dr hab. inż. Artur Janicki, prof. uczelni
Instytut Telekomunikacji
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska
e-mail: Artur.Janicki@pw.edu.pl
tel.: +48 22 2347722

Warszawa, 30 sierpnia 2023 r.

RECENZJA ROZPRAWY DOKTORSKIEJ mgr. inż. MARCINA PLATY pt. „*Zastosowanie zaawansowanych metod sztucznej inteligencji do wybranych problemów bezpieczeństwa informacji*", przedłożonej Radzie Naukowej Instytutu Podstaw Informatyki Polskiej Akademii Nauk

Przedmiot rozprawy, główne tezy pracy

Praca Pana **mgr. inż. Marcina Platy** pt. „*Zastosowanie zaawansowanych metod sztucznej inteligencji do wybranych problemów bezpieczeństwa informacji*" dotyczy kilku wybranych zagadnień cyberbezpieczeństwa, których dla których motywem łączącym jest zastosowanie różnych zaawansowanych metod sztucznej inteligencji. Jedna część rozprawy dotyczy znakowania wodnego w plikach JPEG, druga – różnego rodzaju biometrii: głosowej, wykorzystującej mimikę twarzy i kontur dłoni.

Przedstawiona rozprawa jest pracą badawczą. W swojej rozprawie Autor nie formułuje konkretnych tez, natomiast opracowuje wybrane zagadnienia z obszaru bezpieczeństwa informatycznego.

Rozprawa została napisana w języku polskim, zawiera 182 strony i 7 rozdziałów.

Rozdział 1. wprowadza w tematykę rozprawy i przedstawia motywację prowadzonych badań.

W rozdziale 2. Doktorant prezentuje swoją metodę znakowania wodnego w obrazach opartą na splotowych sieciach neuronowych z wykorzystaniem zaproponowanych przez siebie składników: propagatora i translatora.

W rozdziale 3. Autor rozbudowuje metodę zaprezentowaną w poprzednim rozdziale o schemat dyskryminator-detektor (DD). Przeprowadza różne testy swojej metody, m.in. badając jej odporność na metody kompresji wideo (MJPEG i MPEG).

Rozdział 4. dotyczy metody biometrycznej opartej na mimice twarzy. Doktorant proponuje swoją metodę, która zapewnia wysoką

Politechnika Warszawska
ul. Nowowiejska 15/19
00-665 Warszawa
www.elka.pw.edu.pl

prywatność użytkowników, a także umożliwia usuwanie wzorców biometrycznych.

W rozdziale 5. Doktorant opisuje metodę zapobiegania atakowi poprzez podszywanie się (spoofing) w biometrii głosowej. Prezentuje wyniki eksperymentów przeprowadzonych w ramach konkursu ASVSpoof 2019.

Rozdział 6. prezentuje z kolei własną metodę biometryczną opartą na konturze dłoni. Doktorant omawia jej założenia, a następnie wyniki eksperymentów na własnej bazie oraz bazie *Bosphorus Hand Dataset*, które potwierdzają jej skuteczność.

W rozdziale 7. Autor przedstawia skrótowo podsumowanie swojej pracy.

Mocne strony rozprawy

Wielką zaletą rozprawy jest zaproponowanie kilku ciekawych, wartościowych metod podnoszących bezpieczeństwo informacyjne w różnych jego obszarach. Jeśli chodzi o znakowanie wodne w obrazach, Doktorant zaproponował metodę opartą na splotowych sieciach neuronowych, uczoną w konfiguracji koder-noiser-dekoder. Autor rozszerzył tę konfigurację o zaproponowane przez siebie składniki: propagator oraz translator, które rozkładają ukrytą wiadomość w obrazie, utrudniając tym samym ataki. Zaproponował też ciekawą metodę weryfikacji biometrycznej na podstawie mimiki twarzy, polegającą na kombinacji kilku metod uczenia maszynowego, w tym uczenia głębokiego, oraz algorytmów klasycznych, takich jak DTW. Opracował również szybką metodę autoryzacji na podstawie konturu dłoni, która wykorzystuje kombinację kilku klasycznych algorytmów widzenia komputerowego oraz geometrii obliczeniowej.

