

Poznań, 20.03.2026 r.

Prof. dr hab. inż. Adam Dąbrowski
Politechnika Poznańska
Wydział Automatyki, Robotyki i Elektrotechniki
Instytut Automatyki i Robotyki
Zakład Układów Elektronicznych
i Przetwarzania Sygnałów

OCENA

rozprawy doktorskiej pt.: *„Aktywna ochrona tożsamości w obrazach twarzy z wykorzystaniem odpornego na manipulacje deepfake znakowania wodnego”*
Doktorant **kpt. mgr inż. Tomasz Walczyna**

1 Podstawa formalna opracowania recenzji

Podstawą formalną opracowania tej recenzji jest Uchwała nr 85/RDN ITiT/2025 z 18.11.2025 r. Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego o wyznaczeniu mnie na recenzenta rozprawy doktorskiej mgr. inż. Tomasza Walczyny nt. „Aktywna ochrona tożsamości w obrazach twarzy z wykorzystaniem odpornego na manipulacje deepfake znakowania wodnego” w dziedzinie nauk inżynierjno-technicznych w dyscyplinie Informatyka Techniczna i Telekomunikacja.

2 Ocena trafności doboru tematyki pracy, określenia problemu naukowego oraz celu i zakresu przeprowadzonych badań

Tematem ocenianej rozprawy doktorskiej, złożonej ze zwięzłej (trzydziesto ośmio stronicowej) części w postaci autoreferatu napisanego w języku polskim oraz z zestawu 11 publikacji, głównie w języku angielskim, jest analiza problemu zagrożeń wynikających z coraz bardziej rozpowszechnionych ataków typu „deepfake”, polegających na realistycznych manipulacjach w wypowiedziach i obrazach (w przypadku ocenianej rozprawy — w obrazach twarzy) w celu podmiany tożsamości osoby.

Opracowane i przetestowane przez Doktoranta, a ściślej przez zespół badawczy, którego jest członkiem, techniki tzw. „cyfrowego znakowania wodnego” obrazów pozwalają nie tylko na wykrywanie manipulacji w obrazach twarzy w celu zafałszowania/podmiany tożsamości przedstawionej osoby, ale także na odzyskiwanie prawdziwej tożsamości pierwotnej.

Podjęte i przedstawione w ocenianej rozprawie prace badawcze, programistyczne i eksperymentalne zaliczam do bardzo ważnej i w pełni aktualnej tematyki, która ma coraz większe znaczenie w związku z rozwojem metod i zastosowań biometrii a ogólnie — sztucznej inteligencji.

Tematyka rozprawy została, moim zdaniem, trafnie przypisana do Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja.

Na stronach 16 i 17 tekstu rozprawy Doktorant podał następujące cele badawcze:

cel pierwszy — „przeanalizowanie jak działają metody deepfake, co edytują i w jaki sposób”

cel drugi — „opracowania metod deepfake, które można wykorzystać w dalszej części badań w ramach treningu przyszłej metody znakującej, np. do tworzenia realistycznych scenariuszy ataków”

cel trzeci — „przeanalizowanie jak działają metody ukrywania danych w obrazie, zbadanie możliwości rekonstrukcji w oparciu o znak wodny, opracowania własnych metod znakowania, jak zachowują się znaki wodne w stosunku do deepfake”

cel czwarty — „opracowanie metody znakowania pozwalającej na ukrycie reprezentacji twarzy i jej rekonstrukcję po manipulacjach”.

W tekście rozprawy te cele są poprzedzane jedenastoma szczegółowymi założeniami, które są w istocie mikrotezami badawczymi. Wszystkie je poprzedza je następująca główna teza naukowa:

„Modele sieci neuronowych umożliwiają ukrycie reprezentacji wizerunku twarzy w obrazie oraz jego rekonstrukcję po manipulacjach deepfake.”

Uważam, że sformułowanie czterech celów badawczych jest nadmiarowe. Poza tym pierwsze trzy z nich są raczej szczegółowymi zadaniami badawczymi a nie celami. Rangę właściwego, i w zupełności wystarczającego w rozprawie, ma jedynie cel czwarty.

Krytycznie odnoszę się ponadto do przedzielenia sformułowanych celów licznymi założeniami algorytmiczno-technicznymi, które zamiast rozjaśniać je i wynikające z nich podjęte zadania raczej je zaciemniają. Te założenia, jeśli w ogóle należy je formułować na wstępie a nie jako wnioski z przeprowadzonych badań, co sugerowałbym, powinny być omówione w oddzielnej sekcji tekstu.

