prof. dr hab. inż. Włodzimierz Kasprzak
Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych
Instytut Automatyki i Informatyki Stosowanej
W.Kasprzak@elka.pw.edu.pl

10.08.2020 r.

Recenzja Rozprawy Doktorskiej

mgr inż. Olgi Veselskiej

przygotowana dla Rady Naukowej Instytutu Informatyki Wydziału Nauk Ścisłych i Technicznych Uniwersytetu Śląskiego w Katowicach

Tytuł rozprawy: **Metoda przestrzenno-pikselowa ukrywania informacji w obrazach**

Dyscyplina naukowa: **Informatyka techniczna i telekomunikacja**

1. Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza rozprawy/ i czy zostało ono dostatecznie jasno sformułowane przez autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?

Rozprawa mgr inż. Olgi Veselskiej dotyczy metod ukrywania informacji w kolorowych obrazach cyfrowych i jej bezpiecznego przesyłania w sieci komputerowej od nadawcy do zaufanego odbiorcy.

Tematyka i charakter rozwiązań pozwalają zaliczyć rozprawę do obszarów badawczych informatyki, w szczególności obejmujących metody komputerowej steganografii i stegano-analizy. Steganografia obrazów to obszar wiedzy obejmujący metody ukrywania informacji w obrazie-nośniku. Steganoanaliza to obszar analizy („drążenia") danych służący do oceny stopnia bezpieczeństwa ukrytej informacji przez atakiem użytkownika nieuprawnionego do jej odkrycia lub zniekształcenia.

Teza rozprawy, czyli zagadnienie naukowe (zadanie badawcze) rozpatrywane w pracy, została sformułowana dostatecznie jasno, jednak w mojej ocenie jest ona **mało odkrywcza i zbyt ogólna oraz nie reprezentuje w pełni treści rozprawy**. Teza rozprawy brzmi następująco:

„Istnieje możliwość efektywnej poufnej transmisji dużej ilości informacji przy jednoczesnym zachowaniu wysokiej niezawodności oraz zwiększonej skuteczności, poprzez wbudowanie ukrytych danych w obrazie cyfrowym za pomocą zaproponowanej własnej metody przestrzenno-pikselowej i udoskonalonych wybranych metod(-ach) steganograficznych."

Teza jest mało odkrywcza, gdyż wiemy już z wielu poprzednich prac dotyczących steganografii i znakowania wodnego, że można ukrywać informację w obrazie a także znamy wiele algorytmów do tego przeznaczonych.

Teza jest zbyt ogólna, gdyż nie podaje jakiej zasadniczo nowej wiedzy ma dostarczyć przedmiotowa rozprawa. Nie jest nią sama tytułowa metoda jako taka ani też inne algorytmy konstruowane w tej pracy. Dlatego należy wskazać na zasadnicze szczegóły i charakterystykę, które wyróżniają proponowane rozwiązanie od innych, podobnych. Np. „metoda przestrzenno-pikselowa z losowym wybieraniem rozmieszczania stego-informacji posiada zwiększoną odporność w porównaniu do typowo stosowanych metod ukrywających informację w przestrzeni kolorowego obrazu". W kontekście zamierzonego zastosowania metody – do transmisji ukrytej informacji w sieci – również możliwe byłoby wskazanie szczególnych własności metody wymaganych przez dziedzinę jej zastosowania.

Teza nie oddaje w pełni treści rozprawy, gdyż nazwana w tezie i tytule pracy metoda steganograficzna jest tylko jednym z kilku algorytmicznych zagadnień rozpatrywanych w pracy.

Autorka podaje, że dla osiągnięcia celu pracy (czyli *„opracowanie metody transmisji poufnych informacji w obrazach cyfrowych, która zakłada zwiększenie efektywności funkcjonowania informatycznych systemów bezpieczeństwa poprzez ukrywanie informacji identyfikujących w obrazach oraz podwyższanie odporności ich wykrywania"*) rozwiązano następujące zadania:

1. *przeprowadzono analizę istniejących metod steganografii i uzasadniono kierunek ich poprawy,*
2. *opracowano metody i modele przestrzennie ukrywanych informacji w cyfrowych obrazach różnych klas we współrzędnych funkcji,*
3. *opracowano metodę i model wyodrębniania ukrytych informacji w obrazach cyfrowych za pomocą filtrowania przestrzennego,*
4. *przeprowadzono analizę kanałów transmisji informacji ukrytych,*
5. *opracowano metodykę oraz model, dzięki którym system steganograficzny jest bardziej uodporniony na wykrycie ukrytej informacji w cyberprzestrzeni.*

Niestety pod względem edycji rozprawę cechuje **chaotyczność prezentacji** i **niespójność** treści. Realizację pierwszego z powyższych zadań da się przypisać do rozdziału 1 a realizację zadań 2 i 3 do punktu 2.6. Jednak trudno jest mi powiązać zadania 4 i 5 z konkretną treścią pracy. Nie wiadomo co mają oznaczać *„kanały transmisji informacji ukrytych"*, albo gdzie omówiono *„metodykę i model"*, które zwiększają odporność na wykrycie. Całość pracy robi wrażenie kompilacji różnych odrębnych artykułów i raportów badawczych.

Moim zdaniem zasadniczy dorobek merytoryczny rozprawy, podlegający ocenie, to:

1. Przegląd i próba pewnej kategoryzacji istniejących metod steganografii (rozdział 1);
2. Propozycja dwóch algorytmów steganografii obrazu i algorytmu wykrywania (celowego) wygładzania obrazu,

   Pierwszy z nich dotyczy wstawiania informacji w dziedzinie transformaty SVD (punkty 2.2-2.4, 3.4), w szczególności poprzez modyfikowanie znaku wybranej wartości własnej dla każdego bloku 8x8 obrazu nośnika.

   Drugi algorytm dotyczy wykrywania rozmycia obrazu, co ma symulować atak na nośnik z ukrytą informacją (punkty 2.5, 3.2-3.3).

   Trzecie rozwiązanie to przedmiotowa (wymieniona w tytule i tezie pracy) pikselowo-przestrzenna metoda (w skrócie PPM) steganografii obrazu (punkty 2.6, 4.5). .
3. Badaniu wpływu filtracji obrazu na jakość obrazu (punkt. 3.5).

2. 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?

Praca zawiera 17 stron spisu literatury (151 pozycji, w tym 16 stron WWW). W związku z tematem rozprawy – steganografią obrazu - w tradycyjnej części obejmującej „drukowaną" literaturę znajduje się kilka artykułów przeglądowych, kilkanaście uznanych pozycji literatury przedmiotu i szereg pozycji o przeciętnej wartości naukowej. Większą część tej literatury zajmują pozycje pochodzące z różnych innych obszarów cyfrowej steganografii (ukrywania informacji w tekście, audio czy wideo), kryptografii ([25], [74], [103], [110]), przetwarzania obrazów ([33], [98], [129], [133]), rozpoznawania mowy ([114]), filozofii badań ([24]), cyberbezpieczeństwa ([49], [103]), uczenia maszynowego ([70], [71], [72]), komunikacji w sieciach bezprzewodowych ([95], [132]), metodyki PCA-SVD ([135]) i różnych innych technik komputerowych ([28], [79], [83], [126], [127], [128]).

Do tej sensownej literatury, bezpośrednio związanej z tematem rozprawy, zaliczam nowsze prace doktorskie [1], [37], [55], [89], [93], [122] i prace znanych autorów w uznanych czasopismach [7], [16], [23], [26], [31], [32], [33], [38], [52], [63]-[65], [67], [80], [85]-[87], [108]-[109], [117]-

[119], [123]-[124]. W sumie jest to 30 pozycji, wartościowych z punktu widzenia tematu i szczególnie ważnych dla wykazania tezy pracy. Jednak Autorka nie zatrzymała się na dłużej przy żadnej z tych pozycji, cytując je bez większej refleksji i wyjaśnienia ich związku z treścią rozprawy.

Tak więc przegląd literatury to mieszanka różnych zagadnień, a pozycje **ważne i nieważne** z punktu widzenia tematu rozprawy referowane są przez Autorkę **z jednakową niefrasobliwością** i więcej w tym jest **dezinformacji niż pożytku** dla Czytelnika.

W spisie literatury znalazło się też **25 prac autorskich i współautorskich** Doktorantki, z których jednak tylko 13 jest związanych z tematem rozprawy i uzasadnione jest odwoływanie się do nich w rozprawie.

Strony WWW odnoszą się do opisów metod steganografii, steganoanalizy i kryptografii, w tym skryptów akademickich.

