ZACHODNIOPOMORSKI UNIWERSYTET TECHNOLOGICZNY w SZCZECINIE

WYDZIAŁ INFORMATYKI

KATEDRA INŻYNIERII OPROGRAMOWANIA

mgr inż. Łukasz Nozdrzykowski

Metoda kształtowania kluczy steganograficznych dla cyfrowych środowisk graficznych

Rozprawa Doktorska

PROMOTOR:
prof. dr hab. inż. Korostil Yuriy

SZCZECIN 2013

Podziękowania:

Składam serdeczne podziękowania wszystkim, którzy przyczynili się do powstania niniejszej pracy, a w szczególności:

- prof. dr hab. inż. Jerzemu Korostilowi za opiekę naukową w trakcie moich studiów doktoranckich oraz pomoc merytoryczną podczas realizowania niniejszej pracy naukowej,
- moim rodzicom, siostrze Monice oraz ukochanej Magdzie i wszystkim bliskim za całe wsparcie w motywacji podczas pisania pracy.

Spis treści

1. Wstęp

Rozdział ten stanowi wprowadzenie do omówienia problematyki poruszanej w niniejszej rozprawie doktorskiej. W podrozdziale 1.1 przedstawiono uzasadnienie podjęcia tematu oraz lukę poznawczą, a także dziedzinę problemu, do której została niniejsza praca zakwalifikowana. W podrozdziale 1.2 zdefiniowano cel pracy oraz jej tezę badawczą, a także metodykę prowadzonych badań. W podrozdziale 1.3 przedstawiono strukturę pracy z krótką charakterystyką jej rozdziałów.

1.1 Stan problemu

Od końca lat dziewięćdziesiątych uaktywniły się badania w kierunku cyfrowej steganografii opisującej metody ukrywania informacji w innych wiadomościach stanowiących dla nich kontener. Do rozwoju metod steganografii przyczyniła się także rosnąca popularność Internetu, zwłaszcza w początku XXI wieku, która trwa do dnia dzisiejszego. Internet stał się wygodnym i uniwersalnym medium przesyłu informacji. Jego popularność, rozległość oraz pojemność sprawia, że codziennie w globalnej sieci krąży ogromna ilość danych. To właśnie ta cecha sprawia, że Internet stał się dogodnym medium w transferze informacji ukrywanych metodami steganograficznymi. Ważną zaletą steganografii jest fakt, że umożliwia ona ukrywanie dodatkowych porcji wiadomości w różnych nośnikach, zwanych także kontenerami, a są nimi przykładowo pliki graficzne lub muzyczne. Steganografia jest częścią systemów ochrony informacji.

Systemy ochrony informacji mogą zapewnić wiele usług takich, jak: autoryzacja, identyfikacja i niezaprzeczalność pochodzenia informacji oraz poufność i integralność przekazywanych danych. Najważniejszą usługą jest ukrycie informacji przed osobą niepowołaną. Podział systemu ukrywania informacji przedstawia rysunek 1.

Rys. 1. Podział systemów ukrywania dodatkowej informacji wg Rossa Andersona [1, 2]

Systemy te oznaczają [1, 2]:

- Cyfrowy znak wodny – służy on do umieszczania wewnątrz pewnej informacji nośnej, wiadomości, która w większości przypadków jest sygnaturą autora lub właściciela. Najczęściej znaki wodne są wykorzystywane właśnie do ochrony własności intelektualnej i praw autorskich.
- Funkcje skrótu – są to specjalne procedury, które mogą jednoznacznie określić daną wiadomość. Idea funkcji skrótu jest taka, aby nie istniała żadna inna wiadomość, której skrót byłby taki sam jak skrót bieżącej wiadomości. Ogólnie, cyfrowe znaki wodne stosowane są do sprawdzania oryginalności utworu, natomiast funkcje skrótu do identyfikacji jego konkretnego egzemplarza.
- Łączność anonimowa – jej zadaniem jest zapewnienie komunikującym się podmiotom odpowiedniego poziomu anonimowości i prywatności.
- Kanały ukryte i podprogowe – służą do tajnego komunikowania się podmiotów przy wykorzystaniu innych jawnych kanałów komunikacji. Wykorzystana jest tu nadmiarowość jawnych, weryfikowalnych przez zaufaną stronę trzecią, informacji. W ramach tych informacji przesyłane są dodatkowe dane bez ich ujawnianie stronie, która weryfikuje kanał informacji. Zazwyczaj jako kanały podprogowe rozumie się sytuację, gdy do tego celu stosuje się schematy podpisów cyfrowych.
- Łączność specjalna – są to systemy, których działanie polega na zapewnieniu stronom komunikującym się bezpiecznego kanału komunikacji, trudnego do wykrycia dla przeciwnika.
- Steganografia – tutaj oznacza ona wszystkie inne sposoby ukrywania dodatkowych porcji informacji, co znacznie rozszerza podstawowe znaczenie tego pojęcia.

Steganografia w ogólnie przyjętym pojęciu jest systemem ochrony informacji, w którym wiadomość ukrywana jest w innej wiadomości (zwanej informacją nośną), w taki sposób, aby potencjalny agresor nie był w stanie stwierdzić zaistnienia tego faktu.

Początkowo metody steganograficzne pozbawione były kluczy, które zwiększałyby bezpieczeństwo dla ukrywanej informacji przed jej odczytaniem. Gwarantowane przez nie bezpieczeństwo dla ukrywanej informacji opierało się w głównej mierze na zabezpieczeniu przed wykryciem przekazu steganograficznego. Większość z takich metod przedstawiono w pracy [3]. Ponadto metody takie zabezpieczały głównie przed jednym bądź kilkoma formami ataków na ukrywany przekaz. Systemy takie w znacznej mierze określa się mianem steganografii słabej [4]. Z czasem, aby zwiększyć bezpieczeństwo systemów pozbawionych klucza steganograficznego zaczęto stosować dodatkowe metody kryptograficzne budując systemy steganokryptograficzne. Odmienną zasadę stosuje się w przypadku steganografii silnej, gdzie wiadomości nie można zniszczyć w łatwy sposób, ani też nie można w łatwy sposób wykryć faktu zaistnienia przekazu steganograficznego.

Szczególnie istotnymi dla steganografii są kolorowe obrazy graficzne. Wynika to z ich popularności w wykorzystywaniu takich obrazów jako kontener do przenoszenia dodatkowych porcji wiadomości. Swoją popularność zawdzięczają głównie Internetowi, gdzie obrazy, pliki wideo oraz dźwięk stanowią ogromną część danych jaka jest na co dzień przesyłana. To właśnie obrazy stanowią obok treści tekstowej główną zawartość znacznej części stron internetowych. Obrazy graficzne stanowią niejako budulec stron w ich szablonach oraz uzupełnienie treści, jako zachęta do przeczytania danej zawartości strony oraz w przeróżnych poradach i artykułach jako uzupełnienie treści dla lepszego jej zrozumienia.

Głównym problemem podczas tworzenia nowoczesnych algorytmów steganograficznych dla obrazów cyfrowych w przypadku silnej steganografii jest to, w jaki sposób rozszerzyć dowolną metodę steganograficzną o klucz, w ten sposób, aby zapewnić jak najlepsze bezpieczeństwo dla ukrywanej informacji. Problemem jest tutaj to, jak powiązać klucz ze sposobem ukrywania danych, tak aby jednocześnie zachować możliwość odtworzenia ukrytej wiadomości.

Kolejnym problemem związanym ze steganografią w obrazach cyfrowych jest sposób wyznaczania miejsc ukrywania informacji. Często metody ukrywania wiadomości wykorzystują proste przekształcenia polegające na klasycznej zamianie bitów w kontenerze. Zabezpieczenie przed możliwością wykrycia polega na podmianie

jedynie najmniej znaczących bitów. Problemem jest zatem zapewnienie określonego stopnia niewidoczności przed wykryciem ponieważ wizualna możliwość wykrycia istnienia dodatkowego przekazu dyskwalifikuje proponowaną metodę steganograficzną. Ważny jest zatem dobór miejsc ukrywania wiadomości, tak aby ewentualne zniekształcenia pozostawały nadal niezauważone.

Drugim elementem budowania algorytmów steganograficznych jest określenie w jaki sposób wyznaczać miejsca ukrywania wiadomości metodą steganograficzną w obrazach cyfrowych. Problem ten dotyczy wyznaczania zarówno obrazów przydatnych pod kątem ukrywania w nich określonych porcji danych oraz miejsc ich ukrycia w wybranym obrazie cyfrowym. W pierwszym przypadku należy zapewnić, aby kontener będący nośnikiem wiadomości posiadał odpowiednią pojemność oraz aby istniał silny stopień zróżnicowania pomiędzy pikselami, żeby po ukryciu wiadomości wszelkie zmiany w żaden sposób nie zostały uwidocznione dla ludzkiego oka. W drugim przypadku mowa jest o wyborze konkretnych miejsc ukrywania wiadomości w kolorowych obrazach cyfrowych. Miejsca ukrywania wiadomości powinny charakteryzować się dużą różnorodnością. Nie powinny być to obszary jednolite, tak aby powstające zmiany w obrazie nie zostały ujawnione obserwatorowi.

Trzecim problemem, którym należy się zająć jest odpowiedzenie na pytanie, w jaki sposób połączyć miejsca ukrywania informacji z kluczem steganograficznym. Klucz taki powinien określać w pełni miejsce ukrycia wiadomości w obrazie cyfrowym wraz z wyborem tych miejsc oraz sposób przechodzenia po obrazie określający kolejność wykorzystania konkretnych miejsc do ukrywania kolejnych porcji danych.

Należy podkreślić tu brak istnienia metod steganograficznych z bezpiecznym kluczem steganograficznym, który określa sposób działania tych algorytmów wskazując na sposób ukrywania wiadomości oraz jej uwikłania w obrazie docelowym. Brak jest także zaawansowanych metod klasyfikacji obrazów pod kątem ich przydatności do ukrywania w nich określonej porcji danych oraz zaawansowanych metod doboru miejsc ukrycia wiadomości metodami steganograficznymi w cyfrowych obrazach graficznych. Kolejnym ważnym zagadnieniem jest brak zaawansowanych metod oceny zniekształceń jakie powodują algorytmu ukrywania wiadomości w sposób steganograficzny.

W niniejszej pracy zaprezentowano własne metody określania niewidoczności zmian w obrazach cyfrowych oparte na wybranych parametrach obrazu, które łącząc z funkcją czułości kontrastu pozwalają na wybór odpowiednich obrazów pod kątem ukrywania w nich danych oraz miejsc ukrycia tych wiadomości. Zaprezentowano także

algorytm steganograficzny oparty na kluczu steganograficznym. Metody te mogą zostać zastosowane do budowy algorytmów steganograficznych z kluczem, których wykorzystanie zwiększa bezpieczeństwo dla ukrywanej wiadomości.

Główną ideą zaproponowanego rozwiązania jest wyznaczanie obrazów z bazy obrazów na podstawie parametrów świadczących o stopniu zróżnicowania obrazów oraz wybór miejsc ukrywania informacji zależny od klucza. Wszystkie te operacje są realizowane poprzez zastosowanie funkcji czułości kontrastu jako miary niewidoczności zmian w obrazach cyfrowych.

Dokonano próby zbudowania modelu niewidoczności zmian powstających w procesie ukrywania wiadomości poprzez potraktowanie wiadomości jako szum, a następnie porównanie wyników z rzeczywistym algorytmem steganograficznym.

Celem niniejszej pracy jest wypełnienie luki poznawczej, poprzez opracowanie metod uzupełniania algorytmów steganograficznych o klucz.

Prezentowana praca leży w dziedzinie nauk technicznych, w dyscyplinie naukowej Informatyka. Problematyka w niej poruszania leży w zakresie przetwarzania obrazów, teorii zbiorów przybliżonych oraz kryptografii i steganografii. Wyniki pracy zostały przedstawione zarówno w czasopismach polskich, jak i zagranicznych prezentując je na konferencjach o zasięgu międzynarodowym.

1.2. Cel i teza pracy

Istnieje wiele metod steganograficznych ukrywania informacji w obrazach cyfrowych. W znacznej części są to algorytmy oparte o proste przekształcenia bazujące jedynie na zamianie najmniej znaczącego bitu (metoda LSB), jako gwaranta zapewnienia niewidoczności dla ukrywanej wiadomości. Kolejna część algorytmów rozszerza metodę LSB o prosty klucz. Następną klasą algorytmów są algorytmy oparte o dziedzinę transformat, w których dochodzi do modyfikacji współczynników. Są to zazwyczaj transformaty kosinusowe oraz falkowe. W przypadku pierwszym, algorytmy najczęściej wykorzystują zamianę wybranych par współczynników, zaś w drugim, zamianę współczynników lub zmianę wartości współczynnika poprzez modyfikację jego bitów składowych.

Algorytmy jakie powstawały zostały lub nie zostały rozbudowane o klucz steganograficzny. W przypadku metod, gdzie brakuje klucza, wiadomość ukrywana jest

w kolejnych pikselach/obszarach obrazu bez różnicy czy spowoduje to widoczne czy niewidoczne zmiany w obrazie. W drugim przypadku wykorzystywane są proste algorytmy z kluczem, gdzie klucz ten określa w sposób matematyczny miejsce ukrycia wiadomości. Przykładem mogą być algorytmy oparte o generatory pseudolosowe mówiące, gdzie ukrywana jest kolejna porcja danych.

Bezpieczeństwo proponowanego w pracy przez autora rozwiązania polega na ukrywaniu wiadomości w kolorowych obrazach cyfrowych w sposób niezauważalny dla ludzkiego oka, przy czym cały proces ukrywania zależy od zastosowanego klucza steganograficznego i zapewnia niemożliwość odczytania wiadomości w rozsądnym czasie.

Cel pracy został sformułowany następująco: **Opracowanie metody kształtowania kluczy i metody wyznaczania niewidoczności zmian w obrazach jako mechanizmu zwiększającego bezpieczeństwo metody steganograficznej**.

Prowadzone badania służyły do udowodnienia następującej tezy badawczej.

Zastosowanie metody kształtowania kluczy i połączenie jej z metodą steganograficzną opartą o badanie niewidoczności zmian w obrazach poprawia bezpieczeństwo ukrywanej informacji przed wykryciem.

Dla udowodnienia podstawowej tezy naukowej należy przeprowadzić badania na temat pojemności medium transmisji, niewidoczności wprowadzanych zmian w sposób steganograficzny, opracować algorytm steganograficzny klucza oraz przeprowadzić badania jego efektywności i bezpieczeństwa.

Obecnie stosowane algorytmy steganograficzne nie stosują kluczy steganograficznych lub stosują jedynie klucze proste. Celem prowadzonych przez autora badań było opracowanie metody kształtowania klucza o charakterze rozproszonym, czyli takim, gdzie klucz działałby na każdym etapie algorytmu ukrywania wiadomości.

W pracy pokazano, iż obrazy cyfrowe można z powodzeniem wykorzystywać jako nośniki informacji. Obrazy cyfrowe charakteryzują się dużą pojemnością, a wiadomość w nich ukrywana, po spełnieniu określonych warunków, staje się niezauważalna dla potencjalnego obserwatora. Jednocześnie przesył ukrytej wiadomości w obrazie poprzez Internet sprawia, że wiadomość taka staje się trudna do wykrycia już z samego faktu ilości danych jakie są przesyłane globalną siecią. Przy tak dużej ilości obrazów jaka przesyłana jest poprzez Internet, zastosowanie metody

wykrywania faktu użycia steganografii staje się zadaniem o dużej złożoności obliczeniowej.

Przedstawiono metodę oceny zniekształceń powodowanych poprzez algorytmy steganograficzne wykorzystującą charakterystykę ludzkiego wzroku. Zaproponowano wykorzystanie funkcji czułości kontrastu jako miary niewidoczności zmian w obrazach cyfrowych. Poprzez tą metodę można określać następnie miejsca przydatne pod kątem ukrywania w nich określonych porcji danych.

W odniesieniu do funkcji czułości kontrastu, dokonano oceny możliwości wykorzystania grupy charakterystycznych parametrów obrazu pod kątem opracowania metody wyboru obrazów przydatnych do ukrywania w nich określonej porcji danych w sposób niezauważalny wizualnie. Aby uniezależnić się od dowolnego algorytmu steganograficznego zaproponowano wykorzystanie szumu jako symulacji użycia fizycznego algorytmu ukrywania informacji w obrazach. Przedstawiono analizę istotności tych atrybutów w odniesieniu do poziomu niewidoczności zmian kontrastu reprezentowanych przez funkcję czułości kontrastu.

Na koniec zaprezentowano algorytm steganograficzny z kluczem oparty na prezentowanych w pracy wynikach badań naukowych. Algorytm ten wykorzystuje prezentowaną metodę doboru obrazów z bazy, wybór miejsc ukrycia wiadomości oraz operację ukrywania tej wiadomości w kolorowych obrazach cyfrowych.

1.3. Struktura pracy

Praca została podzielona na sześć rozdziałów, które w całości kolejno służą udowodnieniu stawianej tezy naukowej. Poniżej przedstawiono zawartość merytoryczną każdego z nich.

W rozdziale pierwszych zaprezentowano główne założenia pracy, w tym problematykę, cel i tezę badawczą, motywację do podjęcia tematu rozprawy oraz budowę pracy.

W rozdziale drugim uzasadniono wybór cyfrowego środowiska graficznego jako medium do ukrywania w nim wiadomości algorytmami steganograficznymi.

W rozdziale trzecim przedstawiono aktualny stan wiedzy na tematu ukrywania wiadomości w systemach ochrony informacji ze szczególnym uwzględnieniem metod steganograficznych wykorzystujących klucz steganograficzny.

W rozdziale czwartym przedstawiono wyniki badań nad niewidocznością zmian w obrazach cyfrowych opartą o charakterystyczne parametry obrazu oraz funkcję czułości kontrastu, które służą do budowania algorytmu silnej steganografii wykorzystującego klucz steganograficzny.

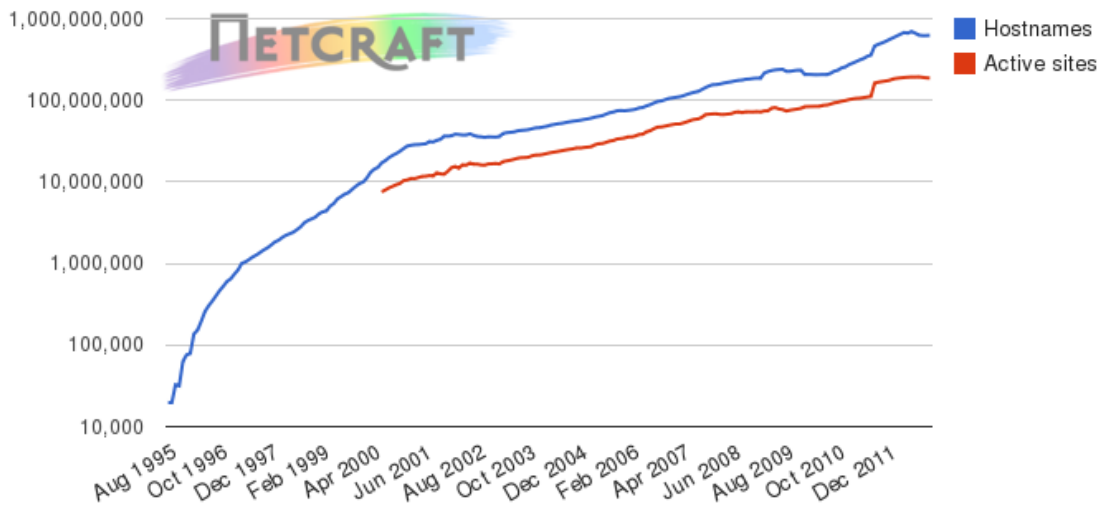
W rozdziale piątym przedstawiono algorytm steganograficzny oparty na badaniach przeprowadzonych w pracy uzupełniony o klucz steganograficzny.

W rozdziale szóstym przedstawiono krótkie podsumowanie proponowanych metod.

