UNIVERZITET CRNE GORE
PRIRODNO-MATEMATIČKI FAKULTET
DOKTORSKE STUDIJE

Crna Gora
UNIVERZITET CRNE GORE
PRIRODNO-MATEMATIČKI FAKULTET
Broj 729
Podgorica, 13 04 2021 god.

VIJEĆU PRIRODNO-MATEMATIČKOG FAKULTETA

Predmet: Ocjena podobnosti doktorske teze i kandidata

U skladu sa članom 35, stav 2, Pravila doktorskih studija, Komisija za ocjenu podobnosti doktorske teze i kandidata koju je imenovao Senat Univerziteta Crne Gore na sjednici održanoj 10. 03. 2021. godine, u sastavu

1. **Dr Slobodan Đukanović**, redovni profesor Elektrotehničkog fakulteta Univerziteta Crne Gore (naučna oblast: mašinsko učenje)
2. **Dr Milenko Mosurović**, redovni profesor Prirodno-matematičkog fakulteta Univerziteta Crne Gore (naučna oblast: vještačka inteligencija)
3. **Dr Igor Đurović**, redovni profesor Elektrotehničkog fakulteta Univerziteta Crne Gore (naučna oblast: obrada signala)

podnijela je Vijeću Prirodno-matematičkog fakulteta **Izvještaj sa javne odbrane polaznih istraživanja doktorske disertacije** i **Ocjenu podobnosti teme doktorske disertacije** (**Obrazac D1**) kandidata **mr Koste Pavlovića.**

Komisija za doktorske studije PMF-a je na sjednici održanoj 07. 04. 2021. godine, zaključila da dostavljeni Izvještaj sadrži sve elemente propisane Pravilima doktorskih studija i Vodičem za doktorske studije i prosljeđuje ga na razmatranje Vijeću Prirodno-matematičkog fakulteta.

Podgorica, 13. 04. 2021. god.

ZA KOMISIJU ZA DOKTORSKE STUDIJE

Doc. dr Goran Popivoda

OCJENA PODOBNOSTI DOKTORSKE TEZE I KANDIDATA

OPŠTI PODACI O DOKTORANDU	
Titula, ime i prezime	MSc Kosta Pavlović
Fakultet	Prirodno-matematički fakultet
Studijski program	Računarske nauke
Broj indeksa	1/2018
Podaci o magistarskom radu	Primjena genetskog algoritma za optimizaciju parametara algoritma izvlačenja informacija iz administrativnih dokumenata, Vještačka inteligencija, Univerzitet Crne Gore, Prirodno-matematički fakultet, 2018, A (10.00)
NASLOV PREDLOŽENE TEME	
Na službenom jeziku	Umetanje vodenih žigova u digitalne audio signale korišćenjem dubokih neuronskih mreža
Na engleskom jeziku	Digital audio watermarking using deep neural networks
Datum prihvatanja teme i kandidata na sjednici Vijeća organizacione jedinice	16.02.2021.
Naučna oblast doktorske disertacije	Vještačka inteligencija
Za navedenu oblast matični su sljedeći fakulteti	
Prirodno-matematički fakultet, Elektrotehnički fakultet	

A. IZVJEŠTAJ SA JAVNE ODBRANE POLAZNIH ISTRAŽIVANJA DOKTORSKE DISERTACIJE

MSc Kosta Pavlović pristupio je odbrani polaznih istraživanja sprovedenih u okviru izrade doktorske disertacije pod nazivom „Umetanje vodenih žigova u digitalne audio signale korišćenjem dubokih neuronskih mreža“ dana 02.04.2021. godine u 13:00h, pred komisijom u sastavu:

- Prof. dr Slobodan Đukanović, redovni profesor Elektrotehničkog fakulteta Univerziteta Crne Gore (predsjednik Komisije)
- Prof. dr Milenko Mosurović, redovni profesor Prirodno-matematičkog fakulteta Univerziteta Crne Gore (član)
- Prof. dr Igor Đurović, redovni profesor Elektrotehničkog fakulteta Univerziteta Crne Gore (mentor)