Bardzo ważnym elementem każdej pracy naukowej jest określenie aktualnego stanu wiedzy (**state-of-the-art)** z podaniem źródłowych pozycji literatury. Doktorantka zrobiła obszerny przegląd istniejących typów metod, obejmujący wstawianie/ukrywanie informacji w tekście, zapisie audio, w pojedynczych obrazach i sekwencji wideo. Jednak teza rozprawy dotyczy ukrywania informacji w pojedynczych obrazach. Dlatego przegląd innych rozwiązań (w szczególności osadzanie w dziedzinie tekstu i audio) uważam za nadmiarowy, a nawet niepotrzebny. W ten sposób „zabrakło" Autorce energii na głębszy przegląd tych metod, które bezpośrednio odnoszą się do tematu rozprawy. Obszerne zestawienia porównawcze metod audio i tekstu podane w tabelach 1.1. i 1.2 nie wnoszą niczego konstruktywnego do dowodu tezy pracy. W zamian za to należało przedstawić i porównać ze sobą przynajmniej kilkanaście konkretnych rozwiązań w zakresie steganografii obrazu. Tymczasem tabela 1.3 nie podaje nazw konkretnych metod i oryginalnych pozycji literatury je opisujących, a jedynie operuje zbiorczymi nazwami grup i typów metod bez odwołania się do literatury.

Odwołania do literatury w treści rozdziału 1, dotyczące zagadnień steganografii obrazu są bardzo wybiórcze, najczęściej mało reprezentatywne, cytują publikacje mało znanych autorów w czasopismach „szybkiej" publikacji lub w typowo komercyjnych konferencjach o małych znaczeniu. Aby nie być gołosłownym przejrzyjmy odwołania do literatury w rozdziale 1 w zakresie steganografii obrazu i wideo.

Przegląd właściwych metod w punkcie 1.2 („Metody ukrywania danych w nieruchomych obrazach") Autorka rozpoczyna od powołania się na pozycje literatury [1, 3, 4, 7, 8, 14, 19]. Ale poz. [3] dotyczy steganografii tekstu (nośnikiem jest tekst). Poz. [4] wprawdzie w nazwie dotyczy steganografii obrazu, ale proponowana w niej metoda dotyczy zakodowania informacji z wykorzystaniem ostatnich 2 bitów LSB i na dołączeniu tego kodu do pliku z (niezmienionym) obrazem a nie polega na wstawieniu informacji w dziedzinie obrazu. Pozycje [3] i [4] to „szybkie" publikacje początkujących naukowców w mało znaczących indyjskich czasopismach „open-access". Podobnego typu jest czasopismo publikacji pozycji [8]. Jej pierwszym autorem jest wprawdzie student, ale krótki przegląd metod osadzania informacji w dziedzinie JPEG jest zupełnie poprawny. Pozycja [14] proponuje wstępne zakodowanie informacji algorytmem Blowfish i następnie osadzenie kodu w obrazie najprostszą metodą LSB. Artykuł jest krótki, z licznymi błędami językowymi, autorzy są mało znani a czasopismo ma podobny charakter co w przypadku pozycji [3] i [4]. To nie jest dobra referencja dla doktoratu. Pozycja [19] to współautorski artykuł konferencyjny Doktorantki, który po tytule sadząc, najwyraźniej nie ma związku ze steganografią obrazu.

Jeszcze gorzej wyglądają odwołania do pozycji [10, 13, 19, 24, 25] zamieszczone podczas omawiania szczegółowych rozwiązań osadzania informacji w dziedzinie obrazu. Współautorskie pozycje Doktorantki [13] i [19] nie są związane z tym zagadnieniem. Pozycja [24] to istne kuriozum w tym kontekście – jest to monografia dotycząca „research design", trochę subiektywnej filozofii. Pozycja [25] dotyczy kryptografii, czyli również nie pasuje w tym miejscu. Kryptografia i steganografia wprawdzie zajmują się bezpieczeństwem danych to jednak w dwóch różnych

aspektach. Kryptografia ukrywa jedynie znaczenie lub zawartość sekretnej wiadomości poprzez tworzenie skrótów, podczas gdy steganografia ukrywa także samo istnienie sekretnej wiadomości.

Przy omawianiu szczegółowych metod osadzania informacji w dziedzinie częstotliwości obrazu, w tym w dziedzinie transformaty DCT, typowej dla formatu JPEG, Doktorantka odwołuje się do pozycji [1,12,13,17,19,23,25] a następnie [14,20,52]. Pozycje [13, 19] to współautorskie prace Doktorantki na konferencjach zasadniczo poświęcone innym zagadnieniom. Pozycja [25] to ponownie książka o kryptografii. Pozycje [14] i [20] są błędnie cytowane, gdyż proponowane w nich metody to osadzanie typu LSB w dziedzinie obrazu. Pozycja [52] to zlepek dwóch dobrych wczesnych publikacji – znanej książki o steganografii i znakowaniu wodnym, zredagowanej przez Katzenbeiser i Peticolas, oraz materiałów znaczącej specjalistycznej konferencji ICIP-2001, która zawierała też sesję poświęconą technikom znakowania wodnego. Jednak w kontekście omawiania szczegółowych rozwiązań należałoby podać odwołanie do konkretnych rozdziałów książki lub konkretnych artykułów w wielotomowych materiałach ICIP-2001 (gdzie jest ok. 200 artykułów!).

W przeglądzie steganografii obrazu nie przedstawiono metod osadzania w dziedzinie transformaty falkowej lub SVD (PCA), ani też bardziej wyrafinowanych metod osadzania informacji w dziedzinie obrazu z wykorzystaniem elementów pseudo-losowych.

Przegląd literatury poświęconej steganografii wideo [9, 16, 19, 25] także zawiera liczne błędne odwołania. Pozycja [9] to artykuł o algorytmach detekcji krawędzi w obrazie. Pozycja [16] to artykuł o łączeniu steganografii tekstu ze wstawianiem w dziedzinie pojedynczego obrazu.

Pozycja [19] to po raz kolejny błędnie referowany artykuł współautorski Doktorantki, podobnie jak ponowne odwołanie do monografii [25] dotyczącej kryptografii. Również szczegółowe odwołania do pozycji [52, 76, 77] nie są dobrze wybrane. Pozycja [52] to zlepek dwóch publikacji - w pierwszej z nich nie ma zagadnień wideo a w drugiej (konferencja ICIP-2001) trudno jest znaleźć właściwy artykuł, jeśli istnieje, wśród kilkuset pozycji – raczej w 2001 r. nie było jeszcze mowy o steganografii wideo. Pozycja [76] omawia steganografię obrazu a pozycja [77] to nieznana praca krajowa o najwyraźniej ogólnym charakterze.

Wnioski wyciągnięte z przeglądu metod również w znacznej części są zaskakujące, gdyż większości z poruszanych kwestii wcześniej w rozprawie Autorka nie analizowała. Wniosek o postaci: *„Zaproponowany w [5] algorytm powinien być odpowiednio zmodyfikowany ..."* bierze się z znikąd, gdyż rozprawa [5] nigdzie dotąd nie była referowana a jej algorytm nie został, nawet jedynie ogólnie, przedstawiony. Podobnie stwierdzenie, że *„Ograniczeniem przedstawionych w [18, 37, 56, 98, 102] metod w dziedzinie transformacji jest to, że badania przeprowadzono tylko dla obrazów w skali szarości"* zdumiewa z dwóch powodów: po pierwsze prace te są cytowane po raz pierwszy w miejscu wyciągania wniosków bez ich uprzedniego przedstawienia, a po drugie – ukrywanie informacji w obrazach kolorowych RGB czy YUV nie jest żadną nowością, a w dziedzinie transformacji dla JPEG istnieje kanał luminancji i dwa kanały chrominancji, które także są wykorzystywane do ukrywania informacji. Szereg cytowanych tu prac po raz kolejny nie jest spójnych z omawianym przez Doktorantkę zagadnieniem. Pozycja [18] stanowi przegląd metod „malware", czyli sposobów ukrywania w plikach różnego typu złośliwego lub niebezpiecznego oprogramowania. Praca [98] dotyczy algorytmów wykrywania krawędzi w obrazach a nie ukrywania informacji. Praca [102] omawia zagadnienie steganografii zapisów audio.

Niczym nie jest poparty kolejny wniosek sformułowany następująco: *„Prace [1, 25, 26, 43] nie tylko wykazały wysoką skuteczność wbudowania i niedostrzegalność metod steganograficznych opartych na obrazie ...:"* Prace [1], [26], [43] nie były wcześniej przedstawione, a pozycja [25] to ponownie cytowany już podręcznik kryptografii.

Kolejny wniosek nie ma bezpośredniego związku z tematem – cytowana w nim pozycja [11] dotyczy bowiem bezpieczeństwa i wydajności Web-serwisów!

Kolejny wniosek zaczynający się od *„zaproponowana w [125] uniwersalna steganoanaliza 3D"* jest niezrozumiały w kontekście badanego zagadnienia. Nie jest wiadome, w jaki sposób analiza pokrycia powierzchni 3D siatką wielokątów ma być rozwijana *„na połączenia sieci"* i jaki to ma związek z tezą pracy?

