

Wydział Informatyki, Elektroniki i Telekomunikacji

INSTYTUT TELEKOMUNIKACJI I CYBERBEZPIECZEŃSTWA

Dr hab. inż. Piotr CHOŁDA, prof. AGH

Kraków, dn. 11 marca 2026 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

**Tytuł rozprawy: AKTYWNA OCHRONA TOŻSAMOŚCI W OBRAZACH TWARZY
Z WYKORZYSTANIEM ODPORNEGO NA MANIPULACJE DEEFAKE ZNAKOWANIA WODNEGO**

Autor rozprawy: KPT. MGR INŻ. TOMASZ WALCZYNA

Promotor rozprawy: DR HAB. INŻ. ZBIGNIEW PIOTROWSKI, PROF. WAT

1. PODSTAWA FORMALNA OPRACOWANIA RECENZJI

Niniejszą recenzję sporządzam w odpowiedzi na datowane 12 grudnia 2025 r. pismo p. dra hab. inż. Zbigniewa Tarapaty, prof. WAT, Przewodniczącego Rady Dyscypliny Naukowej „Informatyka Techniczna i Telekomunikacja” z Wojskowej Akademii Technicznej. W piśmie wyrażono prośbę o sporządzenie recenzji rozprawy doktorskiej na podstawie uchwał tejże Rady nr.: 85/RDN ITIT/2025 (ws. wyznaczenia recenzentów) i 86/RDN ITIT/2025 (ws. powołania komisji doktorskiej).

Przesłana mi w wersji drukowanej praca doktorska napisana przez liczy 191 stron i jest oparta na cyklu publikacji. Pierwsze 7 rozdziałów to napisane po polsku wprowadzenie do cyklu, rozdział 8 zawiera właściwy cykl liczący 11 pozycji, przy czym jedna pozycja jest polskojęzyczna, a pozostałe napisano w języku angielskim. Po dostarczeniu mi rozprawy pod koniec grudnia 2005 r., w umowie zawartej w dniu 13 stycznia br. zobowiązałem się do sporządzenia niniejszej opinii w postępowaniu doktorskim.

2. OCENA STRUKTURY I FORMY ROZPRAWY

Pracę skonstruowano w zasadzie w formie cyklu wcześniej opublikowanych artykułów, przy czym część z nich została umieszczona w czasopiśmie o widoczności międzynarodowej. Na pewno w świetle charakteru przedstawionych badań związanych z praktycznymi zastosowaniami informatyki jest to dobry pomysł.

Struktura rozprawy: główna część została zawarta w rozdziale 8, w którym zamieszczono 11 publikacji. Do każdej z nich najpierw podano krótki komentarz nt. zawartości, roli tekstu z punktu widzenia rozprawy, jak również nt. wkładu Doktoranta (gdyż wszystkie publikacje są współautorskie). Te publikacje to:

- [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.

**Akademia Górniczo-Hutnicza | Wydział Informatyki, Elektroniki i Telekomunikacji
Instytut Telekomunikacji i Cyberbezpieczeństwa**

al. A. Mickiewicza 30, 30-059 Kraków,
tel. +48 12 617 39 37,
e-mail: kt@agh.edu.pl, www.agh.edu.pl

- [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; paperID 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.

Jak sprawdziłem na stronie wydawnictw, dwa ostatnie artykuły zostały już w pełni opublikowane (w rozprawie jeszcze zamieszczono preprinty).

Kluczowy rozdział 8 zawierający cykl został poprzedzony napisanym po polsku wprowadzeniem, którego struktura jest następująca: streszczenia po polsku i angielsku, spis treści, wykaz użytych skrótów, bardzo przydatne glosarium, rozdział 1 „Wprowadzenie” (zawierający motywację pracy, tezę oraz cele szczegółowe służące do wykazania tezy, jak również spis publikacji ujętych w cyklu oraz zwięzły opis struktury rozprawy), rozdział 2 „Kontekst” (streszczający węzłowo główne problemy i techniki dotyczące obszaru pracy), rozdział 3 „Analiza przestrzeni manipulacji” (przybliżający obszar fałszowania w zakresie danych głosowych i obrazowych), rozdział 4 „Opracowanie i adaptacja generatorów *deepfake* do badań nad znakowaniem wodnym” (przybliżenie wyników związanych z wytworzonymi przez Doktoranta metodami wprowadzania manipulacji), rozdział 5 „Metody ukrywania danych w obrazach i ich odporność na *deepfake*” (podsumowanie wyników związanych z wprowadzaniem znaków wodnych), rozdział 6 „Metoda

znakowania wodnego z rekonstrukcją tożsamości” (rekapitulacja kluczowych wyników związanych z propozycją metody tworzenia cyfrowych znaków wodnych, które zapewniają ochronę przez umożliwienie odtworzenie obrazu oryginalnego) i rozdział 7 „Zakończenie” (przede wszystkim odniesienie do tezy i założonych celów częściowych, jak również samokrytyka dotycząca ograniczeń przedstawionych podejść).

