UNIVERZITET SINGIDUNUM
Departman za poslediplomske studije
Danijelova 32, Beograd

VEĆU DEPARTMANA ZA POSLEDIPLOMSKE STUDIJE

Odlukom Veća Departmana za poslediplomske studije broj: 4 – 118/2021 od 25.05.2021. godine, određeni smo za članove Komisije za ocenu i odbranu doktorske disertacije pod nazivom: **„Jedna klasa biometrijskog kriptosistema zasnovanog na konvolucionim neuronskim mrežama"**, kandidata Srđana Barzuta, o čemu podnosimo sledeći

IZVEŠTAJ

1 Osnovni podaci o kandidatu i doktorskoj disertaciji

Kandidat Srđan Barzut rođen je 31.12.1980. god. u Beogradu, gde je završio osnovnu i srednju školu. Višu elektrotehničku školu u Beogradu, završio je 2004. godine i stekao zvanje inženjera elektrotehnike. Osnovne akademske studije završio je 2011. godine na Fakultetu za informatiku i računarstvo, Univerziteta Singidunum, na studijskom programu: „Programiranje i projektovanje" sa prosečnom ocenom 8,94. Master akademske studije završio je 2012. godine na Departmanu za poslediplomske studije i međunarodnu saradnju, Univerziteta Singidunum, na studijskom programu: „Savremene informacione tehnologije" sa prosečnom ocenom 10.

Od 2009. godine kandidat je zaposlen u Akademiji tehničkih strukovnih studija Beograd (nekadašnja Visoka inženjerska škola strukovnih studija Tehnikum Taurunum), prvobitno u zvanju stručnog saradnika za računarstvo i informatiku, zatim u zvanju nastavnika veština za oblast računarstvo i informatika, gde je zadužen za izvođenje teorijske i praktične nastave. Ostvaruje zavidne rezultate u svim sprovedenim studentskim anketama. Rukovodilac je Centra za računarstvo i informatiku na svom odseku Akademije.

Njegova trenutna naučno-istraživačka interesovanja prvenstveno su orijentisana na primenjenu kriptografiju, biometriju i zaštitu informacionih sistema, dok iskazuje želju da usmeri istraživanja na primenu navedenih interesovanja na zaštitu baza podataka, podataka na internetu i elektronskog poslovanja.

Kandidat ima sledeći objavljen rad kategorije M21a čime je ispunjen preduslov za odbranu doktorske disertacije.

[1] **Barzut S.**, Milosavljević M., Adamović S., Saračević M., Maček N., Gnjatović M., *"A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks"*, Mathematics, 2021. [IF: 1,747]

Objavljeni naučni radovi u časopisima kategorije M33:

[1] **Barzut S.**, Milosavljević M., *„A method of forming an XOR biometrics from fingerprints by using Gabor filtration"*, Int. Sci. Conf. of Business-Related Research „Synthesis", Belgrade, 2014.

Objavljeni naučni radovi u časopisima kategorije M63:

[1] **Barzut S.**, Milosavljević M., *„A Survey on Modern Systems for Biometrics based Authentication"*, Sci. Conf. „Network", 2013.

Doktorska disertacija kandidata Srđana Barzuta urađena je na 111 strana, od čega 7 strana čini spisak literature. Spisak literature obuhvata 98 referenci koje čine naučni radovi, knjige, zbornici radova i elektronski izvori. Uz osnovni tekst disertacija sadrži 54 slike i 17 tabela.

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

2 Predmet i cilj istraživanja

Predmet ovog naučno-istraživačkog rada su biometrijski kriptosistemi u funkciji zaštite biometrijskih karakteristika korisnika i njihovog povezivanja sa kriptološkim ključevima, radi uspostavljanja sistema upravljanja kriptografskim ključevima biometrijski zavisnim oslobađanjem. Analizirana je mnogobrojna naučna građa iz ove oblasti i izdvojena su najznačajnija dosadašnja dostignuća, koja su upotrebljena kao polazna osnova za definisanje usmerenih ciljeva i uspostavljanje hipoteza, u skladu sa kojima je napravljen plan daljeg istraživanja, koje je sprovedeno i sumirano u ovom radu. Pojedinačne hipoteze koje su razmatrane glase:

1. Informacije o teksturi otisaka prstiju mogu se upotrebiti za formiranje biometrijskog kriptosistema;
2. Za izdvajanje biometrijskih obeležja moguće je upotrebiti duboke konvolucione neuronske mreže;
3. Izdvojena biometrijska obeležja otisaka prstiju moguće je konvertovati u binarni domen radi formiranja XOR biometrije;
4. Biometrijski kriptosistem može se upotrebiti za zaštitu biometrijskih šablona i kriptoloških ključeva.

