prof. dr hab. inż. Khalid Saeed
Wydział Informatyki
Politechnika Białostocka
ul. Wiejska 45A, 15-351 Białystok

Tel. (+48-85) 746 9196
Fax: (+48-85) 746 9057
k.saeed@pb.edu.pl

Białystok, 24.08.2022 r.

RECENZJA rozprawy doktorskiej

mgr inż. Eweliny Bartuzi-Trokielewicz

z Wydziału Elektroniki i Technik Informacyjnych
Politechniki Warszawskiej

zatytułowanej

"Presentation attack-resistant palm recognition for mobile devices in unconstrained conditions"

Promotor:

Profesor dr hab. inż. Andrzej Pacut
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Niniejszą recenzję przygotowałem na zlecenie zawarte w piśmie z dnia 24.06.2021 (otrzymane dnia 1.07.2022), które otrzymałem od Profesora Jarosława Arabasa Przewodniczącego Rady Naukowej Dyscypliny Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej na podstawie uchwały Rady, podjętej dnia 24.05.2022 r.

I. Zawartość rozprawy

Praca doktorska mgr inż. Eweliny Bartuzi-Trokielewicz jest poświęcona zagadnieniu rozpoznawania cech dłoni na urządzeniach mobilnych w warunkach niekontrolowanych. Autorka przedstawia kilka nowych użytecznych metod i algorytmów dotyczących analizy cech dłoni, jej segmentacji i ekstrakcji cech oraz nowego podejścia zwiększającego bezpieczeństwo systemu biometrycznego w oparciu o wykrywanie fałszywych danych. To zagadnienie i inne cele rozprawy zostały przeanalizowane i przedstawione w rozprawie wraz z eksperymentami.

Rozprawa napisana jest w języku angielskim. Zawiera 99 stron tekstu, rysunków, tabel i ilustracji. Składa się z sześciu rozdziałów, bibliografii oraz czterech dodatków.

Rozdział 1. to „Introduction", gdzie autorka przedstawia wprowadzenie do tematyki rozprawy – biometrii obrazu dłoni (od charakterystyki dłoni do jej wstępnego przetwarzania i ekstrakcji jej cech) poprzez badanie sposobu jej ochrony przed atakiem prezentacji. W tym rozdziale autorka wymienia swoje cztery twierdzenia jako tezy pracy do udowodnienia w swojej rozprawie - główne cele to pokazanie sposobów i podejść autorki do poprawienia metod rozpoznawania odcisków dłoni przy różnych warunkach.

W rozdziale 2. „Biometric databases" autorka umieściła opis trzech kategorii baz danych dla dwóch rodzajów danych: obrazy otrzymane z urządzeń mobilnych oraz dodatkowe obrazy zbierane przy różnych warunkach otoczenia. Tytuł rozdziału sugeruje bazy z różnymi cechami biometrycznymi, ale dotyczy głównie dłoni oraz dwóch innych cech - tęczówki i palca.

W rozdziale 3. „Environment-invariant and accurate palm segmentation" opisano autorską metodę segmentacji obrazu dłoni opartą o głębokie splotowe (konwolucyjne) sieci neuronowe (DCNN - *Deep Convolutional Neural Network*). Metoda ta jest stosowana niezależnie od warunków otoczenia, takich jak światło, typ obrazu lub tło.

Rozdział 4. „Palm verification in unconstrained environment" skupia się na metodach weryfikacji dłoni przy nieograniczonych warunkach otoczenia. Rozdział ten zawiera bardzo ciekawy sposób prezentacji wyników przy wykorzystaniu mapy termicznej dłoni oraz wizualizacji wag dla mechanizmu atencji. Uwidoczniono obszary zainteresowania dłoni, które niosą najważniejsze informacje dla klasyfikatorów.

Rozdział 5. „Presentation attack detection" jest ostatnim rozdziałem merytorycznym i jest poświęcony metodom detekcji ataku prezentacji. Autorka przedstawiła biometryczne metody bezpieczeństwa i stan wiedzy metod PAD (*Presentation Attack Detection*) oraz zaproponowaną własną metodę wykrywania takiego ataku. Ten rozdział jest raczej skromny. Tematyka „*Presentation attack*" jest zawarta w tytule rozprawy i stanowi jeden z jej najważniejszych aspektów. Uważam, że rozdział o ataku prezentacji powinien być umieszczony wśród pierwszych rozdziałów, a tutaj w zamian powinien być rozdział o 'Presentation attack-**resistance recognition**'. Niemniej, zawartość tego rozdziału jest istotna.