Po rozdziale 8 zamieszczono jeszcze w rozdz. 9 bibliografię (ale dotyczącą tylko prac cytowanych we wprowadzeniu, tj. rozdz. 1-7), w rozdz. 10 spis rysunków i tabel (też dotyczący jedynie rozdz. 1-7) oraz oświadczenia o procentowym udziale współautorów publikacji cyklu.

Struktura rozprawy jest zasadniczo poprawna, przy czym w świetle koncepcji oraz tytułu załączenie dwóch pierwszych prac ([1] i [2]) niedotyczących bezpośrednio przetwarzania obrazu nie wydaje się konieczne (choć skądinąd stanowią one cenny materiał przeglądowy). We wprowadzeniu byłoby zasadne umieszczenie jednak wydzielonego rozdziału z pełnym przeglądem literatury przedmiotu. Taki przegląd jest w zasadzie obecny w cyklu jako takim, ale z natury rzeczy ma charakter silnie rozproszony na różne teksty (komentuję tę sprawę jeszcze poniżej). Wprowadzenie stanowi jednak dobry wstęp poprzedzający zapoznanie się z cyklem, porządkuje i uwypukla koncepcje, podaje cele szczegółowe zrealizowane przez pracę itp. Prace w cyklu ułożono niekoniecznie w kolejności publikowania, ale za to w kolejności która umożliwi czytelnikowi obserwację rozwoju koncepcji, w tym przypadku od analizy stanu wiedzy przez zagadnienia fałszowania (tj. manipulowania) z użyciem podejść *deepfake*, aż po metody aktywnej ochrony.

Rezultaty prac zostały przedstawione metodologicznie poprawne i opisane w sposób czytelny. Prace składające się na cykl są wyedytowane z wysoką starannością (również w odniesieniu do jakości językowej), co oczywiście wynika z tego, że na pewno były wielokrotnie rafinowane w procesie recenzji i publikacji (co jest właśnie ogromną zaletą rozpraw opartych na cyklu publikacji). Pewne zastrzeżenia budzi część wstępna, napisana po polsku – tutaj znalazłem nieco potknięć (które podsumowują w jednym z kolejnych punktów). Nie mam jednak żadnych wątpliwości, że Doktorant sprawnie i przekonująco przedstawia swoje koncepcje oraz prezentuje wyniki (np. dbając o zwięzłość, jasność i poprawność redakcyjną rozprawy), dobrze wykorzystując wybraną formę dysertacji.

3. OCENA WARTOŚCI NAUKOWEJ PRACY, W TYM INDYWIDUALNEGO WKŁADU KANDYDATA W POWSTANIE PRACY ZBIOROWEJ

Praca ma charakter konstrukcyjny/wynalazczy, tj. Doktorant proponuje pewne konkretne rozwiązania o charakterze technicznym w odpowiedzi na wyróżnione problemy aplikacyjne. Proponowane pomysły są weryfikowane doświadczalnie. Zawartość teoretyczna nie jest wybita na pierwszy plan, chociaż oczywiście konieczne było opanowanie dziedziny, także w zakresie specyficznych modeli uczenia maszynowego. W samych pracach formalizm matematyczny dotyczy głównie analizowanych wskaźników (funkcje strat na potrzeby uczenia oraz funkcje służące od szacowania jakości działania proponowanych modeli). Charakter rozprawy jest dosyć typowy dla obecnie broniących rozpraw w zakresie informatyki technicznej, gdzie nacisk jest kładziony na twórcze aplikacje uczenia maszynowego.

