AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Wydział Informatyki, Elektroniki i Telekomunikacji

KATEDRA TELEKOMUNIKACJI

Dr hab. inż. Piotr CHOŁDA

Kraków, dn. 19 lipca 2019 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

Tytuł rozprawy: *Skryta transmisja danych w systemie cyfrowej telewizji naziemnej DVB-T*
Autor rozprawy: *mgr inż. Piotr Lenarczyk*

1. WSTĘP

Niniejsza recenzja została przygotowana na potrzeby postępowania ws. nadania stopnia doktora nauk technicznych, prowadzonego przez Wydział Elektroniki Wojskowej Akademii Technicznej (WAT).

Pełną dokumentację dot. rozprawy doktorskiej, wraz z informacją o powołaniu na recenzenta rozprawy przez Radę Wydziału Elektroniki WAT, otrzymałem od Pana Profesora Andrzeja P. Dobrowolskiego, Dziekana Wydziału Elektroniki WAT, w dn. 8 lipca 2019 r.

Oceniana rozprawa została napisana przez Pana magistra inżyniera Piotra Lenarczyka. Nosi tytuł „Skryta transmisja danych w systemie cyfrowej telewizji naziemnej DVB-T" i została napisana w całości po polsku (poza angielskojęzycznym streszczeniem, *Abstract*, zamieszczonym na str. 3). Promotorem doktoratu jest Pan płk. dr hab. inż. Zbigniew Piotrowski, prof. WAT, zaś promotorem pomocniczym Pan mjr dr inż. Jan Kelner.

Dostarczona mi rozprawa doktorska liczy 118 stron. Składa się z sześciu rozdziałów: 1. Wstęp (str. 18-35), 2. Teza i cel pracy (str. 36-37), 3. Projekt i implementacja algorytmów steganograficznych (str. 38-54), 4. Testy algorytmu sygnałowego (str. 55-82), 5. Podsumowanie (str. 83-84), 6. Literatura (str. 85-99). Oryginalne wyniki zasadniczo zawarto w rozdziałach 3-5. Bibliografia, ułożona w kolejności cytowania, liczy 201 pozycji. Uzupełnieniem merytorycznym pracy są: zamieszczony na początku wykaz skrótów i oznaczeń (str. 7-17) oraz zawarte na końcu — spisy rysunków, tabel, skorowidz, wykaz dorobku publikacyjnego autora oraz wykaz cytowań. Pracę uzupełniają także dwa załączniki: pierwszy traktuje nt. testu niedostrzegalności algorytmu steganograficznego (w związku z podrozdziałem 4.2), natomiast drugi (zawarty na płycie DVD) zawiera materiały pracy doktorskiej (system operacyjny ubuntu z oprogramowaniem wytworzonym przez Autora).

Akademia Górniczo-Hutnicza | Wydział Informatyki, Elektroniki i Telekomunikacji
Katedra Telekomunikacji
al. A. Mickiewicza 30, 30-059 Kraków,
tel. +48 12 617 39 37, fax +48 12 634 23 72
e-mail: kt@agh.edu.pl, www.agh.edu.pl

2. **CEL BADAŃ (W ODNIESIENIU DO TEZY ROZPRAWY). Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora?**

Zagadnienia podjęte przez Doktoranta dotyczą steganografii, tj. ukrywania transmisji danych w innym kanale danych. Zagadnienia tzw. skrytej transmisji danych cieszą się zainteresowaniem badaczy od około 20 lat. Zagadnienie jest ważne, szczególnie z punktu widzenia służb specjalnych (cywilnych i wojskowych), stąd nie dziwi podjęcie tematu na Wojskowej Akademii Technicznej, zresztą pod opieką specjalistów wysokiej klasy doświadczonych w tego rodzaju badaniach.

Wprawdzie zagadnienia steganografii są szeroko badane, ale na uwagę zasługuje, że Doktorant podjął problematykę dotychczas bardzo słabo eksploatowaną w literaturze, tj. skrywanie transmisji w systemach cyfrowej telewizji naziemnej standardu DVB-T. Biorąc pod uwagę coraz większe rozprzestrzenianie tego rodzaju sposobu rozsiewania danych, propozycja dostarczona w ramach rozprawy zasługuje na uznanie.

