UNIVERZITET SINGIDUNUM
Departman za poslediplomske studije
Danijelova 32, Beograd

VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE

Odlukom Veća Departmana za poslediplomske studije broj _4 - 123/2021_ od 25.05.2021. godine, određeni smo za članove Komisije za ocenu i odbranu doktorske disertacije kandidata Dušana Markovića pod nazivom „Detektovanje manipulacije u video snimcima stvorenih Deepfake tehnikom sistemom učenja prostorno vremenskih karakteristika“

o čemu podnosimo sledeći

IZVEŠTAJ

1. Osnovni podaci o kandidatu i doktorskoj disertaciji

Kandidat Dušan Marković rođen je 03.05.1989. god. u Beogradu, gde je završio osnovnu i srednju školu. Srednju elektotehničku školu je završio 2008. godine na smeru Elektrotehničar računara. Osnovne akademske studije je završio 2013. god. na Fakultetu za informatiku i računarstvo, Univerziteta Singidunum. Master akademske studije upisuje 2014. god. na smeru „Savremene informacione tehnologije“ na Univerzitetu Singidunum sa prosečnom ocenom 10.

Od 2013. god. kandidat je zaposlen na Univerzitetu Singidunum kao saradnik u računarskom centru a 2015. godine zadržavajući stara zaduženja uključuje se i u realizaciju nastave prvo kao saradnik u nastavi a zatim i kao predmetni asistent. Predmeti na kojima je angažovan su isključivo iz oblasti računarstva (Veb dizajn, Veb platforme, Internet i Veb tehnologije, Veb programiranje, Aplikativni softver, Osnovi informacionih tehnologija, Internet marketing i sl.)

Doktorske akademske studije na studijskom programu Napredni sistemi zaštite na Univerzitetu Singidunum, upisao je 2016. godine.

Kandidat ima objavljene sledeće radove, čime je ispunjen preduslov za odbranu doktorske disertacije:

Radovi objavljeni u kategoriji M21:

- Kicović, D., Vučković, D., **Marković, D.**, Jović, S., Assessment of visitors thermal comfort based on physiologically equivalent temperature in open urban areas, Urban Climate, pp. 33-39, Jun, 2019.

Radovi objajavljeni u kategoriji M24:

- H. Skrijelj, D. Radovanović, **D. Marković**, S. Jović, Aplikacija evolucionog algoritma za estimaciju uticaja sistema farme na prirodu, Zaštita materijala, pp. 42-48, Jun, 2019.

Ostali objavljeni radovi

- Strumberger, M. Sarac, **D. Markovic**, N. Bacanin, Hybridized Monarch Butterfly Algorithm for Global Optimization Problems, International Journal of Computers , Vol. 3, pp. 63-68, Apr, 2018.

- I. Strumberger, M. Sarac, **D. Markovic**, N. Bacanin, Moth Search Algorithm for Drone Placement Problem, International Journal of Computers, Vol. 3, pp. 75-80, Apr, 2018.

- M. Milenkovič, D. Kekić,D. Glavaš, **D. Marković**, V. Nikolić, Modern Database on Human and Material and Technical Resources in Emergency Management Systems, Sinteza 2020 - International Scientific Conference on Information Technology and Data Related Research, pp. 160-166, Oct, 2020.

- M. Milenković, D. Kekić, D. Glavaš, **D. Marković**, Upotreba Savremenih softverskih rešenja u pripremi i obuci za reagovanje u vanrednim situacijama, SINTEZA 2019, pp. 430-435, Apr, 2019.

- **D. Marković**, M. Tair, M. Šarac, D. Stamenković, N. Savanović, Content distribution in education support software, 4nd International Scientific Conference of IT and Business-Related Research SINTEZA 2017, Belgrade, Serbia, pp. 248-253, Apr, 2017.

- **D. Marković**, M. Šarac, S. Adamović, D. Stamenković, N. Savanović, Virtualization of workspace and its application in education, 3rd International Conference on Electrical, Electronic and Computing Engineering IcETRAN 2016, Zlatibor, Serbia, Jun, 2016.

- N. Savanović, M. Šarac, **D. Marković**, D. Radovanović, A. Jevremović, Computer network security on physical layer, 3rd International Conference on Electrical, Electronic and Computing Engineering IcETRAN 2016, Zlatibor, Serbia , Jun 2016, pp. 80-81, Jun, 2016.

Doktorska disertacija kandidata Dušana Markovića je urađena na ukupno 111 strana, od čega 10 strana čini spisak literature. Spisak literature obuhvata 111 referenci koje čine naučni radovi,

knjige, zbornici radova, zakonski propisi kao i elektronski izvori. Uz osnovni tekst disertacija sadrži i 25 slika, 21 tabelu i 6 grafikona.