Podsumowując, w rozdziale poświęconym **analizie literatury** praktycznie nie pojawiają się odwołania do źródłowych publikacji, konkretnych dobrze znanych rozwiązań steganografii obrazów (ich przykładową listę podaję w punkcie 4 recenzji). Jest za dużo błędnych odwołań i odwołania do prac o marginalnym znaczeniu dla przedmiotu. Jednak w spisie literatury ciekawe, źródłowe pozycje występują (wyliczyłem je na początku – to około 30 pozycji). Część z nich cytowana jest w kolejnych rozdziałach pracy, jednak również mało refleksyjnie.

Wspólnym elementem metod ukrytego znakowania wodnego obrazów (czyli technik stosowanych w steganografii obrazów) nazywanych metodami „typu LSB" jest podmienianie (nieistotnych z punktu widzenia jakości) bitów obrazu bitami wiadomości. Są to więc metody osadzające informację w przestrzeni obrazu. To co wyróżnia bardziej zaawansowane metody LSB od prostych metod tego samego typu to stosowanie zaawansowanych reguł wyboru miejsc i obszarów, które mogą zostać zmodyfikowane, a które nie mogą. Głównym powodem wprowadzania takich reguł jest unikanie wprowadzania zauważalnych zakłóceń w modyfikowanym obrazie i zabezpieczanie się przez atakami wrogich użytkowników. Jednym z pierwszych przykładów takich rozwiązań jest metoda BPCS (E. Kawaguchi, R.O. Eason, 1998).

Zasadniczo polega ona na określeniu złożoności (relatywna liczba zmian bitów z 1/0 i 0/1) bloków 8x8 warstwy bitowej i na osadzeniu wiadomości w tych blokach, których złożoność jest większa niż zdefiniowany próg (np. 0.3) przez zastąpieniu całego bloku przez 64 kolejne bity wiadomości.

W rozdziale poświęconym **stanowi wiedzy i technologii** zupełnie pominięto analizę **technologii rynkowych**. W kolejnych latach począwszy od końca XX wieku powstało szereg firm oferujących profesjonalne rozwiązania tego rodzaju. Np. firma Digimarc (https://www.digimarc.com/) przez szereg lat udostępniała do testów swoje opatentowane rozwiązanie nazwane "*perceptual adaptation*". Polegało ono na osadzaniu informacji w kanale luminancji obrazu w obszarach, które albo były bardzo zróżnicowane albo na odwrót były jednorodne, zwiększając jasność w obszarach niejednorodnych i zmniejszając w jednorodnych.

Aktualny stan komercyjnych rozwiązań w zakresie znakowania wodnego danych multi-medialnych można poznać np. poprzez stronę https://digitalwatermarkingalliance.org/ .

Z uwagi na istnienie dojrzałych technologii steganografii obrazu obecnie przedmiotem prac naukowych są bardziej wyrafinowane metody osadzania informacji niż „typu LSB", np. osadzanie w dziedzinie transformaty składowych głównych (PCA, SVD), probabilistyczne schematy osadzania XOR w dziedzinie obrazu lub probabilistyczne osadzanie w dziedzinie transformaty falkowej.

Analiza **dorobku publikacyjnego Autorki**, pozwala stwierdzić, iż dorobek ten jest liczny i różnorodny, a tematyka rozprawy występuje w większości (13) prac Autorki. W spisie literatury umieszczono w zasadzie wszystkie publikacje autorskie i współautorskie Doktorantki, w liczbie 25, niezależnie od ich związku z tematem rozprawy. Część z tych prac nie ma związku z tematem rozprawy (poz. [70], [71], [72], [95], [126], [127]), ale za to w części ten związek jest aż nadmiernie bezpośredni (poz. [131], [133]). Poniższe prace współautorskie Doktorantki nie dotyczą steganografii, dlatego też ich cytowanie w przeglądzie literatury nie jest zrozumiałe:

[70] Martsenyuk V., Babinets L., Dronyak Y., Paslay O., Veselska O., Warwas K., Andrushchak I. and Kłos-Witkowska A. On development of machine learning models with aim of medical differential diagnostics of the comorbid states, 2019.

[71] Martsenyuk V., Karpinski M., Andrushchak I., Mayhruk Z., Milian N., Veselska O. On implementation of decision tree induction in cloud platforms, 2019

[72] Martsenyuk V., Veselska O. On nonlinear reaction-diffusion model with time delay on hexagonal lattice, Symmetry. Vol. 11, No 6, pp. 1(758)-14, 2019

[95] Shevchuk B., Geraimchuk M., Ivakhiv O., Veselska O., Sachenko A. Optimization of Transferring the Information Packets with Limited Time for Wireless Network, 2018

[126] Yesin V. I., Karpinski M., Yesina M. V., Vilihura V. V., Veselska O. and Wieclaw L. Approach to Managing Data From Diverse Sources, 2019.

[127] Yudin O. K., Veselska O. M. Analysis and classification systems access control in the enterprise, 2018.

W 6 pracach Doktorantka jest jedyną autorką lub pierwszą współautorką. Prace te najwyraźniej mają charakter przeglądu literatury na temat steganografii i elementów kryptografii (za wyjątkiem poz. [114]):

[110] Veselska O. M. Cryptographic of wired equivalent privacy protocol and how it can be improved, 2012.

[111] Veselska O. M. Nowoczesne metody wykrywania ukrytych informacji w obrazach statycznych, 2017.

[112] Veselska O. M., Ziubina R. V. Analysis Steganographic Techniques in Spatial and Frequency Domain, 2018.

[113] Veselska O. M., Ziubina R. V., Frolov O. V. Systematization and classification of available steganographic techniques to hide information, 2016.

[114] Veselska O. M., Ziubina R. V., Shunevych Y. Analysis and classification of speech signals recognition, 2017.

[115] Veselska O.M. Methods of detecting and destroying hidden information in a static image using passive attacks, 2018.

Niepokojące są pozycje współautorskie [97], [107], [129]-[133], które mogą mieć bezpośredni związek z treścią rozprawy, a w których Doktorantka nie jest pierwszą współautorką:

[97] Shmatok O., Veselska O. Finding the fact of transfer of the embedded information on the basis of statistical methods of pattern recognition and machine learning, 2020.

[107] Szmatok O., Veselska O. M. Aplication of algorithm of wavelet transformations in steganographic analysis, 2016.

[129] Yudin O. K., Veselska O. M. Digital filtering methods and their impact on image quality different classes, 2017.

[130] Yudin O. K., Veselska O. M. Search options for developing a modern and efficient methods of steganography and steganoanalysis, 2017.

[131] Yudin O. K., Veselska O. M. Space-pixel digital steganography method using spatial filtering to extract the secret message, 2018.

[132] Yudin O., Veselska O. Investigation protection of information resources of wireless networks using WEP circuit, 2012.

[133] Yudin O., Veselska O. Methods of digital filtration and their impacts on the quality of images of different classes, 2018.

Co do zasady, rozprawa doktorska mająca postać monografii powinna zawierać **nową, wcześniej niepublikowaną** wiedzę a Doktorant powinien mieć **decydujący udział** w jej wytworzeniu. Wobec istnienia publikacji referowanych w rozprawie jako pozycje [97], [107], [129]-[133] powstaje pytanie, czy ta zasada jest spełniona w przypadku recenzowanej rozprawy. Niestety w przypadku części z nich nie jest.

Jak zasugerowano w samej rozprawie, prezentacja głównego algorytmu rozprawy, do którego odnosi się teza pracy, pokrywa się w pełni z wcześniejszą publikacją [131], której pierwszym autorem jest dr hab. Oleksandr Yudin. Badania filtracji obrazów, zamieszczone w punkcie 3.5, są tłumaczoną kopią publikacji [133], której pierwszym autorem jest dr hab. Oleksandr Yudin. Analizując dorobek naukowy dr hab. O. Yudina można zauważyć, że specjalizuje się on w przetwarzaniu obrazów, w tym posiada szereg publikacji na temat steganografii obrazów z różnymi autorami. Zakładam, że wniósł on zasadniczy wkład merytoryczny do artykułów współautorskich Doktorantki [131] i [133], na których oparto w rozprawie prezentację głównego algorytmu (pkt. 2.6) i część wyników eksperymentalnych (pkt. 3.5).

3. Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

Rozprawa liczy 116 stron zasadniczego tekstu, podzielonego na 6 rozdziałów, a także zawiera 17 stron spisu literatury. Oprócz nienumerowanych rozdziałów początkowego wstępu i końcowego podsumowania, rozprawa zawiera cztery rozdziały, numerowane od 1 do 4, które jedynie w przybliżeniu (bo nie można w pełni dopasować ich elementów do zadań) dotyczą zadań wymienionych przez Autorkę we wstępie pracy.