2. Analiza ruchu w Internecie dla określenia miary możliwości wykorzystania plików graficznych do steganografii

Dzięki znacznej ilości obrazów jakie są przesyłane codziennie w globalnej sieci Internet, można ukrywać wiadomości w obrazach, które następnie zostaną przesłane w sieci lub umieszczone na witrynach internetowych.

Obecnie w sieci Internet istnieje 625 329 303 stron internetowych (stan na dzień 1.11.2012 rok) wg raportu Netcraft. Liczba witryn w sieci rośnie w znacznym tempie co przedstawiają najnowsze statystyki tej organizacji [5] zaprezentowane na rysunku 2.



Rys.2. Ilość stron internetowych wg statystyk Netcraft [5]

Netcraft jest firmą usług internetowych w Bath w Wielkiej Brytanii. Dostarcza ona wyniki najnowszych badań i analiz związanych z wieloma aspektami Internetu, którego bada od 1995 roku.

W raporcie [6] przedstawiono informacje na temat liczby użytkowników w poszczególnych rejonach świata oraz ogólnoświatowe podsumowanie. Przedstawia to tabela 1.

Tabela 1. Podsumowanie liczby użytkowników Internetu w poszczególnych rejonach świata [6]

Region	Populacja w 2009 roku	Liczba użytkowników Internetu
Afryka	991 002 342	**67 371 700**
Azja	3 808 070 503	**738 257 230**
Europa	803 850 858	**418 029 796**
Środkowy wschód	803 850 858	**57 425 046**
Ameryka Północna	340 831 831	**252 908 000**
Ameryka Południowa i Karaiby	586 662 468	**179 031 479**
Australia i Oceania	34 700 201	**20 970 490**
Świat	6 767 805 208	**1 733 993 741**

W Polsce według danych przedstawionych w roczniku statystycznym Głównego Urzędu Statystycznego [7] z roku 2011, dostęp do komputera w 2010 roku posiadało 59,6% wszystkich gospodarstw domowych, w tym z dostępem szerokopasmowym do Internetu 43,3%, przy czym ogólna populacja kraju wynosiła 38,2 miliona ludzi. Według Małego Rocznika Statystycznego na rok 2012 wzrosła liczba gospodarstw posiadających komputer do poziomu 66.7 procenta. Obecnie 62.3 procent gospodarstw posiada dostęp do Internetu [8].

W pracy [9] przedstawiono dane statystyczne wykorzystania sieci, jakie uzyskano z dwuletniego monitoringu około 110 ISP (dostawców Internetu), włączając w to około 2949 routerów ze 441 528 interfejsów i szacując około 25% całego ruchu pomiędzy domenami. Monitorowana przepustowość wynosiła około 14Tbps i obserwowano transfer około 264 eksabajtów danych. Monitoring sieci był prowadzony w latach 2007-2009. Procentowe przedstawienie wykorzystania wybranych portów/protokołów przedstawia tabela 2.

Tabela 2. Procentowy wykorzystania wybranych protokołów w sieci

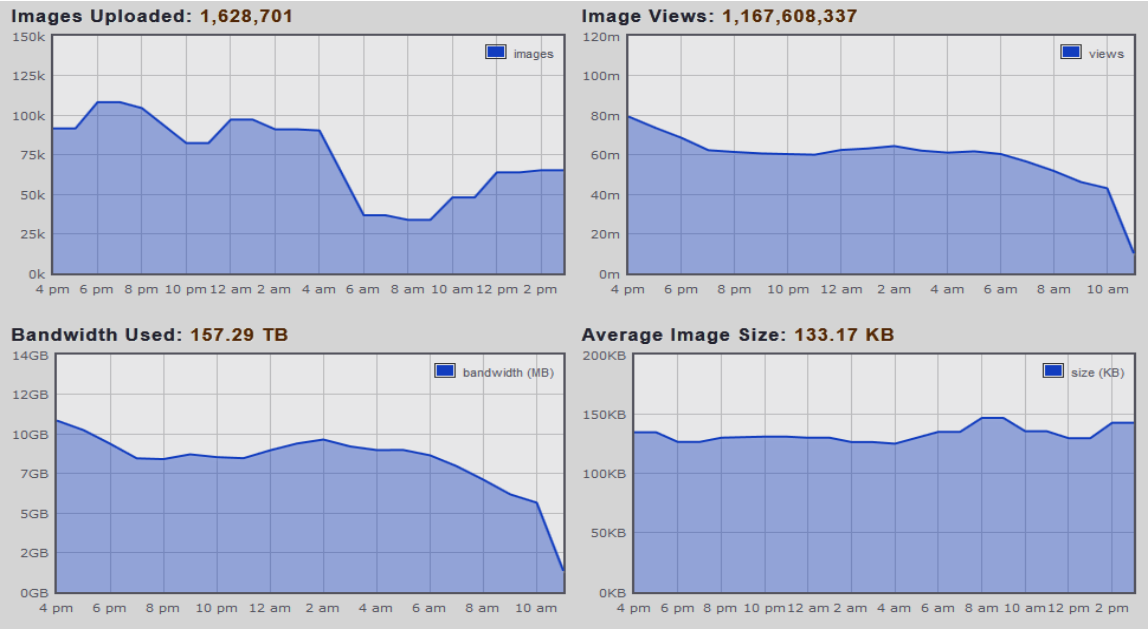
Miejsce	Aplikacja	2007	2009	Zmiana
1	Web	41,68	52,00	+10,31
2	Video	1,58	2,64	+1,05
3	VPN	1,04	1,41	+0,38
4	Email	1,41	1,38	-0,03
5	News	1,75	0,97	-0,78
6	P2P	3,96	0,85	-2,11
7	Games	0,38	0,49	+0,12
8	SSH	0,19	0,28	-0,08
9	DNS	0,20	0,17	-0,04
10	FTP	0,21	0,14	-0,07
	Inne	2,56	2,67	+0,11
	Niesklasyfikowane	46,03	37,00	-9,03

2.1. Analiza możliwości wykorzystania serwisów internetowych

Aby możliwe było mówienie o wykorzystaniu obrazów cyfrowych w steganografii należy przeanalizować trafność wykorzystania obrazów w Internecie do ukrywania w nich informacji.

W Internecie można znaleźć wiele serwisów, które udostępniają statystyki na temat użycia swoich zasobów. W badaniach wybrano dwa serwisy: hosting obrazów imgur.com oraz portal komputerowy HotFix.pl.

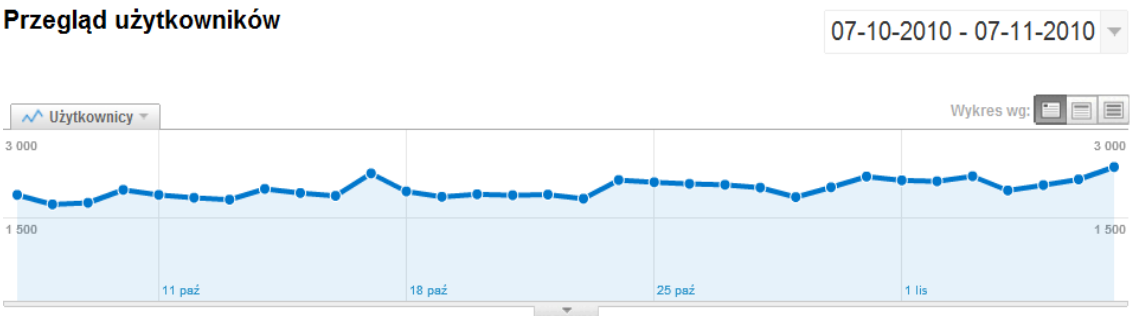
W przypadku hostingu plików imgur.com można uzyskać dane na temat liczby wysyłanych na serwer obrazów, liczby wyświetleń, liczby wysyłanych danych w bajtach oraz średnią wielkość z obrazów na serwerze. Statystyki są zbierane w odstępie 24 godzinnym. Przykładowe dane dla dnia 17 listopada 2012 roku przedstawia rysunek 3 [10].



Rys. 3. Wybrana statystyka dzienna serwisu imgur.com [10]

Statystyki te pokazują jak doskonałym kanałem transmisji mogą być hostingi plików, w tym głównie graficznych. Korzystając z serwisu typu Imgur można uzyskiwać terabajtowe kanały transmisji, co należy uwzględniać podczas określania miary widoczności ukrytej w pliku wiadomości. Niewątpliwą zaletą takich hostingów jest fakt, że pliki pozostają na nich dłuższy czas oraz fakt, że same pliki nie są uwidaczniane na żadnych stronach, więc odbiorca musi znać adres do tak umieszczonego na serwerze obrazu.

Przeprowadzono także analizę ruchu portalu internetowego Hotfix.pl należącego do autora pracy z wykorzystaniem narzędzia Google Analytics [11] w celu zidentyfikowania możliwości wykorzystania specjalnie przygotowanych stron internetowych do umieszczania tajnych informacji. Dane dotyczące miesięcznych odwiedzin strony przedstawia rysunek 4.



Rys.4. Miesięczne zestawienie liczby użytkowników serwisu HotFix.pl

W okresie od 7 października do 7 listopada 2010 roku na testowanej stronie zanotowano następujące statystyki:

- 73 435 odwiedzin,
- 59 532 bezwzględna liczba niepowtarzalnych użytkowników,
- 118 581 odsłon,
- 1,61 średnia liczba odsłon,
- 00:02:22 średni czas spędzony w witrynie,
- 77,88% nowych odwiedzin.

Dane statystyczne witryny dla dnia 7.11.2010 rok:

- 2796 odwiedzin,
- 2423 bezwzględna liczba niepowtarzalnych użytkowników,
- 4352 odsłon,
- 1,56 średnia liczba odsłon,
- 00:02:37 średni czas spędzony w witrynie,
- 77,40% nowych odwiedzin.

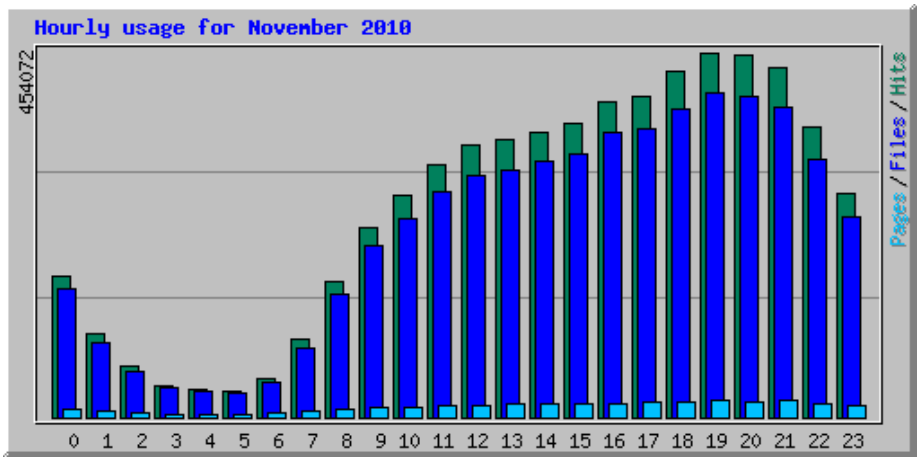
Witryna ta charakteryzuje się stałym poziomem odwiedzalności na poziomie 2500-2700 użytkownik unikalnych dziennie, które średnio przeglądają 1,6 podstron dziennie. Dane te zostały zebrane na podstawie wklejonego kodu języka JavaScript dostarczonego przez firmę Google. Niestety wadą tego mechanizmu jest fakt, że system ten nie rejestruje osób z wyłączoną obsługą tego języka, co też można zaobserwować w statystykach serwera narzędzia Webalizer. W celu pozyskania dokładniejszych danych wykorzystano skrypt Webalizer, który działa bezpośrednio na serwerze hostingu danej witryny. Statystyki za listopad 2010 przedstawia tabela 3.

Tabela 3. Miesięczny przegląd statystyk serwisu HotFix.pl

Daily Statistics for November 2010												
Day	Hits		Files		Pages		Visits		Sites		KBytes	
1	214660	3.46%	192376	3.47%	9292	3.00%	2895	3.05%	4325	3.77%	1471369	3.06%
2	202344	3.26%	181267	3.27%	9575	3.09%	2993	3.15%	4321	3.77%	1378289	2.87%
3	200406	3.23%	179511	3.24%	9955	3.21%	3155	3.32%	4398	3.84%	1319284	2.75%
4	177852	2.87%	159182	2.87%	9281	2.99%	2890	3.04%	4238	3.70%	1185479	2.47%
5	196952	3.18%	173215	3.13%	9273	2.99%	2977	3.13%	4674	4.08%	1477077	3.08%
6	199426	3.22%	180217	3.25%	9108	2.94%	3115	3.28%	5790	5.05%	1787832	3.72%
7	232020	3.74%	209059	3.77%	9862	3.18%	3485	3.67%	6137	5.35%	2032263	4.23%
8	207354	3.34%	187005	3.38%	9168	2.96%	3183	3.35%	5548	4.84%	1818593	3.79%
9	197521	3.18%	177169	3.20%	9019	2.91%	3091	3.25%	5594	4.88%	1713674	3.57%
10	183782	2.96%	165951	3.00%	10275	3.32%	2951	3.11%	5228	4.56%	1614337	3.36%
11	238326	3.84%	213278	3.85%	10820	3.49%	3564	3.75%	6348	5.54%	2128983	4.43%
12	211810	3.42%	187747	3.39%	10459	3.37%	3383	3.56%	5769	5.03%	1858761	3.87%
13	204272	3.29%	181307	3.27%	10416	3.36%	3250	3.42%	5630	4.91%	1804434	3.76%
14	224796	3.62%	204249	3.69%	10409	3.36%	3520	3.70%	5971	5.21%	1977284	4.12%
15	210352	3.39%	186803	3.37%	9852	3.18%	3271	3.44%	5507	4.80%	1836048	3.82%
16	215626	3.48%	190478	3.44%	9999	3.23%	3204	3.37%	5541	4.83%	1894916	3.95%
17	219242	3.54%	195415	3.53%	12106	3.91%	3308	3.48%	5795	5.06%	1927256	4.01%
18	220766	3.56%	194549	3.51%	12115	3.91%	3257	3.43%	5545	4.84%	1936277	4.03%
19	205736	3.32%	185656	3.35%	12152	3.92%	3113	3.28%	5399	4.71%	1877485	3.91%
20	212447	3.43%	191819	3.46%	13616	4.39%	3183	3.35%	5605	4.89%	1978337	4.12%
21	220602	3.56%	197157	3.56%	11578	3.74%	3456	3.64%	4493	3.92%	1523634	3.17%
22	201437	3.25%	178167	3.22%	11931	3.85%	3067	3.23%	3924	3.42%	1285851	2.68%
23	209825	3.38%	182248	3.29%	9854	3.18%	3186	3.35%	4106	3.58%	1277228	2.66%
24	210030	3.39%	187586	3.39%	10459	3.37%	3255	3.43%	4103	3.58%	1336647	2.78%
25	202821	3.27%	181053	3.27%	9863	3.18%	3137	3.30%	3867	3.37%	1274631	2.65%
26	196057	3.16%	174658	3.15%	10162	3.28%	2983	3.14%	3649	3.18%	1270083	2.64%
27	199564	3.22%	177619	3.21%	10207	3.29%	3066	3.23%	3784	3.30%	1291933	2.69%
28	208641	3.36%	187964	3.39%	9628	3.11%	3296	3.47%	4054	3.54%	1324476	2.76%
29	195691	3.16%	174141	3.14%	9487	3.06%	3006	3.16%	3625	3.16%	1256491	2.62%
30	181309	2.92%	163677	2.95%	9986	3.22%	2958	3.11%	3478	3.03%	1162928	2.42%

Analiza prezentowanych danych daje podstawę do zaobserwowania, że największy ruch generowany jest w dni wolne, jakimi są sobota oraz niedziela, z wyłączeniem świąt. Stronę w dniu 7 listopada 2010 odwiedziło 3485 osób, które przeglądały 9862 strony generując ruch w wysokości około 2GB. Dokonując analizy ruchu witryny warto także przedstawić jej ruch godzinowy. Okazuje się bowiem, że

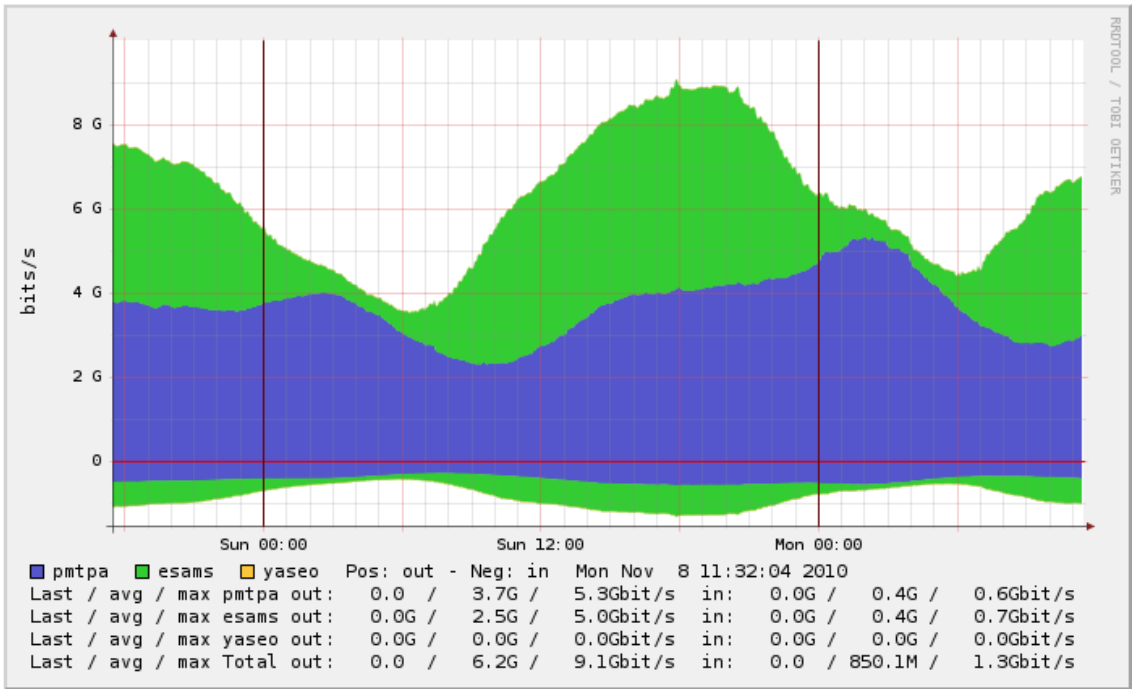
ruch nie jest stały i notowane są godziny najwyższej oglądalności. Sytuację tą przedstawia wykres na rysunku 5.



Rys. 5. Użycie serwisu HotFix.pl dla miesiąca Listopad 2010

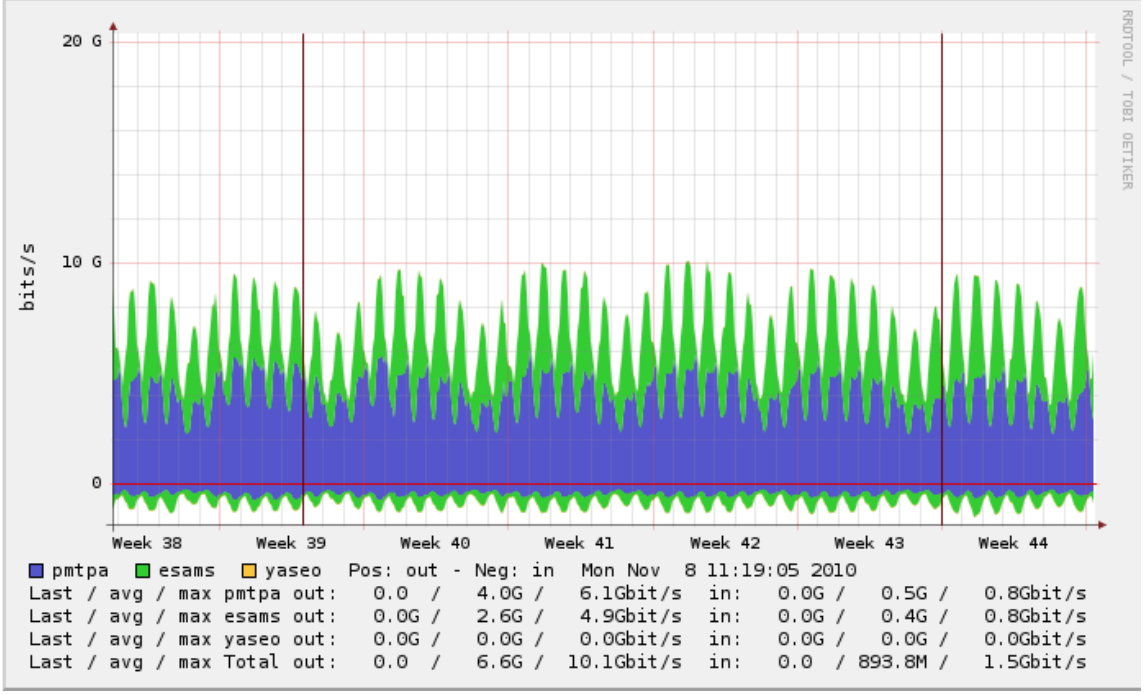
Jak uwidaczniają to dane na prezentowanym wykresie, strona generuje znikomy ruch w okresie nocnym, zaś największy ruch notowany jest w godzinach wieczornych, około godziny 20.00. Sytuację to potwierdzają także dwuletnie obserwacje statystyk tej witryny.