Zastrzeżenia mam też co do zakresu tytułu rozprawy, z którego jednoznacznie wynika, że przeprowadzone badania dotyczą ochrony tożsamości w obrazach twarzy. Jednak Doktorant opisuje i bada także zagadnienia ochrony tożsamości głosu o czym świadczą: schemat potoku analizowanego procesu podmiiany głosu na rys. 2.2 oraz dwie pierwsze publikacje podane w p. 1.3, o których Doktorant pisze, że tworzą „cykl powiązanych artykułów naukowych”, z których „praca składa się”, tj. prace:

1. Tomasz Walczyna, Zbigniew Piotrowski, Overview of Voice Conversion Methods Based on Deep Learning, Applied Sciences, 2023; vol. 13, nr 5, art. 3100, s. 1–13, doi: 10.3390/app13053100
2. Tomasz Walczyna, Zbigniew Piotrowski, Overview of Deep Learning Voice Conversion Methods Using Disentangling Speaker from Linguistic Content, 39th IBIMA Computer Science Conference, 2022, ISBN: 978-0-9998551-9-5.

Zatem należało albo rozszerzyć zakres tytułu pracy oraz sformułowania tezy naukowej i celu badawczego (tj. celu czwartego według numeracji Doktoranta) albo usunąć powyższe publikacje z cyklu powiązanych artykułów naukowych i nie zajmować się w pracy problematyką ochrony tożsamości głosu.



3 Ocena struktury, treści, tekstu rozprawy, analizy źródeł, dorobku publikacyjnego Doktoranta oraz formy rozprawy

Recenzowana rozprawa zawiera streszczenie w języku polskim (str. 5), streszczenie w języku angielskim (str. 7), spis treści (str. 9 i 10), wykaz użytych skrótów (str. 11), glosarium zwrotów (str. 13 i 14) oraz — jak już wspomniałem — trzydziesto ośmio stronicowy autoreferat napisany w języku polskim. W pracy umieszczono ponadto teksty 11 następujących publikacji współautorskich, stanowiących — jak to podał Doktorant — „cykl powiązanych artykułów naukowych” (poniżej podaję ich pełną listę, choć dwie pierwsze pozycje już wymieniłem):

1. Tomasz Walczyna, Zbigniew Piotrowski, Overview of Voice Conversion Methods Based on Deep Learning, Applied Sciences, 2023; vol. 13, nr 5, art. 3100, s. 1–13, doi: 10.3390/app13053100
2. Tomasz Walczyna, Zbigniew Piotrowski, Overview of Deep Learning Voice Conversion Methods Using Disentangling Speaker from Linguistic Content, 39th IBIMA Computer Science Conference, 2022, ISBN: 978-0-9998551-9-5
3. Tomasz Walczyna, Zbigniew Piotrowski, Quick Overview of Face Swap Deep Fakes, Applied Sciences, 2023; vol. 13, nr 11, art. 6711, doi: 10.3390/app13116711
4. Tomasz Walczyna, Zbigniew Piotrowski, Fast Fake: Easy-to-Train Face Swap Model, Applied Sciences, 2024; vol. 14, nr 5, art. 2149; doi: 10.3390/app14052149
5. Tomasz Walczyna, Zbigniew Piotrowski, Zastosowanie rozmycia Gaussa i segmentacji w algorytmach podmiany twarzy, KNTWRE (Konferencja Naukowo-Techniczna Systemy Rozpoznania i Walki Radioelektronicznej), 2024, paper ID 125
6. Zbigniew Piotrowski, Maciej Kaczyński, Tomasz Walczyna, Change and Detection of Emotions Expressed on People's Faces, Applied Sciences, 2024, vol. 14, nr 22, art. 10681; doi: 10.3390/app142210681
7. Tomasz Walczyna, Zbigniew Piotrowski, Image Reconstruction Based on Zero-Bit Watermarking Using a Neural Network, KRiT (Konferencja Radiokomunikacji i Teleinformatyki), 2025, 98, 487–490, doi:10.15199/59.2025.4.111
8. Tomasz Walczyna, Zbigniew Piotrowski, Implementation of a Method for Hiding Data in Images Using Generative Networks, KRiT (Konferencja Radiokomunikacji i Teleinformatyki), 2023, 96, 313–316, doi:10.15199/59.2023.4
9. Tomasz Walczyna, Zbigniew Piotrowski, Robust Data Hiding in Images Using DenseNet Architecture, 39th IBIMA Computer Science Conference, 2022, ISBN: 978-0-9998551-9-5
10. Tomasz Walczyna, Zbigniew Piotrowski, Mutual Effects of Face-Swap Deepfakes and Digital Watermarking - A Region-Aware Study, Sensors, 2025, doi: 10.20944/preprints202509.0333.v1
11. Tomasz Walczyna, Jacek M. Zurada, Zbigniew Piotrowski, RE-Mark: An Identity-Recovery Watermarking Method for Undoing DeepFake Face-Swap, IEEE Access, 2025, doi: 10.36227/techrxiv.175691586.66038128/v1



