Oponent: doc. Ing. Michal Kvet, PhD.
Pracovisko: Žilinská univerzita v Žiline, Fakulta riadenia a informatiky,
Katedra informatiky
Tel.: +421 41 513 4024, +421 908 279 706
Email: michal.kvet@uniza.sk

OPONENTSKÝ POSUDOK NA HABILITAČNÚ PRÁCU

Uchádzač: Ing. Radoslav Forgáč, PhD.
Pracovisko: Akadémia ozbrojených síl gen. M. R. Štefánika, Katedra informatiky
Názov habilitačnej práce: Selected Methods of Artificial Intelligence and Steganography for Image Authentication
Odbor HK a IK: Vojenské spojovacie a informačné systémy

HODNOTENIE

A) Aktuálnosť témy habilitačnej práce

Pán Ing. Radoslav Forgáč, PhD. vypracoval a predložil habilitačnú prácu na vysoko-aktuálnu tému steganografie a s ňou spojené problémy a techniky. Práca je písaná v anglickom jazyku, skladá sa zo 6 publikácií, ktoré komplexne pokrývajú oblasť výskumu autenticity obrazov pomocou steganografie a optimalizovaného modelu pulzne viazanej neurónovej siete. V prvej publikácii sa autor zameriava na definíciu neurónovej siete s cieľom generovania pozičnej matice. Druhá publikácia nadväzuje na predchádzajúce koncepty a zameriava sa na možnosti zabezpečenia vkladaných dát pomocou konvolučných neurónových sietí. Cieľom je zaručiť utajenosť obsahu tak, aby neexistoval mechanizmus na detekciu prítomnosti vloženej správy v krycom obraze. Tretia publikácia sa zaoberá parametrami modelu neurónovej siete pre obrazovú steganografiu a ich správne nastavenými hodnotami. Štvrtá publikácia poukazuje na entropiu. V piatej publikácii sa autor orientuje na návrh metodiky vkladania a extrahovania dát, ako i samotného overovania autencity obrazov. Šiesta publikácia prezentuje prehľad súčasného stavu skúmanej oblasti. Definuje univerzálny model autentifikácie obrazov akejkoľvek veľkosti. Jednotlivé publikačné výstupy vždy definujú východiská, analýzu a prinášajú vlastné metódy. Publikácie vhodne na seba nadväzujú a tvoria tak kompaktný celok.
V uvedených publikáciách ide o prvého autora, vo väčšine prípadov s autorským podielom 50%, v jednom prípade 40%. V poslednej publikácii v kategórii Current Contents Connect (CCC) je autorský podiel 80%. Publikácie sú indexované v databázach Scopus a WoS.
Celkovo má autor evidovaných 25 publikácií v databáze Scopus a 15 v databáze WoS. Na jednotlivé publikačné výstupy má autor aj citácie, aktuálny h-index v databáze Scopus je 4 (ku dňu 7.2.2024). Väčšinu príspevkov autor publikoval na slovenských konferenciách.
Je zrejmý autorov publikačný progres, v roku 2023 má 4 publikácie v databáze Scopus.
Aktuálnosť témy je podotknutá aj referenciami v jednotlivých publikačných výstupoch. Navyše, jednotlivé publikácie sú citované zahraničnými autormi, napr. 2. článok má 5 zahraničných citácií.

B) Splnenie cieľa habilitačnej práce

Cieľ práce je jednoznačne splnený, hlavným vedeckým prínosom predloženej habilitačnej práce je validovaný model na autentifikáciu obrazov založený na obrazovej steganografii, neurónovej sieti OM-PCNN, kryptografickej hašovacej funkcii SHA-256 a šifrovaní AES-256. Publikačné výsledky prešli riadnym recenzným konaním a práca prináša komplexný pohľad s dôrazom na vlastnosti, obmedzenia a bezpečnosť. Výsledky výskumu sú navyše priamo aplikované do výučby (Umelá inteligencia vo vojenských aplikáciách). Autor úspešne viedol diplomové práce, ktoré prinášali čiastkové výsledky.

C) Metódy spracovania habilitačnej práce

Predložená habilitačná práca je spracovaná kvalitne, použité metódy považujem za adekvátne. Práca spĺňa všetky štandardy kladené na tento typ prác a kritériá na habilitačné práce v danom odbore.

D) Úroveň dosiahnutých výsledkov habilitačnej práce a nové poznatky

Dosiahnuté výsledky vykazujú nadpriemernú úroveň a sú deklarované v jednotlivých článkoch. Konkrétne v 1. článku autor predkladá riešenie založené na generovaní rovnakej pozičnej matice pri vkladaní, ako aj pri extrakcii autentifikačných dát. V druhom článku autor diskutuje techniky zabezpečenia citlivých dát šifrovaním. Riešenie je založené na konvolučnej neurónovej sieti. Zameriava sa na osvedčené a rozšírené algoritmy AES-256 a SHA-256. V ďalšom článku sa venuje parametrom na generovanie kanditátov pozičných matíc tak, aby po vložení správy do krycieho obrazu bola vygenerovaná rovnaká pozičná matica i v procese extrakcie dát, tzv. správ. Štvrtá publikácia prináša posúdenie vplyvu pozičnej matice na entropiu.
Výrazný prínos je definovaný v 5. článku, kde sa autor zameriava na kľúčové parametre a algoritmus ich adaptácie. Tieto parametre sú významné práve pri generovaní pozičných matíc. Súčasťou je aj postup implementácie procesu vkladania a extrakcie. Zhrnutie celého výskumu a jeho evalvácia je prezentovaná v poslednom článku, kategorizovanom ako CCC – Current Contents Connect. Súčasťou je aj komplexná analýza skúmanej oblasti – overovania autenticity obrazov. Vyvinuté riešenie je univerzálne, aplikovateľné na akúkoľvek veľkosť obrazov.
Autor je úspešným spoluriešiteľom viacerých národných projektov. V jednom z nich je aj zodpovedným riešiteľom.