Przypuszczenia co do godzinowych wahań w ruchu sieciowym potwierdzają także statystyki sieciowe Nedwords [12] o ruchu do 9,1Gb/s, co zaprezentowano na rysunku 6.



Rys. 6. Statystyki sieciowe dzienne Nedwords w miesiącu listopad 2010 [12]

Zgodnie ze statystykami godzinowymi, najwyższy ruch dochodzący do granicy 9 Gb/s obserwuje się w godzinach popołudniowych oraz wczesno wieczornych. Najwyższe spadki w ruchu notuje się natomiast w godzinach nocnych.
Także wykres statystyk tygodniowych potwierdza stawianą tezę, co prezentuje rysunek 7.



Rys.7. Tygodniowe statystyki sieciowe Nedwords dla miesiąca listopad 2010 [12]

Tendencja w ruchu ma charakter okresowy i powtarzalny każdego dnia. Przedstawione wykresy pokazują także, że serwisy mają charakter lokalny, zgodny z daną strefą czasową. Jeśli nie zachodzi wymiana użytkowników pomiędzy danymi strefami czasowymi, to podczas planowania wykorzystania danego serwisu jako medium przesyłu ukrywanej informacji, należy ten fakt uwzględnić.

Przeprowadzono także analizę szczegółowego logu serwera Hotfix.pl w dniach 7.10.2010:05:46:54 do 8.10.2010:05:46:54. Łącznie odnotowano w nim 228 749 zdarzeń. Oglądalność obrazów wygląda następująco:

- wczytano 16 834 obrazów JPG,
- wczytano 64 030 obrazów GIF,
- wczytano 103 obrazy BMP (mała liczba spowodowana wysoką optymalizacją strony),
- wczytano 83 850 obrazów PNG.

Miesięczne zestawienie wczytanych plików za miesiąc listopad 2010 przedstawia tabela 4.

Tabela 4. Miesięczne wykorzystania pasma dla serwisu Hotfix.pl w miesiącu listopad 2010

File type		Hits	Percent	Bandwidth	Percent
png	Image	2221149	42.2 %	13.01 GB	32 %
gif	Image	1551685	29.5 %	2.75 GB	6.7 %
js	JavaScript file	690819	13.1 %	6.61 GB	16.2 %
jpg	Image	446444	8.4 %	8.67 GB	21.3 %
htm	HTML or XML static page	98790	1.8 %	1.34 GB	3.3 %
swf	Adobe Flash Animation	97062	1.8 %	7.05 GB	17.3 %
css	Cascading Style Sheet file	92820	1.7 %	363.37 MB	0.8 %
php	Dynamic PHP Script file	52496	0.9 %	770.69 MB	1.8 %
bmp	Image	3060	0 %	15.36 MB	0 %
Unknown		1066	0 %	12.11 MB	0 %
reg		447	0 %	480.39 KB	0 %
txt	Text file	390	0 %	647.96 KB	0 %
rar	Archive	44	0 %	26.89 KB	0 %
pdf	Adobe Acrobat file	17	0 %	2.91 MB	0 %
jpeg	Image	10	0 %	87.75 KB	0 %
html	HTML or XML static page	5	0 %	3.85 KB	0 %
zip	Archive	5	0 %	412.71 KB	0 %
doc	Document	4	0 %	28.41 KB	0 %
shtml	Dynamic Html page or Script file	2	0 %	904 Bytes	0 %
pl	Dynamic Perl Script file	1	0 %	71.62 KB	0 %

Na podstawie zestawienia liczby stron w Internecie (Rys. 2), liczby jego użytkowników (Tab.1) oraz analizy danych dotyczących ruchu w sieci oraz w różnych serwisach WWW można przyjąć, że Internet jest doskonałym medium do przesyłania ukrytych informacji w obrazach cyfrowych, ponieważ ilość przesyłanych danych jest na tyle duża, że ich przeanalizowanie jest niemożliwe do zrealizowania. W przypadku umieszczania lub odczytywanie większej ilości informacji, które przekładają się na liczbę obrazów, należy uwzględniać okresy szczytów w ruchu sieciowym, tak aby dodatkowy ruch pozostawał niezauważony.

Na serwerze HotFix.pl w dniu analizy znajdowało się 5560 użytecznych obrazów o łącznej wielkości 170,75MB. Daje to około średnią pojemność jednego obrazu na poziomie 0,0307MB (31,44KB). Za obraz użyteczny uznawany był obraz wchodzący w treść strony. Ogólnie na witrynę składały się także obrazy wchodzące w skład jej budowy.

Przeprowadzono dokładniejszą analizę logu serwerowego wyznaczając liczbę wczytywanych obrazów użytecznych od liczby obrazów wczytywanych jako budulec strony. Wyniki tej analizy przedstawiono w tabeli 5.

Tabela 5. Szczegółowe wykorzystanie obrazów na witrynie HotFix.pl

Typ obrazu	Wszystkich wczytanych	Obrazów stanowiących budowę strony	Obrazów użytecznych	Procent użyteczności
JPG	16 834	19	16 815	99,88%
GIF	64 030	29 552	34 778	54,31%
BMP	103	0	103	100%
PNG	83 850	30 601	53 249	63,5%

Jak uwidaczniają to przedstawione dane, do budowy strony nie użyto obrazów w formacie JPG. Obrazy te stanowią treść strony jednak ze względu na mocną kompresję nie są dobrym nośnikiem dla wiadomości steganograficznej. Podobnie sytuacja wygląda dla obrazów w formacie GIF, jednak tutaj za odrzuceniem tego formatu jako nośnika dodatkowych informacji przemawia mały rozmiar tych plików stosowany na tym portalu. Najlepszym formatem o 100 procentowej użyteczności są obrazy BMP, jednak ich mała liczba sprawia, że analiza poszukiwawcza dodatkowych wiadomości w tych obrazach jest problemem łatwym. Najlepszym formatem pod kątem ukrywania informacji w obrazach na tym konkretnym portalu jest format PNG, którego użyteczność wynosi około 63 procent. Obrazy te cechują się niską kompresją i znacznymi rozmiarami.

Prezentowane dane potwierdzają tezę, że Internet jest doskonałym medium do przesyłania ukrytych informacji w obrazach cyfrowych w sposób niezauważalny dla innych pod względem transferu i pod warunkiem zapewnienia niewidoczności wizualnej faktu steganograficznego ukrycia wiadomości. W przypadku umieszczania lub odczytywania większej ilości informacji, które przekładają się na liczbę obrazów, należy uwzględniać okresy szczytów w ruchu sieciowym, tak aby dodatkowy ruch pozostawał niezauważony.

Warto zauważyć, że zwykłe obrazy PNG stanowią 40,1% wszystkich wczytanych plików. Jak się okazuje to właśnie o pliki graficzne przesyłanych jest największy odsetek zapytań. Potwierdzają to statystyki serwera należącego do Department of Computing Science, Umeå University, Northern Sweden's Premier University, gdzie 51,69% wszystkich zapytań to prośba o wczytanie obrazów PNG, natomiast 0,18% to zapytania o obrazy JPEG [13]. Podobnie dla statystyk [14] 43,81% stanowią zapytania o obrazy JPEG, za 3,50% o GIF. Oczywiście ważną kwestią jest

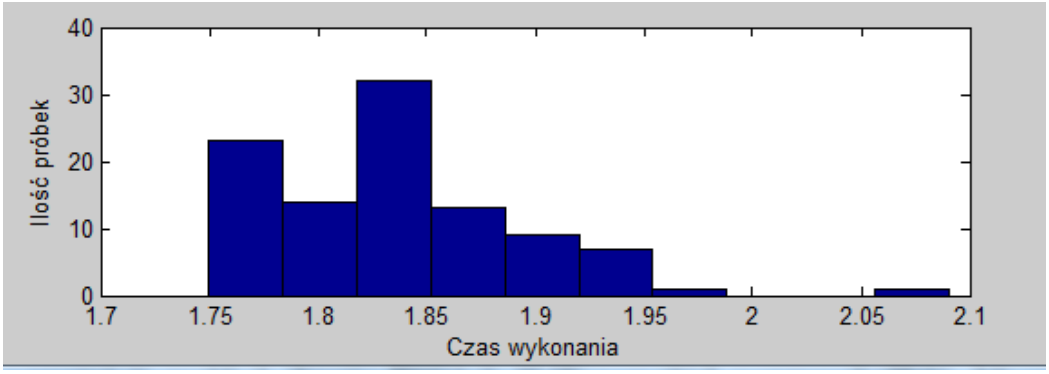
tutaj typ obrazów umieszczanych na stronie stanowiących treść oraz typ obrazów stosowanych do budowy samej strony. W przypadku portalu Hotfix.pl obrazy GIF oraz PNG są głównymi elementami budowy strony. W treści występują obrazy JPEG oraz PNG.

2.2. Złożoność wykrywania przesyłania dodatkowych informacji ukrywanych w obrazach cyfrowych z wykorzystaniem steganografii

Poprzez posiadanie informacji o liczbie obrazów jakie są przesyłane w sieci istnieje możliwość określenia złożoności ataku w celu wykrycia zaistnienia faktu steganograficznego ukrywania wiadomości.

W pracy [15] autor poniższej pracy doktorskiej przedstawił metodę oceny widoczności zmian kontrastu pomiędzy obrazami cyfrowymi z wykorzystaniem znormalizowanej funkcji czułości kontrastu CSF. Poprzez wyznaczenie liczby zmian kontrastów pomiędzy obrazem źródłowym a wynikowym w określonym kącie patrzenia na obraz, wyznacza się widoczność zmian w obrazie. Metodę tą można zastosować do wykrywania steganograficznego przesyłu informacji w obrazach cyfrowych. Atakujący musi posiadać dostęp do obrazu stanowiącego nośnik informacji (kontener) oraz wykonywać nasłuch sieci w celu wykonywania steganoanalizy.

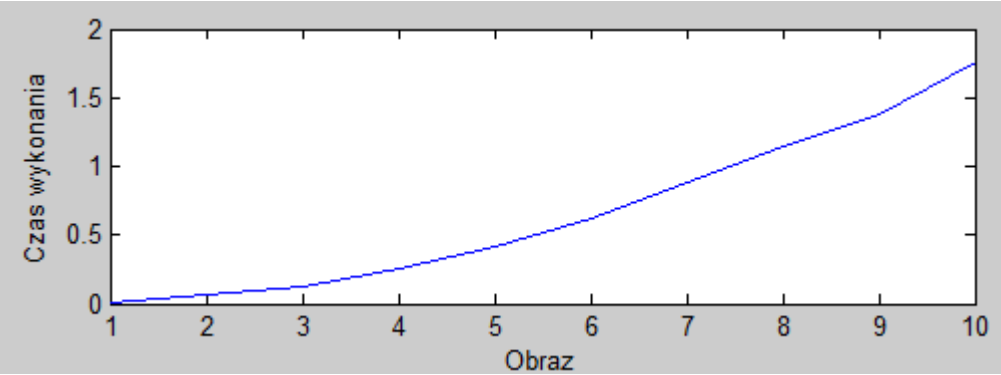
W celu wyznaczenia potrzebnego czasu do wykonania pełnego ataku wykrywającego fakt steganograficznego przekazywania informacji, wyznaczono czas wykonania analizy widoczności zmian kontrastu pomiędzy obrazami. Rysunek 8 przedstawia histogram czasu wykonywania operacji wykrywania widocznych zmian w obrazach dla 100 przykładowych obrazów w rozdzielczości 1024x768 pikseli, na przykładowym komputerze z procesorem Intel C2D E8200.



Rys. 8. Histogram czasu wykonywania operacji wykrywania widoczności zmian w obrazach

Z rysunku wynika, że średni czas wykrywania zmian w obrazach z wykorzystaniem funkcji CSF wynosi średnio 1,85 sekundy. Czas ten waha się w przedziale od 1,75 do 2 sekund i posiada charakter stały.

Wykonano także analizę czasu wykrywania przekazu steganograficzne dla obrazów o zmiennej wielkości dla 10%, 20%, 30%....100% wielkości obrazu 1024x768 pikseli. Wykres wykrywania przekazu dla zmiennej wielkości obrazu przedstawia rysunek 9.



Rys. 9. Wykres wykrywania przekazu steganograficznego dla zmiennej wielkości obrazu

Jak wynika z tego wykresu, czas potrzebny na wyznaczenie widocznych zmian pomiędzy obrazami źródłowym, a wynikowym rośnie wraz ze wzrostem rozmiaru obrazu przy czym wzrost ten ma charakter wykładniczy.

Odnosząc zaprezentowane wyniki do maksymalnej wielkości obrazu jaka jest przechowywana na portalu HotFix.pl, których szerokość wynosi do 700 pikseli, zauważa się, że czas wykrywania przekazu osiąga nawet jedną sekundę. Dla obrazów PNG, gdzie liczba użytecznych obrazów wynosi 53 249 sztuk, czas wykonania analizy tych obrazów wynosi 14,79 godziny. Uwzględniając dodatkowo czas potrzebny na analizę obrazów JPG (16 815 sztuk) potrzeba dodatkowo 4,67 godziny na przeprowadzenie analizy. Zakłada się tutaj, iż atakujący posiada już wszystkie obrazy w postaci kopii na dysku. W przypadku analizy online, należy doliczyć czas potrzebny na pobranie wszystkich obrazów. Analiza taka jest możliwa do przeprowadzenia na małych stronach. Dla wielkich serwisów typu hosting imgur.com analiza taka staje się niemożliwa do wykonania.

3. Analiza systemów ochrony informacji

Steganografia jest systemem ochrony informacji, gdzie wiadomość dodawana jest do innej wiadomości w sposób niezauważalny dla potencjalnego atakującego, tak aby ten nie podejrzewał faktu przesyłania dodatkowo ukrywanej wiadomości [16]. Jako, że podstawowym celem pracy jest opracowanie metody kształtowania klucza steganograficznego, należy dokonać analizy użytkowania kluczy w systemach ochrony informacji ze szczególnym uwzględnieniem metod steganograficznych.

3.1. Użytkowanie kluczy w systemach ochrony informacji

Z prawie każdym systemem ochrony informacji bezpośrednio związany jest klucz, którego budowa jest często warunkiem koniecznym do uznania danego systemu za bezpieczny. Takimi systemami są: kryptografia, ochrona danych w sieciach komputerowych, czy steganografia.

Klucze w systemach ochrony sieci komputerowych związane są z bezpieczną, nienaruszalną wymianą informacji we wzajemnej komunikacji porozumiewających się stron.

Z bezpiecznymi systemami ochrony bezpośrednio związane są takie pojęcia, jak: uwierzytelnianie, poufność, integralność danych i niezaprzeczalność. Wprowadzenie tych usług oraz odpowiednia polityka bezpieczeństwa jest podstawą do zapewnienia bezpiecznego przesyłania informacji między użytkownikami/systemami pracującymi zarówno w prostej architekturze klient-klient, klient-serwer czy w skomplikowanym środowisku rozproszonym [17, 18, 19].

Usługi uwierzytelniania i niezaprzeczalności zapewnione są dzięki podpisom cyfrowym, poufność dzięki szyfrowaniu, a integralność dzięki funkcjom skrótu [20, 21, 22, 23].

Jednym z głównych elementów systemów ochrony informacji jest kryptografia. W kryptografii bezpieczeństwo związane z szyfrowaną wiadomością opiera się na odpowiednim doborze klucza bądź pary kluczy (szyfrowania i deszyfrowania) oraz na tym jak silna jest konfuzja i dyfuzja w stosowanym algorytmie realizowana na podstawie tego klucza (pary kluczy) [24].

Najważniejszymi pojęciami, na których opiera się kryptografia są bijekcja i inwolucja [26]. Dla skończonego zbioru elementów *S*, permutacją *p* na *S* jest bijekcją z *S* na *S*. Inwolucja to funkcja *f* będąca bijekcją taka, że $f=f^{-1}$. Inwolucję można zapisać jako $f(f(x))=x$ dla wszystkich x należących do *S*. Każdy tekst jawny pochodzi ze zbioru wszystkich tekstów jawnych *M*, budowanych nad określonym alfabetem definicji, w tym binarnym alfabetem definicji $A=\{0,1\}$. Natomiast szyfrogramy pochodzą ze zbioru szyfrogramów *C*, definiowanych nad alfabetem definicji, ale niekoniecznie tym samym, co w przypadku zbioru *M*.

Każdy element $e \in K$, gdzie *K* to zbiór kluczy, zwany jest kluczem szyfrującym [26]. Określa on jednoznacznie bijekcję z *M* do *C*. Bijekcję tą oznaczoną jako E_e określa się mianem funkcji szyfrującej. Natomiast funkcja deszyfrująca D_d jest bijekcją z *C* na *M*. Określona jest ona jednoznacznie przez klucz deszyfrujący $d \in K$.

Schemat szyfrowania [26], zwany szyfrem, złożony jest z dwóch wzajemnie sobie odpowiadających zbiorów, tj. zbioru przekształceń szyfrujących $\{E_e: e \in K\}$ oraz przekształceń deszyfrujących $\{D_d: d \in K\}$. Przekształcenie te złączone są zależnością $D_d=E_e^{-1}$, co daje $D_d(E_e(m))=m$, dla wszystkich $m \in M$. Dwa różne klucze *e* i *d* tworzą parę kluczy związaną z kryptografią asymetryczną. Natomiast, gdy oba klucze są sobie tożsame, to kryptografia nosi nazwę kryptografii symetrycznej.

Należy zauważyć, że w wymianie informacji z wykorzystaniem kryptografii, jedyną rzeczą tajną jest użyta para kluczy [26]. Natomiast *M, C, K,* $\{E_e: e \in K\}$ oraz $\{D_d: d \in K\}$ są publicznie znane.

Podczas generowania kluczy należy kontrolować czy klucz, bądź para kluczy nie został wygenerowany powtórnie [25], a odpowiednie przechowywanie kluczy oraz ich kopii bezpieczeństwa powinno się odbywać w sposób bezpieczny i jest ono obok ich generowania niezwykle ważne. Niedopuszczalna jest przykładowo utrata klucza w wyniku krótkiego zaniku napięcia, bądź też przechowywanie klucza w postaci jawnej.

W systemie szyfrowania z kluczem symetrycznym, para kluczy *e* i *d* są sobie równe lub też łatwe obliczeniowo jest wyznaczenie klucza *d* na podstawie *e* i odwrotnie. W szyfrze blokowym wiadomość jawną dzieli się na bloki o stałej długości, które są następnie osobno szyfrowane.

Bezpieczeństwo wielu systemów szyfrowania często zależy od generowanych kluczy lub liczb według, których te klucze będą wyliczane. Powoduje to, że bardzo ważnym faktem jest zastosowanie odpowiedniego generatora liczb losowych, ewentualnie pseudolosowych. Wg definicji generatorem bitów losowych jest urządzenie lub algorytm wytwarzający ciągi statystyczne niezależnych i nieobciążonych cyfr binarnych [26]. Proces generowania klucza symetrycznego powinien się odbywać na specjalizowanym urządzeniu, pod odpowiednią kontrolą [27]. Identyczne zasady dotyczą wektorów początkowych IV stosowanych w różnych trybach szyfrowania.