Praca kończy się wnioskami, rozdział 6. „Summary", w których autorka konkluduje rozwiązanie powierzonych jej zadań oraz osiągnięcie wyznaczonych celów. Podaje również znakomite wyniki swojej pracy w liczbach.

Całość pracy kończy bibliografia „Bibliography", która zawiera 112 pozycji wybranych referatów i artykułów z literatury światowej pokazującej stan wiedzy i odzwierciedlającej szeroką wiedzę autorki. Zabrakło jednak jednej, moim zdaniem, istotnej pozycji o Presentation Attack: „*Ctirad Sousedik and Christoph Busch (2014) - Presentation attack detection methods for fingerprint recognition systems:*

a survey. IET Biometrics, vol. 3, issue 4, pp. 219-233). Chociaż praca ta jest o metodach wykrywania ataku prezentacji na przykładzie odcisków palca, to posiada ważną informację o ataku na prezentację cech biometrycznych i jest jedną z pierwszych prac przeglądowych w tej dziedzinie.

Dodatkowo, autorka opracowała cztery załączniki, w których umieściła ważne informacje: W "Appendix A" umieszczono ważne słownictwo i terminologie biometryczne - podano ich definicje lub wyjaśnienia, co znacznie ułatwia czytelnikom zrozumienie tekstu w rozprawie. Niestety, numeracja podrozdziałów nie jest prawidłowa, gdyż podana jako należąca do rozdz. 6. (6.1, 6.2, … .). "Appendix B" to lista publikacji autorki. "Appednix C" zawiera aktywność konferencyjną autorki, gdzie wygłaszała referaty na konferencjach międzynarodowych. W ostatnim dodatku, "Appendix D", podano listę grantów (jest ich 8), w których doktorantka brała udział jako wykonawca, a w trzech z nich jako główny wykonawca. Świadczy to, iż autorka jest dobrym badaczem naukowym z uznaniem otoczenia naukowego.

II. Opinia o rozprawie doktorskiej

Rozprawę doktorską pani Eweliny Bartuzi-Trokielewicz ocenię w dwóch płaszczyznach: technicznej i merytorycznej oraz klarowności i czytelności rozprawy. Usterki redakcyjne dotyczące klarowności pisowni oraz edycyjne będą umieszczone w załączniku.

A. Techniczne brzmienie i merytoryczna kompletność rozprawy

Autorka wykazała w swojej pracy dobrą znajomość zagadnień popularno-naukowych. Przedstawiła uzyskane przez siebie wyniki w sposób przekonywujący. Cytowana literatura jest prawidłowo dobrana. Według mnie praca jest interesująca, a naukowe osiągnięcia merytoryczne doktorantki są znaczne. Rozprawa jest wzbogacona wieloma przykładami osiągnięć autorki. Bardzo dobre wprowadzenie do tematyki przetwarzania obrazu dłoni jako cechy biometrycznej. Wszystkie aspekty dotyczące tej cechy oraz etapów jej rozpoznawania w różnych warunkach są szczegółowo podyskutowane z odpowiednimi standardami i wymaganymi rysunkami. Autorka poprawnie przedstawiła i wyjaśniła definicje ROI i FIDO. Wskazywała na brak definicji FIDO dla biometrii dłoni i zaproponowała 3 przykładowe stopnie oparte na pokazaniu wydruku, zdjęć na wyświetlaczu oraz wygenerowaniu obrazu przez sieć neuronową. Wskazuje to na wytrwałość i konsekwencje w prowadzonych badaniach. Doktorantka bardzo wyraźnie zaprezentowała problematyczność wykorzystanych baz, co wskazuje na znajomość trudności w analizie poszczególnych korpusów.

Głównymi rezultatami pracy badawczej doktorantki są:

- Wykonanie analizy niezawodności istniejących metod rozpoznawania dłoni przy nieograniczonych warunkach otoczenia.

- Zaprezentowanie metody segmentacji dłoni, która wykorzystuje głęboką splotową sieć neuronową i skutecznie wykrywa obraz dłoni przy różnych warunkach.

- Opracowanie metody ekstrakcji cech dłoni niewrażliwej na nieliniowość zmian tekstury.

- Opracowanie nowego podejścia zwiększającego bezpieczeństwa systemu biometrycznego w oparciu o wykrywanie fałszywych danych.