Doktorant bardzo jasno wyróżnił tezę rozprawy, poświęcając jej rozdział 2. Sformułowana przez niego teza brzmi: „Możliwe jest zestawienie jednokierunkowego, efektywnego stegokanału dla ustalonych warunków transmisji naziemnej telewizji cyfrowej". Pojęcie stegokanału jednokierunkowego jest jasne, natomiast pojęcie „efektywnego stegokanału" zostało następnie scharakteryzowane przez szereg właściwości: 1. bezstratny; 2. o minimalnej przepływności 5 b/s; 3. zapewniający niedostrzegalność stegokontentu określoną wartością szczytowego stosunku sygnału do szumu (PSNR) na poziomie co najmniej 35 dB; 4. zapewniający niewykrywalność z użyciem steganoanalizy histogramowej oraz testu statystycznego chi kwadrat. Natomiast pojęcie „ustalonych warunków transmisji" zostało objaśnione jako dotyczące: 1. bezbłędnej transmisji kanałem komunikacyjnym DVB-T; 2. z założonym niezmiennym formatem wejściowego sygnału wideo.

Tak zdefiniowana wraz z uzupełnieniem ***teza jest jasno postawiona***. Biorąc pod uwagę wyżej podane sformułowanie opatrzone modalnością egzystencjalną, zostało ono udowodnienie przez Doktoranta oczywiście przez zaproponowanie i opisanie odpowiedniego algorytmu steganograficznego. Algorytm ten zapewnia skrytą transmisję w danych wideo przekazywanych z użyciem standardu DVB-T (czyli właśnie standardu naziemnej telewizji cyfrowej). Wprawdzie użycie tego konkretnie standardu nie wynika wprost z tezy pracy i byłoby możliwe oparcie się na innych standardach transmisji telewizji cyfrowej, ale zawężenie do tego standardu jest jak najbardziej dopuszczalne, szczególnie w świetle praktyki, która ma miejsce w Polsce.

3. **CHARAKTER ROZPRAWY. Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

W związku z tym, że Doktorant dowodzi tezy, opierając się przede wszystkim na autorskim opracowaniu algorytmów steganograficznych, z których jeden zostaje poddany dokładniejszym testom obiektywnym i subiektywnym, można stwierdzić, że praca ma charakter przede wszystkim konstrukcyjny (tj. projektowy). Jest to sytuacja typowa (i prawidłowa) w odniesieniu do prac, w których sformułowano tezę o charakterze egzystencjalnym. Biorąc pod uwagę, że duża część pracy skupia się na podaniu wyników testów, które mają dowieść, że zaproponowany algorytm spełnia właściwości założone w tezie (czy też bardziej szczegółowo — w klaryfikacji

niektórych z kluczowych pojęć, wchodzących w jej skład), praca zawiera również silny komponent doświadczalny. To oczywiście nie dziwi, biorąc pod uwagę że dotyczy nauk techniczno-inżynieryjnych. Można więc stwierdzić, że element doświadczalny służy prawidłowemu metodologicznie dla tej dziedziny wzmocnieniu koncepcji konstrukcyjnej. Biorąc więc pod uwagę ***charakter konstrukcyjno-doświadczalny***, praca ma przede wszystkim walor empiryczny.

Jeśli chodzi o zawartość analityczno-teoretyczną, to jest ona zredukowana do minimum i, jak się zdaje, intencją Doktoranta nie było prowadzenie intensywnych prac teoretycznych, w każdym razie nie zostały one odnotowane w rozprawie w szerszym zakresie. Warto tu jednak zwrócić uwagę, że końcowe partie rozprawy, dotyczące pewnych aspektów obliczeniowych mają charakter przeglądowo-analityczny, zaś w odniesieniu do testów obiektywnych Autor posłużyć się wskaźnikami, które często wspierają prace teoretyczne.

4. **SPOSÓB PRZEPROWADZENIA ANALIZY ŹRÓDEŁ. SPOSÓB SFORMUŁOWANIA WNIOSKÓW WYNIKAJĄCYCH Z ANALIZY ŹRÓDEŁ. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczący o dostatecznej wiedzy Autora. Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?**

Lista bibliografii liczy 201 pozycji, przeważnie angielskojęzycznych. Są to prace funkcjonujące w obiegu międzynarodowym, duża część z nich prezentuje uznane wyniki w dziedzinie objętej zainteresowaniem Autora rozprawy doktorskiej i nie dostrzegłem istotnych braków w wyborze literatury (z małym zastrzeżeniem, o którym niżej). ***Dobór tych prac wskazuje na rozeznanie Doktoranta w obszarze steganografii i świadczy o jego znajomości bardzo różnych podejść***. Na pewno Doktorant jest świadom dokonań raportowanych w literaturze światowej oraz wie, jaki jest obecny stan wiedzy.