Dwie pierwsze publikacje nie mieszczą się w obszarze objętym tytułem rozprawy i w związku z tym są, moim zdaniem, nadmiarowe. W ośmiu pozostałych Pan mgr inż. Tomasz Walczyna jest pierwszym współautorem i w ich przygotowaniu ma udziały większościowe. Podaję je w nawiasach dla poszczególnych pozycji: 3 (55%), 4 (55%), 5 (55%), 7 (55%), 8 (55%), 9 (55%), 10 (55%), 11 (40%). Ponadto Pan mgr inż. Tomasz Walczyna jest ostatnim z trzech współautorów artykułu 6 i ma w nim znaczący udział 30%.

Biorąc pod uwagę powyższe zestawienie prac, dorobek publikacyjny Pana mgr. inż. Tomasza Walczyny oceniam jako bardzo wartościowy, z dużym indywidualnym wkładem Doktoranta (polegającym nie tylko na zbieraniu i analizie literatury, ale także na opracowywaniu metod, przeprowadzaniu eksperymentów i przygotowaniu oraz redakcji tekstów) i w dużym stopniu wspierający ocenianą rozprawę.

Tekst rozprawy zamykają: spis literatury na str. 184-187 (zawierający 47 pozycji, w tym cztery współautorskie prace Doktoranta), spis rysunków oraz tabel (str. 188) i oświadczenia o procentowym udziale współautorów w publikacjach będących podstawą rozprawy doktorskiej (str. 190).

Spis literatury oceniam jako niewielki pod względem liczebności cytowanych prac. Nie jest dla mnie jasne dlaczego w tym spisie figurują tylko cztery współautorskie publikacje Pana mgr. inż. Tomasza Walczyny (pozycje [27], [28], [29] i [47]), przy czym tylko trzy spośród jedenastu prac zgłoszonych przez Doktoranta jako cykl powiązanych artykułów naukowych wspierających doktorat (tj. prace [27] – pozycja 1 cyklu, [28] – pozycja 3 cyklu i [47] – pozycja 5 cyklu). Jeszcze raz podkreślam, że praca [27] (tj. pozycja 1 cyklu) w istocie wykracza poza tematykę rozprawy doktorskiej. Z niezrozumiałych dla mnie powodów w cyklu powiązanych artykułów naukowych wspierających doktorat Pan mgr inż. Tomasz Walczyna nie umieścił pracy

[29] P. Duszejko, Tomasz Walczyna, Zbigniew Piotrowski, Detection of Manipulations in Digital Images: A Review of Passive and Active Methods Utilizing Deep Learning. Applied Sciences, 2025; vol. 15, 881

jednoznacznie mieszczącej się w tematyce rozprawy doktorskiej.

Kompozycja tekstu rozprawy, polegająca na poprzedzeniu tekstów cyklu publikacji (stanowiących drugą część rozprawy) częścią pierwszą w postaci „autoreferatu” opisującego i porządkującego uzyskane wyniki, jest w zamyśle prawidłowa. Jednak część pierwsza wydaje się być zbyt lakoniczna i powierzchowna. Brak w niej przeprowadzenia skrupulatnej analizy zastanego stanu wiedzy a następnie uporządkowanego opisanie kolejnych własnych pomysłów Doktoranta, przeprowadzonych badań, eksperymentów i porównawczego omówienia uzyskanych wyników.

4 Ocena uzyskanych wyników i przeprowadzonych eksperymentów oraz poprawności ich przedstawienia

Pan mgr inż. Tomasz Walczyna zaproponował i przetestował metodę nazwaną przez Niego RE-Mark, która polega na takim ukrywaniu cyfrowych znaków wodnych w obrazach twarzy, aby mimo ataku polegającego na tzw. „głębokim zafałszowaniu” („deepfake”) tożsamości (tj. w pełni wiarygodnym dla człowieka podmienieniu twarzy) można to było wykryć a nawet odtworzyć pierwotną tożsamość.