Rozprawa ma niejednorodny charakter. Teza rozprawy mówi o zamiarze opracowania metody steganograficznej ale w treści rozprawy znajdziemy szereg luźno ze sobą powiązanych zagadnień:

1. Porównanie ze sobą dwóch miar podobieństwa obrazów (a w zasadzie 2-wymiarowych macierzy danych) IF_1 i SS (pkt. 2.1);
2. Propozycja metody steganoanalizy w blokach obrazu polegająca na zmianie znaków wybranych wartości własnych (pkt. 2.2-2.4);
3. Propozycja metod wykrywania rozmycia obrazu cyfrowego (pkt. 2.5, 3.2-3.4)
4. Propozycja metody pikselowej ukrywania informacji w obrazie (teza rozprawy) (tłumaczona kopia opisu metody zawartej w publikacji [131]) (pkt. 2.6, 4.5);
5. Eksperymenty z filtracją obrazów 4 klas (tłumaczona kopia opisu metody zawartej w publikacji [133]) (pkt. 3.5);
6. Opisy interfejsów użytkownika do aplikacji testowych (pkt. 4.1-4.4).

W rozdziale 1 dokonano przeglądu istniejących rozwiązań steganografii – nie tylko dla nieruchomych obrazów, ale także dla tekstu, zapisu audio i sekwencji wideo. Przeglądy steganografii obrazu i wideo skupiają się na zasadniczych kategoriach rozwiązań bez jawnego odwołania się do konkretnych znanych rozwiązań akademickich i przemysłowych oraz ich kluczowych implementacji, częściowo dostępnych w sieci Internetu. O ile sama ogólna prezentacja typów rozwiązań byłaby jeszcze do przyjęcia, to jednak zamieszczone tam odwołania do literatury są z reguły kompromitujące dla Autorki – referowane prace są zwykle niezgodne tematycznie z tekstem, mylone są prace na temat steganografii z kryptografią, prace z metodami w dziedzinie obrazu z metodami w dziedzinie częstotliwości a w przeglądach metod cytowani są poczatkujący lub mało znani autorzy i słabej jakości wtórne prace.

Rozdział drugi, a w nim punkt 2.1 rozpoczyna się od raczej oczywistej obserwacji, że *„dla zapewnienia prawdopodobieństwa niezauważalności zniekształceń [...] danego kontenera powinna być utrzymana mała norma macierzy zniekształceń (np. Frobeniusa, spektralna norma macierzowa)*". Jednak w definicji zmiennej H występującej w równaniu (2.8) popełniono prosty błąd (H-liczba obrazów z widocznymi zniekształceniami, zamiast niewidocznymi), który sprawia, że $V = H/H_0$ [%] w równaniu (2.8) jest bezbłędne przy wartości 0%, a V na rysunku 2.1 – na odwrót przy V=100% .

Punkt 2.1.1 staje się na początku niejasny, gdyż macierz A zostaje najpierw nazwana macierzą GW (głównej wiadomości) – czyli zniekształceniem, a zaraz potem jest macierzą nośnika, gdyż macierzą zniekształcenia staje się ΔA. Pomimo kontynuacji tego błędu stwierdzeniem, że *„podczas PS zniekształca się WW macierzy A GW*" błąd staje się oczywisty i można zrozumieć intencję Autorki. Powiązanie minimalizacji normy macierzy zniekształcenia z warunkiem minimalizacji zmian wartości własnych jest oczywiste, gdyż normę Frobeniusa macierzy liczymy m.in. poprzez sumę wartości własnych macierzy. Drugi warunek podany przez Autorkę, aby minimalizować zmiany (jedynie co „mniej ważnych") wektorów własnych jest bardziej intuicyjny niż formalny.

Należy zauważyć, że podane związki zniekształceń obrazu ze zmianami wartości i wektorów własnych stanowią motywację metod ukrywania informacji w dziedzinie transformaty SVD.

Wnioskiem z eksperymentalnego porównania stopnia „reaktywności" dwóch miar jakości na zniekształcenia obrazu (a w zasadzie macierzy danych 2D) przeprowadzonego w punkcie 2.1 - wskaźnika podobieństwa norm Frobeniusa IF_1 i indeksu podobieństwa spektralnego SS (spectral similarity index) - wynika, że większą zmiennością wykazuje się indeks SS. W kontekście celu i tezy rozprawy istnienie rozdziału 2.1 jest nieistotne. Obie miary ocen stopnia zniekształcenia obrazu nie pojawiają się więcej w treści i nie służą do oceny wyników kolejno wprowadzanych algorytmów.

Punkty 2.2. i 2.3 są wstępem do przedstawienia algorytmu ukrywania informacji w dziedzinie SVD (punkt 2.4). Czytelnik jest trochę zdezorientowany, gdyż cel punktów 2.2. i 2.3 nie został

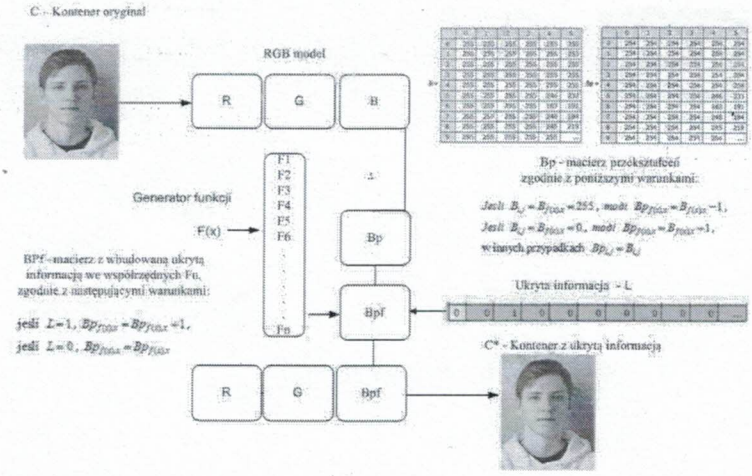
określony a we wcześniejszym przeglądzie literatury zabrakło informacji o metodach steganografii SVD (czyli wykorzystania analizy wektorów i wartości własnych macierzy 2D).

Lekturę tej treści ponownie utrudnia niefrasobliwe, a nawet błędne odwoływanie się do własnych publikacji. Np. na stronie 51, przy okazji opisu eksperymentów z obrazem torby zakupowej z nadrukiem drzewa, Autorka stwierdza: „*Na podstawie przeprowadzonych i opublikowanych badań [12], [97], [111] nasuwa się następujący wniosek*". Patrzymy na wymienione publikacje i nie widzimy żadnego związku z eksperymentem prowadzonym w tym punkcie rozprawy. Wyniki zniekształcania obrazu torby metodą zmiany znaku wybranej wartości własnej i dodawania niewielkiego szumu prezentowane na rys. 2.4 i 2.5 w praktyce nic nie mówią, gdyż przy tej jakości prezentacji grafiki nie są widoczne żadne różnice między wynikami. Można by docenić algorytm wstawiania polegający na modyfikacji znaku wartości własnej, podany w pkt. 2.4, gdyby nie kolejna błędna informacja o źródłach jego pochodzenia. Zapowiadając ten algorytm, Autorka napisała, że „*korygowanie liczb ujemnych [...] zależy od wartości kolejnego wbudowanego elementu sekwencji ID [12, 13, 71, 112]*". W mojej ocenie praca [12] dotyczy ogólnego schematu addytywnego wstawiania informacji do obrazu połączonego z adaptacyjnym przekodowaniem obrazu. Pozycja [13] nię jest dostępna. Przedmiotem poz. [71] jest uczenie się drzew decyzyjnych w chmurze! Pozycja [112] nie jest dostępna. W kroku algorytmu znowu pojawia się błędne odwołanie do literatury: „*zbudować dla B_H rozkład widmowy [6, 10, 92]*", gdzie przez „rozkład widmowy" Autorka rozumie dekompozycję SVD macierzy. Pozycja [6] to opis metody typu LSB - bezpośredniego wstawiania w obraz. Pozycja [10] to krótki przegląd wczesnych metod i narzędzi. Pozycja [92] to propozycja zakodowania bitu sekretnej informacji za pomocą reguły logicznej przy zastosowaniu bitu LCB obrazu jako klucza kodowego a następnie dołączeniu takiego kodu do niezmienionego obrazu. W żadnym z tych artykułów nie występuje dekompozycja SVD!

Uważam, że nie można tworzyć na poważnie **nowej wiedzy stosując metodę dezinformacji** i prezentacji **niejasnych wyników**.