Jednym z zasadniczych kryteriów wpływających na bezpieczeństwo systemu z kluczem symetrycznym jest długość klucza. Stanowi ono górne ograniczenie bezpieczeństwa szyfru na atak brutalny, zwany też atakiem przeszukiwania wyczerpującego przestrzeni kluczy [28]. Dla zwiększenia bezpieczeństwa szyfru podatnego na przeszukiwanie wyczerpujące można stosować kaskady szyfrów [29, 30], będących konkatenacją *2* lub więcej szyfrów blokowych (niekoniecznie tych samych) z tym, że w każdym stopniu kaskady jest używany inny klucz [29]. Inną modyfikacją jest wielokrotne użycie tego samego szyfru z różnymi kluczami, zwane szyfrowaniem wielokrotnym. Udowodniono jednak, że szyfrowanie potrójne z dwoma kluczami jest podatne na atak wybranym szyfrogramem, choć ze względu na wymagania pamięciowe jest on niepraktyczny [26]. Można zauważyć, że potrójne szyfrowanie z dwoma kluczami, może być także mniej bezpieczne niż zastosowanie potrójnego szyfrowania z trzema niezależnymi kluczami [29]. Projektując szyfr blokowy należy zwrócić uwagę, czy nie istnieje w nim zjawisko kluczy komplementarnych. Klucz $\bar{k}$ komplementarny do k (gdzie $\bar{k}$ jest zaprzeczeniem k) to taki, że x i $\bar{x}$ wyniki szyfrowań mają postać: $\bar{y} = E_{\bar{k}}(\bar{x})$ oraz $y = E_k(x)$. Klucze słabe tworzą inwolucję i mają postać $E_k(E_k(x))=x$, a klucze półsłabe powodują, iż $E_{k1}(E_{k2}(x))=x$ [29].

Szyfr strumieniowy jest szczególnym przypadkiem szyfru blokowego, w którym długość bloku jest równa jedności [28, 31]. Szyfrowanie odbywa się zgodnie ze strumieniem klucza, będącego ciągiem symboli $e_1,e_2,...,e_i \in K$. Pełne bezpieczeństwo w stosowaniu szyfru strumieniowego można osiągnąć używając tzw. kluczy jednorazowych tj. takich, które generowane są raz i tylko raz używane do szyfrowania, a jego długość jest równa długości szyfrowanej wiadomości.

Generatorem strumienia klucza nazywany jest algorytm generujący strumień klucza na podstawie pewnego ziarna lub ziarna i wyliczonego wcześniej szyfrogramu. W pierwszym przypadku jest to symetryczny generator strumienia klucza, a w drugim asynchroniczny. Nazwy zastosowanych generatorów jednoznacznie określają rodzaj szyfru strumieniowego tj. synchroniczny lub asynchroniczny szyfr strumieniowy. W przypadku szyfru synchronicznego wymagana jest, aby strony komunikujące się były ze sobą zsynchronizowane, co do stosowanego aktualnie klucza. Utracenie synchronizacji uniemożliwi dalsze deszyfrowanie. Ważne jest tutaj zapewnienie odpowiedniego generatora liczb pseudolosowych, w tym opartych o LSFR [26] i inne, jak liniowe i afiniczne oraz inwersyjne [32, 33].

W kryptografii asymetrycznej (lub też klucza publicznego) oba klucze *e* i *d* mają różne wartości [26, 29, 34]. Ponadto zakłada się, że dla zbioru przekształceń szyfrujących i odpowiadających im przekształceń deszyfrujących, obliczeniowo niewykonalne jest wyznaczenie któregokolwiek z kluczy deszyfrujących *d* na podstawie odpowiadających im kluczy szyfrujących *e* i odwrotnie. Klucz *e* nazywany jest kluczem publicznym, a *d* prywatnym. Nadawca szyfrując wiadomość używając klucza publicznego odbiorcy, a kryptografia klucza publicznego zapewnia, że tylko odbiorca jest w stanie odczytać wiadomość z wykorzystaniem swojego klucza prywatnego. Klucz prywatny powinien być chroniony przez właściciela przed jego ujawnieniem, natomiast klucz publiczny może być publicznie znany (np. poprzez umieszczenie go na specjalnym, publicznie dostępnym miejscu w formie certyfikatu) lub też może być wysłany do nadawcy niezabezpieczonym kanałem.

Podstawowym celem atakującego schemat szyfrowania asymetrycznego jest systematyczne odtwarzanie zaszyfrowanej wiadomości lub dokonywanie odtworzenia klucza prywatnego, który umożliwiłby deszyfrowanie wiadomości.

Schematy szyfrowania z kluczem publicznym oparte są na problemach trudnych obliczeniowo, w tym problemie faktoryzacji liczb całkowitych, RSA, logarytmu dyskretnego, Diffiego-Hellmana [35]. Nigdy nie udowodniono, że systemy szyfrowania asymetrycznego opartego o powyższe problemy są w pełni bezpieczne [29]. Przykładowo problem faktoryzacji dużych liczb całkowitych ma wykładniczy czas obliczeń. W przypadku komputerów kwantowych problem ten będzie potrzebował wielomianowego czasu obliczeń przy wykorzystaniu np. algorytmu Shora [36, 37].

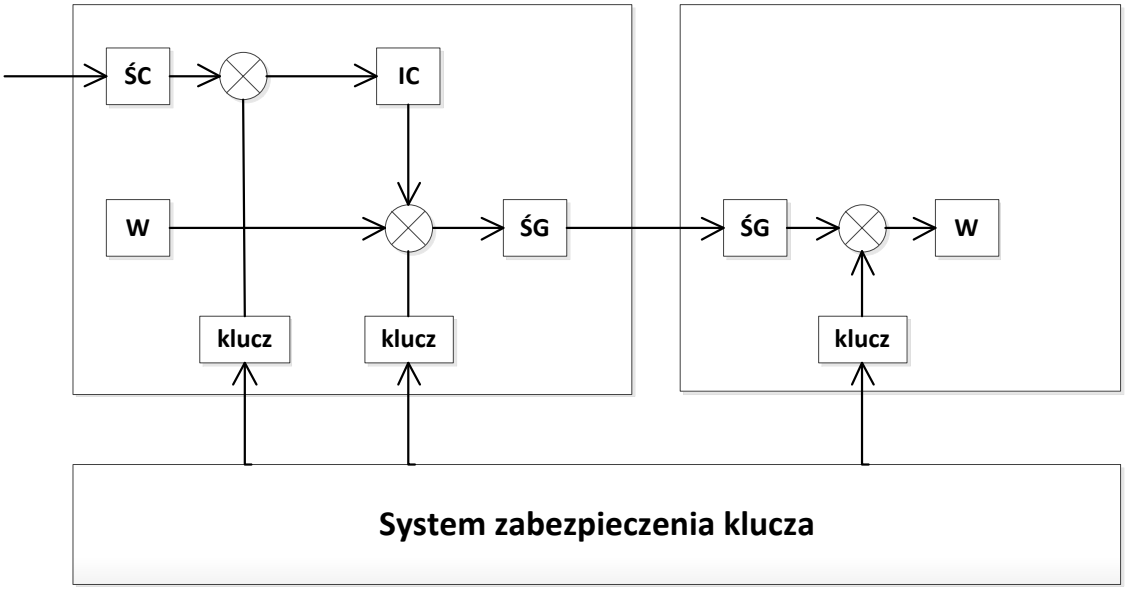
Algorytmy szyfrowania z kluczem publicznym stosowane są do szyfrowania danych oraz do ich podpisywania. W przypadku podpisywania schemat należy uzupełnić o mechanizm kontroli integralności, taki jak funkcja skrótu.

3.2. Wykorzystanie kluczy steganograficznych w znanych systemach

Steganografię dzieli się na słabą (*ang. Fragile*) i silną (*ang. Robust*) [38]. W steganografii słabej ukryta wiadomość jest tracona w momencie najprostszych zmian w informacji nośnej. W steganografii silnej nie da się w prosty sposób zniszczyć ukrytej wiadomości. Możliwe jest to dzięki powielaniu bitów wiadomości tajnej w różnych częściach informacji nośnej, czy też przez stosowanie kodów redundantnych do odtwarzania częściowo utraconej wiadomości tajnej. Klucze steganograficzne najczęściej związane są ze steganografią silną. Klucz ten określa miejsce ukrycia wiadomości w informacji nośnej. Bity klucza mogą przykładowo określać bloki obrazu czy współczynniki transformat np. Fouriera, w których poprzez ich modyfikacje zostanie ukryta wiadomość tajna. System steganograficzny klucza tajnego można opisać następująco:

- K – zbiór wszystkich kluczy,
- E – funkcja ukrywająca informację: $E:CxMxK \rightarrow C$,
- D – funkcja odkrywająca wiadomość tajną: $D:CxK \rightarrow M$,
- $|C| > |M|$,
- $D(E(c, m, k), k)=m$, gdzie $m \in M$, $c \in C$, $k \in K$.

Informacją nośną są pliki graficzne i dźwiękowe oraz ukryte kanały, jak ukryte pliki i partycje na dyskach, ukryte funkcje w oprogramowaniu, rejestry w układach cyfrowych, pola w nagłówkach stosowanych w protokołach sieciowych np. TCP/IP [39, 40]. Odpowiedni schemat systemu steganograficznego prezentuje rysunek 10.



Rys. 10. Schemat systemu steganograficznego dla obrazów cyfrowych

W środowisku cyfrowym (*ŚC*) wyznaczany jest z użyciem klucza kontener (*IC*), w którym ukrywana jest wiadomość (*W*) również z użyciem klucza. Powstałe środowisko graficzne z ukrytą wiadomością przesyłane są dalej do odbiorcy w celu odczytania wiadomości.

Wymagania stawiane systemom steganograficznym to:

-pojemność informacji jaką można ukryć w danym systemie cyfrowym i zależy od typu obrazu cyfrowego, parametrów stosowanego formatu (np. liczba kolorów w obrazie) i cech statystycznych (zmiana tych cech umożliwia wykrycie faktu ukrycia informacji),

- odporność na steganoanalizę pasywną [41] – dotyczy możliwości wykrycia dodatkowej informacji w informacji nośnej, w tym zapewnienie niewidoczności ukrytej wiadomości,

- odporność na steganoanalizę aktywną [41] – dotyczy usunięcia, zmodyfikowania lub zablokowania możliwości odczytu informacji utajnionej.

3.2.1. Klucze steganograficzne w podstawowych metodach ukrywania informacji

Klucze w systemach steganograficznych wykorzystywane są podczas wyznaczania miejsc ukrycia wiadomości i oznacza się je jako KEY_{SEL}. Mogą też służyć

do generowania informacji nośnej: KEY_{GEN}, lub do obydwu opisywanych czynności i oznacza się je jako $KEY_{GEN/SEL}$.

W najczęściej stosowanych metodach ukrywania informacji nie stosuje się kluczy steganograficznych. Wiele z nich przedstawiono w pracy [42]. Niestety metody te gwarantują znikome bezpieczeństwo. Mogą one co najwyżej chronić przed jednym wybranym, prostym atakiem na przekaz steganograficzny, takim jak wykorzystującym przekształcenia geometryczne, kompresje stratne lub konwersje formatów plików, w których ukryto wiadomość. Do ukrywania informacji stosowane są proste metody takie, jak LSB (Najmniej znaczącego bitu) czy modyfikacje algorytmu I.G.D. opartego o transformatę kosinusową DCT, który został opracowany dla znaków wodnych.

Aby zwiększyć bezpieczeństwo systemów steganograficznych, które zazwyczaj pozbawione są klucza KEY_{STEGO}, autorzy algorytmów dodają do nich metody kryptograficzne. Stosuje się tutaj zarówno algorytmy kryptografii symetrycznej, jak i asymetrycznej, a system ukrywania informacji nosi nazwę steganokryptograficznego. Propozycję zastosowania kryptografii symetrycznej przedstawiono w pracy [43], w której łączone są dwa obrazy. Pierwszym obrazem jest zaszyfrowany obraz będący ukrywaną wiadomością, natomiast drugim obrazem jest nośnik dla ukrywanej informacji. Do ukrywania wiadomości stosowany jest algorytm LSB, natomiast samo ukrywanie wykonywane jest w współczynnikach transformaty falkowej. Propozycję stosowania kryptografii asymetrycznej w steganografii przedstawiono w pracy [44], gdzie wiadomość najpierw jest szyfrowana, a następnie ukrywa się ją w kolejnych bajtach obrazu z wykorzystaniem LSB. Prezentowane w literaturze systemy steganograficzne są głównie systemami klucza symetrycznego. W pracy [45] autorzy twierdzą, że nie jest możliwe stworzenie systemu steganograficznego klucza publicznego dającego bezpieczeństwo porównywalne z bezpieczeństwem systemów kryptograficznych klucza publicznego.

W pracy [46] stwierdzono także, że steganografia klucza publicznego jest możliwa do zrealizowana, gdy wprowadzi się ograniczenia, w stosunku do tego, co znane jest z kryptografii. Autorzy pokazują, w jaki sposób można dokonać ataku na taki system. Pokazane zostały ataki polegające na wykrywaniu przekazu steganograficznego i sposób odgadywania kluczy poprzez obserwowanie reakcji porozumiewających się stron na to, co wysyła atakujący. Przedstawiono tam także protokół ustanawiania klucza steganograficznego oparty o założenia protokołu Diffiego-Hellmana [47]. W przypadku metod ustanawiania kluczy stosowane są znane metody kryptograficzne z tym, że

wszelkie dodatkowe informacje, potrzebne do ustanowienia klucza, przesyłane są z wykorzystaniem innych technik, w tym metod steganograficznych np. stosując ukrywanie informacji w obrazach. W pracy [48] przedstawiono szczegółowy schemat ustanawiania wspólnego klucza oparty o protokół D-H realizowany na krzywych eliptycznych. Wszystkie informacje przesyłane są w obrazach cyfrowych.

Większość metod steganograficznych korzysta z niedoskonałości ludzkich zmysłów, aby przykładowo, zabezpieczyć wiadomość tajną ukrytą w obrazie przed jej detekcją przez wzrok ludzki. Efektem tego jest fakt, że w metodach tych wiadomość ukrywana jest w miejscach informacji nośnej, gdzie nie wyrządzi to widocznych zmian, np. metody steganograficzne ukrywające wiadomość w blokach obrazów, w których znajduje się najwięcej linii konturowych [44]. Fakt ten może jednak znacznie ułatwić pracę steganoanalitykom. Stosowane klucze steganograficzne bezpośrednio wskazują miejsca ukrycia wiadomości w kontenerze, bez różnicy czy są to proste metody zastępowania bitów, czy modyfikujące współczynniki wybranej transformaty. W pracy [44] przedstawiono metodę steganograficzną ukrywania informacji w obrazach, będącą modyfikacją metody LSB, gdzie klucz bezpośrednio wskazuje punkt startowy od którego rozpoczyna się ukrywanie informacji. Następne miejsca wyznaczane są przez pewną funkcję zależną od obrazu i klucza. Do klucza dodano też pewną wartość D-gęstość określającą ile bitów może zostać ukryte w obrazie. W pracy [49] przedstawiono inną modyfikację LSB, gdzie informacja nośna traktowana jest jako strumień, a klucz stosowany jest w generatorze pseudolosowym do wyznaczania kolejnych bajtów wiadomości nośnej, w których ukryta zostanie wiadomość.

W przypadku steganografii opartej na modyfikacji współczynników transformaty klucz bezpośrednio wyznacza współczynniki, które po zmodyfikowaniu będą przechowywały bity informacji. Przykładem może być system steganograficzny oparty o modyfikację współczynników transformaty DWT przedstawiony w pracy [50]. Zaproponowana tam metoda jest modyfikacją metody I.G.D. dla transformaty DCT. W metodzie tej klucz wyznacza dwa współczynniki transformaty, których odpowiednia zamiana określa, jaki bit informacji zostaje ukryty.

Niestety modyfikacje wprowadzane do wiadomości nośnej powodują zazwyczaj znaczne zniekształcenia, które można wykryć nie tylko z wykorzystaniem metod opartych na analizie statystycznej, ale w sposób „namacalny” (np. poprzez widoczne zmiany w obrazie). Ponadto odtworzenie samej wiadomości tajnej, a nawet klucza, nie jest problemem trudnym obliczeniowo.

W pracy [51] autor zaproponował metodę wstawiania znaku wodnego opartą na transformacie DCT [52] z wykorzystaniem rozpraszania widma (metodę tą można zastosować do ukrywania dowolnej informacji steganograficznej). Dzięki rozpraszaniu widma możliwe jest osiągnięcie dobrych cech statystycznych, a w powiązaniu z transformatą DCT, wiadomość ukrywana jest w całych blokach obrazu (modyfikowana jest większa ilość współczynników, a nie dwa wybrane, jak zakładały poprzednie algorytmy). Klucz wykorzystywany jest tylko do inicjowania generatora pseudolosowego algorytmu rozpraszania widma, co może osłabiać bezpieczeństwo. Na bezpieczeństwo ma tutaj wpływ odpowiedni wybór generatora ciągów pseudolosowych. Metoda ta może spowodować widoczne zniekształcenia w obrazie (w obszarach o jednolitej teksturze), wiadomość tak ukryta jest odporna na kompresję JPEG (ze względu na modyfikację tylko średnich częstotliwości), ale słabo na przekształcenia geometryczne. Ponieważ w metodach opartych o rozpraszanie widma wiadomość ukrywana jest jako tzw. biały szum, dlatego ważne jest, aby utrzymywać jego niski poziom, co niestety może powodować dużą liczbę błędnie odczytanych bitów (oznaczanych jako BER – *ang. „Bit error Rate”*) ukrytej wiadomości [53].

3.2.2. Analiza metod ukrywania informacji algorytmami steganograficznymi opartymi o transformatę DWT

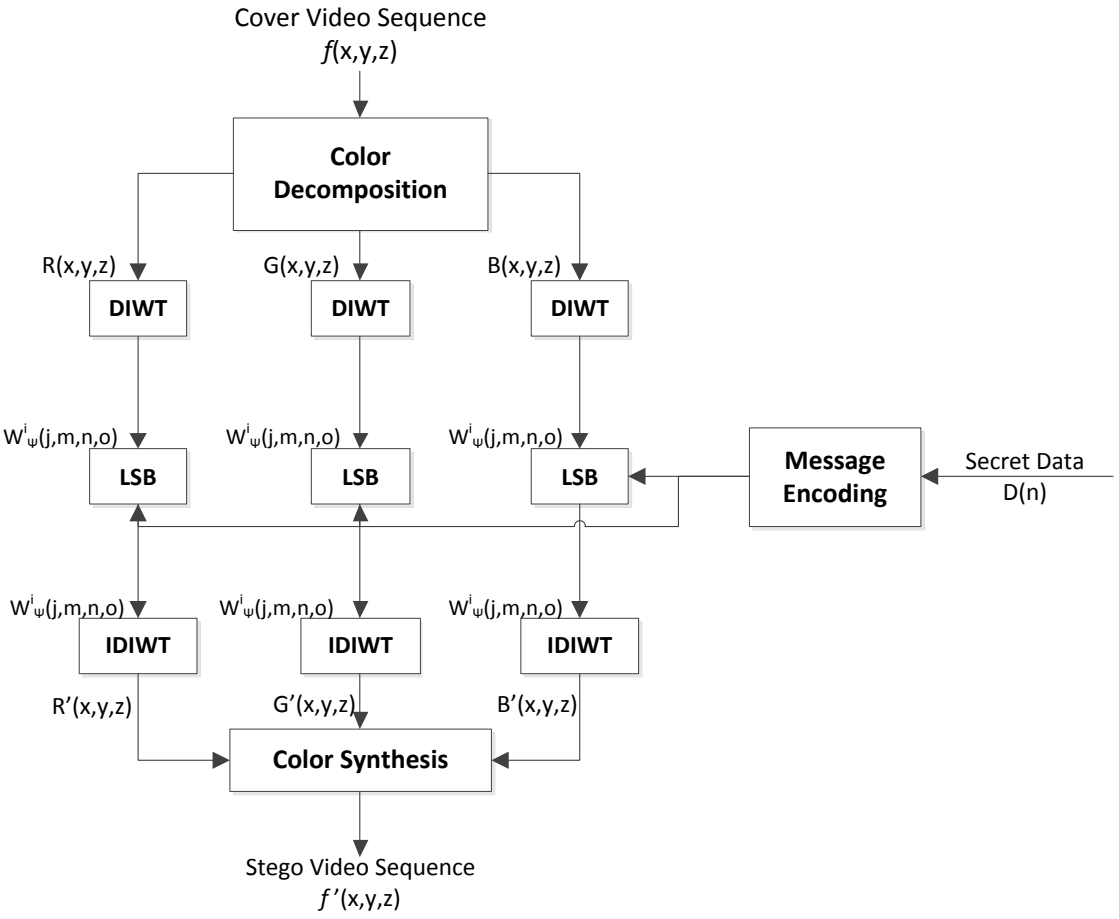
Zaawansowane metody steganograficznego ukrywania informacji w kolorowych obrazach cyfrowych wykorzystują do wprowadzania bitów wiadomości zamianę dziedziny przestrzennej na dziedzinę transformaty (Fouriera DFT, kosinusową DCT lub falkową DWT). Zastosowanie transformaty, zwłaszcza falkowej pozwala oceniać przydatność obrazu pod kątem wprowadzania określonych porcji danych, a także powoduje, że zastosowane metody mogą powodować powstawanie mniejszych zniekształceń, które byłyby widoczne dla ludzkiego oka.