Bardzo ciekawym i wartościowym pomysłem jest wspomniane już opracowanie metody biometrycznej opartej na mimice twarzy. Umożliwia ona przechowywanie wzorców biometrycznych bez obawy o możliwość odtworzenia wizerunku samej twarzy, co zdecydowanie działa na korzyść prywatności użytkowników. W dodatku tę metodę można potraktować jako tzw. biometrię usuwalną. Nie ma takich rozwiązań wiele dla twarzy (choć uważam, że jest ich więcej niż dwa, jak pisze Doktorant na str. 83).

Na uznanie zasługuje metodologia badań, którą stosował Doktorant. Autor nie wprowadzał zbyt upraszczających założeń, typu jednorodne oświetlenie twarzy czy nagrania w warunkach laboratoryjnych. W swoich badaniach Doktorant zazwyczaj stosował środowisko nielaboratoryjne, niekontrolowaną odległość od mikrofonu lub kamery, zezwalał na pozostawienie biżuterii na palcach itd. Dzięki temu osiągnięte wyniki można uznać za dużo bardziej miarodajne, niż gdyby to było w przypadku wyidealizowanych warunków. Także opracowanie zbiorów danych zawierających dane o mimice twarzy czy kontury dłoni, pochodzące od dziesiątków użytkowników, uważam za znaczne osiągnięcie.

Potwierdzeniem znaczenia osiągnięć Doktoranta są publikacje, których jest on współautorem. Autor opublikował 3 artykuły prezentowane na liczących się konferencjach międzynarodowych oraz 1 artykuł w czasopiśmie (1 jest jeszcze w recenzjach). Potwierdza to wysoki poziom prezentowanych badań i ich wyników.

Uważam, że rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego. Osiągnięte wyniki mogą zostać praktycznie wykorzystane w podnoszeniu bezpieczeństwa systemów informatycznych wykorzystujących metody biometryczne, a także znakowanie wodne obrazów. Doktorant wykazał również sprawne posługiwanie się warsztatem badawczym oraz biegłą znajomość teoretyczną z dziedziny informatyka techniczna i telekomunikacja.

Słabe strony rozprawy

Do słabych stron rozprawy zaliczam niejasność co do wkładu Doktoranta w opracowanie problemu zapobiegania atakowi spoofingowemu w rozpoznawaniu mówcy. Autor opisuje rozwiązanie polegające na specyficznym modelowaniu sieci neuronowej, nazwane *Attack-Out Cross Validation*, które polega na odpowiednim rozłożeniu próbek uczących w zbiorze treningowym, walidacyjnym i testowym, co zwiększa zdolność sieci do generalizacji, oraz na wykorzystaniu lekkiej splotowej sieci neuronowej (LCNN) oraz Bayesowskiej sieci neuronowej. Tymczasem Doktorant ocenił swój wkład do publikacji „*Robust Bayesian and Light Neural Networks for Voice Spoofing Detection*" (prezentującej to rozwiązanie na konferencji Interspeech) na 20%. Napisał, że jego udział polegał głównie na „analizie cech technikami redukcji wymiarowości poprzez uczenie dedykowanych sieci neuronowych wykorzystując do tego dodatkowe dane o parametrach ataków". Wygląda więc na to, że wkład Doktoranta w zaprezentowane rozwiązanie, w odróżnieniu od pozostałych, nie był wiodący.

Pewną wadą tej rozprawy jest jej rozwlekłość (i obszerność), która się odbywa kosztem spójności. Moim zdaniem pewne fragmenty rozprawy są nadmiarowe i wiele nie wnoszą. Na przykład Autor poświęca prawie 11 stron jedynie na prezentację metod walidacji systemu antyspoofingowego (Rozdział 5.5). Jest to temat ważny i niełatwy, ale wg mnie wystarczyłoby przedstawić najważniejsze metryki i odesłać czytelnika do innych publikacji, gdzie są one szczegółowo omawiane. Zapewne rozprawa zyskałaby też na spójności, gdyby Doktorant zawęził trochę przedstawiany materiał. W obecnej wersji związek między np. znakowaniem wodnym plików JPEG a biometrią głosową jest dość odległy.