W odniesieniu do zawartości merytorycznej, należy powiedzieć, że praca istotnie obejmuje (a nawet nieco poza nie wykracza) główne aspekty zawarte w swoim tytule:

- ochrona tożsamości: prace są nastawione na zabezpieczenie przeciwko fałszerstwom, tj. modyfikacjom, które co najmniej sugerują, że przedstawiono inną osobę niż w oryginale (Doktorant zawęży prace głównie do twarzy, ale ma to uzasadnienie);
- aktywna ochrona z wykorzystaniem znakowania wodnego: dotyczy wprowadzenia zabezpieczeń z użyciem dodatkowej informacji (w ramach znaku wodnego, tj. w sposób który nie jest wprost postrzegany), z którego można, przynajmniej częściowo, odtworzyć części obrazu poddane operacji podmiany;
- obrazy twarzy: główna część badań istotnie jest nakierowana na pracę z przedstawieniami twarzy ludzkiej (choć część przedstawionych zagadnień obejmuje również kwestie związane z przetwarzaniem dźwięku i podszywaniem się pod inną osobę z tego punktu widzenia – Doktorant porzuca jednak ten kierunek prac z punktu widzenia rozprawy – merytorycznie jest to uzasadnione, tyle że przyczynia się do pewnej niespójności cyklu);
- odporność na manipulacje z pomocą tzw. *deepfake*, tj. metod podmiany obrazu w oparciu o użycie modeli z grupy tzw. głębokich sztucznych sieci neuronowych.

Tak zdefiniowane zagadnienie jest bardzo dobrze i aktualnie zdefiniowane. Fałszowanie danych z użyciem technik *deepfake* (to słowo nie ma raczej zgrabnego polskiego odpowiednika, więc też je tutaj stosuję) to w tej chwili uciążliwy problem, który w szczególności może prowadzić do ataków na tzw. zwykłego użytkownika. Doktorant proponuje pomysłowe rozwiązania w zakresie ochrony przed tego rodzaju manipulacjami akurat w jednym z aktywnych badawczo obszarów (tj. ochrony tożsamości rozpoznawanej na podstawie obrazów twarzy).

Bliżej cel pracy został zdefiniowany w tezie przedstawionej w rozdz. 1. Teza brzmi: „Modele sieci neuronowych umożliwiają ukrycie reprezentacji wizerunku twarzy w obrazie oraz jego rekonstrukcję po manipulacjach *deepfake*”. Jak to często ma miejsce, teza jest opatrzona modalnością i główna koncepcja jej udowodnienia polega na skonstruowaniu odpowiedniego rozwiązania. Teza odpowiada najistotniejszemu, finałowemu wynikowi, chociaż po drodze Doktorant realizuje również interesujące badania. Nie mam wątpliwości, że tak zdefiniowane zagadnienie naukowe jest warte badań. Na pochwałę zasługuje, że Doktorant dodatkowo opracował szereg celów szczegółowych, przy czym za najbardziej trafne i nieoczywiste uważam następujące (podaję je tutaj własnymi słowami): opracowanie potoku przetwarzania danych w celu tworzenia manipulacji *deepfake* (przede wszystkim przedmiot pracy [3]); zaproponowanie własnych metod wprowadzania w obrazach manipulacji z użyciem podejścia *deepfake* w sposób pozwalający na uciążenie tego procesu, co później przydało się w badaniu metod odporności (przede wszystkim przedmiot prac [4], [6], w tym bardziej szczegółowe badania dotyczące zmian emocjonalnych); opracowanie własnych metod znakowania, w tym umożliwiających rekonstrukcję twarzy po manipulacji (przede wszystkim przedmiot prac [10], [11]). Trzeba powiedzieć, że Doktorant potraktował zagadnienie bardzo szeroko i jakkolwiek w ramach tytułu czy tezy skupia się głównie na zagadnieniach ochrony, to jednak – co cenne i praktykowane w zakresie badań nad bezpieczeństwem – sam proponuje własne metody ataków manipulacyjnych.

Praca jest dobrze osadzona w aktualnej i bogatej literaturze przedmiotu, co widać w odpowiednich sekcjach tekstów cyklu oraz w zamieszczonych listach referencji do poszczególnych prac (szczególnie zamieszczonych w periodykach naukowych). Doktorant ze znanostwem przedstawia wiedzę zastaną oraz odnosi się do pomysłów innych autorów, którzy zajmują się zbliżonymi badaniami. Byłoby cenne w ramach wprowadzenia do cyklu przedstawić samodzielny regularny szeroki opis tła literaturowego, ale jest ono obecne w sposób rozproszony w tekstach cyklu, a nawet można powiedzieć, że pozycje [1]-[3] stanowią taki przegląd. W samych pracach tworzących cykl źródła są analizowane w sposób zwięzły i rzetelny. Nie mam wątpliwości, że Doktorant dysponuje wiedzą nt. obszaru, w którym się porusza.