3.2.3. Metody oparte o algorytm LSB

Większość proponowanych obecnie metod ukrywania informacji w obrazach cyfrowych wykorzystuje do ukrywania algorytm najmniej znaczącego bitu LSB, gdzie wiadomość ukrywana jest poprzez zamianę najmniej znaczącego bitu kolejnych bajtów

informacji nośnej na bajty obrazu. Stosowane są także modyfikacje metody LSB polegające na zamianie n-bitów kolejnych bajtów wiadomości. Niestety im większa liczba zmienionych bitów, tym większe prawdopodobieństwo wizualnego wykrycia wiadomości. Istnieje wiele metod wykorzystujących metodę LSB, których celem jest zmniejszenie ilości występowania zniekształceń. Wiele z nich korzysta przy tym z modyfikowania najmniej znaczących bitów transformaty falkowej obrazu.

W pracy [54] zaproponowano wykorzystanie klasycznego algorytmu steganograficznego ukrywającym dane w najmniej znaczących bitach. Przedstawiono tam sposób ukrywania informacji w sekwencjach wideo dla wszystkich barw składowych RGB. Schemat ten przedstawiono na rysunku 11.



Rys. 11 Przykład wykorzystania transformaty falkowej w steganografii [54]

Zaproponowano tutaj wykorzystanie dyskretnej transformaty falkowej do ukrywania wiadomości w kolejnych klatkach filmu. Transformaty dokonuje się dla każdej z barw osobno. Ukrywanie odbywa się poprzez zastosowanie metody LSB. Po

ukryciu wiadomości następuje przetworzenie sygnału odwrotną transformatą falkową do sekwencji wynikowej.

3.2.4. Zmodyfikowana metoda LSB

Przykład zastosowania LSB dla transformaty falkowej obrazów w odcieniach szarości, można znaleźć w pracy [55]. Przedstawiony algorytm ukrywania informacji przed operacją ukrywania stosuje transformację Arnolda dla obrazu stanowiącego ukrywany sekret. Transformata Arnolda [56] ma na celu poprawienie odporności wstawianej wiadomości.

Algorytm ten konwertuje macierz kwadratową *NxN* złożoną z punktów *(i,j)* do macierzy punktów (*i',j'*) wg wzoru (1).

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} i \\ j \end{bmatrix} \cdot (mod\ N) \qquad (1)$$

Po wykonaniu transformacji Arnolda, wykonywana jest jednopoziomowa transformata Falkowa obrazu nośnego oraz zmodyfikowanego obrazu stanowiącego sekret. Następnie wszystkie pasma obrazu ukrywanego są kwantyzowane przy pomocy algorytmu Raw Binary Encoding (RBE). W tym przypadku tablica kwantyzacji musi być znana zarówno odbiorcy jak i nadawcy wiadomości i stanowi pewien klucz.

Wiadomość taka jest ukrywana przy wykorzystaniu czterech oddzielnych kluczy. Ukrywane są wartości A_a w h_a za pomocą rozszerzonego LSB oraz pozostałe korespondujące ze sobą pasma. Dla wartości *p(x,y)* będącego parametrem h_a rozszerzony algorytm LSB składa się z trzech kroków:

1. Ukrywany jest jeden bit sekretu w *p(x,y)* z użyciem standardowego LSB i oznaczamy to jako *u(x,y).*
2. Modyfikowane są wszystkie *u(x,y)* dla maksymalizacji siły. Jeżeli *(i-1)* LSB wynosi 0, Wtedy drugi (*i02*) LSB ustawiany jest na 1. Dla bitu 1 działanie jest odwrotne. Zmodyfikowane *u(x,y)* oznaczane jest jako *v(x,y),* zaś *e(x,y)* jest różnicą pomiędzy *p(x,y)* oraz v(x,y).
3. Dla *(i+1)* LSB z *v(x,y)* oznaczmy *e'(x,y)* jako różnicę pomiędzy *p(x,y)* oraz *v'(x,y).* Jeżeli *e(x,y)<e'(x,y),* wtedy *v(x,y)* jest używane do zamiany *p(x,y).* W przeciwnym wypadku używany jest *v'(x,y),* zaś zmodyfikowany *p(x,y)* oznaczany jest przez *p'(x,y).*

Odczytywalność wiadomości wg autorów wynosi tutaj 0,99996 i zbliża się do 1.

3.2.5. Metoda LSB z wykorzystaniem rejestrów NLFSR i permutacją zależną od klucza

Algorytm LSB zaproponowano także w pracy [57]. W tym przypadku z kolei najpierw każda wiadomość konwertowana jest do jednowymiarowego strumienia danych. Przekształcenie zależy od typu ukrywanej wiadomości. Następnie wiadomość taka jest szyfrowana poprzez algorytm ACHTERBAHN-128. Algorytm ten używa szeregu rejestrów NLFSR połączonych na wyjściu jedną funkcją wielomianową generującą ciąg wyjściowy. W następnym etapie wiadomość ta jest permutowana pseudolosowo dla zwiększenia bezpieczeństwa. Zakłada się, że generator pseudolosowy zależy od klucza steganograficznego. Odtwarzanie kolejności bez znajomości powyższego klucza jest niemożliwe. Kolejnym etapem jest przekształcenie obrazu hosta transformatą falkową z wykorzystaniem funkcji Haara. Dane są ukrywane metodą LSB poczynając od pasma *HH* do *HL*. Ponieważ otrzymujący wiadomość musi znać jej długość, zatem ukrywana jest także i ta informacja. Na koniec transformata falkowa jest odwracana.

3.2.6. Metoda LSB z wyznaczaniem ilości modyfikowanych bitów

W pracy [58] zaproponowano nowe podejście do użycia dziedziny częstotliwości dla obrazów cyfrowych. W tej metodzie używane są pasma *HL*, *LH* oraz *HH* transformaty falkowej. Nienaruszane natomiast pozostaje pasmo aproksymacji *LL*. Na początku obraz hostujący jest transformowany z wykorzystaniem funkcji falkowej Haara na cztery podpasma. Następnie wyznaczana jest liczba bitów jakie można ukryć we współczynnikach Falkowych. Na koniec następuje odwrócenie procesu transformacji.

Dla obrazu hosta *C* i wiadomości ukrywanej *S* definiuje się następujące kroki algorytmu. W kroku pierwszym następuje przekształcenie obrazu *C* z wykorzystaniem transformaty DWT do macierzy *H* złożonej z czterech podpasm. W kroku drugim następuje normalizacja (2) współczynników H_{HL}, H_{LH} oraz H_{HH} w zakresie -510 do 510.

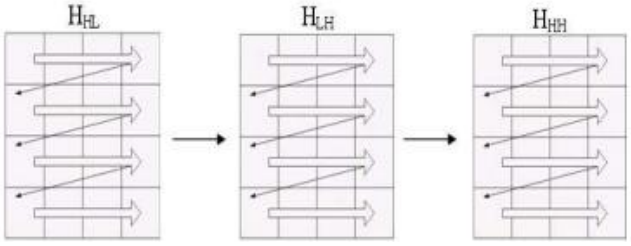
$$N = \frac{C_{1ij}}{510} = \frac{C_{2ij}}{255}, \tag{2}$$

gdzie C_{1ij} - reprezentuje oryginalne wartości współczynników poszczególnych podpasm, C_{2ij} - reprezentuje współczynniki po normalizacji.

Wyznaczenie bitów do ukrycia określane jest zależnością (3).

$$n_{ij} = \left[\frac{1}{2} log_2 \left| C_{ij} \right| \right] \tag{3}$$

Wzór (3) wyznacza ilość bitów ukrywanych na pozycji *(i,j)*. Przykładowo, jeżeli $|Cij|<4$ ukrywamy 1 bit wiadomości na pozycji *(i,j)*. Czwartym krokiem jest proces ukrywania kolejnych bitów wiadomości przedstawiono na rysunku 12.



Rys. 12. Prezentacja nowej metody steganograficznej opartej na DWT [58].

Dane ukrywane są w sposób sekwencyjny poprzez wybieranie kolejnych bloków obrazu przechodząc przez pasm *HL*, *LH* oraz *HH*.

Po ukryciu wiadomości metodą LSB następuje odwrócenie macierzy *H'* przez odwrotną transformatę falkową do obrazu oznaczanego jako *E*, ponieważ nie wszystkie piksele wynikowe posiadają wartości w zakresie od 0 do 255. Tutaj stosuje się macierz kluczową *K* do określania sytuacji, gdzie wartości nie są wartościami stałoprzecinkowymi (0, 0,25, 0,5 i 0,75). Wszystkie zaokrąglenia pikseli *E* stanowią stego-obraz. Do odczytania wiadomości wymagana jest znajomość wektora *K*. Klucz ten jest kluczem słabym:

$$E = \begin{bmatrix} 173,\underline{75} \\ 174,\underline{0} \\ 174,\underline{25} \\ 174,\underline{5} \\ 174,\underline{75} \\ 175,\underline{0} \end{bmatrix} \Rightarrow K = \begin{bmatrix} \underline{11} \\ \underline{00} \\ \underline{01} \\ \underline{10} \\ \underline{11} \\ \underline{00} \end{bmatrix}$$

3.2.7. Metoda oparta na zamianie współczynników

Inne podejście do zagadnienia jest zaprezentowane w [59], gdzie pokazano metodę opartą na zamianie współczynników w celu ukrycia znaku wodnego w obrazie. Na początku podawany jest oryginalny obraz, obraz stanowiący znak wodny oraz próg. Znak wodny jest konwertowany do postaci strumienia bitów. Następnym krokiem jest wykonanie dekompozycji Haara obrazu oryginalnego. Po etapie dekompozycji wybierane są podpasma *LH*, *HL* oraz *HH* na poziomie pierwszym. Wiadomość jest powtarzana w każdym z subpasm. Wiadomość jest ukrywana we współczynnikach falkowych, które mają większe wartości. Po tym etapie następuje odwrócenie transformaty falkowej.

W celu odczytania wiadomości porównuje się dwa obrazy. Jeżeli współczynnik ukryty jest większy od oryginalnego, wtedy ukryto bit 1. W przeciwnym wypadku ukryto 0.

Inne podejście do steganografii opartej na zamianie współczynników zaprezentowano w pracy [60]. W algorytmie tym zaproponowano zastosowanie klucza do wyznaczania współczynników, w których ukrywana będzie wiadomość tajna. Algorytm opisywany w tej pracy dotyczył znaków wodnych, gdzie informacja najpierw jest permutowana w celu zwiększenia bezpieczeństwa ukrywanych danych. Dane są ukrywane według zależności (4) i (5).

$$i_m(x) = i(x) + \alpha \quad if \quad m(x) = 1, \tag{4}$$

$$i_m(x) = i(x) - \alpha \quad if \quad m(x) = 0, \tag{5}$$

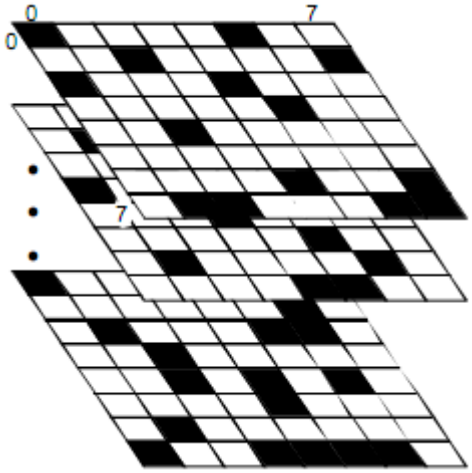
gdzie α - jest pewną liczbą rzeczywistą.

Dla przykładowego obrazu Lena w odcieniach szarości, autorom udało się uzyskać PSNR na poziomie 46,2 decybeli.

3.2.8. Metoda oparta na BPCS z użyciem kodowania EZW

Nowoczesne podejście do steganografii oparte na BPCS (*ang. Bit Plane Complexity Segmentation*) zaprezentowano w pracy [61]. Poprzednie metody stosowały proste podejście LSB do ukrywania wiadomości piksel po pikselu. Obraz na ekranie jest reprezentowany przez pewną ilość bitów odpowiadającym określonej barwie. Z wartości pikseli oraz z tego, jaką część obrazu one reprezentują, można skonstruować

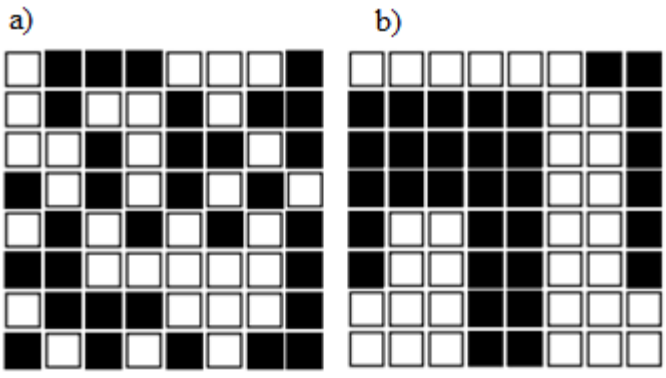
płaszczyznę bitową (*ang. bit plane*). Jest to struktura utworzona ze wszystkich bitów na znaczących pozycjach ze wszystkich liczb w dziedzinie przestrzennej, której przykład prezentuje rysunek 13.



Rys. 13. Prezentacja podziału na płaszczyzny bitowe [61]

Na przedstawionym rysunku 13, piksel (0,0) posiada wartość binarną 01001110. Przyjmuje się, że kolor czarny oznacza 0, zaś biały 1. Na pierwszej płaszczyźnie bitowej punkt o współrzędnych (0,0) posiada wartość zero, natomiast na drugiej jedynkową.

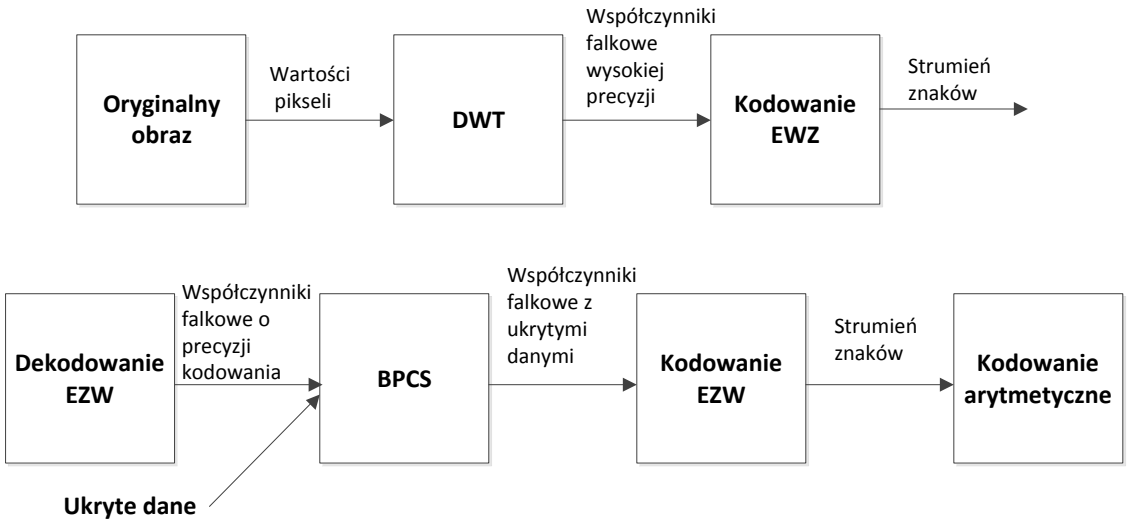
BPCS korzysta z faktu, że ludzkie oko jest czułe na drobne zmiany w jednolitych obszarach, zaś mniej rozpoznaje zmiany w złożonych obszarach. Złożone obszary takie jak drzewa będą miały wiele zmian pomiędzy zerami a jedynkami. Złożoność każdej podsekcji jest dana liczbą wszystkich przejść z 1 na 0 i na odwrót w kierunku poziomym jak i pionowym. Maksymalna złożoność kwadratu *2n x 2n* wynosi *2x2nx(2n-1),* zaś minimum 0. Dla typowych bloków 8x8 pikseli maksymalna złożoność wynosi 112. Przykłady różnych złożoności przedstawiono na rysunku 14.



Rys. 14. Przykłady różnych złożoności bitowych [61].

Rysunek 14 a) posiada stopień złożoności 69, zaś w przypadku rysunku 14 b) stopień złożoności wynosi 29. W przypadku niskiej złożoności ma się do czynienia z fragmentem obrazu jednolitym.. Wykorzystany algorytm EZW koduje bity od najbardziej znaczących do najmniej znaczących.

Zaproponowany algorytm ukrywania danych przedstawia rysunek 15.



Rys. 15. Algorytm ukrywania wiadomości z wykorzystaniem płaszczyzn bitowych [61]

Obraz po przetworzeniu przez DWT jest kodowany do żądanej rozdzielczości koderem EZW. Następuje wyznaczenie płaszczyzn bitowych i ukrycie danych z wykorzystaniem BPCS. Następnie współczynniki z ukrytą wiadomością są odtwarzane do poprzedniej rozdzielczości i na koniec trzy strumienie bitów są łączone w obraz wynikowy. Użycie obrazów RGB daje możliwość uzyskania znacznie większej pojemności dla obrazów niż to jest w przypadku obrazów w odcieniach szarości.

Takie podejście powoduje zniekształcenia na poziomie średnio od 30 do 40 dB współczynnika PSNR.

3.2.9. Podsumowanie rozdziału

Główną wadą algorytmów działających w dziedzinie przestrzeni jest duże zniekształcenie jakie one powodują, gdy używana jest zbyt duża liczba bitów lub podatność na usunięcie przez kompresję w przypadku użycia co najmniej znaczącego bitu. Wadą metod działających w dziedzinie transformaty kosinusowej jest duży poziom zniekształceń powodowanych zmianą głównych współczynników tej transformaty.

Wszystkie prezentowane metody nie stosują analizy widoczności zmian, przez co wprowadzają zniekształcenia w obszarach o jednolitej teksturze. W pracy proponuje się rozwiązać problem wyznaczania miejsc, gdzie wiadomość nie wprowadzi widocznych zmian w obrazie.

4. Metoda analizowania niewidoczności zmian powodowanych ukrywaniem wiadomości w obrazach cyfrowych z wykorzystaniem steganografii

Do analizy bezpieczeństwa jakie gwarantują metody steganograficzne należy opracować metodę badania niewidoczności zmian jakie powodują algorytmy ukrywania wiadomości. Metoda taka pozwala na budowanie algorytmów zabezpieczających przed wizualnym wykrywaniem wiadomości. Opracowanie metody oceny niewidoczności jest jednym z celów określonych na wstępie niniejszej rozprawy i stanowi w dalszej jej części fragment proponowanego algorytmu steganograficznego.