Dokonując recenzji rozprawy doktorskiej trzeba również zwrócić uwagę na jej słabe strony. Należą do nich, moim zdaniem, następujące punkty:

- Dobry system biometryczny zapewniający wysoki poziom bezpieczeństwa cechuje się tym, że jest odporny na przeróbki i przebudowę cechy biometrycznej (ang. *alteration*). Czujniki (jako czytniki, sensory) nie powinny w ogóle przyjąć fałszywych próbek. Ataki na cechy biometryczne są przeróżne, owszem, wiele z nich było wymienionych w rozprawie, jednakże zabrakło tak ważnych fałszerstw jako atak na prezentację, jak na przykład, cięcie lub transplantacja dłoni lub też zastosowania chemii w celu likwidacji wzorców odcisków dłoni. Niestety, zabrakło dyskusji na ten temat – w jakim stopniu system autorki wykrywa te przeróbki i jak je rezystuje?

- Żywotność (ang. *liveness*): Badanie żywotności cechy biometrycznej przez czujnik systemu biometrycznego jest jego drugą ważną charakterystką. Nie zauważyłem poświęcenia dodatkowego podrozdziału dla tego zjawiska. Autorka cytowała kilka pozycji literatury zajmującej się problematyką żywotności cech biometrycznych. Podała to w podrozdziale 5.2, kiedy odniosła się do stanu wiedzy o metodach PAD na przykładach. Jednak, uważam, że powinna być zawarta szersza dyskusja, a w szczególności, jak system autorki traktuje takie zjawiska.

B. Klarowność i czytelność rozprawy

Rozprawa napisana w języku angielskim, czyta się ją dobrze, chociaż nie brakuje błędów gramatycznych i edytorskich. Pewnym usprawiedliwieniem jest to, że nie jest to język ojczysty doktorantki. Mnie się wydaje, że autorka chciała dodać rozprawie charakter światowy pisząc w języku kongresowym, ażeby inni badacze naukowi mogli zapoznać się z jej nowymi osiągnięciami. Algorytmy, twierdzenia, wymagane rysunki i tabele są prawidłowo opracowane. Aktualny stan wiedzy dotyczącej tematyki biometrii dłoni został przedstawiony poprawnie. Istotne dla tematyki pracy zagadnienia omówiono czytelnie.

Mam wrażenie, że autorka nie ustrzegła się pewnej liczby nieścisłości mogących mieć wpływ na zrozumienie tekstu rozprawy. Niektórych szczegółów nie przedstawiono standardowo, podczas, gdy inne zagadnienia można było sformułować trochę inaczej lub w ogóle nie umieszczać w pracy. Oto moje redakcyjne uwagi:

- W opisie bazy danych (rozdział 2.2, str. 24) brakuje informacji, w jaki sposób kodowane były niestandardowe kanały RGB. Baza THID zawiera kanał podczerwieni często kodowany jako UINT16, a korpus CASIA posiada kanał 8-bitowy (dane pomiarowe matrycy CMOS). Informacja o zakresie danych liczbowych pozwoliłaby rozwiać wątpliwości co do normalizacji danych, co z kolei ma znaczący wpływ na pracę sztucznych sieci neuronowych.

- Tabela 2.1 nie jest spójna. Występują w niej zarówno informacje o rozmiarze w postaci rozdzielczości, jak i te, podane w konkretnych wymiarach. Nie jest jednak do końca wiadomo, czy w pierwszych czterech bazach zdjęcia są w postaci kwadratów czy prostokątów. Powiązane jest to z możliwością walidacji rożnych typów sieci neuronowych realizujących mechanizm segmentacji - czy każdy z obrazów ma wymagany wymiar.

- W podrozdziale 2.4., według autorki, jednym z elementów wykonanej pracy, jest rozszerzenie metody segmentacji dłoni w celu ujęcia innych cech i udowodnienia multimodalnego charakteru jej metody. Jednak rozprawa nie zawiera żadnej informacji o multimodalności jej podejścia. Z tego samego powodu, nie widzę sensu dodawania informacji o bazach odcisków palca oraz tęczówki oka.

- W podrozdziale 3.4.1 przedstawiono skrócone opisy dotyczące architektury sieci neuronowych CNN wykorzystanych w procesie segmentacji. Zbrakło jednak krótkiego zestawienia czy modele te wykorzystywały dane wejściowe o stałej (tj. tej samej) wielkości. Czy dane wejściowe były przetwarzane inaczej dla każdej z sieci (skalowanie, okno przesuwne)? W jaki sposób przetworzono dane pochodzące z matrycy CMOS (8 bitowa skala szarości) z korpusu CASIA? Czy wykorzystywano zbiór walidacyjny do doboru hiperparametrów np. liczby epok? Jest wyraźny brak szczegółów technicznych.

- W podrozdziale 3.4.3. autorka decyduje się na zastosowanie technik augmentacji (… *translation, rotation, scaling, adding noise, reflation, changing brightness, contrast, saturation and hue*). Przy czym brak jest jakiejkolwiek informacji dlaczego zdecydowano się na takie modyfikacje, czy wynikają one z literatury czy zaczerpnięte zostały z dziedzin pokrewnych?