Jeśli chodzi o samą realizację prac, które stanowią oryginalne osiągnięcie dysertacji, to Doktorantowi udało się rozwiązać postawione zagadnienie oraz dowieść tezy w tym sensie, że przedstawia przekonujące wyniki dotyczące możliwości ukrycia reprezentacji twarzy. Dane są ukrywane przede wszystkim w postaci specyficznego zanurzenia, służącego jako sygnatura czy odcisk palca (uzyskiwanego głównie w oparciu o autokoder). Daje to szansę na odtworzenie twarzy nawet po manipulacjach jej podmiany (ang. *face swap*). Badane są manipulacje dokonywane z użyciem podejść opracowanych przez Doktoranta, ale też do innych reprezentatywnych metod obecnych w aktualnej literaturze przedmiotu (w ogólności Doktorant dużo badań pokazuje w ujęciu porównawczym, co zasługuje na uznanie). Wyniki prac są jak najbardziej satysfakcjonujące, co przynajmniej do pewnego stopnia jest potwierdzone wartościami adekwatnych wskaźników. Pomysłowość koncepcyjna, sposób raportowania uzyskiwanych rezultatów oraz szerokość tematyczna badań wskazują na duże umiejętności Doktoranta w zakresie samodzielnego prowadzenia prac naukowych. Na tle aktualnego poziomu techniki wyniki prezentują się dobrze, co zresztą przecież zyskało uznanie innych badaczy, czego dowodem jest lista opublikowanych w obiegu międzynarodowym artykułów zawartych w cyklu. Ze względu na charakter badań rozprawa może być przydatna może niekoniecznie w zakresie rozwoju samych podstaw informatyki technicznej i telekomunikacji, ale za to wyniki mogą być zdecydowanie przydatne w obszarze zastosowań informatyki. Dotyczy to zarówno przemysłu ITC (potencjał do opracowania metod ochrony użytkowników przed specyficznymi atakami – szczególnie gdyby podejście rozszerzyć o obrazy ruchome), jak również bezpieczeństwa (zabezpieczenie przed specyficznymi sposobami oszustw itp.). Bez wątplenia takich zastosowań praktycznych można oczekiwać od pracy doktorskiej w obszarze współczesnej techniki. Nie mam istotnych zastrzeżeń w zakresie podejścia i metodologii – przyjęte założenia są dobrze uzasadnione i trafne. Chcę jednak zwrócić uwagę na kilka kwestii, które wymagałyby być może głębszego namysłu, a na pewno stanowią dobry obszar do dyskusji w trakcie ewentualnej obrony doktoratu:

- Poza zagadnieniami przetwarzania specyficznych danych (głównie obrazowych) praca dotyczy oczywiście problematyki uczenia maszynowego. Z tego punktu widzenia pożądanym byłoby głębsze opracowanie różnych kwestii pod kątem formalizmu. Z tego punktu widzenia brak mi prezentacji używanych modeli matematycznych od strony opisu funkcjonalnego, co zwiększałoby czytelność koncepcji. Dawałoby to też szansę na bardziej przekonujące, bo oparte wprost na teorii statystycznego uczenia maszynowego, wykazanie że przedstawione podejścia są generalizowalne i działają poprawnie. To jest w ogóle szersza kwestia metodologiczna i nie neguję sensowności

oraz zasadniczej poprawności oraz akceptowalności powszechnie stosowanego podejścia, które po prostu dowodzi w sposób eksperymentalny z użyciem szerokiego (a nawet bardzo szerokiego, jak w przypadku tego doktoratu) zakresu przypadków przykładowych, że metoda działa w sposób oczekiwany i pożądanym (co jest oczywiście dodatkowo podparte przekonującym uzasadnieniem intuicji stojących za zastosowaniem konkretnych modeli). Byłoby jednak zasadne spróbować podejść do badań od tej strony. W tym przypadku byłoby zapewne również zasadne pogłębienie analizy nt. przestrzeni zanurzeń (wymiarowość, wizualizacja, kwestia regularyzacji), a biorąc pod uwagę, że używane są tzw. modele głębokie, wesprzeć opis wyników z użyciem procedur XAI/XML w celu zwiększenia ich interpretowalności (wyjaśnialności).