E) Prínos pre ďalší rozvoj vedy a techniky

Hlavným vedeckým prínosom predloženej habilitačnej práce je validovaný model na autentifikáciu obrazov založený na obrazovej steganografii, neurónovej sieti OM-PCNN, kryptografickej hašovacej funkcii SHA-256 a šifrovaní AES-256. Tieto výsledky sú nielen publikované, ale aj pretavované do procesu výučby. V závere autor naznačil aj smer ďalšieho výskumu, a to steganografia bez použitia krycích obrazov.

F) Pripomienky a poznámky k habilitačnej práci

Predložená práca je napísaná v anglickom jazyku ako ucelený súbor autorových článkov. Publikácie sú vysoko hodnotené, indexované v databázach Scopus a WoS. Boli publikované na konferenciách organizovaných AOS, resp. v časopise Computing and informatics (SVK). Napriek tomu, že tieto konferencie hodnotím vysoko kladne, sám som viacročným autorom na týchto konferenciách, myslím si, že dosiahnuté výsledky sú aplikovateľné v širšom meradle. Preto by som ocenil publikovanie aj na zahraničných fórach a časopisoch. Túto možnosť by som určite v budúcnosti zvážil.

V článku 4 – Entropy Based Image Quality Assessment of Stego Images Created by Pulse Coupled Neural Network – na str. 53 píšete: „An Optimized Model of PCNN (OM-PCNN) with a reduced number of parameters and a simpler structure of neurons was proposed [15], [16], which achieved better results for feature generation than the basic PCNN model [7]“. Bolo by dobré lepšie kvantifikovať a porovnať výsledky, výraz „better results“ je príliš všeobecný.

Publikované články obsahujú pomerne veľké percento samocitácii. Aktuálny stav a trendy by bolo vhodné pokryť viacerými existujúcimi vedeckými publikačnými výstupmi.

Z formálneho hľadiska, keďže je práca písaná v anglickom jazyku, odporúčal by som aj označenie citácií a kategórie indexu v anglickom jazyku.

Habilitačná práca obsahuje minimálne množstvo preklepov (impementácie (str. 3), crypo key (str. 22)), je písaná zrozumiteľne s vysokou kvalitou angličtiny. Obr. 4 na str. 56 (príspevok č. 4) obsahuje preklep „treshold“. Tento obrázok je použitý aj v príspevku č. 5 - obr. 2 na str. 69. Preklep však odstránený nebol.

Vyššie uvedené pripomienky sú viac menej formálneho charakteru, celková kvalita práce nie je nimi ovplyvnená.

G) Otázky uchádzačovi k riešenej problematike

Do diskusie dávam habilitantovi nasledujúce otázky:

- V závere práce spomínate nové výzvy, ktorým sa chcete venovať v budúcnosti, a to konkrétne steganografiu bez použitia krycích obrazov. Mohli by ste v krátkosti definovať očakávané prínosy a charakteristiky?
- V práci používate kryptografickú hašovaciu funkciu SHA-256 a šifrovanie AES-256. Aký vplyv na riešenie by malo použitie algoritmov s dlhšími šifrovacími kľúčmi a odtlačkami?
- V príspevku 2 – Contribution to Image Steganography Using Pulse Coupled Neural Networks uvádzate rovnakú hodnotu CPU load pre rôzne veľkosti súborov (tab. 1, str. 29). Môžete sa k tomu bližšie vyjadriť? Čím je spôsobená táto nezávislosť, resp. ako je definovaná metodika merania danej hodnoty? Podobne aj v tab. 4 na strane 30 definujete spotrebu pamäte. Podľa textu ide o maximálnu hodnotu. Nebolo by potrebné zohľadniť aj časovú referenciu, teda dĺžku využitia danej kapacity pamäte?
- V príspevku 3 – Impact of Pulse Coupled Neural Network Parameters on Image Steganography – ste nastavili počet iterácií na 15 (viď str. 44). Podobne pre 2. experiment bol stanovený počet iterácií na 5. Aký vplyv má počet iterácií na dosiahnuté výsledky? Prečo bola stanovená práve táto hodnota? Išlo o výsledok experimentov alebo bola stanovená expertne?

CELKOVÉ ZHODNOTENIE HABILITAČNEJ PRÁCE A ZÁVER

Habilitačná práca zodpovedá požiadavkám kladeným na habilitačné práce a spĺňa podmienky kladené na úroveň habilitačnej práce.

Na základe uvedeného hodnotenia

odporúčam

habilitačnú prácu k obhajobe a aby bol po úspešnej obhajobe uchádzačovi **Ing. Radoslavovi Forgáčovi, PhD.** udelený vedecko-akademický titul „docent“ v odbore Vojenské spojovacie a informačné systémy.

V Žiline, dňa: 7.2.2024

.....

doc. Ing. Michal Kvet, PhD.