Należy tutaj jednak sformułować kilka uwag krytycznych:

- Wprawdzie Autor przedstawia ciekawe ujęcie klasyfikacji metod steganografii oraz steganoanalizy i bez wątpienia wskazują one na dobrą znajomość zagadnień, ale w zasadzie w pracy nie wyodrębniono oddzielnego rozdziału, który szczegółowo i wnikliwie podsumowywałby wnioski płynące z tej analizy. Takie wnioski są obecne, jednak bardzo rozproszone w tekście rozprawy i nie zawsze jest jasne, czy podejmowane przez Doktoranta konkretne decyzje związane z realizacją elementów proponowanych algorytmów mają w nich faktyczne umocowanie.
- Wprawdzie Doktorant zwraca uwagę na większość istotnych tekstów, które dotyczą tematyki pracy, ale w zasadzie nie dokonuje głębszej analizy, tj. nie przedstawia szczegółowo sposobów radzenia sobie przez poszczególnych badaczy z problemami konstrukcyjnymi; w szczególności odniesienia do literatury nie wskazują jednoznacznie na źródła inspiracji, zarówno w zakresie wyboru szczegółów tezy (tj. odniesień doprecyzowujących poszczególne pojęcia), jak również w zakresie selekcji sposobów uporania się z przedstawionym zagadnieniem. Nie zawsze jest też jasne, według jakiego klucza wybrano konkretnych reprezentantów poszczególnych poddziedzin.
- Zdawkowo potraktowano kwestię praktycznych zastosowań steganografii, chociaż trzeba zwrócić uwagę, że w przypadku akurat tej dziedziny z jej

natury wynika, że możemy nie mieć zbyt dobrego rozeznania w kwestii otaczania nas przez działające stegosystemy.

- Biorąc pod uwagę, że rozprawa została przedstawiona w roku 2019 dziwi nieco fakt, że bogatszy zbiór przywoływanych źródeł kończy się jak gdyby na 2016 roku. Prac pochodzących z lat 2017-2018 jest zaledwie garstka, a przecież dziedzina nie zamarła. Myślę, że z tego punktu widzenia brakuje co najmniej niektórych wartościowych i nowszych prac przeglądowych, jak choćby: Mehdi Hussain and Ainuddin Wahid Abdul Wahab and Yamani Idna Bin Idris and Anthony T.S. Ho and Ki-Hyun Jung, *Image steganography in spatial domain: A survey*, Signal Processing: Image Communication, vol. 65, pp. 46–66, 2018.

5. ROZWIĄZANIE PRZEDSTAWIONEGO ZADANIA, WŁAŚCIWOŚCI PRZYJĘTYCH METOD I ZAŁOŻEŃ. Czy Autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

W celu udowodnienia założonej tezy Doktorant przeprowadził następujące prace, przedstawione w rozprawie doktorskiej:

1. Opracował dwa algorytmy steganografii wideo w sygnale DVB-T (chociaż szczegółowo skupił się na jednym z nich, tzw. algorytmie sygnałowym).
2. Dla wybranego algorytmu steganograficznego przeprowadził obiektywne testy jakościowe.
3. Dla wybranego algorytmu steganograficznego przeprowadził subiektywne testy jakościowe.
4. Opracował program umożliwiający przesłanie zbioru stegofilmów w kanale naziemnej telewizji cyfrowej DVB-T oraz odniósł się do kwestii sprzętowo-programistycznych.

W zakresie poszczególnych punktów należy powiedzieć, że:

Ad. 1. Opracowane algorytmy zostały przedstawione w rozdziale 3. Doktorant zaproponował dwa algorytmy. Pierwszy z nich, tzw. algorytm warstwy protokołu (podany w podrozdziale 3.1) polega na intencjonalnym wprowadzaniu przekłamań do strumienia danych w celu zapisu skrytej transmisji. Aczkolwiek tego rodzaju koncepcje już pojawiały się w literaturze, tutaj Autor zaproponował zastosowania w specyficznym standardzie. Przedstawił schemat blokowy proponowanego algorytmu oraz ilustrację jego działania. Zrezygnował jednak z bliższej analizy oraz testów, nie skupiając się już na tym rozwiązaniu w dalszej części pracy. Rezygnację z bliższego przebadania tego algorytmu Doktorant tłumaczy kwestią wprowadzania dodatkowych przekłamań przez ten algorytm, co zapewne kłóci się z przyjętym założeniem nt. warunków transmisji, tj. jej bezbłędnością w kanale komunikacyjnym. W związku z tym, że do kwestii założeń klaryfikujących tezę odniosę się na końcu tego fragmentu recenzji, zostawiam w tej chwili to zagadnienie.