W tym rozdziale zostanie zaprezentowana metoda oceny niewidoczności zmian jakie zachodzą pomiędzy sąsiadującymi blokami obrazu oraz pomiędzy obrazami źródłowym i wynikowym powstałym jako wyjście działania algorytmu steganograficznego.

Opracowanie takiej metody pozwala na wybieranie fragmentów obrazu, klasyfikowanych jako miejsca do ukrywania wiadomości w sposób steganograficzny, w których wprowadzone zmiany pozostaną niewidoczne dla potencjalnego agresora.

Ponieważ klasyczne metody oceny zmian w obrazach, jak opieranie się na mierze *PSNR*, nie dają dobrych rezultatów w ocenie zmian jakie zachodzą w cyfrowych obrazach, porównując do tego co potrafi wychwycić ludzkie oko, dlatego należy sięgnąć po metodę oceny opartą na systemie widzenia ludzkiego oka.

Takie podejście pozwala na ocenianie zmian w obrazach w sposób zbliżony do postrzegania ludzkiego.

W dalszym etapie opracowana metoda oceny zniekształceń służyć będzie do wyznaczania miejsc określanych jako przydatne do ukrywania w nich dodatkowych informacji metodą steganograficzną, tak aby zmiany pozostawały niewidoczne.

Metoda ta zostanie rozbudowana o klucz steganograficzny, który dodatkowo będzie determinował sposób ukrywania wiadomości.

4.1. Szum jako ukrywana wiadomość w obrazie

Istnieje cały szereg algorytmów ukrywania informacji w obrazie. Aby uniezależnić się od wybranego algorytmu, czy samej metody ukrywania informacji w

obrazach, fakt ukrycia zastąpiony zostanie poprzez dodanie szumu do obrazu wejściowego, aby na podstawie różnic w obrazach źródłowym i wynikowym wnioskować na temat czy wprowadzane zmiany są widoczne czy nie. Dodawanie szumu do obrazu źródłowego ma charakter wspomagający dalsze badania prowadzone w niniejszej rozprawie doktorskiej i ma na celu uniezależnienie się od wybranego algorytmu steganograficznego w ramach badań nad niewidocznością zmian w obrazach cyfrowych [62].

Szum można generować z wykorzystaniem różnych rodzajów rozkładów. W dalszej części do obrazów będzie dodawany szum Gaussa, który pozwala wprowadzać różne poziomy zniekształceń.

Szum Gaussa stanowi ciąg nieskorelowanych zmiennych losowych, które posiadają zerową wartość oczekiwaną i stałą wariancję. Szum Gaussa określa funkcja opisana wzorem (6).

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}, \qquad (6)$$

gdzie σ - odchylenie standardowe, μ - wartość oczekiwana.

Wygenerowany szum można dodać do obrazu, w wyniku czego uzyskuje się symulację steganograficznego dodania informacji tajnej do obrazu. Poprzez zmianę parametrów generowanego szumu uzyskuje się różny poziom zniekształceń co symuluje zastosowanie różnych algorytmów steganograficznych.

4.2. Określanie widoczności zmian w obrazach cyfrowych

Steganograficzne ukrywanie informacji w kolorowych obrazach cyfrowych nie powinno powodować widocznych zniekształceń w obrazie wynikowym [63, 64]. W celu redukcji możliwości występowania zniekształceń wprowadza się metody ograniczające możliwość wystąpienia zniekształceń, które mogłyby zostać wykryte przez ludzkie oko. Jedną z takich metod przedstawiono w pracach [65, 66]. W pracach tych zaproponowano zastosowanie pewnych metod progowych opartych na statystykach, które powodują odrzucenie bloków obrazu, które posiadają jednolitą

strukturę. Algorytm ten w prosty sposób implementowany jest także w sposób sprzętowy [67].

W celu opracowania metody steganograficznego ukrywania wiadomości w obrazach cyfrowych należy wyznaczyć metodę oceny zniekształceń powodowanych przez algorytm steganograficzny dla analizy jego przydatności pod kątem ukrywania informacji w sposób niezauważalny dla ludzkiego wzroku. Metody oceny zniekształceń w obrazach pozwalają na opracowanie czynników wyznaczania miejsc ukrywania wiadomości, które w powiązaniu z kluczem steganograficznym będą w dalszej części stanowiły fragment proponowanego algorytmu steganograficznego.

4.2.1. Wyznaczenie poziomu zniekształceń z wykorzystaniem badań nad ludzkim wzrokiem

W literaturze, w głównej mierze, do wyznaczania poziomu zmian w kolorowych obrazach cyfrowych wykorzystywany jest współczynnik *PSNR* (*ang. Peak Signal to Noise Ratio*), będący stosunkiem maksymalnej mocy zniekształcenia do błędu średniokwadratowego. Przy zastosowaniu współczynnika *PSNR*, obraz uważa się za dobrej jakości, jeżeli jego współczynnik $PSNR \geq 30$ [68]. Niestety, główną wadą tego współczynnika jest niska korelacja z percepcją ludzkiego wzroku. Z tego też powodu, w niniejszej pracy zaproponowano metodę znacznie bardziej zbliżoną do tego jak zmiany w obrazach postrzega człowiek.

Do badań jakości widzenia można wykorzystać dwie miary: ostrość widzenia oraz kontrast progowy [69].

Ostrość widzenia, nazywana mianem *VISUS*, określa wielkość najmniejszego znaku, zwanego optotypem, który jest prawidłowo rozpoznawany przez człowieka z danej odległości. Miarę tą określa ułamek Sandella będący ilorazem odległości od tablicy testowej, zwanej tablicą optotypów, do odległości z której rozpoznawany jest dany optotyp pod kątem 5 minut. Miara visus równa 5/5 oznacza u człowieka wzrok prawidłowy. Jeżeli ułamek Sandella wynosi 5/15 to osoba taka niedowidzi [69]. Dla wartości 5/100 mamy do czynienia ze ślepotą. W 2002 roku Międzynarodowa Rada Oftamologii rozszerzyła widzenie normalne do wartości 5/6.3.

Badanie ostrości wzroku odbywa się przy maksymalnym kontraście. Zapewnia to umieszczenie optotypu posiadającego barwę czarną na białym tle tablicy. Ponieważ warunki obserwacji w zwykłych warunkach nie umożliwiają na widzenie przy

maksymalnym kontraście, a zatem ważniejszą miarą pozwalającą określić jakość widzenia, jest kontrast [69] i postrzeganie jego zmian.

Kontrast określa stopień wyróżniania się obserwowanego przedmiotu lub elementu od tła. Ponadto kontrast określa wyrazistość szczegółów obserwowanego przedmiotu. Miarę kontrastu można wyliczyć na podstawie zależności (Michaelsona) [66, 70] opisanej wzorem (7).

$$K = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}}, \tag{7}$$

gdzie I_{max} - oznacza obiekt o maksymalnej jasności, I_{min} - obiekt o minimalnej jasności.

W przypadku zależności Michaelsona, kontrast równy 1 oznacza idealny obiekt w kolorze czarnym umieszczony na białym tle. Mniejsze wartości kontrastu oznaczają szary obiekt na szarym tle, czyli kolory powoli zaczynają się zlewać. $K=0$ oznacza obiekt nierozróżnialny od tła, a zatem kolor tła i obiektu są jednakowe.

Rozróżnia się dwa rodzaje kontrastów luminancji. Pierwszy wyraża stosunek miejsca najjaśniejszego do najciemniejszego w obrazie i jest to kontrast globalny. Drugi określa przyrost luminancji do luminancji otoczenia w danym obszarze. Ten rodzaj kontrastu określany jest jako kontrast Webera. Wadą stosowania kontrastu Webera jest to, że jest on prawdziwy tylko dla scen niezawierających wielu częstotliwości. Można go stosować tylko dla obrazów o jednolitej teksturze.

Zdolność do rozpoznawania obiektów złożonych obrazów określa funkcja czułości na kontrast (funkcja wrażliwości na kontrast). Funkcja ta określa wielkość kontrastu, przy którym dany optotyp jest rozpoznawalny. Czułość na kontrast wyrażona jest wzorem (8) [70].

$$C = \frac{1}{K}, \tag{8}$$

gdzie K - określa kontrast.

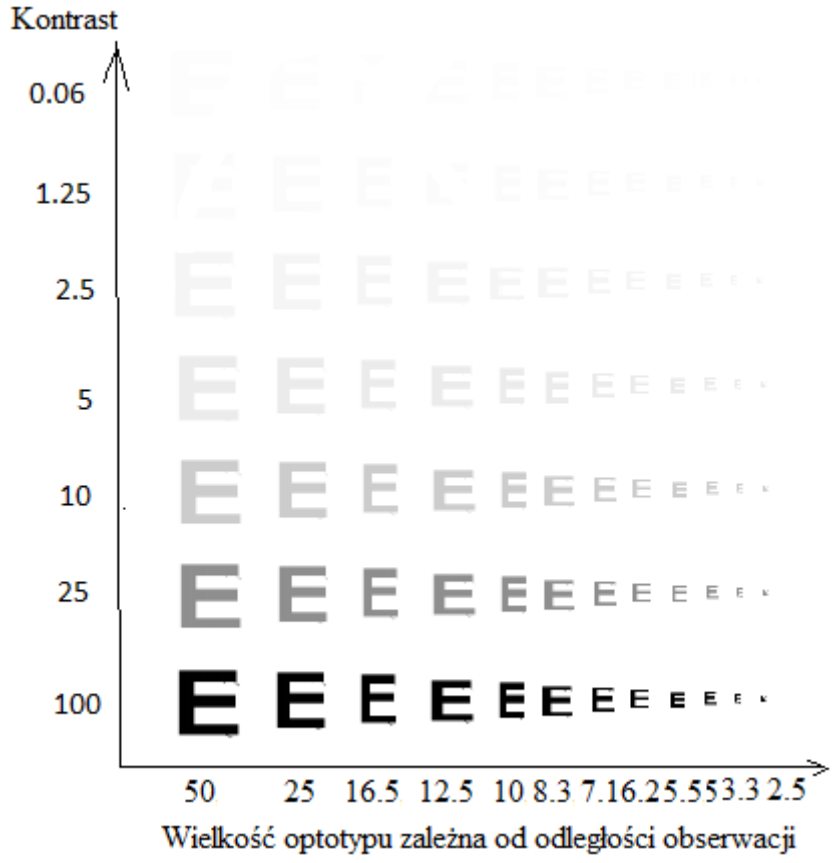
Wprowadza się tutaj pojęcie kontrastu progowego K_p, który wyznacza granicę rozróżnialności obserwowanego obiektu od tła. Kontrast progowy może zostać określony poprzez zastosowanie funkcji czułości kontrastu Mannosa i Sakrisona. W

przypadku wykorzystania funkcji czułości kontrastu Mannosa i Sakrisona, K_p wynosi około 60 cykli na stopień.

Zależność między czułością na kontrast, a wielkością optotypu przedstawia funkcja czułości na kontrast. Funkcja ta jest przedstawiana w skali logarytmicznej ze względu na jej duże wartości czułości na kontrast i nieliniowy charakter. Pozwala ona ocenić stopień pogorszenia sprawności wzroku przy obniżonym kontraście. Jej kształt wyznaczają tablice testowe z optotypami o różnym kontraście względem tła.

Wrażliwość na kontrast można badać stosując tablicę optotypów z wykorzystaniem dwóch tablic [71]:

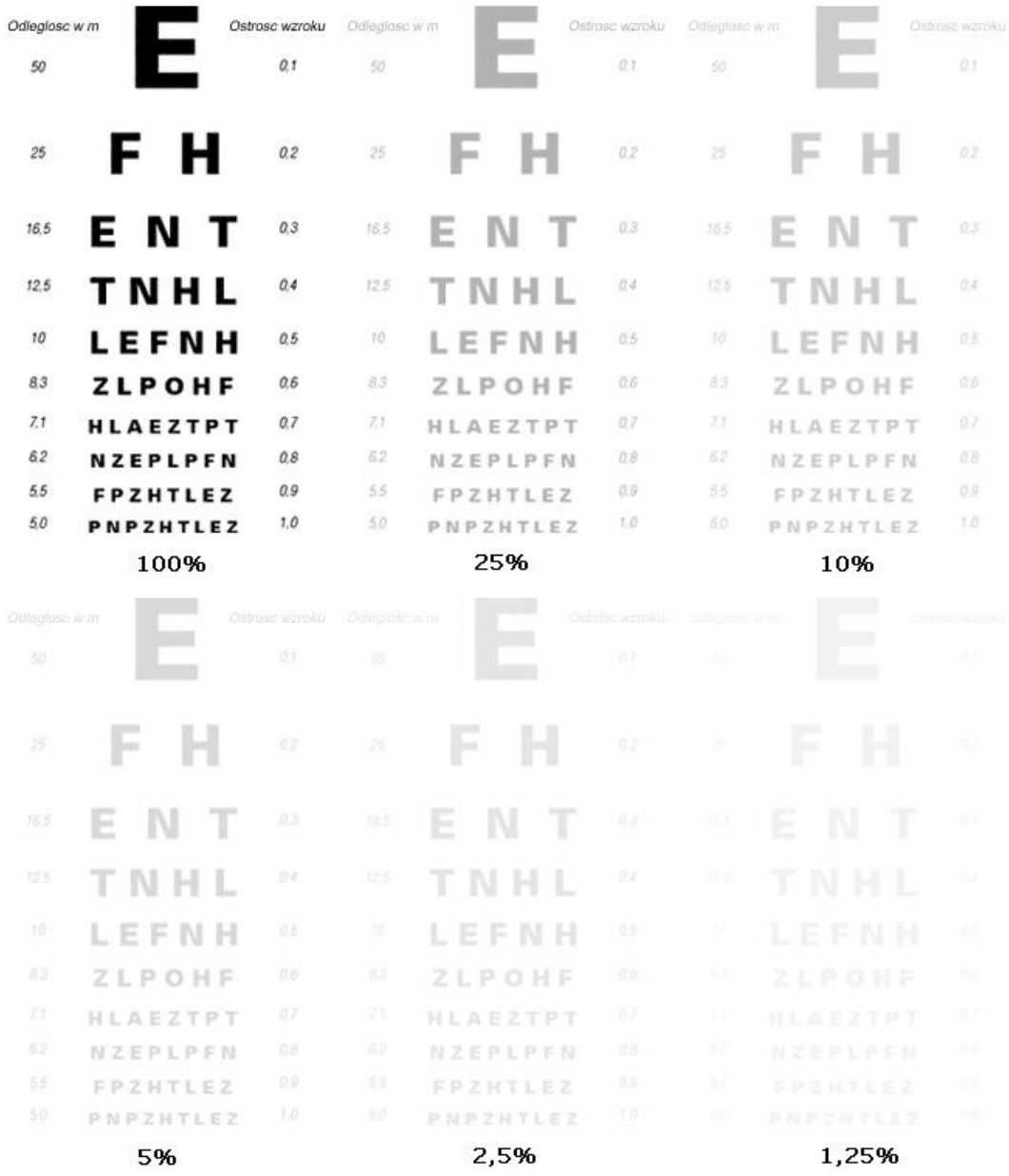
- o symbolach z tym samym rozmiarem, ale o zmiennym kontraście (tablica Pelli-Robson [72]),
- o symbolach z tym samym poziomem kontrastu, ale ze zmienną wielkością liter.



Rys. 16. Tablica Pelli-Robson optotypów do badań poczucia kontrastu [70]

Rysunek 16 przedstawia sposób budowania tablic do badania wrażliwości na kontrast, które powstają na podstawie tablic do badania ostrości wzroku poprzez branie

wierszy wszystkich rozmiarów liter tablicy ostrości dla danego poziomu kontrastu. Optotypy stosowane do badań ostrości zaproponowane zostały przez Hermana Snellena. Według jego propozycji, tzw. badanie widzenia dali odbywa się poprzez zastosowanie tablicy liter o wielkości z szeregu odległości widzenia od 50 metrów do 2,5 metra, gdzie kąt wynosi 5 stopni, zaś wielkość kątowa widzenia szczegółów 1 stopień. Są to kolejne odległości wyrażone w metrach: 50, 25, 16.5, 12.5, 10, 8.3, 7.1, 6.2, 5.5, 5, 3.3 oraz 2.5 metra. Poziomy kontrastu dla tablic optotypów wynoszą kolejno logarytmicznie: 100%, 25%, 10%, 5%, 2.5%, 1.25%, 0.6% co przedstawiono na rysunku 17.



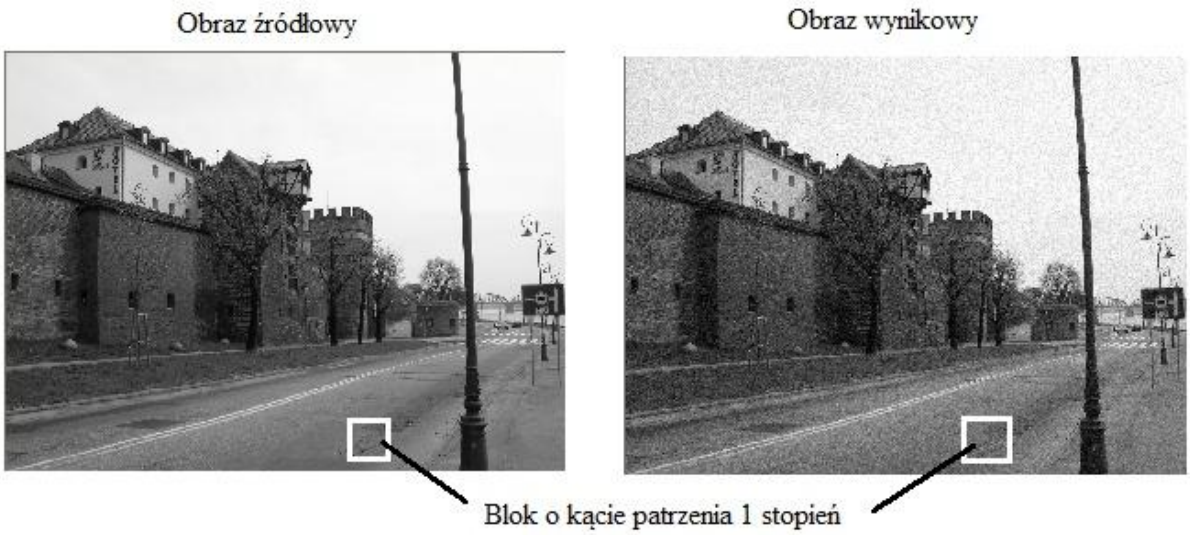
Rys. 17. Tablice optotypów dla kolejnych poziomów kontrastu

Pierwszy wiersz tablicy do badania kontrastu stanowi wybrana kolumna optotypów z tablicy badania ostrości wzroku, gdzie kontrast wynosi 100%. Następnie brane są kolejne tablice do badań ostrości o kolejno zniżających się wartościach kontrastu. W ten sposób stosuje się tablicę optotypów do badania ostrości, jako tablic do badania wrażliwości oka na zmiany kontrastu, a zatem stosowane one są jako miernik poziomu niewidoczności zmian pomiędzy obrazami poszczególnych optotypów. Przeliczanie kontrastu rozpoznawanego przez badanego na współczynnik wrażliwości na kontrast wykonuje się dzieląc 100 przez wartość kontrastu rozpoznawanego. Jeżeli rozpoznawany jest kontrast 2,5% to wrażliwość na kontrast wynosi 100/2,5=40, a jeżeli 0,6% to 100/0,6=167.

Zmiany kontrastu są zauważalne pomiędzy wartościami ostrości między 0 (duże symbole optotypów), a 1 (małe optotypy). Wszystkie zmiany kontrastu powyżej 1 (20/20 cykl/stopień) stają się niezauważalne. Ukrycie informacji w obszarze powyżej 1 cykl/stopień nie spowoduje widocznych zniekształceń w obrazie wynikowym, a zatem są one niezauważalne dla ludzkiego oka. Największe zmiany są zauważalne w obszarze ostrości dla optotypów 0,03 (20/600) oraz 0,1 (20/200), gdzie czułość na kontrast jest największa.