Punkt 2.5 rozpoczyna się od wyjaśnienia, że „*Celem wykrycia [...] zmian w obrazie [...] zaproponowano następującą modyfikację algorytmu wykrywania rozmycia.*" Powstaje od razu pytanie o algorytm wymagający modyfikacji, bo jak dotąd nie został on przedstawiony. Z drugiej strony skoro algorytm już został zaproponowany to przez kogo i gdzie go można zweryfikować? Częściowa odpowiedź na to pytanie pojawi się dopiero w pkt. 3.2 na str. 78, gdzie zostanie przedstawiony zarys bazowego algorytmu wykrywania rozmycia. Przy tej okazji Autorka odwołuje się do pozycji literatury [135], który jednak nie jest źródłem tej metody ani nawet o niej nie wspomina. Zmodyfikowany algorytm wykrywania rozmycia polega na dwukrotnym wykonaniu dekompozycji SVD - najpierw dla bloków 8x8 badanego obrazu a następnie dla wyniku rozmycia tego obrazu przez eksperta – określeniu liniowej regresji wartości własnych od 4 do 8 w obu przypadkach, określeniu średnich współczynników nachylenia prostych funkcji regresji po wszystkich blokach każdego obrazu i ostatecznym sprawdzeniu relacji takich wielkości dla obu obrazów. Motywacją tego rozwiązania, które poznamy dopiero później w punkcie 3.2, jest obserwacja wyników badań eksperymentalnych wskazujących na fakt, że pierwsze Gaussowskie rozmycie obrazu prowadzi do znaczącego zmniejszenia współczynnika nachylenia, ale drugie i kolejne takie filtracje dają jedynie niewielkie jego zmiany, tzn. relacja W_przedtem /W_potem <2. Sam pomysł ponownego rozmyślnego rozmycia badanego obrazu jest ciekawy i sensowny. Powstaje jednak pytanie, czy do wykrycia stopnia zmian nie wystarczy nam porównanie ze sobą średnich wariancji bloków obrazu „przedtem" i „potem", zamiast wykonywać obliczeniowo bardziej kosztowne dekompozycje SVD wszystkich bloków i wyznaczać liniowe regresje wybranych wartości własnych.

Punkt 2.6 dotyczy już tego właściwego algorytmu steganografii obrazu, wymienionego w tytule i w tezie pracy. Za wyjątkiem jednego błędu, całość tego punktu, czyli **główny algorytm rozprawy**, jest tłumaczoną kopią artykułu [131]. Dla ilustracji tego faktu wystarczy porównać poniższe rysunki 1 z 2, 3 z 4, 5a z 5b, 6a z 6b, 7a z 7b.



Rys. 1. Rozprawa O. Veselska zawiera na stronie 60 ilustrację głównego algorytmu pracy: *Rysunek 2.7. Schemat strukturalno-logiczny procesu wbudowania ID w OC na podstawie metody MPP*

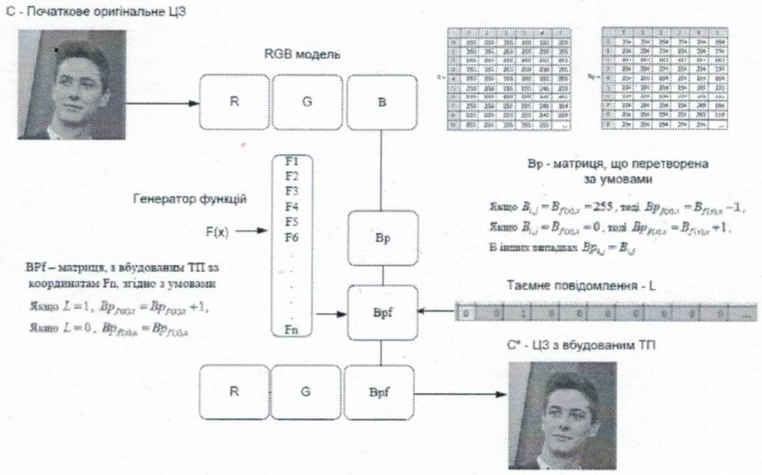
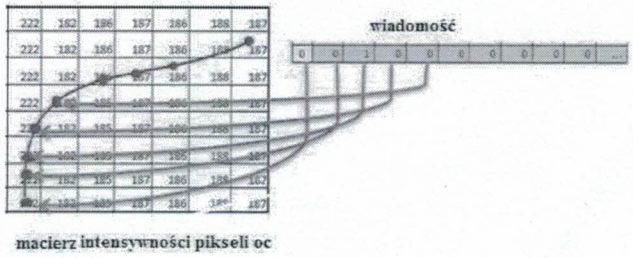
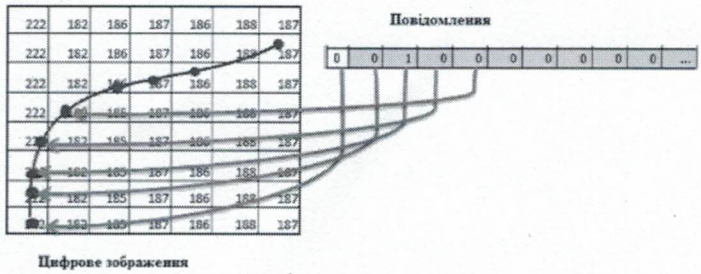


Рис. 1. Процес вбудовування ТП в ЦЗ за просторово-піксельним методом

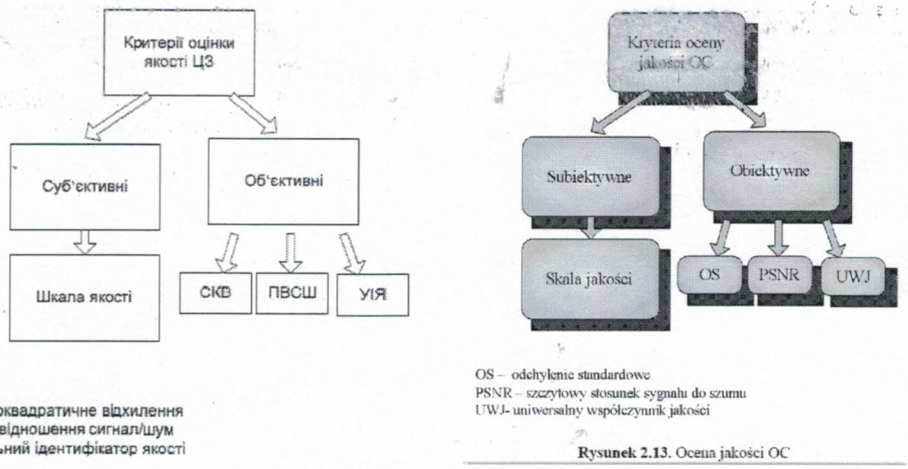
Rys. 2. Ilustracja w rozprawie jest dosłownym tłumaczeniem struktury algorytmu opisanego w pracy [Yudin O. K., Veselska O. M. Space-pixel digital steganography method using spatial filtering to extract the secret message, 2018, DOI: 10.18372/2310-5461.37.12371].



Rys. 3. Rozprawa O. Veselskiej zawiera na stronie 62 ilustrację procesu osadzania stego-obiektu: **Rysunek 2.8.** Proces osadzania wiadomości w kontenerze według współrzędnych funkcji



Rys. 4. Oryginalna wersja rys. 3 zamieszczona w pracy [131].



Rys. 5. Porównanie rysunku 2.13 w rozprawie z rysunkiem w publikacji [131].

Identyfikator UWJ oblicza się za pomocą wzoru:

$$UWJ = \frac{4 \cdot \sigma_{B,Bp} \cdot B^* \cdot Bp^*}{\left[\sigma_B^2 + \sigma_{Bp}^2\right] \cdot \left[(B^*)^2 + (Bp^*)^2\right]} \quad (2.53)$$

gdzie:

$$B^* = \frac{1}{M \cdot N} \cdot \sum_{i=0}^{M} \sum_{j=0}^{N} B_{i,j}, \quad (2.54)$$

$$Bp^* = \frac{1}{M \cdot N} \cdot \sum_{i=0}^{M} \sum_{j=0}^{N} Bp_{i,j} \quad (2.55)$$

$$\sigma_B^2 = \frac{1}{M \cdot N} \sum_{i=0}^{M} \sum_{j=0}^{N} (B_{i,j} - B^*_{i,j}) \quad (2.56)$$

$$\sigma_{B,Bp} = \frac{1}{M \cdot N} \sum_{i=0}^{M} \sum_{j=0}^{N} (B_{i,j} - B^*_{i,j}) \cdot (Bp_{i,j} - Bp^*_{i,j}) \quad (2.57)$$

$$\sigma_{B,Bp} = \frac{1}{M \cdot N} \sum_{i=0}^{M} \sum_{j=0}^{N} (B_{i,j} - B^*_{i,j}) \cdot (Bp_{i,j} - Bp^*_{i,j}) \quad (2.58)$$

$$УІЯ = \frac{4\sigma_{B,Bp} B^* Bp^*}{\left[\sigma_B^2 + \sigma_{Bp}^2\right]\left[(B^*)^2 + (Bp^*)^2\right]}, \quad (2)$$

де $B^* = \frac{1}{MN} \sum_{i=0}^{M} \sum_{j=0}^{N} B_{i,j}$; $Bp^* = \frac{1}{MN} \sum_{i=0}^{M} \sum_{j=0}^{N} Bp_{i,j}$;

$$\sigma_B^2 = \frac{1}{MN} \sum_{i=0}^{M} \sum_{j=0}^{N} (B_{i,j} - B^*_{i,j});$$

$$\sigma_{Bp}^2 = \frac{1}{MN} \sum_{i=0}^{M} \sum_{j=0}^{N} (Bp_{i,j} - Bp^*_{i,j});$$

$$\sigma_{B,Bp} = \frac{1}{MN} \sum_{i=0}^{M} \sum_{j=0}^{N} (B_{i,j} - B^*_{i,j})(Bp_{i,j} - Bp^*_{i,j}).$$

Rys. 6. Porównanie wzorów (2.53-2.58) rozprawy ze wzorem (2) w publikacji [131].