W części dotyczącej eksperymentów nt. identyfikacji twarzy opartej na mimice, Doktorant prowadził badania na bazie 191 nagrań pochodzących od 34 wolontariuszy. Osiągnięty współczynnik identyfikacji (IR) wyniósł 71%. Nie jest to wynik wysoki przy tak niewielkim zbiorze. Brakuje dyskusji na temat, jak bardzo skuteczność tej metody maleje wraz ze wzrostem zbioru i czy w ogóle jej skuteczność może być akceptowalna przy np. tysiącach użytkowników. Na przykład przy eksperymentach z biometrią dłoni, opisywanych przez Doktoranta, przy 60 użytkownikach współczynnik IR wyniósł 100%, a przy 738 osobach (baza *Bosphorus Hand Dataset*) wyniósł 99,80%, co prezentuje się dużo bardziej obiecująco.

W przypadku eksperymentów z weryfikacją opartą na konturze dłoni Doktorant wylicza wartości prawdopodobieństwa fałszywej akceptacji (FAR) oraz fałszywego odrzucenia (FRR). Szkoda, że Autor nie wyliczył błędu zrównoważonego (ang. *equal error rate*, ERR), który wskazałby, kiedy FAR i FRR się sobie zrównają. Ułatwiłoby to porównywanie działania weryfikacji np. dla różnej liczby próbek we wzorcu (Tabela 6.5).

Inne, drobniejsze uwagi:

- W pracy występują pewne niedociągnięcia formy – o czym więcej w następnym rozdziale;
- Str. 13: Doktorant pisze: „Głównym celem w steganografii jest ukrycie wiadomości, a następnie przekazanie jej odbiorcy w sposób uniemożliwiający adwersarzowi stwierdzenie, czy w danym nośniku zostały umieszczone dodatkowe informacje". Taka definicja steganografii jest nieprecyzyjna. Często głównym celem steganografii jest ukrycie już samego faktu istnienia ukrytej komunikacji.
- Str. 51: Obrazy z bazy COCO zmieniono do rozmiarów 256 x 256 pikseli. Doktorant nie podał, jaki był pierwotny rozmiar obrazów i w jaki sposób został zmieniony (np. czy proporcjonalnie).
- Str. 70: Jaką frazę wypowiadali uczestnicy testów? Czy była jakoś szczególnie dobrana?
- Str. 70: Czy wśród uczestników testów, którzy twarze były nagrywane, byli mężczyźni z brodą? Jestem ciekaw, jak wpływałoby to na dokładność rozpoznawania punktów charakterystycznych dolnej części twarzy, a w konsekwencji na poprawność działania systemu identyfikacji twarzy.
- Str. 76, Tabela 4.1: Co oznacza wartość -0.000 i czym się różni od 0.000?
- Str. 76, Tabela 4.1: Czym uzasadniony jest wybór punktów charakterystycznych twarzy: 8, 23 i 62?
- Str. 80: Brakuje szczegółów dotyczących użytego klasyfikatora SVM. Jaka funkcja jądra została użyta? Jak ustawione były hiperparametry?
- Str. 86, Tabela 4.2: Czym uzasadniony jest wybór punktów charakterystycznych twarzy: 30 i 53?
- Str. 119: „Skok czasowy na 512 jednostek, okno Hanna o rozmiarze 2048 jednostek". Rozumiem, że chodzi o okno o długości 2048 próbek? Czy Doktorant ma na myśli jakieś inne jednostki?
- Str. 120: „Próbkowanie źródła dźwięku równe 48000 Hz" – rozumiem, że chodzi o „Próbkowanie sygnału dźwiękowego z częstotliwością 48 kHz"?
- Str. 129: „cechy biometryczne konturu dłoni poszczególnych osób nie są rozpowszechnione publicznie (np. w serwisach społecznościowych), w przeciwieństwie do obrazów twarzy, próbek głosu, czy też informacji o tęczówce oka." Czy informacje o tęczówce oka są rozpowszechnione publicznie w stopniu wystarczającym do zastosowania biometrycznego?