Autor niniejszej pracy doktorskiej proponuje wyznaczanie siły zniekształceń oraz ich niewidoczności na podstawie porównania obrazu źródłowego oraz wynikowego z wykorzystaniem funkcji CSF.

W wybranej barwie dla całego kolorowego obrazu cyfrowego dodawany jest określony rodzaj szumu, z zadanymi parametrami. Szum jest traktowany jako ukryta wiadomość w danym obrazie. Sposób wyznaczania zmian zostanie przedstawiony na przykładzie z rys. 18. Na podstawie średniej zmian kontrastu i funkcji poczucia kontrastu wyznacza się widoczność zmian.



Rys. 18. Wybrany blok ukrywania informacji między obrazem źródłowym, a wynikowym

Zmianę kontrastu między sąsiadującymi blokami obrazu źródłowego wyznacza się według zależności (9).

$$\Delta P = |K_1 - K_2|, \tag{9}$$

gdzie K_1, K_2 - oznaczają średni kontrast dwóch sąsiadujących bloków obrazu wybranego do ukrycia wiadomości.

Zmianę kontrastu między wybranymi sąsiadującymi blokami obrazu wynikowego (zaszumionego) określa zależność (10).

$$\Delta P' = |K_1' - K_2'|, \tag{10}$$

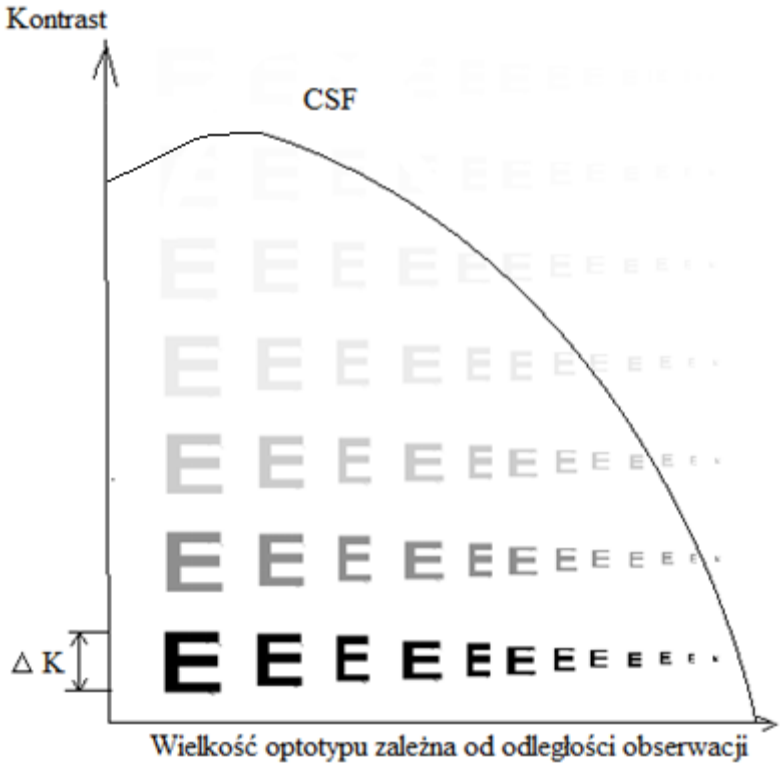
gdzie K'_1, K'_2 - są średnimi kontrastami dwóch sąsiadujących bloków obrazu zaszumionego wyliczanych na podstawie średniej zmian kontrastu w danym bloku obrazu.

Dla obrazu z ukrytą wiadomością (wstawionym szumem) można wyznaczyć zmianę kontrastu ΔK określoną zależnością (11)

$$\Delta K = \Delta P' - \Delta P, \tag{11}$$

gdzie ΔP - określa zmianę kontrastu między blokami w obrazie źródłowym, $\Delta P'$ - określa zmianę kontrastu między tymi samymi blokami w obrazie wynikowym z ukrytą wiadomością.

Jeżeli zmiana kontrastu ΔK między obrazem źródłowym a wynikowym leży nad krzywą kontrastu CSF lub w zakresie wielkości zmian dla danego optotypu w uproszczonym modelu (Rys.19), uznaje się, że zmiany kontrastu pomiędzy blokami są niezauważalne.



Rys. 19. Widoczność zmian w obrazie określona przez zmiany kontrastu wg tablic Pelli-Robson

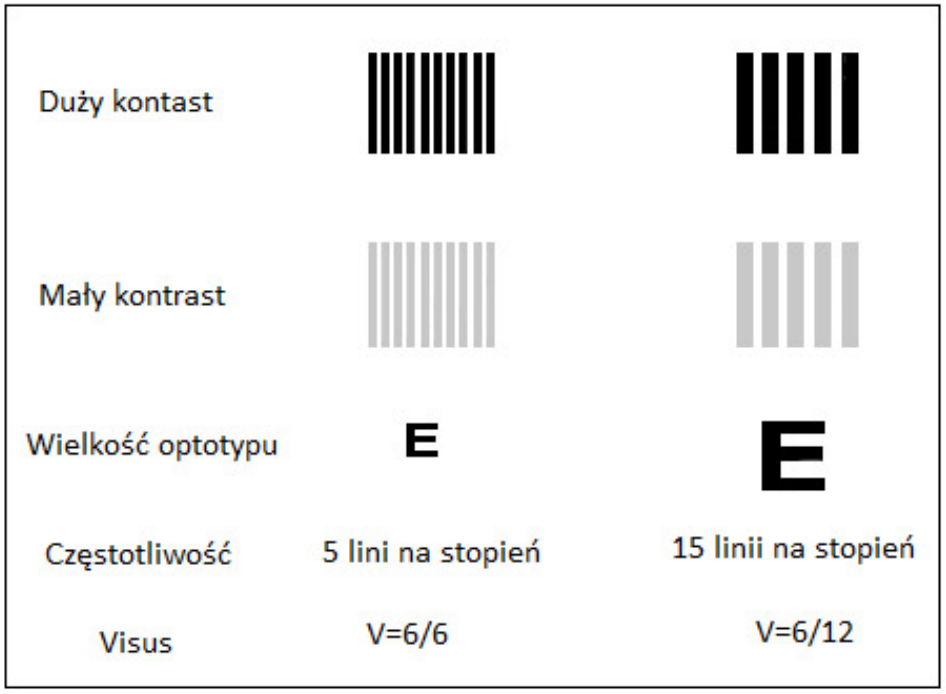
Sterowanie widocznością, a co za tym idzie, siłą ukrywania wiadomości steganograficznej może się odbywać poprzez wielkość zmian pomiędzy poziomami kontrastów na tablicy optotypów.

Poprzez wyznaczenie średniej zmian w kontraście poszczególnych pikseli danych podbloków obrazu i odniesienie zmian na znormalizowaną funkcję czułości na kontrast, stwierdza się, czy dana wiadomość (tutaj szum), spowodowała widoczne zmiany w obrazie poprzez zmianę poczucia kontrastu w danym obszarze. W miejsce dyskretnych zmian optotypów można zastosować funkcję CSF Mannosa i Sakrisona. O

sposobie wyznaczania zmian ilościowych oraz zasadę stosowania znormalizowanej funkcji czułości kontrastu opisano w następnym podrozdziale.

4.2.2. Metoda oceny widoczności zmian w oparciu o znormalizowaną funkcję CSF

Zmodyfikowaną formą wyznaczania niewidoczności dla ludzkiego oka, faktu steganograficznego ukrycia wiadomości w obrazie, jest wykorzystanie znormalizowanej funkcji czułości na kontrast CSF zaproponowana przez Manosa oraz Sakrisona [71], która stanowi przeniesienie zależności odzwierciedlonej na tablicach optotypów do zależności matematycznej. Przedstawia to rysunek 20.



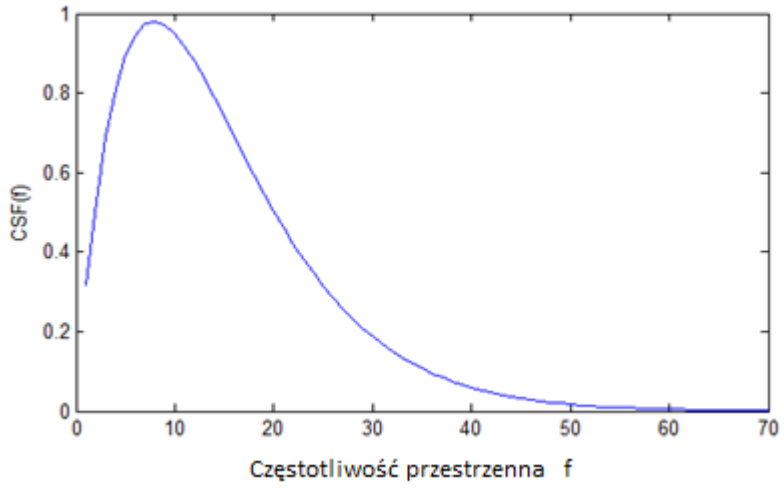
Rys. 20. Zależność kontrastu od częstotliwości prążkowej [69]

Funkcja poczucia wrażliwości kontrastu CSF ma postać określoną wzorem (12).

$$A(f) = 2{,}6 * (0{,}0192 + 0{,}114 * f) * e^{-(0{,}114 * f)^{1{,}1}}, \qquad (12)$$

gdzie f - jest częstotliwością zmian wyrażoną w cyklach na stopień i można utożsamiać ją z częstotliwością prążkową zmian, czyli liczby przejść pomiędzy detalami jakimi są prążki w jednym stopniu obserwacji.

Funkcja ta wskazuje wrażliwość ludzkiego oka na różne częstotliwości impulsów wizualnych, które wyrażają kontrast. Im wyższa częstotliwość zmian impulsów, tym gorsze rozpoznawanie wzorca. Rozpoznawanie wzorców pogarsza się także w przypadku rzadkich zmian impulsów. Maksimum czułości zależne jest dodatkowo od kąta patrzenia. Jeżeli kąt patrzenia będzie maleć, ekstremum funkcji przesunie się nieznacznie w kierunku większych częstotliwości. W przypadku wzrostu kąta patrzenia, ekstremum przesunie się w drugim kierunku [73].Wykres funkcji wrażliwości na kontrast pokazano na rysunku 21.



Rys. 21. Wykres funkcji wrażliwości na kontrast [73]

Według przedstawionej funkcji CSF szczytowa wartość osiągana jest dla około $f=8$, natomiast bez znaczenia są częstotliwości powyżej 60 cykli na stopień (kąt równy 1'). Powyżej $f=60$ wzrok ludzki nie rozróżnia zmian [71], a zatem te zmiany uznaje się za niezauważalne.

Funkcja wrażliwości na kontrast pokazuje, że ludzkie oko jest mało wrażliwe na zmiany kontrastu przy niskiej częstotliwości zmian. Jeżeli zatem w obrazie cyfrowym zachodzą rzadkie zmiany oko ludzkie ich nie widzi dokładnie i mogą pozostać niezauważone. Jeżeli stopień zmian wzrośnie do rzędu 10 cykli na stopień, ludzkie oko zacznie postrzegać zmiany kontrastu wyraźnie, a więc wszelkie zmiany pomiędzy fragmentami obrazu będą w pełni zauważalne. Powyżej częstotliwości zmian

rzędu 10 cykli na stopień, poczucie wrażliwości na kontrast stopniowo maleje, przez co człowiek przestaje widzieć zmiany. Odpowiada to bardzo gęstym zmianom we fragmencie badanego obrazu. Jeżeli w stopniu widzenia człowieka znajdzie się znaczna liczba niewielkich punktów o zmianach kontrastu rzędu 60 cykli na stopień, człowiek tych zmian nie zauważy.

Warunki obserwacji obrazów cyfrowych określają odległość widzenia wynoszącą 80 centymetrów od monitora. Jest to ergonomiczna odległość obserwacji w jakiej przeciętny człowiek siedzi oddalony od monitora.

Funkcja ta oparta jest na ostrości prążkowej i pokrywa znacznie większe pole widzenia niż optotypowa. Wykorzystuje ona zmiany częstotliwości prążkowej opisując poczucie kontrastu w sposób ciągły podczas, gdy optotypowa bazuje na ustalonych poziomach wielkości symboli optotypowych.

W pracy [74] przedstawiono możliwość przejścia między znormalizowaną funkcją czułości kontrastu, a dziedziną transformaty falkowej. Sposób ten zostanie zaprezentowany także w dalszej części pracy, w rozdziale 4.3.5. Możliwość przeniesienia funkcji czułości kontrastu do dziedziny falkowej jest ważny z punktu widzenia działania wielu dzisiaj stosowanych algorytmów steganograficznych oraz algorytmu proponowanego w niniejszej pracy, które operują na zmianach współczynników transformaty falkowej obrazów cyfrowych.

Współczynnik CSF dla pasm biorą swoje wartości bezpośrednio z krzywej CSF dla znormalizowanej funkcji czułości kontrastu z dziedziny przestrzeni.

Budując algorytm steganograficzny należy zatem przewidzieć, że należy wybierać obszary w obrazach, w których zmiany jakie powstaną pozostaną niewidoczne dla agresora, gdyby ten posiadał dostęp do obrazu źródłowego, jak i wynikowego. A zatem, ukrywając dodatkowe porcje danych w obszarach, gdzie częstotliwość przestrzenna w jednym stopniu obserwacji wynosi powyżej 60 cykli/cykl i zakładając, że ukrycie wiadomości nie spowoduje przekroczenia tej granicy, to ukrycie wiadomości pozostanie niezauważalne dla ludzkiego oka.

4.3. Miary charakteryzujące kolorowe obrazy cyfrowe

W pracy wykonano analizę istotności szeregu miar wyznaczanych dla kolorowych obrazów cyfrowych na podstawie znormalizowanego histogramu kolorów

oraz macierzy zdarzeń (*ang. Co-Occurrence Matrix*). Poprzez ich zastosowanie autor proponuje dalsze wyznaczanie miejsc ukrywania informacji w obrazach cyfrowych. W rozprawie doktorskiej zajęto się analizą możliwości wykorzystania charakterystycznych parametrów obrazu w celu zaproponowania rozbudowy opracowanego w dalszej części pracy algorytmu steganograficznego o możliwość przechowywania w bazie informacji o posiadanych obrazach. Baza obrazów oraz informacje w niej przechowywane o poszczególnym obrazie będą dalej służyć do wyboru obrazów w celu ukrycia w nich dodatkowych porcji danych proponowanym algorytmem steganograficznym.

Metoda taka pozwala na rozbudowę dowolnego algorytmu steganograficznego operującego na cyfrowych obrazach o możliwość przechowywania skróconych informacji o obrazach w celu szybkiego wyboru przydatnych obrazów z bazy obrazów. Pojęcie szybkie oznacza tutaj, że przy wyborze obrazów z bazy nie będzie konieczne ciągłe przeliczanie wszystkich miar charakterystycznych dla każdego obrazu. Miary te zostaną wyliczone raz i umieszczone w bazie danych. Rozpoczęcie ukrywania wiadomości będzie polegało na wykonaniu zapytania do bazy w celu otrzymania informacji o obrazach spełniających określone kryteria. Kryteria te zarazem będą stanowiły fragment klucza steganograficznego użytego w procesie ukrywania. Zakładając, że do sieci zawsze będą trafiały wszystkie obrazy z bazy, a wiadomość będzie ukrywana w jednym z nich, to agresor będzie musiał przeglądać wszystkie w celu wykrycia potencjalnych zniekształceń.

4.3.1. Parametry wyznaczane na podstawie znormalizowanego histogramu kolorów

Do określania zmienności cech kolorowych obrazów cyfrowych można wykorzystać pojęcie histogramu jako sposobu empirycznego przedstawiania rozkładu danej cechy. Histogram kolorów znormalizowany H_{ng} otrzymywany jest poprzez dzielenie odpowiednich wartości H_g (liczby wystąpień danego koloru g w bloku obrazu) przez całkowitą liczbę pikseli [75]:

$$Hn_g = \frac{H_g}{L_w * L_k}, \tag{13}$$

gdzie L_w - oznacza liczbę wierszy, L_k - liczbę kolumn

Poprzez wyznaczenie znormalizowanego histogramu kolorów uzyskuje się informacje o prawdopodobieństwie z jakim dany piksel może przyjąć kolor g.

Na podstawie znormalizowanego histogramu kolorów można wyznaczyć jego podstawowe parametry [75, 76]:

a). Średnia określana mianem wartości oczekiwanej, która obliczana jest jako suma wystąpień wszystkich wartości zmiennych pomnożonych przez ich prawdopodobieństwa. Zmiany średniej określane są jako wskaźnik natury technicznej,

$$\mu = \sum_{g=0}^{L_g - 1} g * Hn_g \tag{14}$$

b). Wariancja jako wielkość zawierająca informacje na temat średniego odchylenia sygnału od jego wartości średniej. Wariancja wyjaśnia zmienność danych i jest miarą szerokości rozkładu gęstości prawdopodobieństwa w otoczeniu wartości średniej.

$$\sigma^2 = \sum_{g=0}^{L_g - 1} (g - \mu)^2 * Hn_g \tag{15}$$

c). Skośność czyli asymetria krzywej histogramu. Asymetria ta jest stopniem oraz niecentralnością pomiarów. Zawiera informacje o różnicach między odchyleniami dodatnich oraz ujemnych wartości średniej. Skośność świadczy o asymetrii krzywej gęstości prawdopodobieństwa.

$$\gamma_3 = \sigma^{-3} \sum_{g=0}^{L_g - 1} (g - \mu)^3 * Hn_g \tag{16}$$

d). Kurtoza, określa spiczastość lub płaskość krzywej gęstości prawdopodobieństwa i jej wartość mówi o sile skupienia. Dla rozkładu normalnego kurtoza jest równa 3, dla spłaszczonego jest mniejsza od trzech, zaś dla wysmukłego większa od trzech. Jeżeli kurtoza przyjmuje dużą wartość, to może to świadczyć o występowaniu przejściowej szpilki.

$$K = \frac{\mu_4}{\sigma^4} = \sigma^{-4} \sum_{g=0}^{L_g - 1} (g - \mu)^4 * Hn_g \tag{17}$$

e). Eksces, miara spłaszczenia histogramu. Eksces wyznaczany jest poprzez odjęcie od współczynnika spłaszczenia wartości 3, dzięki czemu jego wartość zerowa oznacza występowanie rozkładu normalnego. Poprzez wartość współczynnika ekscesu otrzymuje się informacje na temat koncentracji wartości zmiennej wokół średniej, a zatem czy jest od niej mniejsza czy większa niż w zbiorowości o rozkładzie normalnym.

$$\gamma_4 = K - 3 = \sigma^{-4} \sum_{g=0}^{L_g - 2} (g - \mu)^4 * Hn_g - 3 \qquad (18)$$

Współczynniki skośności oraz kurtozy są miarami odpornymi na fluktuację jasności obrazu, gdzie błędy spowodowane fluktuacją piksela są błędami poziomów luminancji, a zatem jasność piksela jest nieprawidłowa.

f). Energia histogramu *P(g)* wyrażona zależnością [74]:

$$E = \sum_{g=0}^{L-1} [P(g)]^2 . \qquad (16)$$

4.3.2. Parametry wyznaczane na podstawie macierzy zdarzeń

Macierz zdarzeń C określana także mianem macierzy przejść lub koincydencji pozwala określać relacje pomiędzy kolorami poszczególnych par pikseli. Macierz zdarzeń *C* jest macierzą kwadratową wyznaczaną dla wybranego kierunku oraz odległości pomiędzy parami pikseli, gdzie element $C_{a,b}$ powstaje poprzez wyznaczenie liczby wszystkich takich par pikseli, które posiadają kolory *a* oraz *b*. Jeżeli wartości poszczególnych elementów macierzy zdarzeń zostaną podzielone przez liczbę wszystkich badanych par pikseli m, to uzyskana zostanie znormalizowana macierz zdarzeń [77].

