pokazano je da postoji velika raznovrsnost u pogledu načina identifikacije ljudi i objekata. Svaka od navedenih tehnika ima svoje prednosti i nedostatke. Odluka, koju tehniku primijeniti za konkretnu situaciju, donosi se uzimajući u obzir specifičnosti konkretne primjene.

Prilikom opisa identifikacionih tehnika najveća pažnja posvećivana je opisu samog identifikatora kao i njegovog čitača. Međutim, identifikatori i čitači, iako veoma važni, samo su dio identifikacionog sistema. Kompletan identifikacioni sistem, najčešće, se sastoji iz sljedećih segmenata:

- identifikatora,
- čitača,
- logeri podataka (engl. data loggers),
- baze podataka,
- aplikativnog programa i
- ostale prateće opreme.

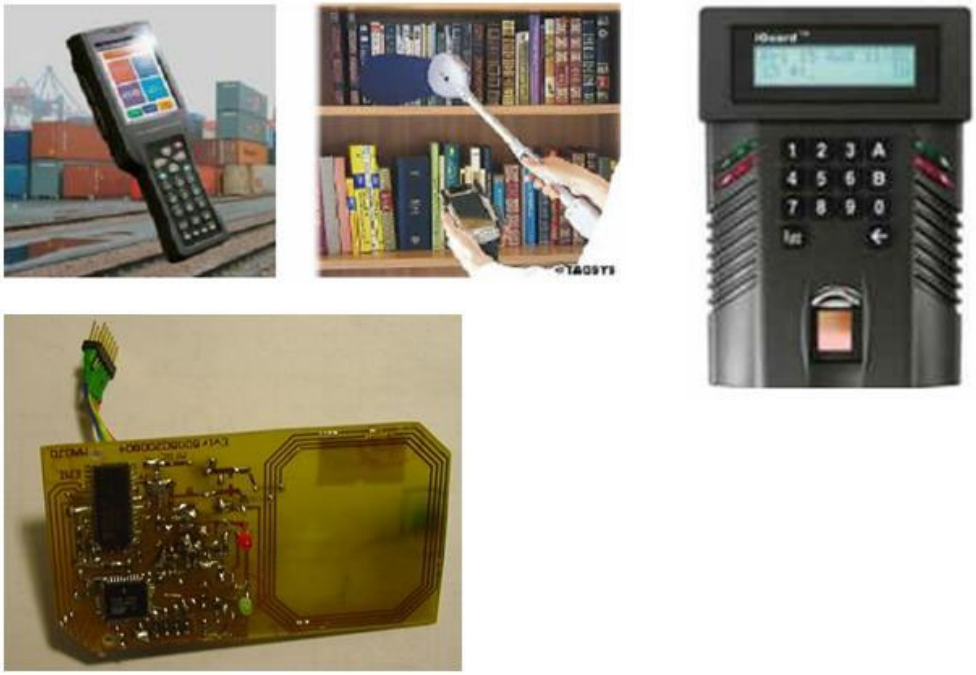
6.1 IDENTIFIKATORI I ČITAČI

Osnovna podjela identifikatora je na tradicionalne i biometrijske (Slika 6.1). U najčešće korištene tradicionalne identifikatore spadaju trakasti kodovi, magnetne kartice, opričke kartice kao i kontaktne i beskontakne pametne kartice. Najčešće korišteni biometrijski identifikatori su prst, dužica oka, lice i glas (Slika 6.1.1).



Slika 6.1.1 Razni tipovi identifikatora

Čitači identifikatora se takođe mogu svrstati u dvije grupe i to, čitači tradicinalnih identifikatora i biometrijski čitači. Prema načinu upotrebe čitači se dijele na fiksno montirajuće i prenosive (ručne) čitače (Slika 6.1.2).



Slike 6.1.2 Čitači identifikatora

O identifikatorima i čitačima već je prilično toga rečeno u prethodnim poglavljima, tokom opisa identifikacionih tehnika. Stoga će se ovo poglavlje pretežno baviti preostalim komponentama identifikacionog sistema.

6.2 LOGERI PODATAKA

Logeri podataka, ili skraćeno logeri, su uređaji koji samostalno prikupljaju podatke i smještaju ih u internu memoriju. Uz pomoć personalnog računara ti podaci se u bilo kom trenutku mogu preuzeti i dalje obrađivati [167], [168].

Izvori podataka za loger mogu biti različiti uređaji. Najčešće su to razni instrumenti i senzori, koji su ponekad i sastavni dio logera. Podaci od strane izvora se mogu biti analogni ili digitalni.

Glavni djelovi logera su mikrokontroler i interna memorija za smještanje podataka. Interna memorija može biti RAM, SRAM, EEPROM, FLASH, USB-FLASH, ...

Logeri se mogu realizovati kao mali, baterijski napajani, prenosivi uređaji.

Najčešće logeri posjeduju interfejs za povezivanje sa računarom. Interfejs može biti bezžični ili sa kablovima. Na računaru se nalazi softver pomoću koga se podaci iz logera preuzimaju i dalje obrađuju. Neki logeri imaju LCD monitor i tastaturu i mogu se koristiti kao samostalni uređaji (Slika 6.2.1).

Prilikom korištenja englenske literature, pretragu za podacima o logerima treba vršti koristeći naziv "data logger", ne samo "logger". Samo "logger" na englenskom znači drvosječa, i vodi ka podacima iz sasvim druge oblasti rada.

Slika 6.2.1 Različite realizacije logera

Primjenom logera, u sistemu se dobija mogućnost autonomnog prikupljanja podataka u dužem vremenskom periodu. To je glavni dobitak od upotrebe logera. Nakon aktiviranja, logeri se, u pravilu, ostavljaju da samostalno prate proces za koji su predviđeni i prikupljaju podatke o njemu.

Kao interesantni primjeri primjene logera mogu se navesti:

- FDR (Flight Data Recorder). Koristi se za snimanje podataka o letu aviona.
- EDR (Evant Data Recoreer). Ovaj uređaj, neki proizvođači ugrađuju u automobile i služi da pruži potrebne podatke o vožnji. Podaci postaju posebno interesantni u slučaju udesa.
- UWDR (Ultra Wideband Data Recorder). Loger koji je u stanju prihvatati podatke brzinom od 2 GigaSample u sekundi.

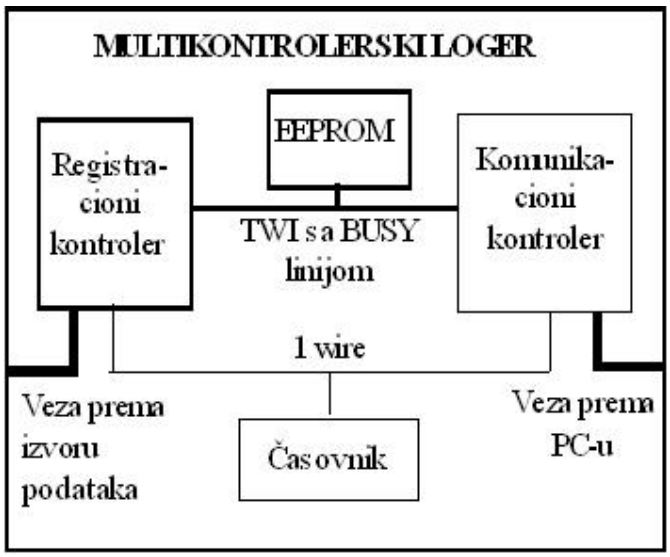
Logeri su, često, sastavni dio identifikacionog sistema. Oni obezbjeđuju da sistem može da funkcioniše bez neprekidnog nadzora od strane PC-a.

U identifikacionim sistemima logeri se realizuju kao samostalni uređaji ili zajedno sa čitačem identifikatora, kao jedan uređaj (Slika 6.2.1).

6.2.1 OPIS STRUKTURE LOGERA

Na Slici 6.2.2 data je blok šema strukture jedne tipične realizacije logera. Sa slike se uočava da loger sadrži više mikrokontrolera u svojoj strukturi. Multikontrolerski koncept logera se primjenjuje jer se uočilo da se funkcije prikupljanja podataka i ostale funkcije logera mogu efikasno razdvojiti i

izvršavati zasebnim mikrokontrolerom. Pod ostalim funkcijama misli se na konfigurisanje logera, komunikaciju sa personalnim računarom, i dr.



Slika 6.2.2 Blok šema multikontrolerskog logera

Predstavljeni loger je realizovan angažovanjem tri mikrokontrolera. Jednim mikrokontrolerom vrši se prikupljanje podataka, drugim mikrokontrolerom obavlja se konfigurisanje logera i komunikacija sa PC-em, dok trećim mikrokontrolerom se obezbjeđuje praćenje realnog vremena (Časovnik). Ovaj koncept, uslovno rečemo, složenijeg hardvera omogućava značajno pojednostavljenje softvera logera te time njegov pouzdaniji i brži rad. Angažovanjem tri mikrokontrolera obezbjeđuje se i veća fleksibilnost u radu logera. Na primjer, loger nesmetano prikuplja podataka i u slučaju kada personalni računar preuzima već prikupljene podatake, pa čak i kada se u ostalim mikrokontrolerima vrši izmjena softvera. Korištenjem više mikrokontrolera obezbjeđuje se i dva puta više procesorskog vremena, više portova, UART-a, A/D konvertora, Tajmera itd.

Sa Slike 6.2.2 uočavaju se sljedeći osnovni sastavni djelovi logera:

- registracioni kontroler
- komunikacioni kontroler
- EEPROM i
- časovnik (mikrokontrole)

Osnovna uloga registracionog kontrolera je da prihvata podatke od strane izvora podataka i da ih putem two-wire serijskog interfejsa (TWI), zapisuje u EEPROM. Izvori podataka mogu biti vrlo različiti, zavisno od konkretne primjene logera. Recimo, kada se loger koristi u RF sistemu za evidenciju radnog vremena, izvori podataka su čitači kartica zaposlenih, koji su odgovarajućom vezom (RS232, RS485, ...) povezani sa registracionim kontrolerom. S druge strane, u sistemu za nadzor napajanja,

izvor podataka je interfejs preko koga loger dobija uvid u stanje napona na mreži.

Osnovni zadatak komunikacionog kontrolera je da komunicira sa personalnim računarom, i da na osnovu te komunikacije vrši upis i/ili čitanje podataka EEPROM-a. Tako, posredstvom komunikacionog kontrolera, PC može da izvrši upis podataka u željeni dio EEPROM-a kao i da pročita podatke iz željenog dijela EEPROM-a. Osim toga PC, posredstvom komunikacionog kontrolera, može da definiše način rada registracionog i komunikacionog kontrolera.