Komisija je imenovana na sjednici Vijeća Prirodno-matematičkog fakulteta, održanoj 16.02.2021. godine. Kandidat je izložio motive za izbor teme disertacije i dao pregled naučne oblasti umetanja vodenih žigova u digitalne signale. Objasnio je postavljene probleme i izazove i predstavio korištene tehnike i metode istraživanja, kao i postignute rezultate. Kandidat je precizno naznačio dalje pravce i ciljeve istraživanja. Komisija je zaključila da ovo istraživanje može predstavljati doprinos oblastima vještačke inteligencije, mašinskog učenja i digitalne obrade signala. Nakon izlaganja kandidata, članovi komisije iznijeli su svoje komentare, sugestije i postavili pitanja. Komisija je, uzimajući u obzir kvalitet sprovedenih istraživanja i odbrane,

jednoglasno donijela odluku da je kandidat uspješno odbranio polazna istraživanja.

B. OCJENA PODOBNOSTI TEME DOKTORSKE DISERTACIJE

B1. Obrazloženje teme

Intelektualnom svojinom, pored ostalog, smatra se bilo kakva duhovna tvorevina u nauci ili umjetnosti, bilo u pisanom, govornom ili nekom drugom obliku i nju je, zbog njene nematerijalne prirode, mnogo teže zaštititi od tradicionalne svojine. Zaštita intelektualne svojine u savremenom, digitalnom svijetu sve više dobija na značaju jer je ekspanzijom Interneta njeno otuđivanje postalo učestalije. Takođe, pojavom dubokih neuralnih mreža javila se mogućnost generisanja vještačkih podataka, koji imaju za cilj stvaranje falsifikata, širenje dezinformacija, diskreditacije javnih ličnosti, krađu identiteta itd. Kreatori audio sadržaja, bilo da se radi o muzičarima, glumcima, političarima ili nekim drugim ljudima koji nijesu javne ličnosti na meti su ovakvih napada i neophodno je da njihova prava budu zaštićena. Iz ovih razloga, umetanje vodenog žiga u audio signale potrebno je ne samo u cilju zaštite intelektualne svojine, već i u cilju zaštite osjetljivih informacija dostupnih u vidu javnih govora i sl.

B2. Cilj i hipoteze

Ciljevi ovog istraživanja su:

- Prikupljanje i organizacija respektabilnog skupa podataka za testiranje sistema za umetanje vodenog žiga u audio signale.
- Razvoj modela - duboke neuronske mreže, slične U-Net enkoderu, koja će vršiti umetanje vodenih žigova, u obliku binarnih poruka, u audio signale, bez narušavanja njihovog kvaliteta.
- Razvoj modela - duboke neuronske mreže (dekodera), koji će vršiti ekstrakciju vodenih žigova iz audio signala.
- Dizajniranje slojeva za simulaciju napada na audio watermarking sisteme.
- Pronalazak domena u kojem je najpogodnije vršiti pomenute transformacije signala.
- Osmišljavanje procesa obučavanja modela kako bi postigli konvergenciju razvijenog sistema.

Postavljene hipoteze su:

- Umetanje vodenog žiga u audio signale je moguće korišćenjem dubokih neuronskih mreža.
- Upotrebom dekoderske mreže moguće je izvršiti ekstrakciju vodenog žiga iz signala nosioca.
- Enkoder mreža će održati kvalitet audio signala na visokom nivou.
- Dekoder će moći da izvrši ekstrakciju vodenog žiga u situacijama kada je signal oštećen određenim vrstama napada.
- Dekoder mreža će pouzdano izbjegavati detekciju pogrešnog vodenog žiga.

B3. Metode i plan istraživanja

Prvi korak u istraživanju je prikupljanje skupa podataka nad kojima će se vršiti obučavanje dubokog modela i nad kojima će cjelokupni sistem biti testiran. Korpus govornih signala prikupljen je za vrijeme zasijedanja Skupštine Crne Gore. Preuzeti su govori sa 90 sjednica

održanih tokom 2016., 2017., 2018. i 2019. godine u ukupnom trajanju od oko 868 časova nakon eliminisanja intervala tišine. Ovaj skup može biti proširen vještački generisanom muzikom i zvukom ili određenim korpusima podataka dostupnim na Internetu.