- Jeśli chodzi o samo przekonujące wykazanie aplikowalności i skuteczności proponowanych podejść, zarówno w zakresie manipulacji jak i ochrony przed nią, nasuwa mi się kwestia zakresu użycia mierzalnych wskaźników, które istotnie mogłyby wesprzeć uzasadnienie, że uzyskano pozytywne efekty. Tymczasem w zasadzie kwestii stosowanych wskaźników więcej miejsca poświęcono głównie w pracach [4], [6], [11] oraz przedstawiono z tego punktu widzenia też wartościową dyskusję w pracach [10] i [11] (znajduje to też odbicie w podrozdz. 6.3, który jest szczególnie cenny w zakresie oceny istotności statystycznej badań), ale skądinąd nacisk nie jest kładziony na ten problem w niektórych innych pracach cyklu. To jest w ogóle trudne zagadnienie w zakresie rzetelnej kwantyfikacji, gdyż skądinąd być może w wielu przypadkach efektywność manipulacji czy też dostarczonej metody obrony przed nią nie powinna być badana z użyciem wskaźników obiektywnych, ale raczej powinna być analizowana na podstawie badań z użyciem grupy ankietowej, czyli przy przyjęciu oceny odbioru subiektywnego (faktem jest że Doktorant zwraca uwagę na to zagadnienie, przynajmniej przedstawiając tło literaturowe w pracy [1]), co przecież jest praktykowane w przypadku różnego rodzaju prac nad jakością postrzeganej obsługi (QoE, *quality of experience*) itd. To oczywiście otwierałoby odrębny obszar badań (zupełnie inna metodologia), niemniej jednak mam pewien niedosyt, gdy oglądam niektóre wyniki i czytam związane z nimi analizy w tekstach cyklu, np. rys. 2-4 w pracy [4], rys. 3 albo A1 w pracy [6], czy rys. 7 pracy [11], gdzie sam nie mam wrażenia skuteczności wprowadzonej manipulacji, ew. odtworzenia z użyciem cyfrowego znaku wodnego. W ogóle w wielu pracach Doktorant zamieszcza liczne przypadki, które oczywiście mają walor ilustracyjny, natomiast faktycznie dopiero w ostatnich pracach cyklu to zagadnienie jest w sposób bogatszy opisane odpowiednimi wskaźnikami.
- Oczywiście uzysk merytoryczny z doktoratu należy widzieć głównie w pewnych propozycjach metodologicznych, a zastosowane modele można potraktować jako opcjonalne elementy wypełniające z mniejszą lub większą koniecznością poszczególne kroki odpowiednich schematów. W odniesieniu do tej dysertacji doceniam kreatywne połączenie opracowanych przez innych badaczy modeli czy metodyk w odniesieniu do specyficznych zastosowań. Sądzę jednak, że zakres stosowanych przez Doktoranta modeli powinien zostać poszerzony czy też poddany głębszej

krytyce. Na przykład bardzo dużą rolę w obszarze badań, głównie w zakresie metod ochrony, zajmuje specyficzny autokoder – U-Net (zresztą on też jest używany w manipulacjach). Jest on wprowadzany od lat znany, dobrze przebadany i świetnie sprawdza się w zakresie przetwarzania obrazu (co zresztą Doktorant dokumentuje w analizie przedstawionej głównie w pozycji [3]), ale jednak jest to konkretny, wyróżniony model, a byłoby pożądanym oczekiwać wyników jak najbardziej ogólnych – Doktorant wykazał tutaj niepokojąco wysoki poziom przywiązania do konkretnego podejścia.

Powyższe punkty należy potraktować nie jako krytykę istotnych aspektów pracy, a raczej jako przyczynek do naukowej dyskusji w ogólności cennych wyników.

W podsumowaniu mojej opinii nt. dorobku Doktoranta warto przywołać sam cykl z punktu widzenia samego charakteru jakościowego. Tutaj na szczególną uwagę zasługuje obszerna publikacja w czasopiśmie IEEE Access [11], jak również pięć dużych artykułów w czasopismach MDPI (Applied Sciences oraz Sensors) czy dwa referaty na konferencjach o pewnej widoczności międzynarodowej. W szczególności teksty pochodzące z periodyków to obszerna prace wskazujące na dużą dojrzałość badawczą. To jest dobry dorobek przed uzyskaniem stopnia doktorskiego, tym bardziej że Doktorant ma, jak udało mi się sprawdzić, jeszcze inne publikacje na swoim koncie. Deklarowany przez Doktoranta (i potwierdzony przez współautorów) indywidualny wkład w poszczególne publikacje jest na typowym poziomie dotyczącym prac w małych zespołach badawczych i potwierdza odpowiednio wysokie zaangażowanie.

