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

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

Białystok, 28.01.2026 r.

RECENZJA rozprawy doktorskiej

mgr. inż. Jalila Nourmohammadiego Khiaraka

z Wydziału Elektroniki i Technik Informacyjnych
Politechniki Warszawskiej

zatytułowanej ***Developing Countermeasure algorithms against subterfuge in mobile biometric systems***

Promotor:

Prof. dr hab. inż. Włodzimierz Kasprzak
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Niniejszą recenzję przygotowałem na zlecenie zawarte w piśmie z dnia 01.12.2025, które otrzymałem od profesora Jarosława Arabasa przewodniczącego Rady Naukowej Dyscypliny informatyka techniczna i telekomunikacja Politechniki Warszawskiej na podstawie uchwały Rady nr 65/2025 z dnia 24.06.2025.

I. Omówienie, opis i ocena zawartości rozprawy

Rozprawa doktorska mgr. inż. Jalila Nourmohammadiego Khiaraka koncentruje się na czterech problemach: wprowadzeniu nowej cechy biometrycznej rozpoznawania ucha dotykowego, zaproponowaniu metody wykrywania ataków prezentacji (Presentation Attack Detection - PAD) opartej na zdjęciu i dotyku ucha oraz zbieraniu danych na urządzeniach mobilnych dla biometrii ucha. Doktorant przedstawia kilka nowych użytecznych algorytmów. Najważniejsze z nich dotyczą badania metod wykrywania ataków prezentacyjnych (PAD lub tak zwany *spoofing*) oraz technik weryfikacji żywotności jako środków przeciwdziałania fałszywym atakom. Dzięki opracowaniu nowej bazy danych oraz badaniom nad nowymi algorytmami rozpoznawania użytkownika i detekcji ataku, badania autora wnoszą znaczący wkład w dziedzinę biometrii oferując rozwiązania problemów uwierzytelniania w urządzeniach mobilnych. Integracja trybu dotyku ze zdjęciem ucha okazuje się obiecującym podejściem, poprawiając dokładność metod zachowania bezpieczeństwa systemów biometrycznych. Rozprawa napisana jest w języku

angielskim i ma charakter teoretyczno-doświadczalny. Zawiera 145 stron formatu C5 tekstu, rysunków i tabel. Składa się z siedmiu rozdziałów, bibliografii oraz czterech załączników. Zawartość załącznika Appendix B jest kontynuacją części merytorycznej rozprawy, gdyż tam znajdują się opisy algorytmiczne (pseudokody) implementacji pięciu programów komputerowych.

Rozdział pierwszy przedstawia wprowadzenie do systemów PAD na urządzeniach mobilnych, wskazując najnowsze trendy i odnosząc się do pojawiających się wyzwań w tej dziedzinie. Dodatkowo, w rozdziale tym, autor opisuje założenia i cel pracy oraz zakres i strukturę rozprawy doktorskiej.

W *rozdziale drugim* doktorant podaje szczegóły wykorzystanej bazy danych WUT-Ear V1.0 (Warsaw University of Technology Ear Version 1.0). Rozdział zaczyna od przeglądu, który przedstawia zakres bazy danych oraz uzasadnienie jej stworzenia, a następnie szczegółowo opisuje cztery kluczowe zestawy danych w bazie. Każdy zestaw koncentruje się na różnych aspektach biometrii ucha i PAD, tj. rzeczywistych zdjęciach ucha, fałszywych zdjęciach ucha, rzeczywistych dotyków ucha oraz zestawie fałszywych dotyków ucha. Rozdział kończy się podsumowaniem, które podkreśla kluczowe omówione kwestie oraz znaczenie bazy danych WUT-Ear V1.0 dla rozwoju badań w dziedzinie biometrii ucha i PAD.