Tabela 2.2

Relacja wartości subiektywnej do obiektywnej oceny OC

UWJ (ocena obiektywna)	Ocena ekspercka (subiektywna)	
1–0.8	"5"	„Bardzo dobry"
0,8–0,6	"4"	„Dobry"
0,6–0,4	"3"	"Dostateczny"
0,4–0,2	"2"	„Dopuszczający"
0,2–0	"1"	„Niedostateczny"

Tabela 2.3

Ocena jakości OC różnych klas z wbudowaną IT

Metody oceny jakości	Klasa 1	Klasa 2	Klasa 3	Klasa 4
OS	0,135	3,803	1	1,238
PSNR	43,828	42,33	40.132	43.203
UWJ	0,999	0,971	1	1
Ocena ekspercka	5	5	5	5

(a) Tabele 2.2. i 2.3 w rozprawie

Таблиця 1

Відповідність значень суб'єктивної і об'єктивної оцінки зображення

УІЯ	Експерт оцінка	
1-0.8	«5»	«Відмінно»
0,8-0,6	«4»	«Добре»
0.6-0.4	«3»	«Задовільно»
0.4-0.2	«2»	«Погано»
0.2-0	«1»	«Дуже погано»

Таблиця 2

Оцінка якості ЦЗ різних класів з вбудованим ТП

Методи оцінки якості	Клас 1	Клас 2	Клас 3	Клас 4
СКВ	0,135	3,803	1	1,238
ПВСШ	56,828	42,33	48,132	47,203
УІЯ	0,999	0,971	1	1
Експертна оцінка	5	5	5	5

(b) Tablice 1 i 2 w publikacji [131]

Rys. 7. Porównanie (a) tabel 2.2 i 2.3 w rozprawie z (b) tablicami 1 i 2 w publikacji [131].

Główne niedociągnięcie algorytmu (błąd), które uniemożliwia poprawną detekcję "zera" w drugim scenariusze (braku oryginalnego obrazu-nośnika u odbiorcy) polega na wzorze (2.45), w którym bit L informacji wstawiany jest do obrazu-nośnika następująco:

Jeśli L=1, wtedy $Bp_{f(x),x} = Bp_{f(x),x} + 1$,

Jeśli L=0, wtedy , $Bp_{f(x),x} = Bp_{f(x),x}$.

W drugim scenariuszu detekcji mylnie zakłada się, że *„jeśli w bitach, które zostały poddane procesowi wbudowania IT, jest jedynka, oznacza to, że wartość bitu piksela został zmieniona na 1, jeżeli zero – wartość piksela nie uległa zmianie*". Błąd polega na tym, że podczas wstawiania nie określa się, który bit ulega zmianie, gdyż ewentualnie (dla L=1) inkrementowana jest wartość piksela, a nie pojedynczy bit. Warto zauważyć, że drugi scenariusz detekcji nie występuje w źródłowej publikacji [131].

Rozdział 3 obejmuje komputerowe symulacje opisanych algorytmów i eksperymenty z filtracją obrazów. Motywacją zastosowania dolno-przepustowej filtracji obrazu (w pkt. 3.5) jest wykrywanie ataku (zniekształcenia) polegającego na wygładzaniu obrazu. Opis tego punktu jest tłumaczoną kopią współautorskiego artykułu [33] (ilustracją tego faktu są rysunki 8-10).

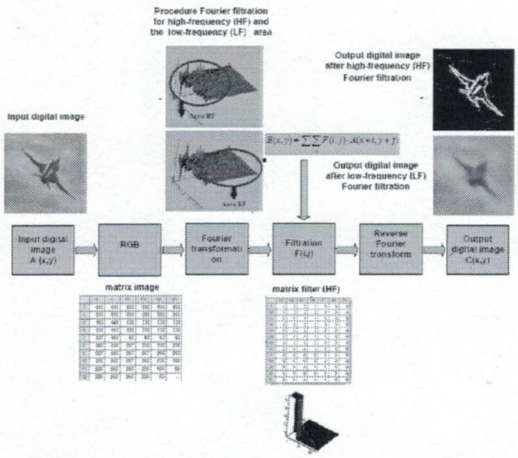
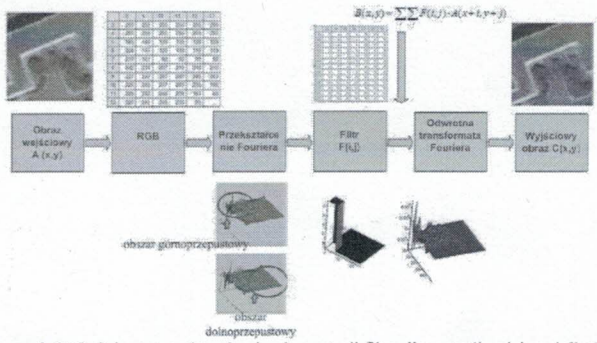


Fig 2. The block diagram of the implementation of frequency filtration for digital image



Rysunek 3.13. Schemat strukturalny implementacji filtracji częstotliwościowej dla OC

(a) (b)

Rys. 8. Porównanie rysunków implementacji filtracji obrazu (a) w publikacji [33] i (b) w rozprawie.

Tabela 3.7
PSNR po zastosowaniu filtrowania typu GP

Przestrzeń barw	PSNR							
	klasa 1		klasa 2		klasa 3		klasa 4	
	%	dB	%	dB	%	dB	%	dB
RGB	19,771	53,668	16,643	53,246	21,435	55,643	12,165	51,175
R	21,205	54,088	17,9	54,053	21,755	55,981	12,568	51,388
G	20,281	55,21	16,966	53,552	21,883	56,011	12,934	51,537
B	17,97	51,706	15,064	52,135	20,666	54,937	10,995	50,601

Tabela 3.8
PSNR po użyciu filtrowania typu DP

Przestrzeń barw	PSNR							
	klasa 1		klasa 2		klasa 3		klasa 4	
	%	dB	%	dB	%	dB	%	dB
RGB	0,343	44,93	7,866	48,525	7,04	48,446	2,475	46,162
R	0,366	45,287	9,741	49,974	7,063	48,635	2,649	46,428
G	0,376	45,257	7,571	48,855	7,261	48,7	2,696	46,417
B	0,287	44,247	6,285	46,746	6,798	48,003	2,08	45,643

Table 1

PSNR after using HF filtration

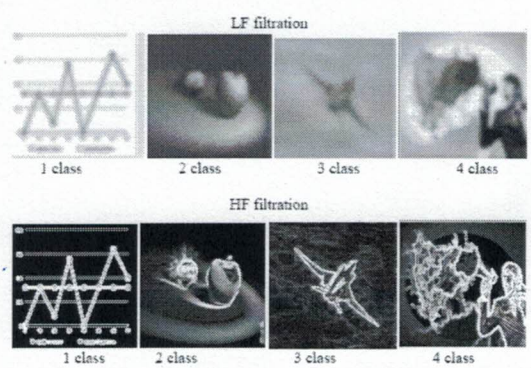
	PSNR τ							
	1 class		2 class		3 class		4 class	
	%	dB	%	dB	%	dB	%	dB
RGB	16.771	53.489	16.321	53.264	20.099	55.153	11.566	50.887
R	17.97	54.088	17.90	54.053	21.755	55.981	12.568	51.388
G	20.281	55.21	16.966	53.552	21.883	56.011	12.934	51.537
B	21.205	55.706	18.064	54.135	21.666	55.937	10.995	50.601

Table 2

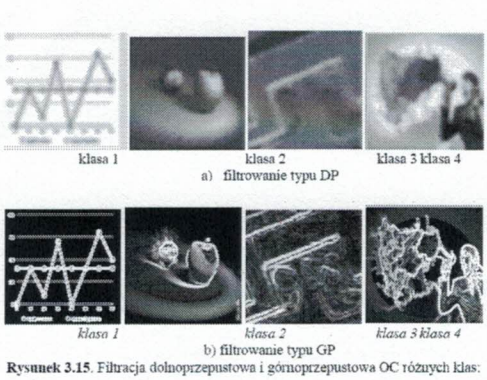
PSNR after using LF filtration

	PSNR							
	1 class		2 class c		3 class		4 class	
	%	dB	%	dB	%	dB	%	dB
RGB	0.598	45.402	10.519	50.363	7.78	48.993	3.324	46.765
R	0.366	45.287	9.741	49.974	7.063	48.635	2.649	46.428
G	0.376	45.257	7.571	48.855	7.261	48.7	2.696	46.417
B	0.287	45.247	9.285	49.746	7.798	49.003	3.08	46.643

Rys. 9. Porównanie wyników liczbowych filtracji zamieszczonych: a) w rozprawie, b) w publikacji [33].