Główny nurt doktoratu jest poświęcony drugiemu z algorytmów, który został nazwany „algorytmem sygnałowym". W celu jego wprowadzenia Doktorant reprezentuje sygnał w postaci wielowymiarowej i na takiej postaci proponuje dokonywać odpowiednich operacji. Następnie przedstawia czytelnie (z użyciem schematów przebiegu algorytmów) sposób działania odpowiedniego kodera oraz dekodera steganograficznego, z których pierwszy odpowiada za skrywanie transmisji, a drugi za jej pozyskiwanie. Ukrywanie transmisji zasadniczo polega na operowaniu na współczynnikach transformaty kosinusowej jednego ze składników

obrazu, co jest podejściem znanym i uważanym za poprawne. W przypadku tego algorytmu Doktorant odniósł się w bogatszy sposób do tła naukowego, tj. porównał parametry zaproponowanego algorytmu z parametrami innych algorytmów znanych z literatury. Jak rozumiem, porównanie ma charakter przede wszystkim dyskusji, gdyż Doktorant nie zdecydował się zaimplementować innych algorytmów, żeby w praktyce pokazać ich działanie na tle swojego algorytmu. Do jakiegoś stopnia można zrozumieć taką decyzję, choćby dlatego że porównywane algorytmy nie w każdym przypadku mają dużo wspólnego z transmisją danych w założonym standardzie DVB-T.

Następnie, w rozdziale 4, zostały rozwinięte i zrealizowane przedstawione wcześniej punkty 2-4.

Ad. 2. Doktorant przeprowadził testy obiektywne w odniesieniu do działania algorytmu sygnałowego. Oczywiście samo pojęcie testów obiektywnych jest mocno obciążone semantycznie, więc Autor rozprawy doprecyzował w tekście, co pod nim rozumie, do czego oczywiście ma prawo. Chodzi w tym przypadku o pokazanie niepodatności algorytmu na steganoanalizę histogramową oraz test statystyczny chi kwadrat. Steganoanaliza histogramowa została oparta na szeregu uznanych wskaźników (np. współczynnik korelacji Pearsona, błąd średniokwadratowy, szczytowy stosunek sygnału do szumu itd.). Prezentowana analiza wydaje się zasadniczo poprawna, chociaż mam kilka wątpliwości dotyczących opisu wyników, zawartych w tabelach 4 i 5 (piszę o nich niżej).

Ad. 3. Autor przeprowadził na grupie 17 osób testy subiektywne (takie badania są dosyć drogie, w związku z czym można zrozumieć niewielką populację), które miały na celu stwierdzenie, że wprowadzanie stegokontentu jest niedostrzegalne. Ta część pracy dotyczy zresztą ważnych i aktualnych zagadnień tzw. QoE (*Quality of Experience*), tj. jakości postrzeganej przez użytkownika. Co więcej, badania takie, z natury swojej interdyscyplinarne, są często pomijane w pracach związanych ze steganografią; podejście przyjęte przez Doktoranta jest więc nowatorskie i jako takie warte uznania. Autor rozprawy posługuje się generalnie wskaźnikiem (nienazwanym przez siebie) typu MOS (*Mean Opinion Score*). W zakresie metodologii testów subiektywnych Doktorant posłużył się rekomendacjami dotyczącymi badań tego rodzaju na sygnale wideo. Z zaprezentowanych wyników można wywnioskować, że zaproponowany algorytm z punktu widzenia niedostrzegalności istotnie się sprawdza. Ciekawym i wartościowym dodatkiem do rozprawy jest również arkusz samego testu podany w Załączniku 1.

Ad. 4. Doktorant skonstruował całe środowisko laboratoryjne, z użyciem którego przedstawił działanie poprawnie skonfigurowanego systemu transmisji, który używa zaproponowanego algorytmu sygnałowego. W szczególności zaprezentowano testy przesyłania sygnału wzorcowego i przesyłania stegosygnałów. Autor rozprawy zrezygnował niestety z użycia transmisji bezprzewodowej, która urealistyczniałaby zaprezentowany eksperyment. Można zrozumieć takie podejście, ponownie biorąc pod uwagę założenie dotyczące bezbłędności transmisji (chociaż Autor rozprawy tłumaczy tę kwestię raczej kwestiami administracyjnymi, tj. brakiem zezwoleń na transmisję — nie wydaje mi się to rozumowaniem poprawnym, bo przecież chodzi tylko o środowisko laboratoryjne).