EEPROM je centralni dio logera. U EEPROM-u se nalaze konfiguracioni podaci koji definišu način rada logera kao i podaci o evidentiranim događajima. Unutar EEPROM-a podaci su raspoređeni (prema svojoj namjeni) u memorijske cjeline, nazvane fajlovi. Na slici 6.2.3 data je memoriska mapa EEPROM-a logera.

DIREKTORIJA
FAJL 1
FAJL 2

FAJL N

Slika 6.2.3 Memorijska mapa EEPROM-a

Na najžim adresama u EEPROM-u nalazi se fajl Direktorija. Fajl Direktorija daje informaciju na kojoj adresi u EEPROMu se nalaze počeci ostalih fajlova. Na slici 6.2.4 data je memoriska mapa fajla Direktorija.

Niži oktet adrese početka prvog fajla (LOW1)	Viši oktet adrese početka prvog fajla (HIGH1)
Niži oktet adrese početka drugog fajla (LOW2)	Viši oktet adrese početka drugog fajla (HIGH2)
Niži oktet adrese početka trećeg fajla (LOW3)	Viši oktet adrese početka trećeg fajla (HIGH3)
…	
Niži oktet adrese početka n-tog fajla (LOWn)	Viši oktet adrese početka n-tog fajla (HIGHn)
(0)LOW	(0)HIGH

Slika 6.2.4 Memorijska mapa fajla Direktorija

U fajlu Direktorija adresa početka fajla data je sa dva okteta koji označavaju memorikjski segment. Veličina segmenta zavisi od veličine memorijskog prostora koji se želi adresirati. Na primjer ukoliko se želi adresirati memoriski prostor veličine do 1MB, veličina segmenta je 16 okteta. Fizička adresa se dobija kao

AdresaPočetkaFajla-n = ((HIGHn)*256+LOWn)*16

Kraj fajla Direktorija označava se sa dva okteta vrijednosti 0. Okteti od kraja fajla Direktorija pa do prvog okteta sa adresom djeljivom sa 16, se preskaču. Njihova vrijednost nije od značaja

Na Slici 6.2.5 data je memorijska mapa EEPROMA-a logera kada se on koristi u sistemu za evidenciju radnog vremena.

DIREKTORIJA
Konfiguracioni fajl
Fajl korisnia
Fajl prava korisnika
Fajl dogadjaja

Slika 6.2.5 Memorijska mapa EEPROM-a kada se loger koristi u sistemu za evidenciju radnog vremena

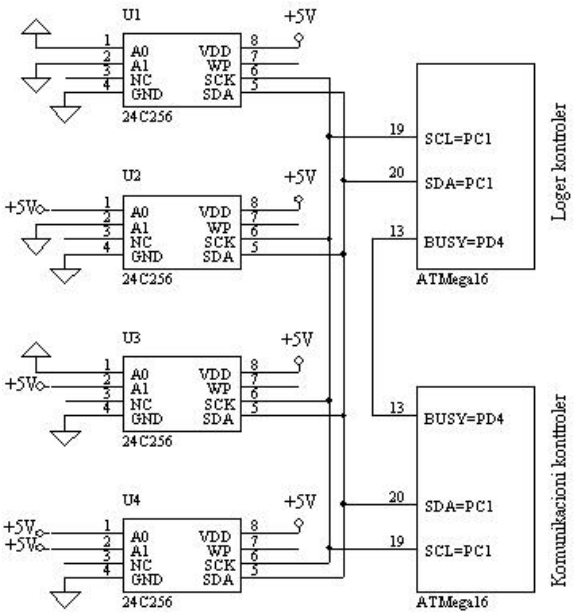
Svaki fajl u EEPROM-u sastoji se od zapisa. Kraj fajla se označava zapisom u kojem svaki oktet ima vrijednost nula

U svakoj primjeni logera, poslednj fajl u EEPROM-u (fajl na najvišim adresama) je fajl u koji se upisuju podaci o dogadjajima u procesu koji se prati (Fajl dogadjaja)

Za fajl događaja rezervisan je memorijski prostor od naznačenog početka fajla pa sve do kraja EEPROM-a. U fajl događaji registracioni kontroler kružno upisuje podatke pri čemu kraj uvijek označava sa zapisom u kojem svaki oktet ima vrijednost 0.

Podatke sa logera može preuzimati više personalnih računara koji imaju ostvaren komunikacioni put do logera. Svaki PC vodi računa dokle je stigao sa preuzimanjem podataka.

Na slici 6.2.6 prikazan je način povezivanja 128K EEPROM-a sa registracionim i komunikacionim kontrolerom. Za pristup EEPROM-u, kontroleri koriste two-wire serijski interfejs (TWI). TWI je idealan za tipične mikrokontrolerske aplikacije. TWI protokol dozvoljava povezivanje do 128 različitih uređaja korištenjem samo dvije bidirekcione magistralne linije, jednu za takt (SCL) i jednu za podatke (SDA) [169].



Slika 6.2.6 Povezivanje EEPROM-a sa komunikacionim i registracionim kontrolerom

Da ne bi dolazilo do dužeg zastoja u radu registracionog ili komunikacionog kontrolera usljed, čekanja na slobodan pristup EEPROM-u, nijedan kontroler ne smije, u jednom pristupu, dugo zauzeti magistralu EEPROM-a. Tako na primjer, ako se usvoji da maksimalno vrijeme jednog zauzimanja EEPROM-a ne smije biti duže od 50ms. Brzinom od 100kHz za TWI, koju podržavaju čak i najsporiji EEPROM-i moguć je upis 256 okteta u EEPROM može za 25ms. Kako jadan zapis od strane registracionog kontrolera, u većini aplikacija, ne prelazi 32 okteta, njegovo zauzimanje EEPROM-a traje čak znatno kraće. Može se podasiti da komunikacioni kontroler u jednom pristupu čita, odnosno upisuje, maksimalno 256 okteta EEPROM-a. Na ovaj način je obezbijeđeno da korištenje istog EEPROM-a komunikacionom i registracionom kontroleru ne predstavlja smetnju za obavljanje njihovih osnovnih funkcija [170].

6.3 BAZA PODATAKA

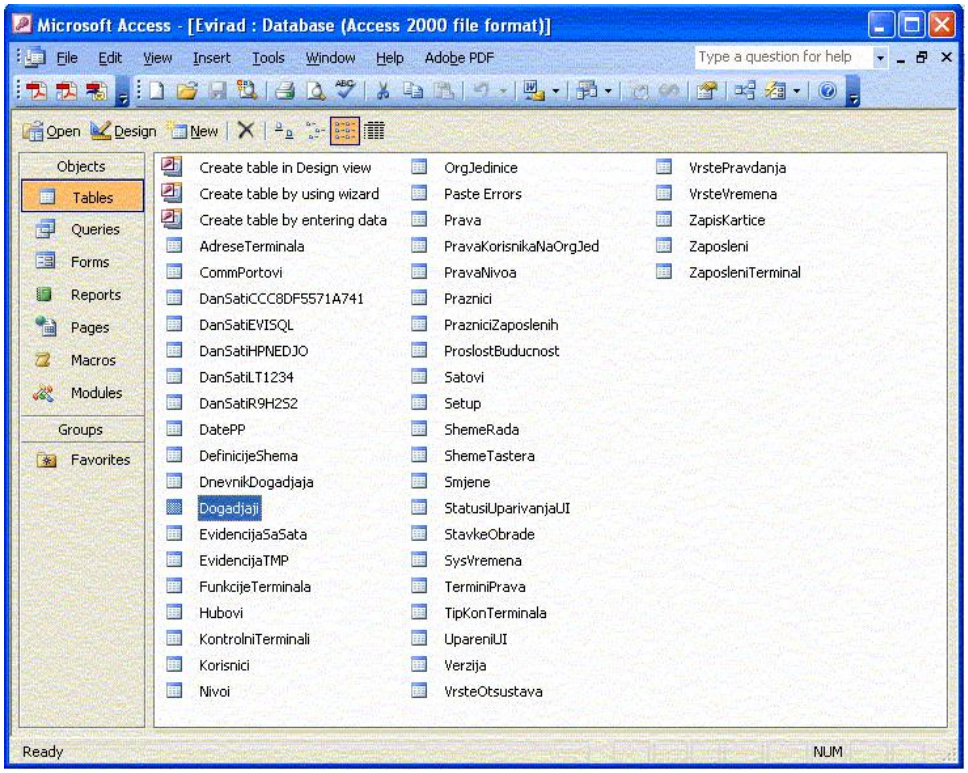
Baza podataka je neizbježan pratilac većine identifikacionih sistema, posebno onih u kojima je potrebno prikupljanje podataka o identifikacionom procesu.

U bazi podataka se nalaze:

- Konfiguracioni podaci, neophodni za definisanje načina rada komponenti sistema (čitača, logera, identifikatora, ...);
- Podaci o korisnicima sistema i njihovim pravima na sistemu;

- Podaci o izvršenim identifikacijama. Bez obzira da li se po izvršenoj identifikaciji podaci o tome odmah šalju računaru ili se smještaju u memoriji logera, njihovo krajnje odredište je baza podataka.

Na Slici 6.3.1 prikazana je glavna forma mdb baze podataka koja se koristi u identifikacionom sistemu za evidenciju radnog vremena.



Slika 6.3.1 Glavna forma mdb baze podataka u sistemu za evidenciju radnog vremena.

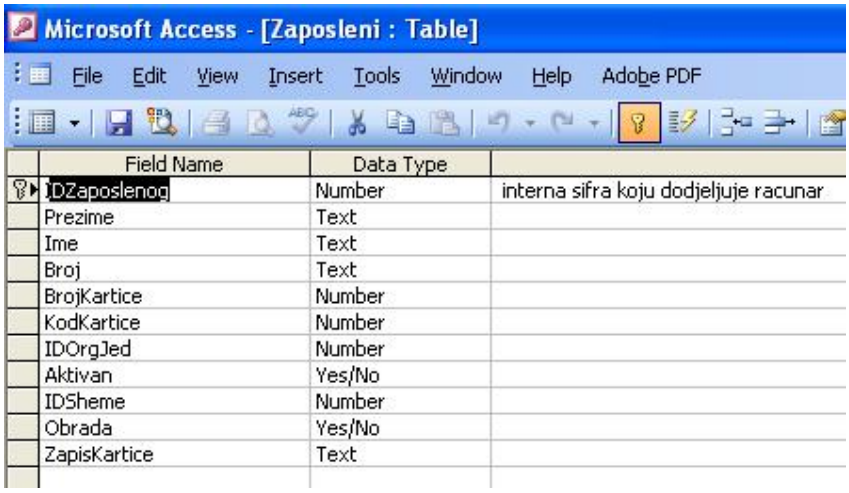
Iz mnoštva relacija koje se mogu vidijeti u bazi na Slici 6.3.1 ima smisla posebno izdvojiti relacije

- 'Zaposleni' i
- 'EvidencijaSaSata'.