W *rozdziale trzecim* doktorant analizuje szczegółowe badanie na temat oceniania skuteczności uwierzytelniania ucha na urządzeniach mobilnych. W szczególności bada wydajność algorytmów wykrywania ataków prezentacji oraz metod weryfikacji użytkownika na podstawie nowo opracowanej bazy danych. Bezpieczeństwo systemów uwierzytelniania na podstawie ucha spotyka poważne wyzwania, szczególnie w przypadku ataków prezentacji, gdy fałszerze próbują oszukać system, prezentując fałszywe lub przerobione obrazy ucha. Autor analizując problem, zajął się tym aspektem oraz opracował odpowiednie algorytmy z obiecującymi wynikami.

Rozdział czwarty bada różne sposoby i możliwości wykorzystania dotyku ucha jako metody uwierzytelniania użytkownika telefonu komórkowego oraz kontroli ich dostępu. Przedstawiono propozycję metody rejestrowania danych dotyku ucha. Autor przedstawia rozwiązanie bardzo ważnego problemu w aspekcie dotyku ucha przez telefon, a mianowicie problemu brakujących punktów dotyku (*missing data points*), które są zasadnicze do obliczania elementów wektora cech. Doktorant twierdzi, iż jego zaproponowana metoda rozwiązuje ten problem skutecznie, z wysokim poziomem wydajności. Twierdzi, że wspomniany brak nie ma dużego wpływu na jego metodę: „*By focusing on the consistent elements of the ear's structure, the proposed system can extract meaningful biometric data even when some points are missing*" – cytat ze str. 125 rozprawy doktorskiej. Moim zdaniem, problem ten nie może być rozwiązany na tej podstawie i dalej jest poważnym wyzwaniem, gdyż brak niektórych punktów dotyku może pojawić się w różnych miejscach i na różne sposoby u użytkowników, w zależności od wielu czynników. Chciałbym więc, aby doktorant ustosunkował się do tej uwagi podczas obrony, z naciskiem na wpływ braku tych punktów na wektor cech.

W *rozdziale piątym* autor przedstawia nowatorskie podejście łączące zdjęcia ucha z jego dotykiem, aby dostać biometryczny multimodalny system do uwierzytelniania użytkownika telefonu komórkowego. Otrzymany model jest ciekawym rozwiązaniem – fuzją dwóch cech. Zdjęcie ucha rejestruje wizualne szczegóły unikalnej budowy ucha, natomiast dane dotykowe ucha rejestrują konkretne wzory powstające, gdy ucho styka się z ekranem dotykowym telefonu. Jednak, moim zdaniem, obawy wymienione powyżej odnośnie „*missing points*" będą również nadal przeszkodą przy wdrożeniu algorytmów takiej metodologii.

Rozdział szósty skupia się na opracowaniu nowatorskiej techniki wykrywania ataków prezentacji z użyciem dotyku ucha i jego fotografii. Wszystkie szczegóły są podane z naciskiem na wydajność algorytmu biometrii ucha odnośnie *spoofingu*. Osiągnięcia doktoranta oraz wyniki podane w tym rozdziale są pozytywne i na dobrym poziomie. Autor słusznie zauważył, iż systemy biometryczne stają się coraz powszechniej stosowane, napotykają coraz bardziej wyrafinowane próby oszustw, gdzie atakujący wykorzystują wysokiej jakości obrazy, filmy, a nawet modele 3D, aby wprowadzić w błąd systemy rozpoznawania. Tradycyjne metody detekcji *spoofingu* poczyniły znaczące postępy w przeciwdziałaniu tym zagrożeniom, ale zmieniająca się natura ataków wymaga opracowania bardziej zaawansowanych, odpornych i kompleksowych strategii detekcji PAD. Stąd uważam, że pomysł doktoranta w kierunku opracowania nowego podejścia jest słuszny. Pomimo to, rozdział nie jest pozbawiony usterek. Moim zdaniem, pokazane wyniki w tabeli 6-3 nie są do końca zgodne z informacją prezentowaną w tabeli 2-5 w rozdziale drugim. W tabeli 6-3 podane, że dla Dell-GA7 oraz PADNet-1 osiągnięto miarę 12,2 APCER, dla Dell-NL1020 - 0.91, natomiast według tabeli 2-4 liczebność ataków dla pierwszego scenariusza to 2134, a dla drugiego 101. Czy oznacza to, że w pierwszym przypadku jest 260.348 błędnych rozpoznań, a w drugim 0.91? Dodatkowo dla S3D-GA7 osiągnięto 0.37, co przy liczbie 16 uczestników daje 0,0592 uczestnika niesłusznie akceptowanego. Rachunki liczbowe wyglądają wątpliwie i być może wystąpił tu błąd numeryczny. Prosiłbym o wyjaśnienie i interpretację tabeli 6-3.