Do wyników opisywanych w ramach tego punktu zaliczyłbym także przedstawione w podrozdziale 4.5 rozważania dotyczące praktycznych aspektów obliczeń numerycznych. Autor zawarł w nich bardzo dużo ciekawych koncepcji odnoszących się do strony informatycznej realizacji przetwarzania sygnałów na potrzeby steganografii. Widać, że tematyka jest przez niego bardzo dobrze rozpoznana, co

zresztą potwierdzają niektóre z jego publikacji. Jest to jakby jeszcze jeden wymiar pracy, poza propozycją algorytmu i jego analizą z użyciem testów obiektywnych i subiektywnych. Autor rozważa zarówno zagadnienia programistyczne, jak również sprzętowe. Niestety, podrozdział ten nie do końca jest zintegrowany z wcześniejszą częścią pracy, co najmniej w takim rozumieniu, że Doktorant, który wprawdzie podaje pewną liczbę wyników numerycznych (np. dotyczących szybkości przetwarzania danych przez procesory, które mogą wspierać odpowiednią obróbkę danych), nie uzyskał ich — na ile rozumiem prezentację wyników — porównując działanie różnych opcji z użyciem algorytmu, który opracował (bo byłoby pożądane). W ogólności brak tutaj też rozważań o charakterze algorytmicznym, które bez wątpienia są związane z kontekstem informatycznym, a które wzmocniłyby rozprawę od strony teoretycznej.

Podsumowując moją ocenę przedstawionego sposób podejścia do problemu, mogę stwierdzić, że zasadniczo ***przyjęte metody są używane poprawnie i w taki sposób, w jaki używają ich badacze publikujący w obszarze steganografii***. Z punktu widzenia całości zaprezentowanych badań krytycznie odniósłbym się tylko do pewnej niekonsekwencji w podejściu do różnych pomysłów, które Doktorant przedstawił w rozprawie. Część z nich nie jest po prostu rozwinięta (tzw. algorytm warstwy protokołu z podrozdziału 3.1 oraz rozważania dotyczące wykorzystania sprzętu z podrozdziału 4.5), a także nie została w pełni zintegrowana z główną propozycją, służącą do udowodnienia tezy, tj. z badaniami dotyczącymi algorytmu sygnałowego (np. algorytm warstwy protokołu mógł także zostać poddany testom obiektywnym i subiektywnym; zaś różne rozwiązania dotyczące sprzętu i oprogramowania zyskałyby na prezentacji, gdyby wyniki podano na podstawie implementacji zaproponowanego algorytmu sygnałowego). Faktem jest, że w niektórych przypadkach decyzję nt. rezygnacji z pewnych aspektów badawczych można zrozumieć w kontekście przyjętych założeń.

W odniesieniu do założeń opisujących tezę, stwierdzam że zasadniczo są one poprawne, a Doktorant dowiódł, że udało mu się do nich dostosować. Dotyczy to przede wszystkim założeń odnoszących się do „efektywnego stegokanału", tj. jego bezstratności, zapewniania niedostrzegalności i niewykrywalności (dowiedzione z użyciem testów obiektywnych i subiektywnych). Moich wątpliwości nie budzi również założenie o niezmiennym formacie wejściowego sygnału wideo, dotyczące „ustalonych warunków transmisji". Zastanowienie budzą natomiast dwa inne założenia:

- minimalna przepływność: 5 b/s (dot. „efektywnego stegokanału");
- bezbłędna transmisja (dot. „ustalonych warunków transmisji");

Przyjęcie tych założeń nie jest zasadniczo niesłuszne, gdyż w przypadku steganografii przepływności często są na niskim poziomie, a przyjęcie braku zakłóceń w transmisji może być zasadne. Chcę jednak zwrócić uwagę, że być może relaksacja tych ograniczeń prowadziłaby do uzyskania wyników jeszcze bardziej ambitnych (np. znaczne podwyższenie użyteczności stegokanału przy zwiększonej przepływności), chociaż z drugiej strony wymagałaby przebadania algorytm warstwy protokołu oraz bogatszych (i bardziej realistycznych) testów przesyłania sygnału.

W podsumowaniu stwierdzam, że ***opierając się na poprawnie użytej metodologii, Doktorantowi udało się udowodnić postawioną przez siebie zasadną tezę rozprawy*** „Możliwe jest zestawienie jednokierunkowego, efektywnego stegokanału dla ustalonych warunków transmisji naziemnej telewizji cyfrowej".