Strona edycyjna pracy

Rozprawa doktorska mgr. inż. Marcina Platy jest napisana starannie, jej format jest zgodny z ogólnie przyjętymi standardami dla prac naukowych w dziedzinie nauk technicznych. Układ pracy jest logiczny i przyjazny dla czytelnika. Rysunki i tabele są staranne, choć niektóre rysunki są słabiej czytelne ze względu na zbyt małą czcionkę (np. Rysunek 2.1, 2.3, 3.1, 3.2). Z kolei obrazy różnicowe (Rys. 2.5 i Rys. 2.6) mogłyby być bardziej czytelne, gdyby wartości pikseli zostały przemnożone np. przez 10, gdyż obecnie na wydruku widnieją w większości jako czarne kwadraty.

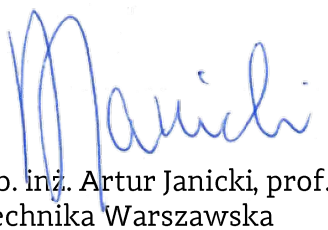
W pracy występują też pewne niedociągnięcia natury językowej. Są to m.in.:

- Używanie terminów niezgodnych z terminologią ugruntowaną w naszym środowisku naukowo-technicznym, np. „Gaussian Mixture" (powinno być: „mieszanina Gaussowska"), „steganoanaliza" (powinno być: „steganaliza", z ang. „*steganalysis*"), „potok treningowy" (lepiej np. „proces uczenia"), „*fold*" (przy walidacji krzyżowej używa się raczej formy „złożenie"), „urna melowa" („przedział na skali melowej"?), „jądro konwolucji" (lepiej „jądro splotu"), „warstwa poolingu" (lepiej „warstwa łącząca"), „augmentacja zbioru" (lepiej „rozszerzanie zbioru").
- Stosowanie kalek z języka angielskiego, np. „enkoder" (zamiast „koder"), „metoda do detekcji" (zamiast „metoda detekcji"), „system do automatycznej weryfikacji mówcy" (zamiast „system automatycznej weryfikacji mówcy") czy „zaadresować problem" zamiast „podjąć problem".
- Błędy językowe, np. „wzorzec biometryczny oparty o mimikę twarzy" (powinno być: „wzorzec biometryczny oparty na mimice twarzy", str. 154).
- Błędy literowe, np. „Zaproponowane" (zamiast „Zaproponowany", str. 26), „sieci nieurnowe" zamiast „neuronowe" (str. 42), „wygody" zamiast „wygodny" (str. 89) itd.
- Niezręczne sformułowania, np. „przestrzenne rozprzestrzenianie" (str. 39), „zdjęcie twarzy pobieranej niezależnie od jej ustawienia" (str. 80) itp.
- W języku polskim przecinek jest znakiem dziesiętnym, tymczasem Doktorant używa kropki, jak w notacji anglosaskiej.
- Braki w interpunkcji lub nadmiarowe przecinki.

Uchybienia edycyjne nie umniejszają jednak w żadnym stopniu dorobku Doktoranta.

Wnioski końcowe

W podsumowaniu stwierdzam, że problemy badawcze postawione w rozprawie zostały opracowane i rozwiązane. Doktorant zaproponował rozwiązania zwiększające bezpieczeństwo informatyczne metod opartych na biometrii twarzy, dłoni i głosu, a także metod wykorzystujących znakowanie wodne obrazów, i udowodnił ich skuteczność.
Stwierdzam, że przedstawiona rozprawa doktorska **spełnia** warunki określone w art. 187 ustawy Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2023 r. poz. 742 t.j.), dlatego niniejszym wnioskuję o dopuszczenie Doktoranta, Pana **mgr. inż. Marcina Platy**, do publicznej obrony jego rozprawy doktorskiej.



dr hab. inż. Artur Janicki, prof. uczelni
Politechnika Warszawska