Relacije 'Zaposleni' i 'EvidencijaSaSata' su osnovne relacije u bazi podataka identifikacionog sistema za evidenciju radnog vremena. Relacije analogne sadržine i značenja sadrži baza podataka i u većini identifikacionih sistema drugačije namjene. Na primjer, relacije slične sadržine postoje u bazi podataka identifikacionog sistema za:

- kontrolu pristupa,
- novčane transakcije,
- evidenciju i kontrolu točenja goriva na benzinskim pumpama,
- kontrolu pristupa računaru i aplikacijama,
- itd..

U sistemu za evidenciju radnog vremena, relacija 'Zaposleni' sadrži zapise o zaposlenim radnicima, korisnicima sistema. Na Slica 6.3.2 prikazana je struktura relacije 'Zaposleni'.



Slika 6.3.2 Struktura relacije 'Zaposleni' u bazi podataka sistema za evidenciju radnog vremena

IDZaposlenog je ključni atribut relacije 'Zaposleni'. To je šifra pomoću koje aplikativi program prepoznaje zaposlenog. Atribut je numerički a vrijednost mu interno dodjeljuje aplikativni program. Po djeljivanju, vrijednost ovog atributa, za datog zaposlenog, se ne mijenja dok god je on korisnik identifikacionog sistema. Često se kao tip podatka za ovaj atribut bira AutoNumber.

Osim identifikacionog broja, tabela 'Zaposleni', kao i slična tabela u bilo kojem drugom identifikacionom sistemu, sadrži atribute za ime i prezime svakog korisnika sistema, kao i atribut koji sadrži jedinstveni kod (serijski broj) njegovog identifikatora. Serijski broj identifikatora u tabeli 'Zaposleni' sadrži nalazi se u atributi 'ZapisKartice'.

Ostali atributi koji se mogu vidijeti na Slici 6.3.2 su više ili manje usko vezani za specifičnosti sistema za evidenciju radnog vremena i ne moraju se nalaziti u analognoj relaciji identifikacionog sistema druge namjene.

Na Slici 6.3.3 prikazano je nekoliko zapisa relacije 'Zaposleni'.

Microsoft Access - [Zaposleni : Table]

File Edit View Insert Format Records Tools Window Help Adobe PDF

IDZaposlenog	Prezime	Ime	Broj	BrojKartice	KodKartice	IDOrgJed	Aktivan	IDSheme	Obrada	ZapisKartice
213	Administrator	Broj 1	1001	3.1039682E+12	3.1039682E+12	0	☑	2	☑	A9D32D91
214	Administrator	Broj 2	3103968220017	2	2	0	☑	0	☑	A9D11131
215	Administrator	Broj 3	1003	1003	1003	0	☑	0	☑	A9D300E1
216	Administrator	Broj 4	1004	1004	1004	0	☑	0	☑	467DD574
217	GOST	01	10001	10001	10001	28	☑	1	☑	86DBA7F2
218	GOST	02	10002	10002	10002	28	☑	0	☑	84FD2484
219	GOST	03	10003	10003	10003	28	☑	0	☑	887DF284
220	GOST	04	10004	10004	10004	28	☑	0	☑	93E14E34
221	GOST	05	10005	10005	10005	28	☑	0	☑	88FC78F4
222	GOST	06	10006	10006	10006	28	☑	0	☑	88FC7874
223	GOST	07	10007	10007	10007	28	☑	0	☑	93E12554
224	GOST	08	10008	10008	10008	28	☑	0	☑	88F6B344
225	GOST	09	10009	10009	10009	28	☑	0	☑	93E2C574
226	GOST	10	10010	10010	10010	28	☑	0	☑	93E2B424
227	GOST	11	10011	10011	10011	28	☑	0	☑	88FC0F44
228	GOST	12	10012	10012	10012	28	☑	0	☑	7C24E034
229	GOST	13	10013	10013	10013	28	☑	0	☑	8BFA00B6
230	GOST	14	10014	10014	10014	28	☑	0	☑	8269EEB4
231	GOST	15	10015	10015	10015	28	☑	0	☑	63C26692
232	GOST	16	10016	10016	10016	28	☑	0	☑	86DC1742
233	JAKOVLJEVIĆ	VELISAV	0612947260036	138727	138727	23	☑	0	☑	B4F7D556
234	MIŠOVIĆ	MITAR	1012952260016	214478	214478	23	☑	0	☑	89E4E144
235	VUJICIC	MILENKO	2212960260036	186502	186502	23	☑	0	☑	0ADF4484

Slika 6.3.2 Zapisi relacije 'Zaposleni'.

Relacija 'EvidencijaSaSata' u sistemu za evidenciju radnog vremena sadrži zapise o registracijama radnika, prilikom dolaska na posao ili odlaska sa posla. Drugačije rečeno, ova rečeno ova relacija sadrži podatke o izvšenim identifikacijama odnosno toku identifikacionog procesa.

Na slici 6.3.3 prikazan je struktura relacije 'EvidencijaSaSata'.

Microsoft Access - [EvidencijaSaSata : Table]

File Edit View Insert Tools Window Help Adobe PDF

Field Name	Data Type	
IDZaposlenog	Number	
Vrijeme	Date/Time	Vrijeme provlacenja
Smjer	Number	0 - Ulaz , 1 - Izlaz
IDSata	Number	
KodKartice	Number	Kod kartice
Obradjen	Yes/No	
VrKom	Date/Time	Vrijeme komunikacije
IDSheme	Number	ID sheme rada radnika u renutku ocitanja kartice
IDReason	Number	Razlog izlaska radnika

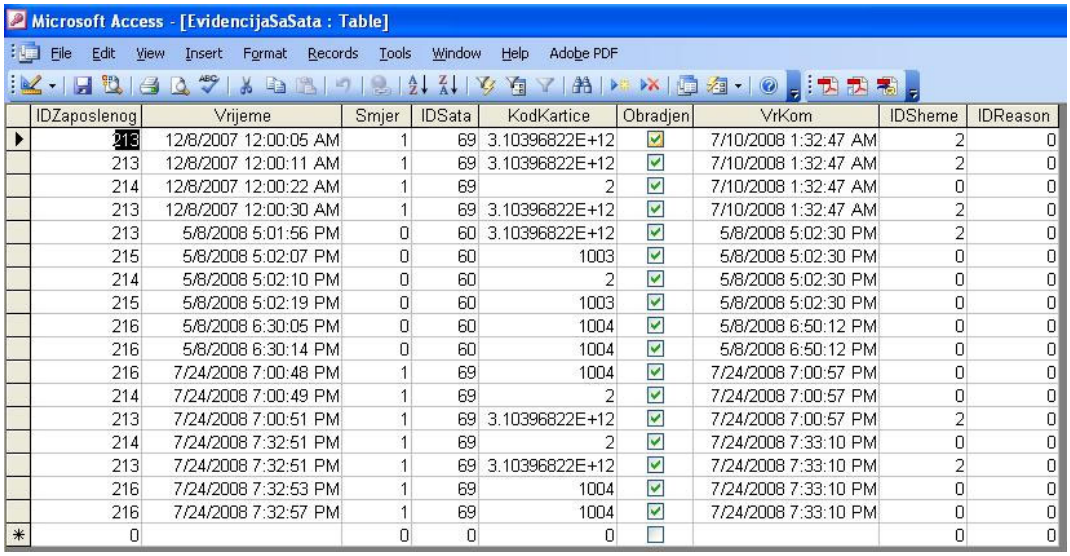
Slika 6.3.3 Struktura relacije 'EvidencijaSaSata' u bazi podataka sistema za evidenciju radnog vremena

Atribut IDZaposlenog povezuje zapis iz relacije 'EvidencijaSaSata' sa odgovarajućim zapisom iz relacije 'Zaposleni'. Na taj način se zna koji podaci o izvršenoj identifikaciji (registraciji na posao) pripadaju kojem korisniku.

Drugi nezaobilazan atribut relacije 'EvidencijaSaSata' je Vrijeme. U ovom atributu smješten je podatak o vremenu kada je izvršena identifikacija korisnika. U sistemu za evidenciju radnog vremena ovaj atribut nosi informaciju o tome kada je zaposleni došao ili otišao sa posla.

Ostali atributi relacije 'EvidencijaSaSata', koji se mogu vidijeti na Slici 6.3.2 su više ili manje uslovljeni specifičnostima sistema za evidenciju radnog vremena i ne moraju se nalaziti u analognoj relaciji identifikacionog sistema druge namjene.

Na Slici 6.3.4 prikazano je nekoliko zapisa relacije 'EvidencijaSaSata'.



IDZaposlenog	Vrijeme	Smjer	IDSata	KodKartice	Obradjen	VrKom	IDSheme	IDReason
213	12/8/2007 12:00:05 AM	1	69	3.10396822E+12	☑	7/10/2008 1:32:47 AM	2	0
213	12/8/2007 12:00:11 AM	1	69	3.10396822E+12	☑	7/10/2008 1:32:47 AM	2	0
214	12/8/2007 12:00:22 AM	1	69	2	☑	7/10/2008 1:32:47 AM	0	0
213	12/8/2007 12:00:30 AM	1	69	3.10396822E+12	☑	7/10/2008 1:32:47 AM	2	0
213	5/8/2008 5:01:56 PM	0	60	3.10396822E+12	☑	5/8/2008 5:02:30 PM	2	0
215	5/8/2008 5:02:07 PM	0	60	1003	☑	5/8/2008 5:02:30 PM	0	0
214	5/8/2008 5:02:10 PM	0	60	2	☑	5/8/2008 5:02:30 PM	0	0
215	5/8/2008 5:02:19 PM	0	60	1003	☑	5/8/2008 5:02:30 PM	0	0
216	5/8/2008 6:30:05 PM	0	60	1004	☑	5/8/2008 6:50:12 PM	0	0
216	5/8/2008 6:30:14 PM	0	60	1004	☑	5/8/2008 6:50:12 PM	0	0
216	7/24/2008 7:00:48 PM	1	69	1004	☑	7/24/2008 7:00:57 PM	0	0
214	7/24/2008 7:00:49 PM	1	69	2	☑	7/24/2008 7:00:57 PM	0	0
213	7/24/2008 7:00:51 PM	1	69	3.10396822E+12	☑	7/24/2008 7:00:57 PM	2	0
214	7/24/2008 7:32:51 PM	1	69	2	☑	7/24/2008 7:33:10 PM	0	0
213	7/24/2008 7:32:51 PM	1	69	3.10396822E+12	☑	7/24/2008 7:33:10 PM	2	0
216	7/24/2008 7:32:53 PM	1	69	1004	☑	7/24/2008 7:33:10 PM	0	0
216	7/24/2008 7:32:57 PM	1	69	1004	☑	7/24/2008 7:33:10 PM	0	0
0		0	0	0	☐		0	0

Slika 6.3.4 Zapisi relacije 'EvidencijaSaSata'

6.4 APLIKATIVNI PROGRAM

Aplikativni program je sastavni dio gotovo svakog identifikacionog sistema. On, na neki način, predstavlja vezu između baze podatakla i ostatka identifikacionog sistema.