W tej części mojej recenzji przy okazji chcę zwrócić uwagę na kilka nieścisłości merytorycznych, które znalazłem w rozprawie:

- Str. 7: nie jestem pewien, czy pojęcie „Deep Belief Network" na pewno można poprawnie przetłumaczyć jako „model graficzny sieci neuronowej".
- Str. 21, 39-40: zagadnienia dotyczące kodowania korekcyjnego opartego na kodzie Reeda-Solomona — przypuszczam że w ogólnym opisie zawartym na str. 21 powinno mówić się o bajtach lub słowach (a nie bitach, jak jest w przypadku np. „204 bitów"), ponadto w podrozdziale 3.1 Autor używa pojęcia odległość (błędu) Reeda-Solomona; czy nie chodzi jednak o odległość Hamminga?
- Str. 44: Autor przedstawia swoje ujęcie sygnału wielowymiarowego, np. z użyciem wzoru (2), nie jest jednak jasne w jaki sposób możliwe jest przejście z sumy wektorów o niższych wymiarach na wektor o wyższym wymiarze.
- Str. 58: Wskaźnik podobieństwa strukturalnego przedstawiony z użyciem wzoru (10) nie zawiera zmiennych M, N, ale zostały one użyte w jego opisie w kontekście rozmiaru splatanego filtru Gaussa — jak należy to interpretować w odniesieniu do zmiennych m, n?
- Wyniki zamieszczone w tabelach 4-5:
  - Nie jest dla mnie jasne znaczenie wierszy oznaczonych przez „uwzględniono [%]", tym bardziej że prawie we wszystkich przypadkach wartość wynosi 100.
  - W niektórych przypadkach wartość wariancji podano jako 0, przy czym najwyraźniej wartości minimalne i maksymalne różniły się. Jak to jest możliwe? Czy powodem jest fakt, że w tabelach podano jedynie wartości do 4 miejsca po przecinku, a wariancja po prostu musi być w tych przypadkach wyrażona z większą dokładnością?

6. ORYGINALNOŚĆ ROZPRAWY, SAMODZIELNY DOROBEK AUTORA, POZYCJA ROZPRAWY W STOSUNKU DO STANU WIEDZY (POZIOM TECHNIKI) PREZENTOWANEGO W LITERATURZE ŚWIATOWEJ. Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek Autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?

Oryginalności rozprawy upatruję głównie w podjęciu problematyki skrywania transmisji w danych przesyłanych z użyciem standardu DVB-T, przy czym oczywiście najbardziej wartościowe jest opracowanie przez Doktoranta tzw. algorytmu sygnałowego. ***Algorytm ten stanowi wartościowy i samodzielny dorobek Autora rozprawy w obszarze bezpieczeństwa systemów telekomunikacyjnych***. W odniesieniu do tła literatury światowej, należy zwrócić uwagę, że problematyka tego rodzaju była podejmowana bardzo rzadko. Steganografia zajmująca się skrytą transmisją ma specyfikę polegającą na tym, że należy spodziewać się, że jej wyniki niekoniecznie są publicznie prezentowane (bez wątpienia z natury tej dziedziny wynika, że na przykład w przeciwieństwie do kryptografii cywilnej nie obowiązuje w niej nic przypominającego Zasadę Kerckhoffsa), więc oczywiście Autorowi i mnie nie pozostaje nic innego, jak odniesienie do literatury, do której wszyscy mają dostęp. Z tego punktu widzenia, ***Doktorant przedstawia rozwiązanie nowe na tle rozwiązań dyskutowanych w literaturze światowej***. Przyjęta metodologia związana z opracowaniem

algorytmu, jak również z poddaniem go testom obiektywnym i subiektywnym, mieści się w poziomie jakości porównywalnym z większością publikacji na temat steganografii.

Chciałbym tutaj jednocześnie zwrócić uwagę na dorobek Autora wspierający samą rozprawę doktorską (zapoznałem się również z publikacjami Autora, które przywołano na str. 108-109), a który wymaga pochwały w co najmniej dwóch punktach:

- Doktorant jest już autorem dwóch publikacji, które ukazały się w periodykach o zasięgu międzynarodowym. Są to uznane czasopisma z dziedziny telekomunikacji, oba znajdujące się na liście JCR (i na Liście A MNiSW). Co najmniej jedno z nich (*Multimedia Tools and Applications*) jest uznanym miejscem publikacji z dziedziny, której dotyczy rozprawa. Jedna z tych publikacji była już cytowana 11 razy.
- Dotychczasowy dorobek Doktoranta nie ogranicza się jedynie do wyników zawartych w pracy, a jego zainteresowania są dużo szersze. Np. jego dorobek obejmuje także prace dotyczące rozpoznawania mówców czy znakowania obrazów cyfrowych, a więc zagadnień wprawdzie mieszczących się w bardzo szerokim zakresie zagadnień przetwarzania sygnałów, ale jednak są to tematy nie tak bliskie rozprawie.

Wszystkie wspomniane tu aspekty wskazują na istotny dorobek Autora rozprawy.