Radi boljeg i efikasnijeg prezentovanja signala neuronskoj mreži i njenim konvolucionim slojevima, neophodno je izvršiti odgovarajuću obradu i preprocesiranje signala. Tradicionalni pristupi koriste vremensko-frekvencijsku obradu signala i tom prilikom se mogu vršiti različite transformacije signala, kako bi se otkrio domen u kojem je najpogodnije rješavati postavljene zadatke. Spektrogram kao najčešći način reprezentacije audio signala. U ovom slučaju ne može biti idealan izbor zbog toga što je njegova inverzija veoma složena i ostavlja posledice na proces umetanja i ekstrakcije vodenog žiga. Zbog toga se upotreba kratkotrajne Furijeove transformacije (STFT) nameće kao prvi izbor. Međutim, treba preispitati da li je potrebno uopšte vršiti transformaciju signala, jer su tradicionalne konvolucione mreže najbolje rezultate ostvarile u radu sa realnim signalima, što takođe predstavlja mogući pravac istraživanja.

Arhitektura sistema će se sastojati od najmanje dvije neuronske mreže, enkodera i dekodera. Enkoder će biti mreža slična U-Net mreži i sastojaće se od niza konvolucionih slojeva. Konvolucioni slojevi vrše ekstrakciju obilježja eliminacijom redudantnih informacija čime se smanjuje dimenzija ulaza. Zadatak ove mreže će biti da ovim smanjenjem ulaznih dimenzija signala, odnosno njegove vremensko-frekvencijske reprezentacije, pronađe određeni nestandardni domen u kojem će biti umetnut vodeni žig u obliku binarne poruke. Dekoder mreža će biti vrsta klasifikatora, koja će se sastojati od konvolucionih i potpuno povezanih slojeva i koja će se nadovezati na enkoder mrežu i pokušati da iz signala u koji je umetnut vodeni žig detektuje svaki njegov bit.

U poznatoj literaturi predložen je i opisan veoma veliki broj napada na audio watermarking sisteme. Ova oblast i dalje je predmet istraživanja. Nove vrste napada neprekidno se dizajniraju i zbog toga se prilikom kreiranja audio watermarking sistema mora odabrati ograničen skup napada i sistem se pripremati i testirati tako da bude otporan barem na te napade. Kako za robustnost ne postoje definisane mjere kao za procjenu kvaliteta audio signala, na dizajnerima audio watermarking sistema je da se potrude da taj skup napada na koje njihov sistem nije otporan učine što manjim.

Napadi se razlikuju u zavisnosti od toga kakav efekat pokušavaju ostvariti nad procesom detekcije. Postoje napadi koji pokušavaju da onemoguće detekciju vodenog žiga, napadi koji izazivaju detekciju pogrešnog vodenog žiga i napadi koji dovode do neautorizovane detekcije umetnutog vodenog žiga. Vrsta napada od interesa bira se u skladu sa planiranom namjenom sistema za umetanje vodenih žigova. U prvom dijelu istraživanja sistem će biti obučavan da se suprotstavi napadima koji pokušavaju dovesti do toga da dekoder ne može pravilno detektovati umetnuti vodeni žig. Takođe, u početku se neće pretpostavljati nikakvo znanje o samom vodenom žigu prilikom dizajniranja napada, kao ni postupku umetanja vodenog žiga. U kasnijim fazama istraživanja proširivaćemo ovaj skup i uvodićemo druge tipove napada.

U nekim situacijama, napadač može doći u posjed skupa primjeraka watermark-ovanih i originalnih signala. Ovo se može iskoristiti za obučavanje posebne neuronske mreže koja bi na osnovu ovih primjeraka pokušala da nauči kako da onemogući detekciju vodenih žigova u svim audio snimcima.

Napadima se nekada pokušava dovesti do detekcije pogrešnog vodenog žiga. Ovo se ostvaruje tako što se estimira vodeni žig u jednom signalu, a zatim se on iskopira u drugi signal nosioc. Od ovakvog napada sistem se može zaštititi uvođenjem korelacije između vodenog žiga i signala nosioca, a sama estimacija vodenih žigova može se vršiti primjenom dubokih neuronskih mreža.

Procedura obučavanja ovakvog sistema mora biti strogo kontrolisana iz razloga što enkoder i dekoder imaju suprotstavljene zadatke, pa može doći do toga da jedna mreža nadvlada drugu i onemogući njenu konvergenciju tj. obučavanje. Funkcija gubitka ovakvog sistema mora biti pažljivo osmišljena i regulisana tokom obučavanja, kako bi čitav sistem konvergirao. Pored samih mjera za preciznost rekonstrukcije originalnog signala, odnosno očuvanja kvaliteta signala (zadatak enkodera) i mjere za preciznost ekstrakcije vodenih žigova (zadatak dekodera), u funkciju gubitka eventualno treba dodati i odgovarajuće mjere korelacije signala i vodenog žiga kako bi se postigao veći stepen robustnosti i olakšao zadatak dekoder mreži.