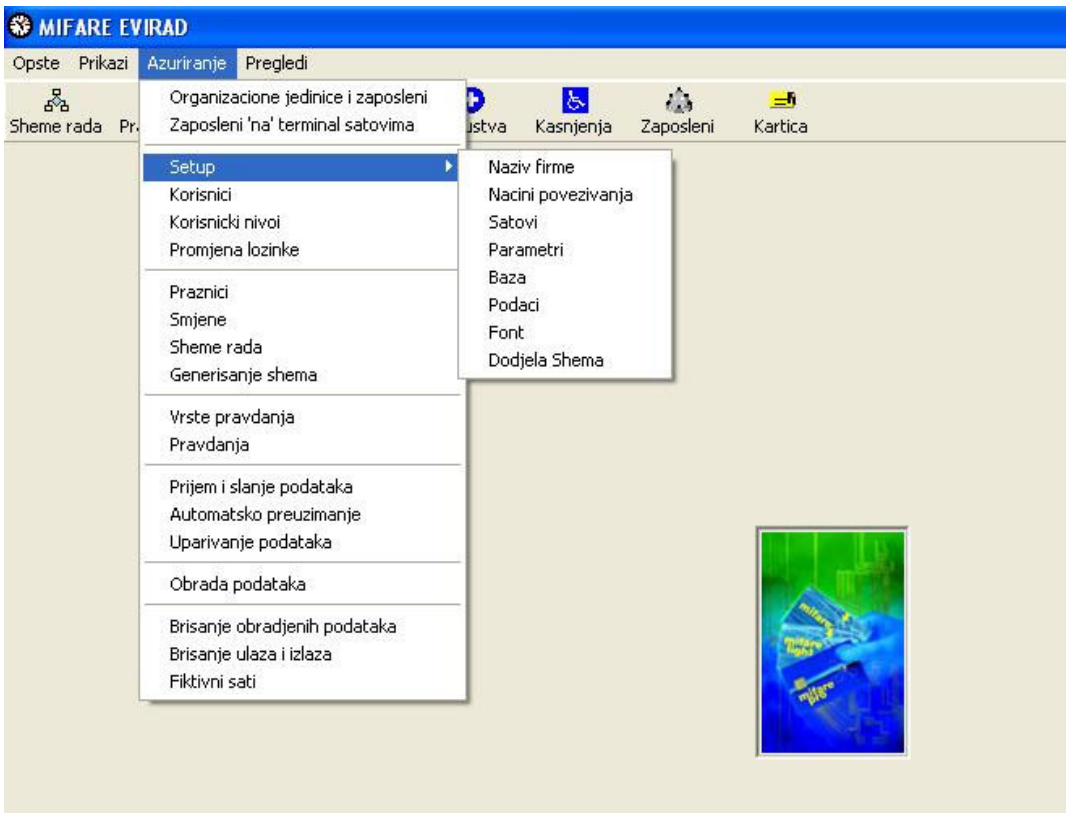
Aplikativni program komunicira sa čitačima, logerima i nadređenim sistemima.

Posredstvom logera i čitača ili direktno aplikativni program upravlja radom izvršnih organa, kao što su brave, semafori, displeji, itd..

Koristeći konfiguracione podatke iz baze podataka, aplikativni program konfiguriše sistem. Pod konfuigurisanjem sistema podrazumijeve se da aplikativni program zadaje način rada čitačima i logerima u sistemu.

U kominikaciji sa logerom apikativni program predaje logeru konfiguracione podatke, kao i podatke o korisnicima i pravima korisnika sistema. Osim toga, aplikativni program preuzima podatke iz logere. Preuzete podatke obrađuje, prilagođava i upisuje u bazu podataka.

Aplikativni program ažurira bazu podataka. Upisuje podatke preuzete iz logera ili dobijene on-line od strane čitača. Pomoću aplikativnog programa vrši se upis novih korisnika sistema, kao i brisanje ili izmjena podataka postojećih korisnika. Na Slika 6.4.1 prikazana je glavna forma aplikativnog programa u identifikacionom sistemu ze evidenciju radnog vremena. U prikazanom opadajućem meniju mogu se vidijeti razne mogućnosti ažuriranja baze podatka.

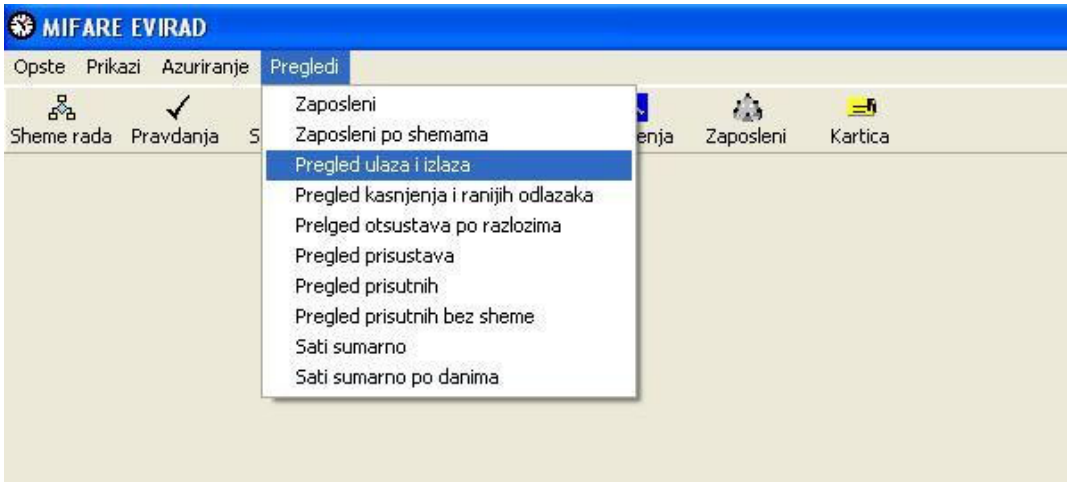


Slika 6.4.1 Opcije za ažuriranje podataka baze u aplikativnom programu sistema za evidenciju radnog vremena

Tako se, na primjer, aktiviranjem opcije 'Organizacione jedinice i zaposleni' mogu ažurirati podaci o organizacionim jedinicama preduzeća i zaposlenima. U podmeniju 'Setup' mogu se ažurirati, konfiguracioni podaci kojima se određuje način rada čitača, logera i ostalih dijelova identifikacionog sistema, kao i samog aplikativnog programa. Opcijama 'Korisnici', 'Korisnički nivoi' i 'Promjena lozinke' ažuriraju se podaci operatera na aplikativnom programu. Stavkama menija 'Praznici', 'Smjene', 'Sheme rada', 'Generisanje shema', 'Vrste pravdanja' i 'Pravdanja' omogućava se ažuriranje podataka o pravima zaposlenih, pojedinačno ili

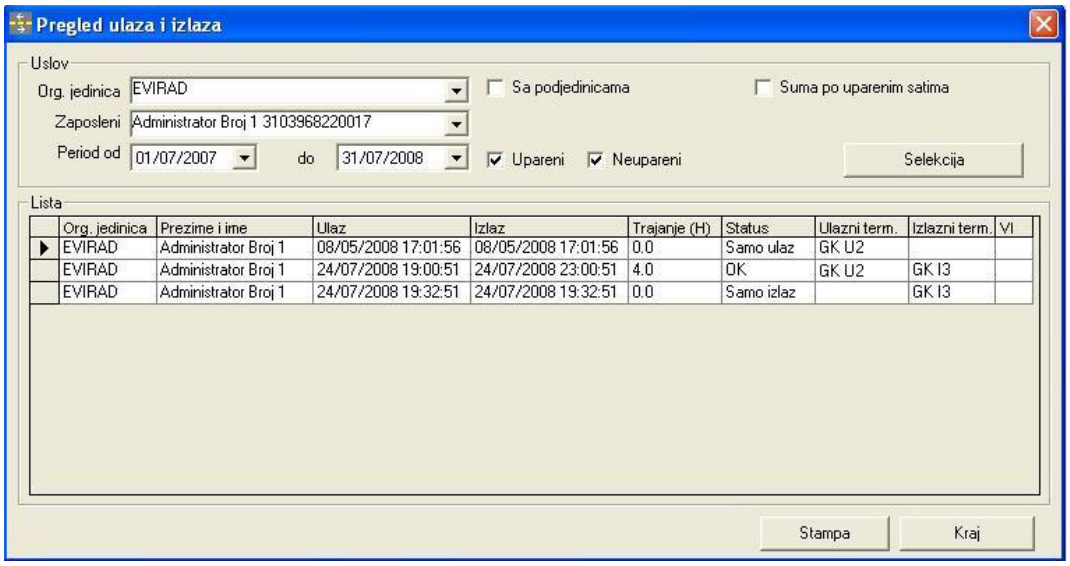
grupno. Opcijama 'Prijem i slanje podataka' odnosno 'Automatsko preuzimanje' aktivira se komunickacija aplikativnog programa sa čitačima, odnosno logerima u sistemu. Shodno potrebi, uređajima se mogu slati ili preuzimati podaci. Aktiviranjem opcija 'Uparivanje podataka' ili 'Obrada podataka' pokreće se obrada prikupljenih podataka o izvršenim identifikacijama. Ova obrada se sprovodi u cilju obezbjeđivanja podataka za izvještaje o toku identifikacionog procesa.

Osim mogućnosti ažuriranja podataka u bazi, aplikativni program obezbjeđuje dobijanje različitih izvještaja o toku identifikacionog procesa. Na Slika 6.4.2 u opadajućem meniju prikazani su izvještaji koje je u mogućnosti da da aplikativni program u identifikacionom sistemu za evidenciju radog vremena.



Slika 6.4.2 Izvještaji koji se mogu dobiti od strane aplikativnog programa za evidenciju radnog vremena

Na primjer, izvještaj 'Pregled ulaza i izlaza' daje pregled vremena dolaska na posao i odlaska sa posla jednog, grupe ili svih zaposlenih korisnika u željenom vremenskom intervalu (Slika 6.4.3).