7. Poprawność przedstawienia uzyskanych wyników (zwięzłość, jasność, umiejętność przekonywania, poprawność redakcyjna)

Doktorant na pewno ***posiada umiejętność poprawnego przedstawiania wyników swoich prac z punktu widzenia merytorycznego***. Dowodzi tego nie tylko treść samej rozprawy, ale także treść artykułów, w których zawarł już szczegółowe wyniki. Myśli są formułowane w sposób zwięzły (zresztą cała prac nie jest długa, co zasługuje na uznanie). Zdania są konstruowane jasno i zrozumiale. Jeśli chodzi o umiejętność przekonywania do postawionych przez Doktoranta argumentów, to mogę stwierdzić, że posiada on również takie umiejętności, chociaż w samej pracy korzysta z nich niezbyt równo i najbardziej tego rodzaju zdolności można zaobserwować w końcowych partiach rozdziału 4.

Bardziej krytycznie muszę odnieść się do zagadnień poprawności redakcyjnej. W rozprawie można dojrzeć pewną liczbę niedoróbek edycyjnych. Wprawdzie nie umniejszają one wartości pracy i przeważnie nie przeszkadzają w odbiorze treści, niemniej jednak jestem w obowiązku zwrócić na nie uwagę (uszeregowałem potknięcia w kolejności od nieco bardziej istotnych do dużo mniej ważnych):

- Rozdziały nie mają zrównoważonej długości, a niektóre z nich zapewne można byłoby połączyć z innymi (np. zapewne rozdział 2 zawierający tezę rozprawy mógłby zostać włączony do rozdziału wstępnego).
- Biorąc pod uwagę, że rozprawa doktorska ma jednak charakter monograficzny, można byłoby oczekiwać ułożenia kolejności literatury nie według cytowania, a raczej z uwzględnieniem porządku opartego na nazwisku pierwszych autorów prac, do których odwołuje się Autor.
- Drobne niedopatrzenia redakcyjne, np.:
    - Niekonsekwencje lub niewielkie niepoprawności opisu, np.:
        - tytuły rozdziałów nie są wyjustowane;
        - „Wykaz skrótów i oznaczeń" i in.: zamienne używanie myślnika oraz dywiza;

- str. 8: tłumaczenie ECC należałoby raczej podać w liczbie pojedynczej („kod" zamiast „kody");
- str. 8: FLOSS to raczej Free Libre Open Source Software;
- str. 13: definicja algorytmu została przedstawiona w sposób nieczytelny lub zgubiono przecinek po słowie „postępowania";
- str. 16: w definicjach „steganografii oprogramowania" i „steganografii sprzętowej" dwa razy mówi się o dziale steganografii wtrącającym dodatkowe dane, ale chodzi raczej o dział zajmujący się specyficznym sposobem wtrącania określonych danych (steganografia jako abstrakcyjne pojęcie nie może przecież nic wtrącać);
- str. 17: definicja „otwartego oprogramowania" w zasadzie mówi o pewnej właściwości oprogramowania, ale nie o nim samym, podobnie sprawa ma się z definicją „zamkniętego oprogramowania";
- str. 18 i in.: nadużywanie słowa „ilość" w odniesieniu do rzeczowników policzalnych;
- str. 51: w wierszu drugim tekstu Autor odnosi się do rysunku 1, ale mam duże wątpliwości czy naprawdę dotyczy to rysunku zamieszczonego na str. 20;
- str. 55: na początku podrozdziału 5.1, który traktuje nt. testów obiektywnych, Autor pisze jak gdyby nt. testów subiektywnych;
- str. 71: niejasne jest umieszczenie objaśnień skrótów MGPGPU, GPU, GFLOPs akurat w tym miejscu (skoro wcześniej zamieszczono przecież wykaz skrótów);
- literatura:
  - niekiedy brak bliższych danych bibliograficznych (np. w przypadku [11]);
  - czasem wielkie litery błędnie zastąpiono małymi (np. w przypadku [15] jest napisane „reed-solomon");
  - pozycja [79] to powtórzona pozycja [59];
  - autorzy prac są opisywani w odmienny sposób w przypadku różnych pozycji (np. w przypadku [86] „Paulin, Catherine, Selouani, Sid-Ahmed, Hervet, Eric", zaś w przypadku [87] „T. Zseby, F. Iglesias Vázquez, V. Bernhardt, D. Frkat and R. Annessi");
  - opis pozycji [139] kończy się zagadkowymi trzema przecinkami;
  - brak tytułu pozycji [143].