B4. Naučni doprinos

Primjena dubokih neuronskih mreža je jedan od najmodernijih pristupa za umetanje vodenih žigova u digitalne signale, kao i za njihovu detekciju. Očekuje se da se primjenom ovih tehnika dostignu visoke mjere očuvanja kvaliteta signala (SNR iznad 30dB, PESQ iznad 4). Takođe, očekuje se da se postigne visok nivo preciznosti detekcije vodenih žigova u audio signalima od iznad 90% i otpornost na veliki broj različitih napada, između ostalih i napada desinhronizacije koji predstavljaju najveći problem tradicionalnim pristupima za umetanje vodenih žigova.

B5. Finansijska i organizaciona izvodljivost istraživanja

Mišljenje komisije je da kandidat uz sopstvene napore i podršku Prirodno-matematičkog fakulteta može obezbijediti odgovarajuće organizacione uslove za izradu ove doktorske disertacije.

Mišljenje i prijedlog komisije

Komisija za ocjenu podobnosti teme i rada kandidata, nakon detaljnog razmatranja prijave teme, nakon javne prezentacije programa istraživanja, datih odgovora na postavljena pitanja, mišljenja je da su polazna istraživanja kandidata MSc Koste Pavlovića originalan naučni poduhvat koji će dati vrijedan doprinos oblasti umetanja vodenih žigova u digitalne audio signale. Metode i ciljevi istraživanja, kao i problemi koje treba riješiti su precizno definisani. Razvoj tehnika dubokog učenja u poslednjih nekoliko godina i njihova upotreba u različitim oblastima daju dobru osnovu za istraživanje i poboljšavanje trenutnih rezultata. Kandidat će predložiti nove metode za umetanje i detekciju vodenih žigova zasnovane na dubokom učenju i time poboljšati trenutne rezultate. Predložena tema je multidisciplinarna, čime još više dobija na kvalitetu.

Uzimajući u obzir sve navedeno, komisija smatra da je tema istraživanja aktuelna i da odgovara nivou istraživanja za doktorsku disertaciju. Stoga komisija predlaže Vijeću Prirodno-matematičog fakulteta da se podrži prijava disertacije kandidata MSc Koste Pavlovića.

Prijedlog izmjene naslova

Prijedlog promjene mentora i/ili imenovanje drugog mentora

Planirana odbrana doktorske disertacije		
2022/zimski semestar		
Izdvojeno mišljenje		
Napomena		
ZAKLJUČAK		
Predložena tema po svom sadržaju **odgovara** nivou doktorskih studija.	**DA**	NE
Tema **je** originalan naučno-istraživački rad koji odgovara međunarodnim kriterijumima kvaliteta disertacije.	**DA**	NE
Kandidat **može** na osnovu sopstvenog akademskog kvaliteta i stečenog znanja da uz adekvatno mentorsko vođenje realizuje postavljeni cilj i dokaže hipoteze.	**DA**	NE
Komisija za ocjenu podobnosti teme i kandidata		
Prof. dr Slobodan Đukanović, Elektrotehnički fakultet Univerziteta Crne Gorez		
Prof. dr Milenko Mosurović, Prirodno-matematički fakultet Univerziteta Crne Gore	Milenko Mosurović	
Prof. dr Igor Đurović, Elektrotehnički fakultet Univerziteta Crne Gore		
U Podgorici, 06.04.2021.	MP	DEKAN