Slika 6.4.3 Izvještaj 'Pregled ulaza i izlaza'

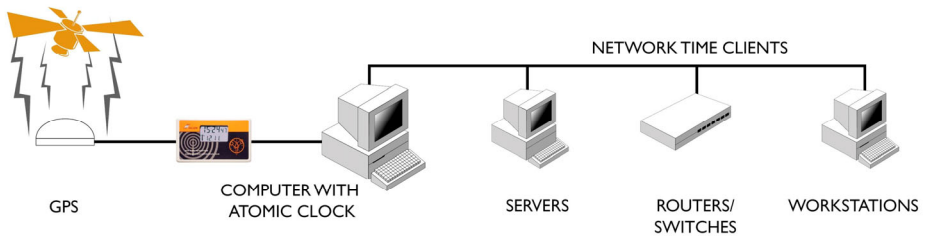
6.4.1 VRIJEME U IDENTIFIKACIONOM SISTEMU

Vrlo važan podatak u identifikacionom sistemu je tačno vrijeme. Ono mora biti dostupno aplikativnom programu, tako i ostalim dijelovima sistema (čitačima i logerima). Aplikativni program usklađuje vrijeme u sistemu. Prilikom svake komunikacije sa čitačima i logerima aplikativni program im prosljeđuje tačno vrijeme. Čitači i logeri preuzimaju vrijeme i dalje ga samostalno ažuriraju.

Aplikativni program preuzima tačno vrijeme sa vremenskog servera.

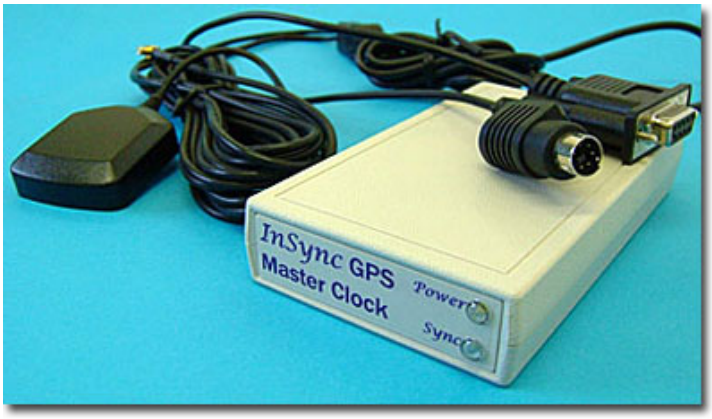
Vremenski server (engl. time seerver) je serverski računar koji tačno vrijeme dobija od referentnog časovnika i prosljeđuje ga putem računarske mreže [171]. Vremenski server se može nalaziti unutar lokalne računarske mreže ili dostupan putem interneta. Najčešće korišteni protokol za slanje sinhronizacionog vremena je Network Time Protocol (NTC) [172]. U upotrebi ima i drugih manje popularnih protokola.

Vremenski server referentno vrijeme može uzimati od drugog vremenskog servera, putem radio signala ili od atomskog časovnika. Najčešći izvor tačnog vremena je GPS ili GPS master clock. GPS master clock obezbjeđuje sinhronizacioni sinhronizacioni takt dobijen kombinovanjem taktova dobijenih od strane više satelitskih atomskih časovnika.



Slika 6.4.4 Računar sa atomskim časovnikom podešenim od strane GPS master clock-a

Prijemnici, GPS master clock ne koriste za direktno izračunavanje vremena ili frekvencije, već za podešavanje vlastitiog oscilatora. Usljed toga GPS master clock prijemnici se još nazivaju i GPS-disciplined oscillators (Slika 6.4.5) [173].

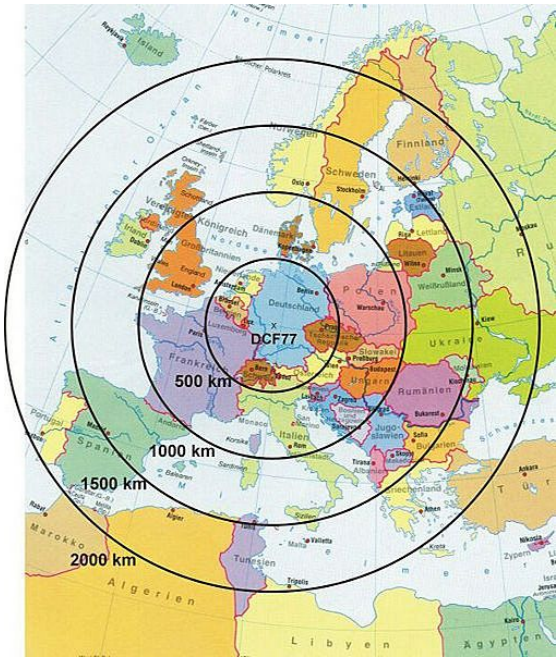


Slika 6.4.5 Primjer GPS master clock prijemnika

Interesantan izvor sinhronozacionog vremena je i DCF77 [174]. DCF77 je dugotalasni radio signal koji nosi informaciju o sinhronizacionom vremenu. Predajnik je lociran u Mainflingen-u, oko 25km jugo-istično od Frankfurt-a, Njemačka (Slika 6.4.5). U vlasništvu je Media Broadcast GmbH, a radi za porebe Njemačke nanacionalne fizičke laboratorije. DCF77 postoji kao emiter standardne frekvencije od 1959. godine. Informacije o datumu I vremenu dodate su 1973.

Slika 6.4.5 DCF77 u Mainflingen-u

Signal nosilac frekvencije 77.5KHz generisan je iz locak atomic clock-a povezanog sa German master clock-om u Braunschweig-u. Stanica emituje snagom od 50KW. Signal se može primati iz velikog dijela Evrope, do rastojanja od oko 2000km od Frankfurt-a (Slika 6.4.6).



Slika 6.4.6 Domet DCF77 signala

Veći domet zavisi od uslova propagacije signala. Na primjer, u Portugalu je dobar prijem moguć tokom noćnih sati.

DCF77 signal nosi amplitudsko-modulisani, širinsko-impulsno kodirani signal podataka, bit rate-a 1 bit/sec. Isti signal podataka je takođe fazno-modulisan upotrebom 511 bita dugačkom pseudorandom sekvence (DSSS - direct-sequence spread spectrum modulacija).

Podaci se prenose jednom u minuti i sadrže:

- tekući datum i vrijeme,
- leap second upozoravajući bit,

- bit ljetnjeg vremena
- primarni/backup identifikacioni bit predajnika,
- nekoliko bitova parnosti.

Od 2003 godine, 14 do tada nekorištenih bitova u podacima vremena upotrijebljeno je za signaliziranje opasnosti sližbama civilne odbrane.

Nazov DCF77 je formiran iz: D=*Deutschland* (Germany), C=long wave signal, F=Frankfurt, 77=frequency: 77.5 kHz.

Ovaj signal je od kraja 1980-ih godina postao veoma popularan u Evropi. Mnoge radio stanice i mnogi časovnici koriste ovaj signal za automatsko podašavanje vremena.

6.5 PRATEĆA OPREMA

U prateću opremu koja je koja u upotrebi u najvećem broju identifikacionih sistema spada:

- neprekidno napajanje,
- električne brave i
- komunikaciona infrastruktura.

Neprekidno napajanje se koristi u cilju obezbjeđivanja rada identifikacionog sistema i pri nedostatku mrežnog napajanja. Obično je zasnovano na upotrebi akumulatorske baterije. Za vrijeme kada je mrežni napon prisutan, sistem se napaja mrežnom energijom, a akumulator se dopunjava do optimalnog naponakog nivoa, koji se održava. Kada zahvali mrežnog napajanja, sistem nastavlja da radi zahvaljujući energiji akumulisanoj u bateriji. Vremenski interval u kojem će sistem funkcionisati, u tim uslovima, zavisi od potrošnje sistema i kapaciteta akumulatorske baterije. Najčešće se nastoji obezbijediti da sistem može da radi bez mrežnog napajanja bar nekoliko sati.

Obzirom da se identifikacioni sisteme veoma često koriste za kontrolu pristupa raznim prostorima i objektima električne brave, automati za otvaranje vrata, trokrake poluge i slični uređaji su neizbježan sastavni dio sistema.

Djelove identifikacionog sistema potrebno je medjusobno povezati u cilju obezbjeđivanja razmjene podataka među njima. Osim toga često je potrebno čitač i logere povezati sa centralnim računarom. Sva ta medjusobna povezivanja čine komunikacionu infrastrukturu sistema.

Za povezivanje uređaja unutar sistema koriste se rezličiti komunikacioni interfejsi kao što su: RS232, RS485, ProfiBus [175], Modbus [176], WorldFIP [177], Foundation Fieldbus [178], HART [179], CAN [180], AS-i itd. Osim pomenutih, za povezivanje sa centralnim računarom koriste se i Ethernet [182], GSM, GPRS, GPS [183], i drugi interfejsi.

6.6 OFF-LINE IDENTIFIKACIONI SISTEMI

Poznato je da identifikacioni sistemi, bez obzira na primijenjenu tehnologiju, svoju punu snagu razvijaju ukoliko se djelovi sistema (čitači i/ili logeri) povežu sa centralnim računarom (tzv. on-line sistemi). Međutim, pojavom i razvojem pametnih identifikatora, sve je više primjena u kojima se zadovoljavajuća funkcionalnost postiže i bez povezivanja na centralni računar. Funkcionalnost je moguće ostvariti zahvaljujući tome što pametni identifikatori posjeduju vlastitu memoriju i mogućnost obrade podataka. Identifikacioni podaci se mogu čuvati i ažurirati unutar pametnog identifikatora bez potrebe za intervencijom od strane više instance (logera, PC-a, …).

Identifikacioni sistemi u kojima ne postoji veza sa PC-em nazivaju se još off-line identifikacioni sistemi.

Da bi jedan identifikacioni sistem mogao pouzdano funkcionisati u dužem vremenskom periodu on mora biti u mogućnosti da:

- dodijeli prava pristupa novim korisnicima,
- ukine prava pristupa nekim od postojećih korisnika,
- kao i da u slučaju potrebe izmijeni prava pristupa korisnicima.

Do pojave pametnih identifikatora ovo nije bilo moguće uraditi bez upotrebe računara i ostale infrasrukture svojstvene on-line sistemima. Na primjer, u off-line sistemima bez pamatnih identifikatora (identifikator sa trakastim kodom, magnetnim zapisom,…) veliki problem je predstavljalo gubljenje identifikatora od strane nekog korisnika. Mogućnost da taj identifikator bude zloupotrijebljen smanjivala je sigurnost identifikacionog sistema. Ukidanje prava pristupa tom identifikatoru zahtijevalo je povezivanje sistema sa računarom, što je često bilo dosta nepraktično i zahtijevalo je vrijeme (intervenciju od strane prodavca sistema).

Pametni identifikatori donijeli su mogućnost da se podaci u njih, mogu jednostavno upisivati, brisati ili mijenjati. Osim toga moguće je jednostavno mijenjati i uslove pristupa podacima, odnosno kripto ključeve ili algoritme obrade podataka. Sva navedena ažuriranja u stanju je uraditi čitač identifikatora, bez povezivanja sa računarom. Prema tome, off-line sistemi koji koriste pametne identifikatore mogu zadovoljiti osnovne funcije identifikacionog sistema.