Puc. 4. LF filtration and HF filtration for digital imaging of different classes



Rysunek 3.15. Filtracja dolnoprzepustowa i górnoprzepustowa OC różnych klas:
a) filtrowanie typu DP; b) filtrowanie typu GP

Rys. 10. Porównanie wyników filtracji zamieszczonych: a) w rozprawie, b) w publikacji [33].

Rozdział 4 jest luźno związany z poprzednią treścią rozprawy. Pokazano zrzuty ekranu różnych aplikacji, których przeznaczeniem ma być testowanie metod steganografii i przetwarzania obrazu. Na uwagę zasługuje pkt. 4.5, który podaje zbiorcze wyniki testów głównej metody rozprawy - przestrzenno-pikselowej metody (MPP) steganografii obrazu. Wykonano jedynie eksperymenty własnej metody. Tabela 4.2 podaje wyniki efektywności wstawiania mierzone wartością współczynnika korelacji obrazu nośnika z obrazem zawierającym ukrytą informację sparametryzowane dwoma parametrami: rozmiarem ukrywanej informacji (100%, 75%, 50%, 25% dostępnej pojemności obrazu) i numerem najwyższego zakłócanego bitu. Sugerowana jest zasadnicza wada proponowanej metody do zdolności ukrycia informacji. Jeśli dodanie 1 do wartości piksela powoduje zmianę bitu od dużej wadze (odległego of bitu LSB) to współczynnik korelacji znacznie spada (do 70-90%), co oznacza widoczną zmianę obrazu nośnika po wstawieniu danych. Jednak proponowana metoda **takiej wady nie ma**! Niejasne są dla mnie warunki testów prowadzące do uzyskania wyników zamieszczonych w tabeli 4.3, dlatego nie będę ich komentował. Odporność i podatność metody na różnorodne ataki przedstawiono w tabeli 4.5. Niestety w jednej tabeli najwyraźniej przedstawiono obie, przeciwstawne sobie cechy i zastosowano binarny wskaźnik +/-. Jest to przyczyną mojej dezorientacji pogłębionej jeszcze stwierdzeniami w tekście. W obecnej postaci ten wynik pozostaje niepewny. Pozytywny wynik uzyskano przy konwersji na format gif i jpeg (ale z zastrzeżeniem, że RGB czyli format bezstratny). To odpowiada symbolom plus w tablicy. Ale dlaczego obcięcia i transformata falkowa są też na plus skoro przez to „*doprowadzono do awarii detektora*"? Dlaczego skalowanie i rozciąganie/kompresja są w pelni na plus, skoro „*prowadzi to do częściowego uszkodzenia dekodera*"?

Na koniec w punkcie 4.6 Autorka stara się wyjaśnić strukturę swojej pracy podając schemat blokowy jakiegoś systemowego algorytmu i przez to wytworzyć przynajmniej luźne powiązania pomiędzy elementami tej pracy. Najlepszym miejscem na takie wyjaśnienie struktury pracy (ilustrowanej rysunkiem) powinien być wstęp, a miejscem schematu blokowego systemu – początek rozdziału 4 o tytule „realizacja praktyczna". Niestety schemat na rys. 4.7 pokazuje jedynie, że istnieją 4 równoległe potoki obliczeń, rzadkie powiązania pomiędzy nimi są niezrozumiałe, a numeracje bloków nie odpowiadają numeracji pod-rozdziałów, w których algorytmy poszczególnych bloków są opisane.

Podsumowując analizę treści rozprawy stwierdzam, iż **główny cel rozprawy**, rozumiany jako **nowatorska** metoda steganograficzna, poprawna pod względem algorytmicznym, o nietrywialnej koncepcji bądź implementacji, **nie został osiągnięty** a postawiona teza **nie została pozytywnie zweryfikowana**, ani na podstawie opisu algorytmu ani w wyniku eksperymentów. Rozprawa jest chaotycznym zlepkiem różnych, luźno ze sobą powiązanych rozwiązań algorytmicznych, odwołania do literatury zawierają żenujące błędy, proponowanej metody MPP ani drugiej metody wstawiania w dziedzinie SVD nie porównano z żadną znaną metodą tego typu ani nawet jednej metody z drugą, a udział Doktorantki w opracowanie kluczowych dla rozprawy (współautorskich) algorytmów nie jest dominujący.

4. 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?

Zasadnicza oryginalność rozprawy polega na zaproponowaniu prostej metody MPP do ukrywania informacji, która jednak poza prostotą implementacji nie ma istotnych zalet w porównaniu z szeregiem istniejących rozwiązań. Proponowane są dwie wersje etapu detekcji metody MPP – w warunkach znajomości oryginalnego obrazu nośnika lub przy jego braku. Metoda może być stosowana poprawnie jedynie w pierwszym scenariuszu detekcji, przy założeniu znajomości oryginalnego obrazu nośnika przez odbiorcę. Jednak jest to jedynie nieznaczna modyfikacja podstawowej metody typu LSB, słusznie krytykowanej w rozprawie, ale trywialna w porównaniu z istniejącymi zaawansowanymi metodami wstawiania informacji w dziedzinie obrazu a tym bardziej w dziedzinie częstotliwości czy transformaty SVD. Proponowany algorytm MPP

wstawiania informacji nie może być stosowany w drugim zakładanym scenariuszu detekcji, czyli wtedy, gdy odbiorca nie zna oryginalnego obrazu nośnika. Wymagana jest zmiana algorytmu wstawiania, który powinien wtedy polegać na podstawowym algorytmie typu LSB.

Dużo ciekawsze od głównego algorytmu rozprawy jest metoda wstawiania w dziedzinie SVD i metoda wykrywania ataku wygładzania obrazu. Jednak ich nowatorstwo również jest na niskim poziomie.

W kontekście zastosowania, jakim ma być transmisja ukrytej informacji w Internecie, niezrozumiałe jest stosowanie dziedziny obrazu do ukrywania informacji, zamiast dziedziny kompresji stratnej JPEG czy JPEG2000. Istnieją popularne metody ukrywania informacji w dziedzinie JPEG takie, jak JSteg, OutGess, f5. Przesyłane obecnie obrazy kolorowe z reguły są zadane w postaci skomprymowanej i informacja wstawiona w dziedzinie obrazu zazwyczaj zostanie zniekształcona w wyniku kompresji stratnej obrazu. Autorka jest wprawdzie świadoma istnienia popularnych metod steganografii obrazów, w tym wstawiania w dziedzinie JPEG, gdyż już we wstępie powołuje się na nie, pisząc: „*zwłaszcza Hide and Seek, Jpeg-Jsteg, OutGuess, Steganos, JPHide, F5, Stegdetect i inne, często bazują na metodach i algorytmach pochodzących z badań naukowych*". Jednak w treści rozprawy nie nawiązano bezpośrednio do żadnej z tych metod i nie podjęto wysiłku eksperymentalnego porównania z nimi swoich rozwiązań.

Nie sięgając daleko, Doktorantce zapewne znana jest jej współautora dr hab. O. Yudina - artykuł [Yudin O., Simoniczenko J.A., Simoniczenko A.A.: *Researches of modern steganographic methods and tools for digital image treatments* (tłumaczenie angielskie oryginału w języku ukraińskim), 2017, DOI: 10.18372/2310-5461.34.11610], w którym przebadano 20 metod i narzędzi do steganografii obrazów, publicznie dostępnych w Internecie dla każdego, wstawiających informację w przestrzeni obrazu, czyli będących takiego samego typu jak metoda proponowana w rozprawie: Camouflage, Clotho, DeEgger Embedder, FIRA2, HexaStego – BMP, Hide&Reveal, ImageSpyer, ImageSpyer G2, JHide, Our Secret, QuickStego, Shusssh!, SilentEye, Steganos Privacy Suite 18, Steganos Security Suite 2007, SteganoG, SteganographX Plus, S-Tools, Xiao Steganography, Anubis, Hallucinate, OpenPuff.

Jako przykłady metod wstawiających stego-informację w dziedzinie transformaty DCT w obrazach JPEG można przyjąć, np.: JSteg (D. Upham, 2012) [http://zooid.org/paul/crypto/jsteg/], OutGuess (N. Provos, 2001) http://www.citi.umich.edu/ techreports/reports/citi-tr-01-1.pdf , F5 (A. Westfeld, 2001), StegHide (S. Hetzl, P. Mutzel, 2005).

5. Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?

Pod względem redakcyjnym praca zawiera szereg mankamentów, które sprawiają, że pomimo niektórych ciekawych aspektów treści wymaga ona zasadniczych zmian. Nie cechuje jej ani jasność i czytelność tezy, ani zwięzłość i zogniskowanie badań wokół jednego głównego zagadnienia, ani poprawność metodyczna polegająca na logicznym następstwie zdarzeń – motywacja wskazująca na istniejący problem badawczy, szczegółowa teza pracy, analiza stanu rzeczy i istniejących rozwiązań problemu, propozycja i wyprowadzenie nietrywialnego, poprawnego rozwiązania poprawiającego niedomagania istniejących rozwiązań, wyczerpująca eksperymentalna weryfikacja postawionej tezy rozprawy.

Teza, że coś można zrobić co rozwiązuje zadany problem z pewnym skutkiem jest za słaba w obszarze w którym już istnieją dziesiątki, jeśli nie setki rozwiązań. To nie jest **nowa wiedza,** której powinien dostarczać doktorat. Należy wskazać i eksperymentalnie zweryfikować zalety własnego rozwiązania wobec innych typowych. Nie porównano wyników z żadną inna metodą. A przecież szereg rozwiązań jest dostępnych, nawet z kodem źródłowym.

Eksperymentalna weryfikacja porównawcza powinna uwzględniać kilka ważnych kryteriów. Są nimi: efektywność (robustness), odporność (security), pojemność (capacity). **Efektywność** to minimalizacja wprowadzanych zakłóceń do nośnika (przykłady miar jakości obrazu z ukrytą

informacją – miar podobieństwa z obrazem-nośnikiem: PSNR, SSI, NCC, miara Euklidesa). **Odporność** na ataki polegające na detekcji i rozpoznaniu informacji. **Pojemność** to zdolność do ukrywania długich informacji.

Eksperymentalna weryfikacja powinna być oparta o **dużą bazę obrazów**, dla której istnieją porównywalne wyniki innych metod, a jeśli ich nie ma to przynajmniej zawierać porównanie z innymi znanymi rozwiązaniami tego samego problemu, dla własnej bazy obrazów i różnych długości ukrywanej informacji. Jeśli występuje własna baza obrazów to powinna być dobrze opisana- poprzez podanie typu obrazu – nośnika, jego rozdzielczości, liczby obrazów, z przykładami ilustracji treści obrazów. Warunki wykonania testów i wyznaczania prezentowanych wyników powinny być jasno i szczegółowo wyjaśnione.

6. Jakie są słabe strony rozprawy i jej główne wady?

Praca zawiera szereg istotnych wad:

1. Teza rozprawy jest **mało odkrywcza i zbyt ogólna** oraz **nie reprezentuje w pełni treści rozprawy** (wyjaśnienie podałem w punkcie 1).
2. W analizie „state-of-the-art" porównywane ze sobą są **jedynie typy algorytmów** zamiast odwołania się do konkretnych algorytmów i źródłowych pozycji literatury (patrz punkt 2). Pominięto przedstawienie **konkretnych algorytmów/narzędzi** a także omówienie metod wstawiania w dziedzinie SVD i falkowej oraz metod z elementami pseudo-losowego wstawiania. Pominięto analizę technologii komercyjnych.
3. **Cytowania zawierają zbyt dużo błędnych** odwołań do pozycji nie mających widocznego związku z omawianym tekstem a także odwołania do **słabych artykułów, mało znaczących** w skali międzynarodowej. Niespójność literatury z treścią dla której są cytowane ma charakter **stałej dezinformacji** czytelnika. Relatywnie nieliczne są pozycje literatury istotne z punktu widzenia tematu i tezy rozprawy, ale on także cytowane są bez należytej refleksji i bez ich merytorycznego przedstawienia (patrz uwagi w pkt. 2 i 3).
4. Należy poprawić **strukturę rozprawy**. Rozdział 1 powinien zawierać szczegółowy przegląd metod steganografii obrazu a także podawać stan techniki i technologii komercyjnych w tym obszarze. Prezentacja algorytmu w pkt. 2.5 **„zmodyfikowanej metody wykrywania rozmycia obrazu cyfrowego"** nie może pojawiać się bez uprzedniej **motywacji** i prezentacji **podstawowego algorytmu** (który omawiany jest przypadkowo w pkt. 3.2). Badania filtracji obrazu w pkt. 3.5 są oderwane od głównej treści a powinny stanowić motywację dla algorytmu z pkt. 2.5 i go poprzedzać. Proponowane miary jakości obrazu IFI i SS (pkt. 2.1) nie zostały nigdzie wykorzystane w eksperymentach rozdziału 3 i 4. Punkt 4.6 nie może być podsumowaniem implementacji a powinien być wstępem do rozdziału 4.
5. Na podstawie cytowania w rozprawie i analizy porównawczej prac Doktorantki stwierdzono, że dużą część istotnej treści rozprawy, w tym główny algorytm steganografii obrazu MPP i badania metody filtracji obrazu, **była wcześniej publikowana a Doktorantka nie posiada decydującego udziału** w jej powstaniu (patrz wyjaśnienie w punkcie 3). Należy zmienić tezę pracy, a oba wymienione algorytmy zastąpić wynikami prac o autorskim charakterze.
6. Prawdziwy sens istnienia zmodyfikowanej metody wykrycia rozmycia (pkt. 2.5) może jedynie nadać eksperymentalna weryfikacja tego, że jest skuteczniejsza od prostszych metod. W tym kontekście należy pokazać m.in., że do wykrycia stopnia zmian obrazu nie wystarczy nam proste porównanie ze sobą średnich wariancji bloków obrazu „przedtem" i „potem" (patrz uwaga w pkt. 3).
7. Główny algorytm steganografii obrazu, do którego odnosi się teza pracy, biorąc pod uwagę obecny stan wiedzy i technologii w tej dziedzinie, implementuje **trywialną koncepcję,**

posiada prosty błąd logiczny (w scenariuszu detekcji nr 2), a jego przydatność **nie została zweryfikowana** w wyniku eksperymentalnego porównania z żadną istniejącą metodą (patrz wyjaśnienie w punkcie 3).

8. Rozprawa ma **niejednorodny charakter**, gdyż obok głównego algorytmu proponowane są dwa dalsze algorytmy, jedynie luźno związane z pierwszym i z tezą pracy. Nie podjęto próby ich wykorzystania w procesie eksperymentalnej weryfikacji głównego algorytmu. Pominięto przy tym dużo ważniejsze zagadnienia dotyczące oceny jakości i stopnia bezpieczeństwa algorytmu steganograficznego, jakimi są ocena: minimalizacji wprowadzania zakłóceń **(robustness)**, stopnia bezpieczeństwa przed wykryciem i zniszczeniem **(security)**, dostępnej pojemności – zdolności do ukrywania dużych informacji **(capacity)** (patrz wyjaśnienia w punkcie 4 i 5).
9. Eksperymentalna weryfikacja powinna korzystać z **wystarczająco dużej bazy obrazów**, najlepiej takiej, dla której istnieją porównywalne wyniki innych metod. Alternatywnie można porównać dostępne implementacje innych metod z własnym rozwiązaniem na wystarczająco licznym własnym zbiorze obrazów i stego-obiektach różnej długości (wyjaśnienie w punkcie 5).

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Z uwagi na uprzednio wskazane wady pracy jej przydatność dla nauk technicznych nie jest znacząca. Autorka wprawdzie posiada szereg publikacji badawczych, jednak oceniana rozprawa nie stanowi spójnej i kompletnej metodycznie prezentacji osiągnięcia badawczego o istotnych walorach poznawczych, a **autorski wkład** Doktorantki w powstanie głównego algorytmu i badań filtracji obrazu nie jest dominujący.

Główny cel rozprawy **nie został osiągnięty** a postawiona teza nie została pozytywnie zweryfikowana, gdyż oba algorytmy steganograficzne nie są nowatorskie a ich poprawność i ewentualne zalety nie zostały zweryfikowane w wyniku eksperymentalnego porównania z innymi metodami tego typu. Na negatywną ocenę rozprawy wpływają również: chaotyczna narracja i niespójność elementów pracy, niewłaściwa kolejność i niedociągnięcia struktury pracy, niespójność treści z tezą rozprawy, referowanie wielu mało znaczących prac i ciągła dezinformacja błędnymi odwołaniami do literatury,

8. Do której z następujących kategorii Recenzent zalicza rozprawę:

Końcowa ocena rozprawy jest **negatywna**. Dlatego też rozprawę zaliczam do kategorii

„nie spełniającej wymagań".

Stwierdzam, że recenzowana rozprawa **nie może** być podstawą dla dopuszczenia do dalszych etapów przewodu doktorskiego.

Kasprzak

.....

/ Włodzimierz Kasprzak /