W *rozdziale siódmym* doktorant konkluduje swoją pracę podając jej streszczenie, które zawiera opis osiągnięć autora oraz dodatkowe informacje o ograniczeniach swoich metod takich, jak praktyczne kwestie - koszty i dostępność użytkownika.

Całość merytorycznej pracy kończy *Bibliografia*, która zawiera 74 pozycje wybranych referatów i artykułów z literatury światowej pokazującej stan wiedzy i odzwierciedlającej dobrą wiedzę doktoranta. Wszystkie pozycje są cytowane w pracy. Można zauważyć brak pewnych prac na temat rozpoznawania ucha oraz baz danych ucha. Przykładem jest brak pracy Dariusza Frejlichowskiego i Natalii Tyszkiewicz zawierającej bazę uszu do możliwego wykorzystania. Poza tym cytowano dwie prace [54] i [55], które należą do tego samego źródła, które z resztą nie jest opublikowane. Praca pod numerem [46] cytowana w rozprawie jako „*recent study*" sugeruje, że jest nową, chociaż pochodzi z 2006 roku.

II. Opinia o rozprawie doktorskiej

Wyniki rozprawy doktorskiej mgra inż. Jalila Nourmohammadiego Khiaraka chciałbym oceniać w dwóch płaszczyznach: technicznej i merytorycznej oraz klarowności i czytelności rozprawy.

A. Techniczne brzmienie i merytoryczna kompletność rozprawy

Autor wykazał w swojej pracy umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników. Cytowana literatura jest interesująca, chociaż, nie jest kompletna.

Merytoryczne osiągnięcia doktoranta są na dobrym akceptowanym poziomie. Najważniejsze z nich to:

(1) Rozwinięcie metod mobilnej biometrii z wykorzystaniem algorytmów maszynowego uczenia.
(2) Badanie biometryczne oparte na uchu (zdjęcie ucha i dotyk ucha) w celu wzmacniania systemów bezpiecznego uwierzytelniania mobilnego.
(3) Opracowanie przyzwoitego systemu PAD do wykrywania ataków prezentacyjnych w rzeczywistych scenariuszach.
(4) Wprowadzenie zbioru danych WUT-Ear V1.0 do trenowania i testowania modeli rozpoznawania.
(5) Ważnym osiągnięciem przy dopasowaniu wzornika dla scenariusza bez brakujących punktów (*matching scenario without missing points*) jest wykorzystanie wyników prac profesora Andrzeja Pacuta (str. 72 rozprawy) przy rozwiązywaniu problemu optymalizacji równania:

$$(R^*, l^*, P^*) = \underset{(R,l,P)\in\mathcal{R}\times\mathcal{L}\times\mathcal{P}}{\operatorname{argmin}} \sum_{i=1}^{N} \|t_i - (Rx_{\pi i} + l)\|^2$$

Andrzej Pacut opracował swoją metodę optymalizacji na bazie algorytmu Kabsch-Umeyama, ale nie uwzględniał permutacji. Doktorant rozwinął tę metodę i opracował odpowiedni algorytm, żeby pasował do wymagań swojego podejścia. Pseudokod B1 pokazuje szczegóły algorytmu doktoranta.