4. ZASTRZEŻENIA I UWAGI KRYTYCZNE

Moim zdaniem, praca nie ma istotnych słabych stron, w szczególności takich które by ją dyskwalifikowały, czy podważały całość przedstawionych wyników. Każdą koncepcję czy tekst można wydoskonalić, więc tutaj zbieram i podsumowuję wyrażone we wcześniejszych punktach uwagi krytyczne:

- Od strony merytorycznej mam trzy uwagi o charakterze ogólnym:
 - Nadmierne ograniczenie opisu formalnego używanych modeli statystycznego uczenia maszynowego.
 - Kwestia braku adekwatnego skupienia na metodologii subiektywnych badań jakości obserwowanej w obszarze, w którym faktycznie dużo może zależeć od wrażeń odbiorcy.
 - Przywiązanie do konkretnych modeli, które warto byłoby poddać głębszej krytyce oraz zwiększyć wariantowość ich użycia (też poszukać bogatszego zestawu alternatyw itd.).
- Nieobecność w rozprawie jednolitego przeglądu literatury. Ze względu na fakt, że w ogóle elementy przeglądu są zawarte w poszczególnych pracach cyklu, a nawet w dużym stopniu teksty [1]-[3] mogą być potraktowane jako przegląd stanu wiedzy, tę uwagę uznaję nawet bardziej za uwagę o charakterze w zasadzie redakcyjnym.
- Potknięcia (głównie edycyjne) w zakresie części wprowadzającej w rozdziałach 1-7 (oraz w odnośnym spisie bibliografii w rozdz. 9). Tutaj wymieniłem tylko kilka przykładów:
 - nie zawsze konsekwentne tłumaczenie pojęć anglojęzycznych (np. w glosariuszu na str. 13 występuje „pipeline”, potem zamiast

tego słowa jest używane pojęcie „potoku”, mimo że ono akurat w glosariuszu nie wystąpiło w tym kontekście) lub ich różnoraki zapis (np. przeważnie „deepfake” ale np. na str. 19 znajdują „DeepFake”);

- zrozumiałe, ale nieco irytujące przez brak elegancji, kolokwializmy typu „uczyć pod konkretny kanał” na str. 17 albo „działają w trybie dość binarnym” na str. 32;
- niepotrzebne użycie anglicyzmów (semantyczny, np. „zmapowano” zamiast „odwzorowano” na str. 31 czy strukturalnych jak „odporność na nieliniowe przekształcenia” zamiast „...przekształcenia nieliniowe” na str. 28);
- niedostatki edycyjne, np. przeniesienie tytułu rys 1.1 na inną stronę niż zawartość opisywanego rysunku (str. 17-18); kilkukrotny zapis „Rys.” dużą literą (np. str. 17, 25); brak pełnych danych bibliograficznych (np. dla pozycji 2, 5, 7, 24... na str. 184-185).

Opisane wady w żaden sposób nie podważają mojej wysokiej oceny całości przedstawionej rozprawy doktorskiej.

5. PODSUMOWANIE

Moja ocena pracy jest jednoznacznie pozytywna. Oceniany dorobek bez wątpienia spełnia wymagania określone w art. 187 ustawy Prawo o szkolnictwie wyższym. Rozprawa prezentuje wysoki poziom wiedzy Doktoranta w zakresie dyscypliny informatyka techniczna i telekomunikacja (przede wszystkim w obszarze przetwarzania obrazów i dźwięku oraz użycia modeli uczenia maszynowego, przede wszystkim sztucznych sieci neuronowych – wszystko to stanowi istotny obszar w dyscyplinie). Przedmiotem rozprawy jest szereg oryginalnych rozwiązań problemu naukowego w zakresie ataków manipulacyjnych typu *deepfake*, przede wszystkim na zmianę tożsamości osób, jak również w zakresie obrony przed takimi atakami. Jest to istotny aspekt dotyczący współczesnego bezpieczeństwa użytkowego cyberprzestrzeni. Przedstawione wyniki w akceptowanej przez ustawę postaci (głównie cyklu/zbioru opublikowanych i powiązanych tematycznie artykułów naukowych) dowodzą umiejętności samodzielnego prowadzenia pracy naukowej.

Biorąc pod uwagę bogactwo publikacji, szczególnie w zakresie periodyków międzynarodowych, moim zdaniem rozprawa spełnia wymagania z wyraźnym nadmiarem. W związku z wszystkimi podanymi powyżej argumentami wnioskuję o dopuszczenie Doktoranta do publicznej obrony ocenianej tutaj rozprawy.



Piotr Chołda