Do głównych zadań podjętych i wykonanych przez Doktoranta oraz do najważniejszych uzyskanych przez Niego wyników należy, moim zdaniem, zaliczyć:

- przeanalizowanie przestrzeni manipulacji zwłaszcza w obrazach twarzy i opracowanie modelu warstwowego typu analiza → mapowanie → rekonstrukcja
- opracowanie i adaptacja generatorów podmieniania twarzy z ciągłą kontrolą intensywności ingerencji
- zbudowanie modeli podmiiany twarzy do przeprowadzania eksperymentów na małych zbiorach danych
- pokazanie i przebadanie wzajemnego wpływu podmiiany twarzy na degradację znaku wodnego ukrytego w obrazie i wpływu „twardości” znaku wodnego na pogorszenie stabilności/jakości procesu podmiiany twarzy
- opracowanie metody RE-Mark polegającej na wprowadzaniu rekonstruującego znaku wodnego, który umożliwia odtworzenie pierwotnej twarzy po jej podmianie w obrazie na podstawie pojedynczego obrazu bez żadnych dodatkowych danych zewnętrznych
- eksperymentalną weryfikację poprawności opracowanych rozwiązań w zróżnicowanych warunkach i przy zróżnicowanych jakościach obrazów.

Wymienione powyżej osiągnięcia Doktoranta oceniam wysoko. Świadczą one nie tylko o Jego pomysłowości i dużej wiedzy w zakresie rekonstrukcji tożsamości po atakach polegających na podmianie twarzy w obrazach, ale także o systematyczności, skrupulatności, pracowitości i skuteczności osiągnięcia założonych celów badawczych.

Mam jednak duże zastrzeżenia do nazewnictwa w języku polskim stosowanego w pierwszej części rozprawy doktorskiej. Od osoby, która pracuje nad stosunkowo nową dziedziną o nieugruntowanym jeszcze nazewnictwie w języku polskim, oczekuje się podjęcia wysiłku w kierunku standaryzacji tego nazewnictwa, czyli podania właściwych propozycji nazw i nie stosowania a tym samym nie rozpowszechniania określeń „żargonowych”. Doktorant niestety z tego zadania w ogóle się nie wywiązał. Język polski Jego tekstu jest na granicy akceptowalności a właściwie już poza tą granicą.

Dla przykładu w tekście rozprawy występują liczne, dla mnie zwłaszcza w pracach naukowych całkowicie nieakceptowalne, do tego odmieniane tak jak słowa polskie określenia: „deepfake’ów” (np. str. 22), „deepfake’u” (np. str. 24), „fake newsy” (np. str. 15), „trójkąt watermarkingu” (np. str. 14 i 25), „embedder” (np. str. 28), „po face-swapie” (np. str. 17 i str. 32), „wieloetapowość pipeline’ów” (np. str. 50), „postporocessingu (np. str. 32)”.

5 Uwagi szczegółowe

Poniżej zebrałem wybrane uwagi szczegółowe, które nasunęły mi się podczas czytania tekstu rozprawy:

- w tekście pracy brak numerów stron parzystych
- str. 5 (wiersz 10_d): Doktorant używa poprawnego określenia „potok”, podobnie w podpisach rysunków 2.1 i 2.2, jednak w wielu innych miejscach, np. już na str. 13, pojawia się nieprzetłumaczone na język polski określenie „pipeline”



- str. 14 (wiersze 1 i 3_d): Doktorant używa poprawnego określenia „znak wodny”, jednak już w wierszu 6^g na tej stronie pojawia się nieprzetłumaczone na język polski określenie „trójkąt watermarkingu”; nieprzetłumaczone określenie „watermark” jest użyte w wielu miejscach tekstu rozprawy np. w Założeniu 8 na str. 17
- str. 32 (wiersz 1^g): co oznacza sformułowanie „ramy artykułów”?
- str. 32 (wiersz 12_d): co oznacza określenie „w trybie dość binarnym”?
- str. 187: brak danych o miejscu publikacji artykułu [47]
- str. 189: strona jest zatytułowana „Załączniki”, ale w pracy jest tylko jeden załącznik.

6 Konkluzja

Podsumowując tę recenzję podkreślam, że uzyskane przez Doktoranta wyniki zasługują na pozytywną ocenę. Mają nie tylko wartość poznawczą, ale przede wszystkim duże walory aplikacyjne. Doktorant rozwiązał postawione problemy, dowodząc, że posiadał umiejętności związane z metodyką i metodologią prowadzenia badań naukowych.

Stwierdzam więc, że Pan kpt. mgr inż. Tomasz Walczyna zamieścił w niej wartościowe i oryginalne wyniki prac przeprowadzonych przez Niego pod kierunkiem Promotora rozprawy Pana dr. hab. inż. Zbigniewa Piotrowskiego, profesora WAT.

Oceniam, że Doktorant osiągnął zakładane cele badawcze i wykazał prawdziwość postawionej tezy naukowej. Zatem, przedłożona praca spełnia wymagania stawiane przez stosowne przepisy rozprawom doktorskim i uważam, że Pan kpt. mgr inż. Tomasz Walczyna powinien być dopuszczony do dalszych etapów procedury doktorskiej, w tym do publicznej obrony ocenionej przeze mnie rozprawy.