Osiągnięcia te doprowadziły do uzyskania bezpiecznych modeli biometrycznych wykorzystujących obraz ucha oraz jego dotyk do telefonu komórkowego. Najważniejsze skutki i efekty tych prac to: uzyskanie bezpiecznego modelu fuzji dotyku i zdjęcia ucha jako systemu multimodalnego; wnioskowanie, iż podejścia głębokiego uczenia (VGG16, MobileNetV2, Vision Transformers) poprawiły dokładność systemu; osiągnięto EER na poziomie 0.04, co dowodzi przydatność biometrii ucha do uwierzytelniania.

Pomimo, że doktorant starał się, żeby praca była klarowna i czytelna, nie ustrzegł się pewnych niedoskonałości formalnych i językowych.

Uwagi

- Opis bazy WUT-Ear jest nieprecyzyjny. Doktorant podaje różne liczby w różnych miejscach: Na str 27 pisze, że rzeczywistych danych było 8000 (sztucznych 8662), ale na stronie 29, że w bazie jest 137 osób z 60 zdjęciami, czyli

8220. Liczebność jest w formie mało precyzyjnej. Natomiast na stronie 30 - pojawia się histogram bez zestawienia tabelarycznego.

- Nie podano pełnej informacji na stronie 31, gdzie doktorant pisze: "*Almost 35 images from 5 different positions are taken in one session from each side therefore totally there are almost 70*". Dalej pisze "*It should be noted that images however some subjects have more than 70. It should be noted that more than 10 subjects have earrings*." Brak informacji, dlaczego liczba zdjęć dla niektórych uczestników wzrosła do 70 oraz czy obecność kolczyków miała znaczenie.

- Sztuczne dotknięcia uszu (str. 26 – "*The dataset not only includes authentic ear images, but also features a comprehensive collection of presentation attack instruments (PAIs), such as printed images and 3D models*" oraz str 43 – "*Figure 2-13*"): Czy faktycznie wykorzystano odciski uszu? Rysunek 2-13 pokazuje tylko dotknięcia palców dłoni.

- Na tej samej stronie istnieje napis "*…. the raw images have a resolution of 4608×3456 pixels, while the preprocessed images have 1992×3120 pixels*". Tutaj wypadałoby napisać, na czym konkretnie polegało wstępne przetwarzanie (preprocessing), że doprowadziło do takich zmian.

- Na rysunku Figure 2-7 widzimy „*Sample visualization by t-SNE*". Czy zwykłe wrzucenie wizualizacji danych do t-SNE jest poprawne? A może była wykorzystana np. biblioteka: (https://opentsne.readthedocs.io/en/stable/examples/01_simple_usage/01_simple_usage.html) - stworzyć embedding dla zbiorów treningowych, optymalnizować, a następnie użyć transformacji dla nowych danych testowych. Zwykle sklearn.manifold.TSNE, prawdopodobnie, nie ma takich możliwości. Proszę o wyjaśnienie tego aspektu, czy doktorant w ten sposób wykonał wizualizacji danych.

- Figure 3-5: na *flowchart* jest strzałka pokazująca pomijanie ekstrakcji cech. To jest błąd, gdyż można pominąć augmentację do ewaluacji, ale nie "*feature extraction*".

- Strona 67 zawiera ważną informację oraz fakty o biometrii ucha, ale bez żadnego cytatu. Autor powinien podać źródło wymienionych faktów i informacji.

- Brak lub błędne informacje podano w źródłach [52] i [53]. Powinny brzmieć tak:
[52] M.D. Atkinson: An Optimal Algorithm for Geometrical Congruence, Journal of Algorithms 8 (1987), pp. 159–172.
[53] Alt, H., Mehlhorn, K., Wagener, H., & Welzl, E.: Congruence, Similarity, and Symmetries of Geometric Objects. Discrete and Computational Geometry 3 (1988), 237-256. doi:10.1007/BF02187910.

Z drugiej strony brak informacji, jak zostały te źródła wykorzystane w rozprawie w odniesieniu do biometrii ucha (strona 69).