PRILOG

PITANJA KOMISIJE ZA OCJENU PODOBNOSTI DOKTORSKE TEZE I KANDIDATA	
Prof. dr Slobodan Đukanović	Da li je poznato u kojem vremenskom trenutku je vodeni žig umetnut? **Odgovor:** Vodeni žig se ubacuje duž čitavog signala i tačni vremenski trenuci u kojima su umetnuti biti vodenog žiga nijesu predefinisani, niti uvijek isti. Iscrtavanja aproksimacije vodenog žiga nakon njegovog umetanja u audio signal pokazuju da su u različitim audio snimcima biti vodenog žiga drugačije raspoređeni.
	Da li je korišćenje Mel spektrograma razmatrano kao jedan način reprezentacije ulaznog signala, pošto se ova reprezentacija pokazala kao optimalna u zadacima klasifikacije audio signala? **Odgovor:** Korišćenje Mel spektrogram kao načina reprezentacije, barem za enkoder mrežu, u ovom slučaju je problematično zbog nemogućnosti rekonstrukcije signala iz Mel spektrograma. Moguće je da bi dekoder mreži ova reprezentacija odgovarala.
	Da li trenutna dužina vodenog žiga od 512 bita dovoljna za prenos nekih značajnijih informacija i da li se planira njeno povećanje? **Odgovor:** Glavni razlog umetanja vodenih žigova u digitalne signale je očuvanje autentičnosti, dok je količina prenesenih informacija sporedna. Prenos skrivenih informacija, a samim tim i težnja ka povećanju veličine poruke, je zadatak steganografije, koja je oblast donekle slična umetanju vodenih žigova. Kapacitet, kao mjera performansi sistema za umetanje vodenog žiga, je manje bitna u odnosu na robustnost, preciznost detekcije vodenog žiga i kvalitet izlaznog signala. Pored toga, kapacitet trenutne arhitekture od 256 bps je na nivou pristupa iz literature. Povećanje dužine vodenih žigova za sada nije prioritet u istraživanju.
Prof. dr Milenko Mosurović	Kolika je dužina vodenog žiga i da li je fiksna? **Odgovor:** Dužina vodenog žiga je fiksna. Trenutno koristimo vodene žigove od 512 bita.
	Da li je broj vodenih žigova ograničen? **Odgovor:** Broj vodenih žigova mora biti ograničen. Polazna istraživanja su sprovedena sa 8 slučajno generisanih vodenih žigova, ali je cilj da se taj skup proširi.
	Da li se u nekim napadima ima pristup dijelu sistema za ekstrakciju vodenog žiga? **Odgovor:** Sistem za umetanje vodenih žigova se na neki način može smatrati kriptografskim. U skladu sa

	Kirhofovim principom sve pojedinosti takvog sistema moraju biti poznate javnosti, osim tajnog ključa. U sistemu kakav je dizajniran u okviru ovog istraživanja, dekoder mreža se može posmatrati kao tajni ključ. Međutim, u literaturi se pominje i vrsta napada kod kojih napadač ima pristup dekoderu i tada napadač može vršiti prilagođavanja svojih napada sve dok oni ne budu uspješni.
	Da li bi se Furijeova transformacija mogla vršiti u nekom polju po modulu prostog broja? **Odgovor:** Kako bi u ovom slučaju audio signal morao biti predstavljen kao niz cijelih brojeva, vjerovatno se ne bi došlo do boljih rezultata. Ovaj način računanja Furijeove transformacije bi mogao biti pogodniji za primjenu u obradi slike. Operacije u nekom polju po modulu prostog broja se mogu razmotriti i iskoristiti kao tehnika za umetanje vodenih žigova.
Prof. dr Igor Đurović	Koji su drugi mogući pravci istraživanja? **Odgovor:** Imali smo nekoliko drugih pravaca u istraživanju, ali umetanje vodenog žiga se za sada ispostavilo kao najplodnije. Pokušali smo da sa različitim tehnikama estimacije frekvencije signala dobijemo precizniju reprezentaciju signala, ali ovi pokušaju su se za sada pokazali kao neuspješni. Pored toga, mogućnost za dalje istraživanje vidimo i u korišćenju cikličnih kodova kao jednog sredstva za pomoć prilikom detekcije vodenih žigova, kao i u dizajniranju sopstvenih napada na audio signale, moguće korišćenjem dubokih neuronskih mreža.
	Na koje vrste napada je trenutni sistem otporan? **Odgovor:** Za sada je naš sistem obučen da bude otporan na sljedeće napade: dodavanje šuma, niskopropusni Batervortov filtar sa graničnom frekvencijom na 3.4kHz i poništavanja nasumično odabranih 1000 odbiraka signala, odnosno postavljanje njihove vrijednosti na 0.
PITANJA PUBLIKE DATA U PISANOJ FORMI	
ZNAČAJNI KOMENTARI	