Doktorska disertacija kandidata Dušana Markovića je bila podvrgnuta proveri softverom za ustanovljavanje preklapanja/plagijarizma (iThenticate Plagiarism Detection Software). *Ukupan procentualni iznos zapaženih preklapanja iznosi 7% disertacije.*

2. Predmet i cilj istraživanja

U ovoj disertaciji analizirali smo i radili komparaciju metoda za preciznije i tačnije detektovanje manipulisanih video materijala uz pomoć Deepfake tehnike. Istraživanje je započeto analizom prethodnih modela predviđenih za detekciju manipulacije video materijala kroz Deepfake tehniku. Analizirani su prethodno obučeni moduli i njihovi parametri. Analizirani prethodno obučeni modeli su XceptionNet, EfficientNetB i EfficientNetV. Parametri ovih modela koji su menjani u procesu preobučavanja su konfiguracija mreže SingleDLCNN, broj fold-ova kao i vrednost za Hold-out tehniku. Korišćen je DataSet sa preko 6000 datoteka od kojih je većina datoteka korišćena za treniranje neuronske mreže a ostale datoteke su korišćene za testiranje i validaciju. Za izdvajanje najboljih rezultata korišćen je CV (Cross-Validation), a tačnost istih je uvećana tehnikom težinskog usrednjavanja tj. optimizacijom težine.

Naučni cilj istraživanja se može opisati kao potreba i želja za definisanjem novog pouzdanijeg metoda detektovanja manipulacijom u savremenom video materijalu današnjice.

Praktični cilj ovog istraživanja je razvoj sopstvenog modela detekcije deepfake video materijala, verifikovan sa aspekta teorijsko informacione analize, opisanim procesom razvoja, upotrebe, analize performansi i poređenja sa ostalim srodnim rešenjima.

Društveni cilj ovog istraživanja je pomoć organizacijama različitih delatnosti (vlade zemalja, vojska, bezbednosne službe, veliki privredni subjekti) koje imaju neizostavnu potrebu za zaštitom važnih informacija. Takođe jedan od društvenih ciljeva jeste i smanjivanje zastupljenosti zlonamernih video materijala na globalnoj mreži koji može da diskriminiše svakog pojedinca.

3. Hipotetički okvir istraživanja

Opšta hipoteza od koje bi se krenulo u istraživanje u disertaciji je: *„Manipulacija video materijalima predstavlja realni problem. Pouzdana detekcija i forenzika video materijala je moguća primenom algoritama prostorno vremenskih karakteristika"*

Posebna hipoteza koja proizilazi iz opšte je: *„Modeli i algoritmi spatiotemporal su dovoljno sofisticirani kako bi sa velikom pouzdanošću detektovali manipulaciju u video materijalu"*

Pojedinačne hipoteze koje su korišćene u disertaciji su:

1. Metode dubokog učenja su značajne za automatizaciju i pouzdanost modela detekcije manipulacije u video materijalima
2. Neuronske mreže pomažu povećavaju pouzdanost detekcije
3. Ekspanzija deepfake tehnike predstavlja problem koji je potrebno pravilno adresirati
4. 3D konvulucione mreže omogućavaju bolje i preciznije profilisanje i detekciju

4. Metodologija istraživanja

Istraživanje je sprovedeno upotrebom dostupnih saznanja i informacija iz navedene oblasti, koristile su se informacije prikupljene putem Interneta, dostupne literature, časopisa i radova. Prikupljeni sadržaj je analiziran i ustanovljeno je postojeće stanje. Nakon toga teži se novim metodama i eksperimentima koji dokazuju da se može doći do boljih rezultata u otkrivanju manipulisanih video snimaka Deepfake tehnikama.

Od naučnih metoda koristila se analitičko-deduktivna metoda, od opšte-naučnih hipotetičko-deduktivna, uporedna i komparativna metoda, a od metoda i tehnika koristila se eksperimentalna metoda ispitivanja.

Prikupljanje i analiza podataka izvršena je:

- postavljanjem kriterijuma za poređenje i klasifikaciju,
- analizom prikupljenih podataka
- upoređivanjem prikupljenih podataka,
- utvrđivanjem relevantnih činjenica i veza među podacima,
- preispitivanjem hipoteza,
- testiranjem i proverom zaključaka do kojih smo došli
- postavljanjem budućih ciljeva.

5. Kratak prikaz sadržaja doktorske disertacije

Proces naučnog istraživanja je podeljen u nekoliko koraka

- Uvod
- Pregled u oblasti istraživanja
- Neuronske mreže
- Duboko učenje
- Novi metod konfiguracije učenja prethodno obučenih modela

- Zaključak sa sumarnim rezultatima i predlog daljeg rada

U nastavku disertacije, drugom poglavlju urađen je pregled u oblasti istraživanja. Opisana je sama Deepfake tehnika, način funkcionisanja iste kao i njena upotreba. Pored opštih metoda objašnjene su i metode koje su zasnovane na vremenskoj doslednosti, vizuelnim artefaktima, otiscima prstiju kamere i biološkim signalima

U trećem poglavlju disertacije opisane su neuronske mreže. Preciznije su definisane jednoslojne neuronske mreže kao i višeslojne neuronske mreže. Takođe opisuju se i vrste veza između neurona i smerovi kretanja informacija, kako povratni tako i nepovratni smer.