Off-line sistemi ne posjeduju komunikacionu infrastrukturu što ih čini znatno jednostavnijim za montažu i jeftinijim od on-line sistema.

Off-line sistemima se obično pokrivaju one primjene gdje ne postoji potreba za kontinualnim prikupljanjem podataka o identifikacionom procesu. Usljed toga, u takvim off-line sistemima ne postoji potreba za logerima, aplikativnim programom i bazom podataka, što još više smanjuje njihovu cijenu.

Osnovni sastavni djelovi off-line identifikacionog sistema su pametni identifikatori i čitači identifikatora. Od prateće opreme najčešće se koristi basprekidno napajanje (ukoliko baterijsko ne može da zadovolji), brave, i

slična oprema neophodna za funkcije kontrole pristupa, objektima, uređajima i sl.

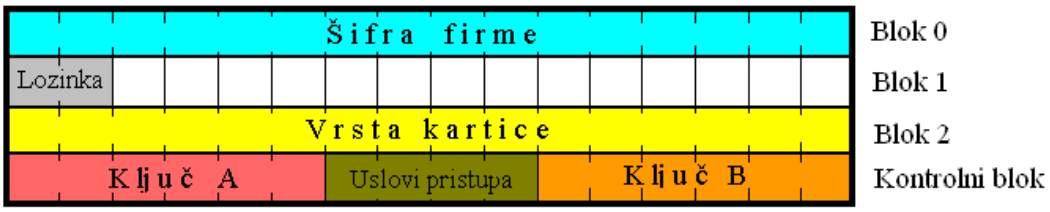
6.6.1 OFF-LINE MIFARE SISTEM ZA KONTROLU PRISTUPA

Kao primjer jednog off-line identifikacionog sistema u ovom poglavlju opisan je off-line sistem za kontrolu pristupa u kojem se kao pametni identifikator koristi Mifare® 1 S50 kartica (vidi poglavlje 3.10).

Osnovni dijelovi ovog sistema su:

- Mifare® 1 S50 i
- čitač Mifare® 1 S50 kartica (vidi poglavlje 3.10).

U ovom off-line sistemu, kontrola pristupa vrši se na osnovu zapisa u sektoru memorije Mifare® 1 S50 kartice. Samo kartice sa odgovarajućim zapisima u sektoru mogu proći kontrolu pristupa. Struktura podataka upotrijebljenog sektora prikazana je na Slici 6.6.1.



Slika 6.6.1 Struktura podataka prvog sektora Mifare® 1 S50 kartice

U opšem slučaju kao identifikacioni sektor, može se upotrijebiti bilo koji sektor osim sektora 0. Sektor 0 nije podesan jer njegov nulti blok sadrži serijski broj kartice i podatke proizvođača. Ovi podaci se ne mogu mijenjati (vidi poglavlje 3.10).

Blok 0 identifikacionog sektora uporijebljen je za naziv firme. Prvih 2 okteta bloka 1 upotrijebljena se kao niži i viši oktet lozinke kartice. Preostali okteti bloka 1 ne koriste se u kontroli pristupa. U bloku 2 upisani su podaci o vrsti kartice. Podaci bloka 0 i bloka 2 su nepromjenjivi, odnosno sistem ne mijenja ove podatke. Sadržaj okteta lozinke kartice može biti promijenjen od strane sistema (čitača kartica).

U Off-line Mifare sistemu za kontrolu pristupa postoje dvije vrste kartica:

- obična kartica za ostvarivanje prava pristupa i
- Master kartica.

Sistem funkcioniše tako što čitač pokuša pročita blokove podataka prvog sektora kartice, koja se našla njegovom polju. Komunikacija između kartice i čitača kriptovana je shodno uslovima pristupa definisanim u čitaču i kontrolnom bloku sektora kartice. Ukoliko čitač ne uspije pristupiti prvom sektoru, on ispituje sljedeće. Kada uspije pročitati podatke nekog sektora,

prelazi na analizu blokova podataka tog sektora.

Ukoliko čitač zaključi da se u njegovom polju nalazi kartica za ostvarenja prava pristupa u sistemu, prelazi u režim kontrole pristupa i poredi naziv firme i lozinku sa kartice sa svojim nazivom firme i lozinkom. Sve kartice u sistemu, u principu, imaju isti naziv firme i istu lozinku. Čitač lozinku vidi kao broj od 0 do 65535. Pristup će biti dozvoljen onim karticama koje imaju imaju istu šifru firme kao čitač i lozinku koje nije manja od lozinke čitača. Ukoliko je lozinka na kartici veća od lozinke čitača čitač će svoju lozinku izjednačiti sa lozinkom kartice. Ubuduće čitač će prihvatati samo one kartice koje imaju lozinku ne manju od njegove nove lozinke. Na ovaj način je omogućeno da svaka kartica koja ima noviju loziku, može isporgramirati čitač na tu novu lozinku.

Ukoliko nakon očitanja blokova podataka prvog sektora kartice čitač zaključi da se radi o njegovoj Master kartici prelazi u režim programiranja. U ovom režimu čitač će se naći nakon uklanjanja Master kartice iz njegovog polja. Dok se nalazi u ovom režimu, čitač će u odgovarajući sektor kartice koje se nađe u njegovom polju upisati svoj naziv firme i svoju lozinku. Takođe u kontrolni blok tog sektora čitač će upisati specifične uslove pristupa definisane za sistem. Kao sektor u koji će upisati identifikacione podatke čitač će odabrati prvi sektor čijim podacima može pristupiti sa specifičnim uslovima pristupa sistema ili prvi sektor kojemu se može pristupiti uslovima definisanim od strane proizvođača kartica. Na taj način čitač će isprogramirati karticu, i ona će se ubuduće moći koristiti za ostvarivanje prava u sistemu.

Za izlazak čitača iz režima programiranja potrebno je ponovo Master karticu umatnuti u njegovo polje, kratko zadržati i ukloniti iz polja. Nakon nekoliko sekundi čitač će se resetovati i time izaći iz režima programiranja.

Režim rada koji čitač poprima nakon reseta i kada nema kartice u polju a nije urežimu programiranja, naziva se slobodan režim rada čitača. U ovom režimu rada čitač se nalazi u odgovarajućem modu smanjene potrošnje i samo povremeno provjerava ptisustvo kartice u njegovom polju.

Osim prevođenja čitača u režim programiranja Master karticom se može:

- promijeniti lozinka čitaču,
- izbrisati čitačeve podatke o šifri firme i lozinci.

Lozinka čitača se mijenja tako što se u polje čitača, kada se on nalazi u slobodnom režimu rada, unese Master kartica i zadrži u polju dok se čitač ne uzvrati odgovarajućom signalizacijom. Nakon toga potrebno je izvući Master karticu iz polja čitača. Lozinka čitača je time inkrementirana a čitač ostaje u režimu programiranja. Važno je znati da je nova lozinka čitača, upisana i u blok 1 odgovarajućeg sektora Master kartice.

Brisanje podataka o šifri firme i lozinci iz čitača vrši se tako što se u polje čitača unese Master kartica i zadrži u polju dok se čitač na uzvrati odgovarajućom signalizacijom. Nakon toga potrebno je izvući Master karticu iz polja čitača. Čitač se resetovati. Njegovi podaci o firmi i lozinka su izbrisani. Za brisanje podataka iz čitala Master karticu treba zadržati

nego za promjenu lozinke. Čitač kojemu su izbrisani podaci o šifri firme i lozinka, preuzeće ove podatke iz prve kartice koja se nađe u njegovom polju, a ima odgovarajući identifikacioni sektor.

Na kraju se može dati osvrt kako jedan ovakav off-line sistem može prevazići problem gubljenja kartice. U slučaju gubitka neke kartice, potrebno je promijeniti lozinku na ostalim karticama i »reći« čitačima da pređu na tu lozinku. Ovo se izvodi tako što se, pomoću Master kartice, inkrementira lozinka čitača i preostale kartice isprogramiraju na uvećanu lozinku [184].

LITERATURA

[1] Craig K. Harmon, ″Lines of Communication: Bar Code & Data Collection Technologies for the 90s,″ Helmers Publishing, Maj 1994.

[2] Roger C. Palmer, ″The Bar Code Book: Reading, Printing, & Specification of Bar Code Symbols,″ Helmers Publishing, Jun 1993.

[3] Uniform Code Council. Homepage. http://www.uc-council.org

[4] ″UPC Coupon Code Guidelines Manual,″ Uniform Code Council (UCC), 1989.6.

[5] Theo Pavlidis and Ynjiun P. Wang, ″Two–Dimensional Bar Codes,″ IEEE Industrial Automations Conference, Toronto 1990.

[6] http://www.mag-stripe.com/

[7] http://www.magtek.com/

[8] Joseph Nsoh Egbe, ″Bar codes and magnetic stripes in manufacturing industries,″ Didax Educational Resources , January 1, 1994.

[9] ″Landp/DOS and Landp/2 Support for Financial Magnetic Stripe Readers/Enciders,″ IBM Readbooks, IBM, January 1996.

[10] Wolfgang Rankl, Wolfgang Effing, ″Smart Card Handbook,″ John Wiley & Sons, 3 edition, January 20, 2004.

[11] Timothy M. Jurgensen, Scott B. Guthery, Tim Jurgensen, Scott Guthery, ″Smart Cards: The Developer's Toolkit,″ Prentice Hall PTR; 1st edition, July 9, 2002

[12] Dominique Paret, ″RFID and Contactless Smart Card Applications,″ Dominique Paret, John Wiley & Sons, October 17, 2005.

[13] Mike Hendry, ″Smart Card Security and Applications,″ Artech House Publishers; 2nd edition, April 2001.

[14] ″HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements,″ Smart Card Alliance, MarketResearch.com, September 1, 2003.

[15] Aneace Haddad, ″A New Way To Pay: Creating Competitive Advantage Through The Emv Smart Card Standard,″ Gower Publishing Company, September 2005.

[16] ″Using Smart Cards for Secure Physical Access,″ Smart Card Alliance, MarketResearch.com, July 1, 2003.

[17] Chuck Wilson, ″Get Smart: The Emergence of Smart Cards in the United States and their Pivotal Role in Internet Commerce,″ Mullaney Publishing, June 1, 2001.

[18] Steven Shepard, ″RFID″, McGraw-Hill Professional; 1 edition, August 16, 2004.

[19] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, ″Biometrics: A Grand Challenge″, Proceedings of International Conference on Pattern Recognition, Cambridge, UK, Aug. 2004.

[20] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, SpecialIssue on Enabling Security Technologies forDigital Rights Management, Vol. 92, No. 6, June 2004.

[21] Roger C. Palmer, "The Bar Code Book: Reading, Printing, & Specification of Bar Code Symbols", Helmers Publishing, Jun 1993.