Glavni cilj ovog istraživanja je da se ostvari visok nivo zaštite biometrijskih podataka otisaka prstiju i pridruženih asociranih kriptoloških ključeva u biometrijskim kriptosistemima. Od presudne važnosti je bilo ostvariti transformaciju obeležja otisaka prstiju u vektorski opis

fiksne dužine, koji se diskretizacijom može prevesti u binarni domen. Na taj način omogućena je ravnopravna primena globalnih i lokanih informacija o teksturi otiska prsta, u odnosu na minucije koje su do sada primarno korišćene u sistemima za prepoznavanje otisaka prstiju. Ostvarenje cilja ogleda se u predlogu praktičnog rešenja za povećanje sigurnosti biometrijskih podataka i mogućnost njihove primene u vrhunskim autentifikacionim sistemima, kao i u kriptografskim sistemima prilikom čuvanja i upravljanja kriptološkim ključevima.

3 Hipotetički okvir istraživanja

Opšta hipoteza od koje se krenulo u istraživanje u disertaciji je: *„Biometrijske karakteristike ljudi mogu se primeniti u kriptografiji"*.

Posebna hipoteza koja proizilazi iz opšte je: *„Reprezentaciju fizičkih osobina i karakteristika ponašanja čoveka možemo prilagoditi uspostavljenim kriterijumima i potrebama kriptografije, kako bismo ih iskoristili za upravljanje kriptološkim ključevima"*.

4 Metodologija istraživanja

Metodologija istraživanja u ovom radu obuhvata složen i organizovan postupak zasnovan na logičkim načelima i strogim matematičkim principima tipičnim za analizu i sintezu kriptografskih mehanizama dokazive bezbednosti. Složenost predmeta istraživanja zahteva primenu:

- analitičkih osnovnih metoda – metod analize, metod apstrakcije, metod specijalizacije i metod dedukcije;
- sintetičkih osnovnih metoda – sintezu, konkretizaciju, generalizaciju i indukciju;
- opšte naučnih metoda – hipotetičko-deduktivnu, analitičko-deduktivnu, komparativnu, matematičku i statističku metodu modelovanja.

Ovaj izbor istraživačkih metoda je upotrebljen da se istraživanje i tok istraživačkog procesa u svim fazama, odnosno identifikaciji i definisanju problema, planiranju dizajna istraživanja, kritičkoj analizi sistema, kao i formulaciji zaključaka korektno sprovede u skladu sa osnovnim principima naučno istraživačkog rada. Primenom ovih metoda, kako pokazuju prezentovani rezultati istraživanja, moguće je validno ostvarenje naučnog i društvenog cilja istraživanja.

5 Kratak sadržaj doktorske disertacije

Rad se sastoji iz 5 poglavlja, sadržajno strukturiranih na sledeći način:

U okviru prvog poglavlja ukratko je izložen problem koji je predmet istraživanja ove disertacije, kroz opšte podatke i istorijski pregled ove oblasti. Metodološki pristup, kao i struktura rada prezentovani su u okviru ovog poglavlja.

U drugom poglavlju dat je pregled i podela biometrijskih sistema za autentifikaciju, prikazan je konceptualni model ovakvih sistema i parametri kojima se performanse mere, kvantifikuju i izražavaju. Detaljno su istražene i analizirane biometrijske tehnike za autentifikaciju na osnovu: otiska prsta, dužice oka i crta lica. Predstavljeni su rezultati analize upotrebe više biometrijskih izvora podataka istovremeno za formiranje multibiometrijskih sistema.

Treće poglavlje posvećeno je sigurnosti sistema i biometrijskih podataka koji se koriste u njemu. Analizirana je sigurnost biometrijskog sistema, dat prikaz istraživanja o poznatim napadima na ove sistema, posledicama koje proističu iz njih, kao i odgovarajućim protivmerama. Poseban deo ovog poglavlja posvećen je zaštiti biometrijskih podataka i pitanjima privatnosti korisnika, odnosno načinima zaštite biometrijskih šablona, s posebnim akcentom na biometrijske kriptosisteme.