U četvrtom poglavlju disertacije objašnjeno je duboko učenje i postojeće metode na vremenskim odlikama. Objašnjene su tri postojeće metode ovih karakteristika.

U petom poglavlju disertacije opisan je novi metod konfiguracije učenja prethodno obučenih modela. Opisana su tri prethodno obučena modela koja su korišćena u eksperimentu. Detaljno je opisan postupak konfiguracije DataSeta koji je korišćen kao i konfiguracija neuronske mreže sa konvolucijom. Takođe opisani su i modeli koji su korišćeni. Nakon toga predstavljeno je istraživanje i rezultati istog. U istom poglavlju predočeno je i poređenje sa drugim radovima.

Šesto poglavlje predstavlja zaključak. Prikazan je rezultat i doprinos disertacije. U istom poglavlju predstavljen je i predlog daljeg rada.

6. Postignuti rezultati i naučni doprinos doktorske disertacije

Istraživanje je započeto analizom prethodnih modela predviđenih za detekciju manipulacije video materijala kroz Deepfake tehniku. Analizirani su prethodno obučeni modli i njihovi parametri. Analizirani prethodno obučeni modeli su *XceptionNet, EfficientNetB* i *EfficientNetV.* Parametri ovih modela koji su menjani u procesu preobučavanja su konfiguracija mreže *SingleDLCNN*, broj *fold-ova* kao i vrednost za *Hold-out* tehniku. Korišćen je DataSet sa preko 6000 datoteka od kojih je veći broj datoteka korišćen za treniranje neuronske mreže a ostale datoteke su korišćene za testiranje i validaciju. Za izdvajanje najboljih rezultata korišćen je *CV (Cross-Validation)* a tačnost istih je uvećana tehnikom težinskog usrednjavanja tj. optimizacijom težine. Prikazani su rezultati za sva tri prethodno obučena modela a najbolji rezultat je ostvaren uz pomoć *EfficientNetbB4.*

Iz prethodno opisanog istraživanja i eksperimenta može se zaključiti da je najbolji ostvareni rezultat 96.8% *(FAR = 5.97%)*koji je dobijen uz pomoću *EffecientNetB4* preobučenog modela. Takođe predstavljeni su i rezultati druga dva posmatrana preobučena modela. Model *XceptionNet* ostvario je rezultat od 96.45% dok je model model *EfficientNetV2* ostvario isti taj rezultat odnosno 96.45%. Iako je tačnost ova dva modela na prvi pogled ista vrednost FAR *(fake images classified as real image)* se razlikuje. U prvom slučaju za *Xception net je iznosila* 5.97%

a u drugom slučaju za *EfficientNetV2* iznosila je 6.72%. U poređenju sa ostalim rezultatima smatramo da je ovaj rezultat dobar i da se dodatnim unapređenjem može dodatno poboljšati. Ideja za dodatno unapređivanje je opisana u sledećem poglavlju.

Predloženo rešenje se može primeniti u mnogim oblastima. Razvijanje Deepfake tehnologije pokazalo je da se može koristiti u dobre, ali da može koristiti i u zlonamerne svrhe. Ovakvim rešenjem možemo sa velikom tačnosti i preciznosti odrediti koji video materijali su modifikovani tj. sa kojim video materijalima je vršena manipulacija i na takav način možemo smanjiti učinak zloupotrebe. Npr. ukoliko je neko kreirao zlonamerni manipulisani video uz pomoć Deepfake-a u nameri da diskredituje određenu osobu, na ovaj način možemo dokazati manipulaciju i demantovati diskreditaciju.

7. Mišljenje i predlog Komisije o doktorskoj disertaciji

Na osnovu svega izloženog Komisija je mišljenja da doktorska disertacija kandidata Dušana Markovića po svojoj temi, pristupu, strukturi i sadržaju rada, kvalitetu i načinu izlaganja, metodologiji istraživanja, načinu korišćenja literature, relevantnosti i kvalitetu sprovedenog istraživanja i donetim zaključcima zadovoljava kriterijume zahtevane za doktorsku disertaciju, te se može prihvatiti kao podobna za javnu odbranu.

Sagledavajući ukupnu ocenu doktorske disertacije kandidata Dušana Markovića pod nazivom „Detektovanje manipulacije u video snimcima stvorenih Deepfake tehnikom sistemom učenja prostorno vremenskih karakteristika“predlažemo Veću departmana za poslediplomske studije i Senatu Univerziteta Singidunum da prihvati napred navedenu doktorsku disertaciju i odobri njenu javnu odbranu.

Beograd, 28/06/2022.

Članovi komisije:

prof. dr Marko Šarac

prof. dr Nebojša Bačanin Džakula

prof. dr Petar Spalević