[22] Theo Pavlidis and Ynjiun P. Wang, "Two–Dimensional Bar Codes", presented to IEEE Industrial Automations Conference, Toronto 1990.

[23] Russ Adams, "Sourcebook Of Automatic Identification And Data Collection", Januar 1990.

[24] Wang, Yuing P. & Bravman, "PDF 417, A Two-Dimensional Bar Code System", Richard, Symbol Tehnologies, 1990.

[25] Kevin R. Sharp,"Automatic Identification: Marking It Pay", Reinhold Computer, Jun 1990.

[26] http://en.wikipedia.org/wiki/DataMatrix

[27] Stephen B. Wicker, Vijay K. Bhargava, and Stephen B Wicker, "Reed-Solomon Codes and Their Applications" (Paperback - Sep 28, 1999)

[28] http://www.lasercard.com/

[29] http://www.meteora.us/Home_Page.html

[30] "LaserCard Corporation Comments on Italian National ID Program Moving Into Full Implementation; Cards Contain LaserCard Corporation's Optical Memory Stripe". Business Wire. April 12, 2005. FindArticles.com. 04 Aug. 2008.

[31] http://www.laserfocusworld.com

[32] O. Yamada et al., IEEE Int. Symp. on Info. Theory and its Appl. 6(5), 95 (1990).

[33] Identity theft, by John R. Vacca - 2002 - Social Science - 512 pages

[34] http://travel.state.gov/visa/temp/types/types_1266.html

[35] http://www.reuters.com/article/pressRelease/idUS85004+01-May-2008+BW20080501

[36] http://www.lasercard.com/applications

[37] Klaus Finkenzeller, ″RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification″, John Wiley & Sons; 2 edition, May 9, 2003.

[38] Manish Bhuptani, Shahram Moradpour, ″RFID Field Guide: Deploying Radio Frequency Identification Systems″, Prentice Hall PTR, 2005.

[39] Robert Kleist, Theodore Chapman, David Sakai, Brad Jarvis, ″RFID Labeling: Smart Labeling Concepts & Applications for the Consumer Packaged Goods Supply Chain″, Banta Book Group, August 2004.

[40] Nahid Jilovec, ″EDI, UCCnet & RFID: Synchronizing the Supply Chain″, 29th Street Press, November 10, 2004.

[41] http://www.go-4-best.com/index.php?to=rfid+applications

[42] Royal Air Force. History: 1940. http://www.raf.mod.uk/history/line1940.html.

[43] Alfred R Koelle, Steven W. Depp, Jermy A. Landt, and Ronald E. Bobbett, ″Short-Range Passive Telemetry by Modulated Backscatter of Incident CW RF Carrier Beams,″ Biotelemetry, 3:337–340, 1976.

[44] Auto-ID Center, ″Draft Protocol Specification for a Class 0 Radio Frequency Identification Tag,″ February, 2003.

[45] http://www.righttag.com/

[46] www.vanskee.com

[47] Steven Shepard, ″RFID″**,** McGraw-Hill Professional; 1 edition, August 16, 2004.

[48] Jim Crane, ″Benetton Clothing to Carry Tiny Tracking Transmitters,″ Associated Press, March 2003.

[49] International Standards Organization. ISO/IEC 15693: Identification cards – Contactless integrated circuit(s) cards - Vicinity cards. http://www.iso.org, 2000.

[50] Charles Spurgeon, ″Ethernet: The Definitive Guide″, O'Reilly Media, Inc., 1 edition, February 9, 2000.

[51] Benny Bing, ″Broadband Wireless Access,″ Kluwer Academic Publishers, 2002.

[52] Robert M. Metcalfe and David R. Boggs, ″Ethernet: Distributed Packet Switching for Local Computer Networks,″ Communications of the ACM, 19(5):395–404, July 1976.

[53] P. Hawkes, ″Anti-collision and Transponder Selection Methods for Grouped "Vicinity" Cards and PFID tags″, IEE Colloquium on RFID Technology, Ref. No. 1999/123.

[54] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels, ″Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,″ Security in Pervasive Computing, 2003.

[55] Pete Lindstrom, Frank Thornton, ″RFID Security,″ Syngress; 1 edition, November 1, 2005.

[56] Ronald L. Rivest, ″Personal correspondance,″ May 2003.

[57] International Telecommunications Union, ″Radio Regulations,″ 1998. Volume 1.

[58] Tom Ahlkvist Scharfeld, ″An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Indentification System Design,″ Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, August 2001.

[59] Mifare Standard Card IC MF1 IC S50, Philips Semiconductors Gratkom GmbH, Mikron- Weg, A-8101 Gratkom, Austria

[60] ISO/IEC FDIS 14443

[61] Mifare MF RC531, ISO 14443A Reader IC, Philips Semiconductors Gratkom GmbH, Mikron-Weg, A-8101 Gratkom, Austria

[62] Youngjae Choi, Jinseok Song, Hyoungjun Kang, Sangheon Pack, Byoungwook Lee, and Taekyoung Kwon, "RFID Management System and RFID Tag Location Tracking Scheme: Bi-directional," Korea Patent, No. 2004-0107290, Pending, December 2004.

[63] I.D. Robertson, M. Blewett, J. Amin, I. Butt, F. Donnelly, P. Harwood, A. Woolven, ″A simple radio-frequency system for asset tracking within buildings″, IEE Colloquium on RFID Technology, Ref. No. 1999/123.

[64] Hähnel, W. Burgard, D. Fox, K. Fishkin, and M. Philipose, ″Mapping and Localization with RFID Technology″, IEEE International Conference on Robotics and Automation (ICRA), 2004.

[65] Masayuki Iwai, Hideyuki Tokuda, ″RFID-Based Location Information Management System with Privacy Awareness″, The 2005 Symposium on Applications and the Internet Workshops (SAINT-W'05), January 31 - February 04, 2005**,** Trento, Italy

[66] Lynn Hazlewood, ″RFID in the Department of Defense the bottom line,″ : An article from: Defense Transportation Journal, Defense Transportation Journal (Magazine/Journal), February 1, 2006.

[67] http://en.wikipedia.org/wiki/Smart_Card

[68] Wolfgang Rankl, Wolfgang Effing, "Smart Card Handbook", Hardcover - Jan 16, 2004.

[69] http://www.avesodisplays.com/

[70] Wolfgang Rankl, Kenneth Cox Smart, "Card Applications: Design models for using and programming smart cards", Hardcover - Jun 15, 2007.

[71] Keith Mayes and Konstantinos Markantonakis, "Smart Cards, Tokens, Security and Applications", Hardcover - Jan 7, 2008

[72] http://en.wikipedia.org/wiki/Symmetric_key_algorithm

[73] http://en.wikipedia.org/wiki/DES_supplementary_material

[74] http://en.wikipedia.org/wiki/Horst_Feistel

[75] Douglas Stinson, "Cryptography- Theory and Practice", mart 2000.

[76] http://en.wikipedia.org/wiki/EFF_DES_cracker

[77] M.Markovic, "Tehnike zašite i kriptografski protokoli u savremenim računarskim mrežama", februar 2004.

[78] http://en.wikipedia.org/wiki/Key_whitening

[79] B. Beckett, "Introduction to Cryptology", Blackwell, Oxford 1988.

[80] http://en.wikipedia.org/wiki/Asymmetric_key_algorithm

[81] http://os2.zemris.fer.hr

[82] http://en.wikipedia.org/wiki/RSA

[83] http://en.wikipedia.org/wiki/Digital_signature

[84] http://fly.srk.fer.hr

[85] D. Osten, H. Carlin, M. Arneson, B. Blan, “Biometric, Personal Identification System”, U.S. Patent 5,719,950, Feb. 17, 1998.

[86] H. T. F. Rhodes, ″Alphonse Bertillon: Father of Scientific Detection,″ Abelard-Schuman, New York, 1956.

[87] FVC2004: Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2004.

[88] A. Ross, S. Dass and A. K. Jain, "A Deformable Model for Fingerprint Matching", Pattern Recognition, 2004.

[89] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, ″Handbook of Fingerprint Recognition″, Springer-Verlag; Bk & DVD edition, May 1, 2003.

[90] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld. ″Face recognition: A literature survey,″ ACM Comput. Surv., 35(4):399–458, 2003.

[91] P. Phillips, P. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, W. Worek., ″Overview of the Face Recognition Grand Challenge,″ In Proc. of IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), San Diego, CA, June 2005.

[92] Face Recognition Vendor Test 2005. URL:
http://www.frvt.org/FRVT2005/.

[93] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, ″Biometrics: A Grand Challenge,″ Proceedings of International Conference on Pattern ecognition, Cambridge, UK, Aug. 2004.

[94] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, ″Guide to Biometrics,″ Springer, 2003.

[95] A. K. Jain and S. Pankanti, ″Biometrics Systems: Anatomy of Performance″, IEICE Transactions Fundamentals, Vol. E84-D, No. 7, pp. 788-799, 2001.

[96] Stan Z. Li, Jianhuang Lai, Tieniu Tan, Guocan Feng, Yunhong Wang, "Advances in Biometric Person Authentication: 5th Chinese Conference on Biometric Recognition, SINOBIOMETRICS 2004," Guangzhou, China, December 13-14, 2004, Springer; 1 edition, January 12, 2005.

[97] Harry Hollien, ″Forensic Voice Identification,″ Academic Press, September, 2001.

[98] S. Furui, ″Recent Advances in Speaker Recognition″, Pattern Recognition Letters, Vol. 18, No. 9, 1997, pp. 859-872.

[99] U.V. Chaudhari, J. Navratil, G.N. Ramaswamy, R.D. Zilca, ″Future speaker recognition systems: Challenges and solutions,″ Proceedings of AUTOID-2002, Tarrytown, NY, March 2002.

[100] D. Osten, H. Carlin, M. Arneson, B. Blan, ″Biometric, Personal Identification System,″ U.S. Patent 5,719,950, Feb. 17, 1998.

[101] J. L. Wayman, "Technical Testing and Evaluation of Biometric Identification Devices," Biometrics: Personal Identification in Networked Society, Kluwer Academic, December 1998.

[102] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication", Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-40.

[103] James L. Wayman, ″Error-Rate Equations for the General Biometric System,″ IEEE Robotics and Automation Magazine, pps 35-48. Vol. 6, No. 1, March 1999.

[104] NYC Visit homepage,
http://www.nycvisit.com/content/index.cfm?pagePkey=57.

[105] James Wayman, Anil Jain, Davide Maltoni, Dario Maio, ″Biometric Systems: Technology, Design and Performance Evaluation,″ Springer, 1 edition, December 16, 2004.

[106] A. K. Jain and A. Ross, "Multibiometric Systems," Communications of the ACM, Special Issue on Multimodal Interfaces, Vol. 47, No. 1, pp. 34-40, January 2004.

[107] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 8, pp. 1010-1025, August 2002.