- Ewidentne literówki, np.:
  - str. 2: „na potrzebe" zamiast „na potrzebę";
  - str. 2: „Nz opisana": niejasny fragment;
  - str. 9: należy pisać raczej nazwisko matematyka Markowa w spolszczonej wersji (a nie „Markova");
  - str. 10: kB to „kilobyte";
  - str. 11: MiB to „mebibyte";

- str. 16: w jednym przypadku niepotrzebnie wprowadzono spacje między słowami a nawiasami, które powinny z nimi bezpośrednio sąsiadować (podobnie na str. 58);
- str. 19 i in.: niepotrzebnie powtórzone kropki (np. „itp.."), potknięcia interpunkcyjne (np. brak ujęcia wtrącenia „jaki należy wziąć pod uwagę" w nawiasy lub objęcia przecinkami);
- str. 27 i in.: drobne literówki polegające na przestawieniu liter w słowie lub zgubienie/dodanie liter (np. „przdestawiony" zamiast „przedstawiony" na str. 27, „algrytmów" na str. 30, czy „porzedstawiony" na str. 31);
- str. 28: „N podstawie" zamiast „Na podstawie";
- str. 28 i in.: zakończenie zdania nie kropką, a przecinkiem (tutaj np. „pod kątem steganoanalizy,");
- str. 29 i in.: sklejenie słów (np. „zostałzaimplementowany");
- str. 44: w niektórych przypadkach przy pisaniu zmiennych zgubiono kursywę matematyczną;
- str. 46: na początku sekcji 3.2.2 zawarto wypunktowanie, które nie zostało wyjustowane;
- str. 56 i in.: zdarza się użycie kropki dziesiętnej (charakterystycznej dla języka angielskiego) w miejsce przecinka dziesiętnego.

8. Słabe strony rozprawy, jej główne wady

W przypadku rozprawy można wskazać trzy słabsze punkty:

- Zbyt uboga analiza literaturowa (szerzej pisałem już o tym w punkcie 4 niniejszej recenzji): niewyodrębnienie w jasny sposób części dotyczącej analizy bibliografii wraz z jasnymi wnioskami i źródłami inspiracji oraz skromniejsze podejście do prac opublikowanych po 2016 r.
- Niekonsekwentne zintegrowanie dosyć licznych pomysłów przedstawionych przez Doktoranta w ramach pracy z mieszczącym się najwyraźniej w głównym nurcie prac algorytmem sygnałowym oraz poświęconym mu testom. Rozbudowanie koncepcji drugiego z algorytmów steganograficznych oraz przetestowanie różnych rozwiązań informatycznych wprost na opracowanych algorytmach stanowiłoby cenne dopełnienie pracy.
- Potknięcia edycyjne obecne w pracy. Rozprawa zyskałaby na usunięciu niektórych niestaranności, które na szczęście nie zaburzają jasności samego tekstu od strony merytorycznej.

9. Przydatność rozprawy dla nauk technicznych, przemysłu, obronności kraju itp.

Rozprawa wnosi wkład w zakresie bezpieczeństwa współczesnej telekomunikacji. Można tutaj wskazać na cenne kontrybucje na pewno w dwóch obszarach, mianowicie:

- ***Nauki techniczne***: zawartość koncepcyjna pracy poszerza nasz zasób metod steganograficznych w odniesieniu do transmisji wideo z użyciem

standardu DVB-T. Interesujące są również koncepcje Autora dotyczące testów subiektywnych dotyczących obserwacji transmisji skrytej, jak również jego rozważania dotyczące zagadnień obliczeniowych niezbędnych do ukrywania transmisji (zarówno z punktu widzenia doboru architektury, jak również rozwiązań sprzętowo-programistycznych).

- ***Obronność kraju***: ze względu na specyfikę dziedziny związaną z ukrywaniem transmisji w systemie powszechnie dostępnej telewizji, warto podkreślić potencjał zaprezentowanych wyników z punktu widzenia zastosowań przez służby wojskowe (lub innego rodzaju służby zajmujące się bezpieczeństwem kraju).

10. Podsumowanie (czy rozprawa spełnia wymagania przez obowiązujące przepisy)

Moim zdaniem przedstawiona rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego poprawnie postawionego przez Doktoranta w zakresie nauk techniczno-inżynieryjnych w obszarze związanym z telekomunikacją. Treść pracy potwierdza, że Autor posiada odpowiednią wiedzę praktyczną na tematy związane z rozprawą. Autor wykazał, że umie prowadzić badania naukowe oraz je opisywać.

Stwierdzam zatem, że recenzowana rozprawa doktorska spełnia wymagania stawiane przez obowiązujące przepisy. Z tego powodu wnoszę o dopuszczenie jej do publicznej obrony.

Piotr Chołda