B. Klarowność i czytelność rozprawy

Rozprawa jest napisana zrozumiałym językiem - algorytmy, twierdzenia, rysunki i tabele są czytelne i starannie opracowane**.** Istotne dla tematyki pracy

zagadnienia omówiono czytelnie i przejrzyście. Autor włożył dużo pracy w klarowne przygotowanie manuskryptu. Pomimo wysiłków autora, by praca prezentowała jego osiągnięcia w sposób klarowny, niemożliwym do uniknięcia są drobne usterki językowe lub błędy typograficzne, których przykłady zostały wymienione poniżej.

Drobne usterki

- Str. 18: „a biometric" oraz na str. 19 „biometrics". Biometrics to nie liczba mnoga dla biometric. Biometrics to rzeczownik i może być uzywany jako przymiotnik (a biometrics feauture) – ang. compound noun.

- Tabele 3-1 i 3-2 wskazują na modele neuronowe z funkcją wyjściową sigmoid czyli zakresy typowo 0-1, natomiast tabele 3-3 i 3-4 pokazują wskaźniki bez jasno określonego progu decyzyjnego.

- Figure 4-15 pokazuje wyniki dla przypadków trzech dotyków i dla jednego dotyku a w podrozdziale 4.4.1, jest informacja, że dla 17 osób nie ma *missing points*, ale brak informacji o liczbie użytkowników z jednym dotykiem.

Znalezione błędy edytorskie

- W wielu miejscach stosowano nieprawidłowe „possessive 's' " jak: PAD's, subject's, image's, dataset's, model's, study's, etc.
- Podobna sytuacja jest z „while", gdzie używane w większości przypadków w sensie „whilst", przykłady są na str. 1, 2, 4, 45, 67, … itd.
- Str. 27 i w 7. innych miejscach autor pisze „Let's" zamiast „Let us" – (The general rule is to avoid using contractions for academic and other formal writing.)
- Str. 69: In [51], The authors → … authors,
  to matching → to match
- Str. 70: featured → feature lub features
- Str. 103: Section 5-2, 5-3, 5-4 and 5-5 → 6-2, 6-3, 6-4 and 6-5
- Str. 110: Where → where

III. Merytoryczne osiągnięcia doktoranta

Pan mgr inż. Jalila Nourmohammadiego Khiaraka ma na koncie bardzo dobry dorobek naukowo-publikacyjny. Doktorant jest współautorem 9. publikacji naukowych w indeksowanych czasopismach oraz referatów naukowych na konferencjach krajowych i międzynarodowych. Poza tym doktorant ma 4 artykuły przygotowane do złożenia w czasopismach. Dorobek publikacyjny świadczy o znaczeniu osiągniętych wyników pracy naukowej doktoranta w dziedzinie multimodalnej biometrii ucha. Oznacza to, iż problematyka rozprawy wpisuje się bezpośrednio w bieżący nurt zagadnień z tej właśnie dziedziny. Autor uczestniczył w *European Union Horizon 2020 Grant*: *AMBER Project* w roli *Early Stage Researcher*.

IV. Wnioski końcowe

Wystawiam pozytywną ocenę rozprawie doktorskiej Pana mgr. inż. Jalila Nourmohammadiego Khiaraka pt. "*Developing Countermeasure algorithms against subterfuge in mobile biometric systems*". Rozprawa stanowi oryginalne rozwiązanie postawionych zadań oraz osobisty wkład Doktoranta w rozwój metod przeciwdziałania fałszerstwa w mobilnych systemach biometrycznych. Stwierdzam, że praca spełnia wymagania i warunki nakładane przez ustawę o stopniach naukowych (art. 190 ust. 2 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce - Dz. U. z 2024 r. poz. 1571, z późn. zm.).

Na tej podstawie wnioskuję o dopuszczenie Autora wymienionej rozprawy doktorskiej do jej obrony.

Khalid Saeed