- Autorka napisała w podrozdziale 4.5.3: “The experiments were carried out with a ten-fold subject-disjoint division of the data into training and test sets in the ratio of 80:20.”. Nie jest to typowo stosowany sposób walidacji i dlatego wymaga dopowiedzenia.

- W podrozdział 4.5.4. pomimo, że doktorantka prezentuje wagi map w sposób graficzny dla mechanizmu atencji, brak jest zwięzłego podsumowania. Z prezentowanych grafik wynika, że w zdecydowanej większości przypadków wysokie wagi koncentrowały się w obszarach dłoni, pomijając palce. Brak jest wnioskowania w tekście.

- Rysunek 5.1: brak źródła danych, w jaki sposób wykresy zostały wygenerowane.

- Na stronie 64 w 5.3. jako *Proposed type of attacks* zaproponowano 3 przykłady stopni FIDO dla analizy zdjęć dłoni. Przy czym dużą część rozdziału poświęcono na sztuczne modelowanie obrazu przez sieci neuronowe. W dużym stopniu pominięto aspekty techniczne, jak np. współpracę z rejestratorami obrazu. Rozprawa zyskałaby na jakości przy odwołaniu się do literatury przeglądowej. Jako przykład wskazałem pracę opublikowaną w IET Biometrics i podałem w opisie bibliografii.

Powyżej wymienione uwagi mają charakter dyskusyjny i nie obniżają wartości rozprawy, jednakże chciałbym, żeby autorka ustosunkowała się do nich na obronie.

III. Merytoryczne osiągnięcia doktorantki

Mgr inż. Ewelina Bartuzi-Trokielewicz osiągnęła cele pracy i udowodniła wyznaczone tezy rozprawy doktorskiej, która wnosi nowe aspekty do nauk technicznych w zakresie informatyki.

Pani Ewelina jest współautorką 10. recenzowanych referatów i artykułów opublikowanych w międzynarodowych czasopismach i konferencjach. Wszystkie znajdują się na liście Ministerstwa Edukacji i Nauki. Są to 2 artykuły w recenzowanych czasopismach, jeden rozdział w książce wydawnictwa Springer Nature oraz 7 referatów konferencyjnych. Autorka ma znaczny udział w projektach naukowych (osiem grantów naukowo-badawczych). Świadczy to o wysokim znaczeniu osiągniętych wyników jej pracy naukowej w dziedzinie biometrii. Oznacza to, iż problematyka rozprawy wpisuje się w bieżący trend zagadnień z tej właśnie dziedziny.

IV. Wnioski końcowe

Wystawiam pozytywną ocenę rozprawie doktorskiej mgr inż. Eweliny Bartuzi-Trokielewicz pt. „*Presentation attack-resistant palm recognition for mobile devices in unconstrained conditions*". Stwierdzam, że praca spełnia wymagania i warunki nakładane przez ustawę o stopniach naukowych i wnoszę bez zastrzeżeń o dopuszczenie doktorantki do obrony pracy w celu uzyskania stopnia doktora nauk technicznych w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

Khalid Saeed

Załącznik do opinii

Drobne usterki

1. Strona 12 – Appendix A w spisie treści: numeracja podrozdziałów jest podana jako należąca do rozdziału 6.
2. Podrozdział 1.2.3 wymaga cytowania.
3. Strona 18 – drugi paragraf wymaga cytatu.
4. "2. Biometric databases", zbyt ogólny tytuł rozdziału. Lepiej byłoby podać precyzyjnie, np. "Databases for selected biometric features".
5. Warto podać cytat o *Grayworld algorithm* (str. 34).
6. Rysunek 3.1 – brak podpisanych osi.
7. W podrozdziale 3.4.2 autorka pisze: „*For each palm image, one mask, the most accurate from all four methods, was subjectively selected by an expert (here: the Author)"*. Nie jest do końca klarowne kim jest ekspert/autor. Czy jest to autor rozprawy, publikacji czy bazy danych?
8. Strona 49 – pojedyncze referencje [46, 47, 48, 49, 50, 51, 52] zamiast ogólnego standardu [46-52].
9. Rysunek 4.6 – brak legendy.

10. Praca posiada błędy gramatyczn, literówki. Poniżej kilka takich przykładów:
    - "in a form of the following" (str. 18)
    - Datum liczba pojedyncza, a mnoga data. Chociaż stosuje się data w liczbie pojedynczej, ale trzeba trzymać jeden standard. Autorka raz pisze "data were" a drugi raz "data was"
    - The Table 3.1 (str. 37)
    - The Table 3.2 (str. 41)