[108] Nelini Rahta, Ruud Bolle, Nalini K. Rahta, ″Automatic Fingerprint Recognition Systems″, Springer-Verlag, November 1, 2003.

[109] Kingston, C.R. and P.L. Kirk, ″Historical Development and Evaluation of the '12 Point Rule' in Fingerprint Identification, ″ International Criminal Police Review, 1965.

[110] Ching-Tang Hsieh, Zhuang-Yuan Lu, Tan-Chi Li, Kung-Chen Mei, ″An Effective Method to Extract Fingerprint Singular Point,″ The Fourth International Conference on High-Performance Computing in the Asia-

Pacific Region-Volume 2 , May 14 - 17, 2000, Beijing, China.

[111] http://en.wikipedia.org/wiki/Gabor filter.

[112] Milana M. Vladić, "Izdvajanje karakterističnih detalja iz slike otiska prsta".

[113] Henry C. Lee, ″Advances in Fingerprint Technology,″ Second Edition, CRC, 2nd edition, June 15, 2001.

[114] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security & Privacy Concerns," IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, March-April 2003.

[115] R. Derakhshani R, S.A.C. Schuckers, L. Hornak, L. O'Gorman, "Determination of Vitality From A Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners," Pattern Recognition, No.2, pp. 383-396, 2003.

[116] www.ebioshop.com

[117] http://www.easyintech.com

[118] Daugman J., Downing C., ″Epigenetic randomness, complexity, and singularity of human iris patterns,″ Procedings of the Royal Society, B, 268, Biological Sciences, pp 1737 – 1740, 2001.

[119] F.H. Adler, ″Physiology of the Eye: Clinical Application,″ fourth ed., London: The C.V. Mosby Company, 1965.

[120] J. Rohen, ″Morphology and pathology of the trabecular meshwork,″ The Structure of the Eye, Smelser, Ed. New York: Academic Press, 1961,″ pp. 335-341.

[121] Daugman, J., ″High confidence visual recognition of persons by a test of statistical independence,″ IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15(11), pp. 1148-1161., 1993

[122] Daugman, J., "U.S. Patent No. 5,291,560: Biometric Personal Identication System Based on Iris Analysis," Issue Date: 1 March 1994.

[123] Daugman J., ″How iris recognition works,″ IEEE Trans. CSVT, vol. 14, no. 1, pp. 21 – 30, 1994.

[124] http://hr.wikipedia.org/wiki/Oko

[125] N. Lekic, “Doprinosi razvoju savremenih identifikacionih sistema”, ETF Podgorica, 2006.

[126] Libor Masek, “Recognition of human iris patterns for biometric identification” http://www.csse.uwa.edu.au/~pk/studentprojects/libor/, The University of Western Australia

[127] W. Kong and D. Zhang, “Detecting eyelash and reflection for accurate iris segmentation”. International Journal of Pattern Recognition and Artificial Intelligence, 17(6):1025–1034, 2003.

[128] http://en.wikipedia.org/wiki/Gaussian_filter

[129] Xiaomei Liu, B.S., M.S., “Optimizations in Iris Recognition ” , Graduate Program in Computer Science and Engineering Notre Dame, Indiana, 2006.

[130] http://homepages.inf.ed.ac.uk/rbf/HIPR2/gsmooth.htm

[131] Tai Sing Lee, Image Representation Using 2D Gabor Wavelets, IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 18, NO. 10, OCTOBER 1996

[132] http://cnx.org/content/m12493/latest

[133] J. Daugman (2003) “Demodulation by complex-valued wavelets for stochastic pattern recognition”, Int'l Journal of Wavelets and Multi-resolution Information Processing

[134] Celine Mancas-Thillou, Bernard Gosseli, “Character Segmentation-by-Recognition Using Log-Gabor Filters”

[135] http://homepages.inf.ed.ac.uk/rbf/HIPR2/log.htm

[136] http://en.wikipedia.org/wiki/Iris_scan

[137] Daugman J., ″The importance of being random: Statistical principles of iris recognition,″ Pattern Recognition, vol. 36, no. 2, pp 279-291, 2003.

[138] Daugman J., "Biometric decision landscapes." Technical Report No. TR482, University of Cambridge Computer Laboratory, 2000.

[139] http://www.iridiantech.com/news.php?page=1&rel=062303

[140] http://www.accessexcellence.org/WN/SU/irisscan.html

[141] http://news.bbc.co.uk/2/hi/uk_news/england/2638075.stm

[142] P. Phillips, P. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek., ″Overview of the Face Recognition Grand Challenge,″ In Proc. of IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), San Diego, CA, June 2005.

[143] Shaohua Kevin Zhou, Rama Chellappa, Wenyi Zhao, ″Unconstrained Face Recognition (International Series on Biometrics)″, Springer; 1 edition, November 30, 2005.

[144] Daugman J., "Phenotypic versus genotypic approaches to face recognition", Face Recognition: From Theory to Applications, Heidelberg: Springer-Verlag, pp 108 – 123, 1998.

[145] Stan Z. Li, Anil K. Jain, ″Handbook of Face Recognition″, Springer; 1 edition, March 15, 2005.

[146] H. Moon and P. J. Phillips, “Computational and performance aspects of PCA-based face recognition algorithms,” Perception, vol. 30, pp. 303–321, 2001.

[147] J. R. Beveridge, D. Bolme, B. A. Draper, and M. Teixera, “The CSU face identification evaluation system,” Machine Vision and Applications, 2004.

[148] V. Blanz, T. Vetter, ″Face recognition based on fitting a 3D morphable model,″ IEEE Trans. on Pattern Analysis and Machine Intelligence, 25(9):1063–1074, 2003.

[149] Kyong I. Chang, Kevin W. Bowyer, Patrick J. Flynn, “An evaluation of multi-modal 2d+3d face biometrics,” IEEE Trans. PAMI, vol. 27, no. 4, pp. 619–624, 2005.

[150] http://www.visionics.com/

[151] http://www.biometrix.at/page21.html

[152] http://www.cs.colostate.edu/evalfacerec/index.html

[153] R. Beveridge, B. Draper, ″Evaluation of face recognition algorithms,″ release version 5.0, online: http://www.cs.colostate.edu/evalfacerec/index.html.

[154] Phillips, P. J., P. J. Rauss, and S. Der., “FERET (face recognition technology) recognition algorithm development and test results,” Army Research Laboratory technical report, ARL-TR-995, 1996.

[155] Blackburn, D. M., J. M. Bone, and P. J. Phillips., ″FRVT 2000 Report″, Technical Report, 2001.

[156] P.J. Phillips, P.J. Grother, R.J. Micheals, D.M. Blackburn, E. Tabassi, and J.M. Bone, “Face recognition vendor test 2002: Evaluation report”, Tech. Rep. NISTIR 6965, National Institute of Standards and Technology, 2003.

[157] P.J. Grother, ″Face recognition vendor test 2002: Supplemental report″, Tech. Rep. NISTIR 7083, National Institute of Standards and Technology, 2004.

[158] Face Recognition Vendor Test 2005. URL:
http://www.frvt.org/FRVT2005/.

[159] A. Hampapur, S. Pankanti, A.W. Senior, Y-L Tian, L. Brown, R. Bolle, "Face Cataloger: Multi-Scale Imaging for Relating Identity to Location," IEEE conference on Advanced Video and Signal Based Surveillance, Miami, FL, July 21-22, 2003.

[160] http://www.epic.org/privacy/facerecognition/

[161] http://zones.advisor.com/doc/07246

[162] Edmund S Crelin, ″The human vocal tract: Anatomy, function, development, and evolution,″ Vantage Press; 1st ed edition, 1987.

[163] Richard L. Klevans, Robert D. Rodman, ″Voice Recognition (Artech House Telecommunications Library),″ Artech House Publishers, September 1997.

[164] J. Liu and Y. Ye, "Conversational Speech Biometrics," E-Commerce Agents Marketplace Solutions, Security Issues, and Supply and Demand, Springer Verlag, 2001, Pages 166-179.

[165] "An instantiable speech biometrics module with natural language interface: Implementation in the telephony environment," Proc. of the ICASSP 2000, Istanbul, Turkey, June 2000.

[166] http://www.research.ibm.com/VIVA_Demo/

[167] Kevin James, "PC Interfacing and Data Acquisition : Techniques for Measurement, Instrumentation and Control", Newnes (August 10, 2000).

[168] Kenneth J Leap, "The design of a microprocessor-based data logger (Open-file report / U.S. Geological Survey)", Kenneth J Leap, U.S. Geological Survey (1982).

[169] 2- Wire Serial EEPROMs AT24C128, AT24C256, Atmel Corporation 2004.

[170] Nedjeljko Lekić, Zoran Mijanović, Radovan Stojanović, ″Multikontrolerski loger,″ XLIX konferencija za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu fiziku - ETRAN, Budva 2005.

[171] http://en.wikipedia.org/wiki/Time_server

[172] http://en.wikipedia.org/wiki/Network_Time_Protocol

[173] http://en.wikipedia.org/wiki/Radio_clock#GPS_clocks

[174] http://en.wikipedia.org/wiki/DCF77

[175] Klaus Bender, Marianne Katz ″Profibus: The Fieldbus for Industrial Automation″, Prentice Hall, June 1993.

[176] Eduardo Tovar and Francisco Vasques, "Real-Time Fieldbus Communications Using Profibus Networks", IEEE Transactions on Industrial Electronics, 46(6): 1241-1251, December 1999.

[177] John Park, "Practical Data Communications for Instrumentation and Control", Newnes, (June 2003).

[178] Walt Boyes, "Instrumentation Reference Book", Third Edition, Butterworth-Heinemann; 3 edition (November 2002).

[179] Ian Verhappen, Augusto Pereiro, Augusto Pereira, Marilyn J. Landis, ″Foundation Fieldbus: A Pocket Guide″, ISA - The Instrumentation, Systems, and Automation Society, July 2002.

[180] Romilly Bowden, ″HART Field Communications Protocol″, FISHER- ROSEMOUNT, August 1997.

[181] Wolfhard Lawrenz, ″Can System Engineering: From Theory to Practical Applications″, Springer Verlag, Book and Disk edition, October 1997.

[182] Charles Spurgeon, "Ethernet: The Definitive Guide," O'Reilly Media, Inc., 1 edition, February 9, 2000.

[183] Timo Halonen, Javier Romero, Juan Melero, ″GSM, GPRS and EDGE Performance: Evolution Towards 3G/UMTS,″ John Wiley & Sons, 2 edition, December 2, 2003.

[184] Nedjeljko Lekić, Zoran Mijanović, Rada Dragović-Ivanović, Radovan Stojanović, ″Off-line Mifare sistem za kontrolu pristupa,″ XLVIII konferencija za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu fiziku - ETRAN, Čačak 2004.