Četvrto poglavlje se nadovezuje se na treće i u njemu je predložena nova klasa biometrijskog kriptosistema zasnovanog na inovativnom rešenju da se primene duboke konvolucione neuronske mreže za izdvajanje obeležja. Kako bi se formirao biometrijski kriptosistem zasnovan na fazi povezivanju, predloženo je efikasno rešenje za diskretizaciju, kojom je izvršena transformacija izdvojenih obeležja u binarni domen. Rezultujuća binarna reprezentacija fiksne dužine, testirana je u scenariju autentifikacije sa pridruženim mehanizmom izdvajanja asociranih kriptoloških ključeva, zasnovanim na principima kodova za ispravljanje grešaka. U ovom poglavlju su analizirani eksperimentalni rezultati predložene klase biometrijskog kriptosistema, čija evaluacija je potvrdila efektivnost predloženog pristupa.

U petom poglavlju je iznet kritički osvrt i rezime istraživanja, pregled glavnih doprinosa disertacije, kao i predlog budućih pravaca istraživanja u ovoj oblasti.

6 Postignuti rezultati i naučni doprinos disertacije

Glavni naučni doprinos predstavlja nov pristup automatskom izdvajanju obeležja iz teksture otiska prsta, u potpunosti zasnovanom na dubokim konvolucionim neuronskim mrežama. Pored toga, ističu se sledeći doprinosi prikazani u radu:

- Unapređeni su postojeći pionirski sistemi za autentifikaciju bazirani na teksturi otisaka prstiju, primenom novih metoda za određivanje referentne tačke i tehnike određivanja pouzdanosti bita.
- Predložena je kvantizacija izdvojenih obeležja kodovanjem sa dva bita, čime su biometrijski šabloni prevedeni u binarni domen.
- Generisanjem binarnih šablona otisaka prstiju fiksne dužine, postavljeni su okviri za formiranje biometrijskog kriptosistema fazi povezivanjem izdvojenih obeležja i kriptografskog ključa.

- Problem varijabilnosti biometrijskih podataka rešen je primenom BCH kodova za ispravljanje grešaka, koji rade na nivou bloka što ih čini otpornim na poznate statističke napade.

- Predložena je primena tehnika za poboljšanje slike i segmentaciju regiona od interesa u odnosu na referentnu tačku, pre izdvajanja obeležja u CNN modulu, čime je značajno povećana međuklasna diskriminativnost i smanjena je greška lažnog prihvatanja.

- Problem kratkih obučavajućih skupova, inherentan biometriji, rešen je generisanjem dodatnih instanci svake klase rotacijom izvornog otiska prsta, čime je povećana tačnost i robusnost sistema na rotacije otisaka uradnom režimu sistema.

- Predloženi biometrijski kriptosistem može upravljati ključevima dužine 265 bita, uz prihvatljivu marginu EER (Equal Error Rate) greške od 1%, što je značajno bolje u poređenju sa drugim sistemima baziranim na teksturi otisaka prstiju i zadovoljava potrebe savremenih kriptografskih sistema.

7 Mišljenje i predlog Komisije o doktorskoj disertaciji

Na osnovu svega izloženog, Komisija je mišljenja da doktorska disertacija kandidata Srđana Barzuta po svojoj strukturi i sadržaju rada, kvalitetu i načinu izlaganja, metodologiji istraživanja i izvedenim zaključcima, zadovoljava kriterijume zahtevane za doktorsku disertaciju.

Sagledavajući ukupnu ocenu doktorske disertacije kandidata Srđana Barzuta pod nazivom **„Jedna klasa biometrijskog kriptosistema zasnovanog na konvolucionim neuronskim mrežama“**, predlažemo Veću departmana za poslediplomske studije i Senatu Univerziteta Singidunum da prihvati napred navedenu doktorsku disertaciju i odobri njenu javnu odbranu.

Beograd, 18.11.2021.

Članovi komisije:

prof. dr Milan Milosavljević, mentor

prof. dr Saša Adamović, predsednik

dr Branko Kovačević, prof. emeritus, Elektrotehnički fakultet Univerziteta u Beogradu