Metodę wyznaczania współczynników macierzy zdarzeń przedstawia rysunek 22.

a)

0	0	0	0	0	0
1	1	0	1	1	0
0	2	2	0	2	2
0	0	0	0	0	0

b)

	0	1	2
0	10	1	2
1	2	2	0
2	1	0	2

c)

	0	1	2
0	0,5	0,05	0,1
1	0,1	0,1	0
2	0,05	0	0,1

d)

	0	1	2
0	10	2	1
1	1	2	0
2	2	0	2

e)

	0	1	2
0	20	3	3
1	3	4	0
2	3	0	4

f)

	0	1	2
0	0,5	0,075	0,075
1	0,075	0,1	0
2	0,075	0	0,1

Rys. 22. Przykłady macierzy zdarzeń [77] a) wartości pikseli obrazu; b) macierz dla dw=0, dk=1; c) macierz (b) po normalizacji; d) transponowana macierz (b); e) suma macierzy (b) i (d); f) macierz (e) po normalizacji

Poszczególne współczynniki macierzy zdarzeń informują o tym, ile razy w sąsiedztwie, określonym odległością *d* i kątem t_m, występują punkty o intensywności *i,j*. Charakter macierzy zdarzeń można określić poprzez szereg parametrów:

a). Energia (*ASM*), która informuje o rozłożeniu par pikseli w obrazie.

$$ASM = \sum_{a,b} (C_{a,b})^2 \tag{17}$$

b). Kontrast (*CON*) wyznacza zakres poziomów jasności występujących w obrazie. Określa odwzorowanie w ostrości krawędzi elementów tekstury.

$$CON = \sum_{a,b} ((a-b)^2 * C_{a,b}) \tag{18}$$

c). Jednorodność, odwrotny moment różnicowy (*ang. Inverse difference moment; Homogenity*). Pozwala na uwydatnienie tych elementów macierzy zdarzeń, które są skoncentrowane wzdłuż lub blisko głównej przekątnej.

$$IDM = \sum_{a,b} \frac{C_{a,b}}{1+(a-b)^2} \tag{19}$$

Wartości parametru jednorodności pozwalają wnioskować na temat zmienności obszarów w obrazach. Duże wartości jednorodności informują o występowaniu obszarów o podobnych lub zbliżonych poziomach jasności. Dzieje się tak, gdyż występuje duża liczba par pikseli o jednakowych lub bliskich wartościach, co przekłada się na powstawanie dużych wartości poszczególnych współczynników macierzy zdarzeń leżących w pobliżu głównej przekątnej. Z kolei niskie wartości występują tam, gdzie obrazy posiadają nieregularny rozkład poziomów jasności.

4.3.3. Analiza istotności atrybutów obrazu, pod kątem określenia widoczności zmian w poszczególnych obszarach obrazów cyfrowych

Stosowanie algorytmów steganograficznych w obrazach cyfrowych powoduje wprowadzanie do nich określonych zniekształceń. Ponieważ każdy algorytm steganograficzny z założenia powinien zapewniać niewidoczność faktu jego zastosowania, a zatem ważne jest odpowiednie dobieranie obrazów, aby ewentualne zmiany pozostawały niezauważalne. Niewidoczność zmian zapewnia po części odpowiedni dobór obrazów. Wiadome jest, że zmiany w obrazach o jednolitych odcieniach są bardziej zauważalne, a zatem ważne jest aby dobierać obrazy o dużym zróżnicowaniu. Poprzez zastosowanie takiego podejścia oraz poprzez wybór konkretnego miejsca ukrycia wiadomości uzależnionego od zastosowanego klucza, istnieje możliwość zbudowania algorytmu steganograficznego z kluczem, który nie będzie powodował występowania widocznych zmian w obrazach wynikowych. Należy tutaj podkreślić, że algorytmy steganograficzne z założenia nie powinny powodować występowania widocznych zmian w obrazach wynikowych na danym poziomie widoczności.

W tym celu proponuje się w niniejszej pracy stosowanie przedstawianych atrybutów obrazu jako wyznacznika ilości zmian poziomów barw w obrazach, zaś do oceny widoczności tych zmian (zróżnicowania) znormalizowaną funkcję czułości kontrastu CSF.

Wykonano analizę istotności poszczególnych parametrów obrazów. Analiza ta została przeprowadzona w oparciu o następujące atrybuty warunkowe:

a). liczba odcieni barwy czerwonej,

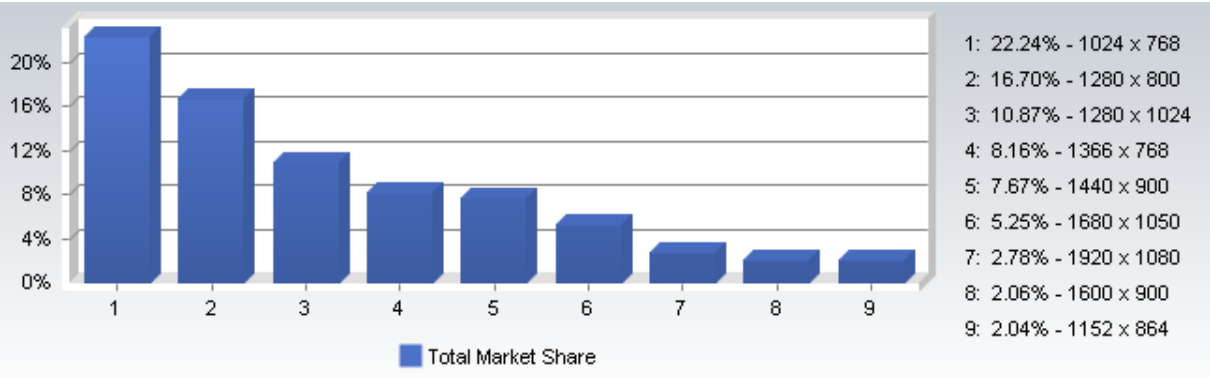
b). dla histogramów: średnia, wariancja, skośność, kurtoza, energia histogramu,

c). dla macierzy zdarzeń: energia, kontrast, jednorodność dla danych wertykalnych.

Do obliczeń użyto biblioteki 100800 obrazów powstałych z podzielenia 320 obrazów o rozmiarach 1024x768 pikseli na podobrazy 47x47 pikseli, których rozmiar stanowi kąt o rozwarciu jednego stopnia patrzenia na monitor 19 cali o rozdzielczości 1280x1024 w odległości 0,8 metra. Z jednego pełnego obrazu powstaje 315 podobrazów w rozmiarze 47x47 pikseli.

W analizie wykorzystano monitor o rozdzielczości 1280x1024 pikseli. Za jego wyborem przemawia fakt, że rozdzielczość ta stała się jedną z trzech głównych rozdzielczości obserwowanych wśród użytkowników Internetu, co przedstawia wykres

online firmy Net Applications na rysunku 23 (stan na listopad 2011). Firma ta na bieżąco monitoruje Internet w celu dostarczenia podstawowych informacji na temat charakterystyki użytkowników [78].



Rys. 23. Wykres użytkowania poszczególnych rozdzielczości ekranu w Internecie [78]

Istotność atrybutów wyznaczana była z wykorzystaniem teorii zbiorów przybliżonych i jej miękkiej redukcji atrybutów warunkowych opartą o względne prawdopodobieństwo reguł użytecznych [79]. Miękka redukcja atrybutów warunkowych pozwala na odrzucenie tych atrybutów, których usunięcie nie powoduje znacznego spadku liczby przykładów, które generują całkowicie pewne reguły. Cecha ta daje elastyczność tej metody i pozwala na analizę tych atrybutów, które mogą generować sprzeczne reguły. W metodzie tej można dokonać oceny jakości zbioru reguł na podstawie względnego prawdopodobieństwa reguł atomowych, które wyrazić można wzorem:

$$P_w = \frac{P}{L}, \tag{20}$$

gdzie P - suma prawdopodobieństw atomowych reguł użytecznych, L – liczba elementarnych zbiorów warunkowych.

Regułą atomową określa się jako regułę wygenerowaną dla pojedynczego zbioru elementarnego. Można ją uznać za użyteczną, jeżeli jej prawdopodobieństwo jest większe od 0,5.

W dalszej części odrzucono eksces, którego wartość wynikała bezpośrednio z kurtozy. Jest to rezultat tego, że liczony on jest na podstawie kurtozy poprzez odjęcie od niej stałej 3. Pozostawienie kurtozy generowałoby atrybuty decyzyjne identyczne z tymi, które dotyczyły tej pierwszej.

Analiza z wykorzystaniem teorii zbiorów przybliżonych polega na odpowiednim kodowaniu atrybutów decyzyjnych oraz warunkowych, a następnie poprzez redukcję poszczególnych atrybutów warunkowych określić ich istotność w generowaniu całkowicie pewnych reguł.

Zastosowana metoda miękkiej redukcji atrybutów warunkowych pozwala na ich redukcję przy niedużym spadku liczby przykładów, które generują całkowicie pewne reguły.

W metodzie tej najpierw należy dokonać kodowania atrybutów poprzez klasyfikację poszczególnych wartości do określonych przedziałów. Następnie generuje się dla wszystkich przykładów reguły decyzyjne (E) dla wszystkich atrybutów warunkowych (q). Ponieważ wiele reguł jest powtarzalnych, należy więc wykonać redukcję reguł identycznych, co przedstawia poniższa warunkowa tabela informacyjna w przestrzeni $P=\{q_1,q_2,q_3\}$, dla przykładu z 27 obrazami i trzema atrybutami warunkowymi q_i oraz jednym atrybutem decyzyjnym d_1.

Tabela 6. Przykładowa warunkowa tabela decyzyjna

Nr rysunku	**q1**	**q2**	**q3**	**Elementarne zbiory warunkowe**
0	3	3	1	E0
1	1	1	2	E1
2	2	1	3	E2
3	3	3	1	E0
4	1	1	3	E3
5	3	3	1	E0
6	2	2	3	E4
7	2	2	1	E5
8	1	1	2	E1
9	2	2	2	E6
10	1	1	2	E1
11	1	1	3	E3
12	2	1	2	E7
13	2	2	2	E6
14	3	2	2	E8
15	2	2	2	E6
16	2	2	2	E6
17	1	1	2	E1
18	2	1	2	E7
19	3	3	2	E9
20	3	1	3	E10
21	1	1	3	E3
22	2	2	3	E4
23	3	2	2	E8
24	3	2	2	E8
25	2	1	2	E7
26	3	3	2	E9
27	2	1	1	E11

Dla wszystkich zakodowanych atrybutów warunkowych generowana jest tabela zredukowana, gdzie nie bierze się pod uwagę atrybutu decyzyjnego. Wszystkie identyczne wystąpienia atrybutów warunkowych są zapisane jedną regułą decyzyjną E_i. Dla przykładu, w wierszu 0, 3 i 5 występuje ta sama sekwencja atrybutów warunkowych. Można je zatem zapisać jako jedna elementarna reguła atomowa E_0. Łącznie dla przedstawionego przykładu uzyskano jedenaście elementarnych reguł decyzyjnych:

$E_0=[0\ 3\ 5]$
$E_1=[1\ 8\ 10\ 17]$
$E_2=[2]$
$E_3=[4\ 11\ 21]$
$E_4=[6\ 22]$
$E_5=[7]$
$E_6=[9\ 13\ 15\ 16]$
$E_7=[12\ 18\ 25]$
$E_8=[14\ 23\ 24]$
$E_9=[19\ 26]$
$E_{10}=[20]$
$E_{11}=[27]$

Następnie klasyfikuje się wszystkie reguły decyzyjne w postaci ciągu X_i.

Tabela 7. Klasyfikacja przykładowych reguł decyzyjnych

Nr rysunku	**d1**	
0	1	X_1
1	3	X_3
2	3	
3	3	
4	3	
5	1	X_1
6	2	X_2
7	1	X_1
8	2	X_2
9	1	X_1
10	3	X_3
11	3	
12	2	X_2
13	2	
14	2	
15	2	
16	2	
17	2	
18	2	
19	1	X_1
20	3	X_3
21	3	
22	1	X_1
23	3	X_3

24	1	X_1
25	3	X_3
26	1	X_1
27	2	X_2

Podobnie jak dla atrybutów warunkowych generuje się zredukowaną tablicę informacyjną dla atrybutu decyzyjnego. Wszystkie identyczne poziomy atrybutu decyzyjnego oznaczane są zmienną z ciągu X_i. Dla prezentowanego przykładu uzyskano ciągi:

$$X_1=[0\ 5\ 7\ 9\ 29\ 22\ 24\ 26]$$
$$X_2=[6\ 8\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 27]$$
$$X_3=[1\ 2\ 3\ 4\ 10\ 11\ 20\ 21\ 23\ 25]$$

Przy takim zbiorze pełnych trzech atrybutów warunkowych uzyskuje się 12 elementarnych zbiorów warunkowych E_i. Poprzez wyznaczenie dolnych przybliżeń $DP(X_i)$ atrybutów warunkowych wyznaczany jest „Pozytywny obszar rodziny D*" dla wszystkich atrybutów warunkowych jako iloczyn wszystkich $DP(X_i)$. Dla konceptów decyzyjnych X_i wyznaczenie dolnych przybliżeń dla prezentowanego przykładu odbywa się następująco:

$X_1=[0\ 5\ 7\ 9\ 19\ 22\ 24\ 26]=\{0\}\cup\{5\}\cup E_5\cup\{9\}\cup E_9\cup\{22\}\cup\{24\}$

$DP(X_1)= E_5\cup E_9=[7\ 19\ 26]$

$X_2=[6\ 8\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 27]= \{6\}\cup\{8\}\cup\{12\}\cup\{13\}\cup\{14\}\cup\{15\}\cup\{16\}\cup\{17\}\cup\{18\}\cup E_{11}$

$DP(X_2)= E_{11}=[27]$

$X_3=[1\ 2\ 3\ 4\ 10\ 11\ 20\ 21\ 23\ 25]=\{1\}\cup E_2\cup\{3\}\cup E_3\cup\{10\}\cup E_{10}\cup\{23\}\cup\{25\}$

$DP(X_3)=E_2\cup E_3\cup E_{10}=[2\ 4\ 11\ 20\ 21]$

A zatem pozytywny obszar rodziny D wynosi:

$PosD^*=E_5\cup E_9\cup E_{11}\cup E_2\cup E_3\cup E_{10}=[7\ 19\ 26\ 27\ 2\ 4\ 11\ 20\ 21]=[2\ 4\ 7\ 11\ 19\ 20\ 21\ 26\ 27]$

Zawiera on 9 przykładów co daje jakość przybliżenia wynoszącą: $\gamma=9/28=0{,}32$

Niestety wiele reguł może generować sprzeczności. Miękka redukcja pozwala brać pod uwagę te reguły, których prawdopodobieństwo znajduje się na odpowiednim poziomie. Poszczególne kroki tej metody wyglądają następująco [79]:

1. Oblicz $p_{waru}(Q)$ dla bazy przykładów z pełną liczbą atrybutów warunkowych
2. Usuń jeden atrybutów warunkowych (q_i) i oblicz $p_{waru}(Q-q_i)$ dla bazy ze zredukowanych atrybutem. Jeżeli obniżenie wartości względnego prawdopodobieństwa $p_{waru}(Q)-p_{waru}(Q-q_1)$ jest akceptowalnie małe, to atrybut q_i może zostać usunięty na stałe ze zbioru atrybutów.

Względne prawdopodobieństwo p_{waru} jest to stosunek sumy prawdopodobieństw atomowych reguł użytecznych do liczby elementarnych zbiorów warunkowych.

Zredukowany zbiór reguł po usunięciu reguły q_3 przedstawiono poniżej.

Tabela 8. Przykład zredukowanego zbioru reguł

Nr	**q1**	**q2**		**d**
0	3	3	E_0	1
1	1	1	E_1	3
2	2	1	E_2	3
3	3	3	E_0	3
4	1	1	E_1	3
5	3	3	E_0	1
6	2	2	E_3	2
7	2	2	E_3	1
8	1	1	E_1	2
9	2	2	E_3	1
10	1	1	E_1	3
11	1	1	E_1	3
12	2	1	E_2	2
13	2	2	E_3	2
14	3	2	E_4	2
15	2	2	E_3	2
16	2	2	E_3	2
17	1	1	E_1	2
18	2	1	E_2	2
19	3	3	E_0	1
20	3	1	E_5	3
21	1	1	E_1	3
22	2	2	E_3	1
23	3	2	E_4	3
24	3	2	E_4	1
25	2	1	E_2	3
26	3	3	E_0	1
27	2	1	E_2	2

Dla taki zdefiniowanej tabeli informacyjnej uzyskuje się następujące zbiory reguł.

$E_0=[0\ 3\ 5\ 19\ 26]$

$E_1=[1\ 4\ 8\ 10\ 11\ 17\ 21]$

$E_2=[2\ 12\ 18\ 25\ 27]$

$E_3=[6\ 7\ 9\ 13\ 15\ 16\ 22]$

$E_4=[14\ 23\ 24]$

$E_5=[20]$

Dla tak przygotowanej redukcji obliczana jest liczba zbiorów elementarnych (niepowtarzalnych), liczba atomowych reguł użytecznych, sumaryczne prawdopodobieństwo reguł użytecznych, względne prawdopodobieństwo atomowych reguł użytecznych p_{waru} oraz istotność redukowanego atrybutu wyrażona dla prezentowanego przykładu zależnością:

$$Ist(q_3)=(p_{waru}(q1, q2, q3)-p_{waru}(q1, q2))/p_{waru}(q1, q2, q3)$$

W przypadku zastosowania twardej redukcji istotność wyznaczana była jako iloraz jakości przybliżenia po redukcji do jakości przybliżenia bez redukcji atrybutów warunkowych. Jeżeli istotność jest akceptowalnie mała, to atrybut taki można zredukować.

4.3.3.1. Kodowanie atrybutów

Przyjęto, że atrybutem decyzyjnym przeprowadzonej analizy, będzie liczba zmian kontrastu w obrazie. Atrybut ten został wybrany jako współczynnik zniekształceń spowodowanych steganograficznym ukryciem informacji w obrazie. Dyskretyzację dokonano metodą równej liczby próbek w przedziałach. Dla 100800 próbek, równy podział zostałby osiągnięty dzieląc je na pięć przedziałów po 20160 każdy.

Atrybut decyzyjny kodowano do 5 przedziałów, a próbki przydzielano w zależności od tego, do którego przedziału należały. Ze względu na charakter badanej bazy obrazów i konieczność stosowania bloków obrazu 47x47 pikseli możliwe było uzyskanie równego podziału dla połowy obrazów w bazie.

Tabela 9. Kodowanie atrybutu decyzyjnego

Atrybut decyzyjny	⟨0; 0,03)	⟨0,03;0,036)	⟨0,036; 0,041)	⟨0,041; 0,087)	⟨0,087-1⟩
Kodowanie	1	2	3	4	5

Jako atrybut decyzyjny wykorzystano znormalizowaną funkcję czułości kontrastu. W analizie stosowano sumę wszystkich odniesień częstotliwości zmian poziomych obrazów w jednym stopniu patrzenia na monitor 19 cali w odległości 0,8 metra, a zatem w kwadratach 47x47 pikseli. Dla porównania monitor 24 cale o rozdzielczości 1920x1080 pikseli cechuje się kwadratem w przybliżeniu o rozmiarze 50x50 pikseli dla jednego stopnia obserwacji.

Poprzez tak przyjęte kodowanie otrzymano rozkład próbek zgodny z tabelą 10.

Tabela 10. Liczba próbek atrybutu decyzyjnego dla zastosowanego kodowania

Atrybut decyzyjny	⟨0; 0,03)	⟨0,03;0,036)	⟨0,036; 0,041)	⟨0,041; 0,087)	⟨0,087-1⟩
Liczba próbek	50793	13130	11142	11719	14016

Dla atrybutów zastosowano takie samo kodowanie, jak dla atrybutu decyzyjnego z wykorzystaniem dyskretyzacji metodą równej liczby próbek w przedziałach. Zastosowano kodowanie atrybutów warunkowych zgodne z tabelą 11.

Tabela 11. Kodowanie atrybutów warunkowych

	Kodowanie atrybutów				
Atrybut	**1**	**2**	**3**	**4**	**5**
Liczba odcieni czerwieni	⟨0;57)	⟨57;111)	⟨111;155)	⟨155;203)	≥ 203
Średnia	⟨0;65)	⟨65;112)	⟨112;151)	⟨151;194)	≥ 194
Wariancja	Poniżej 310	⟨310;702)	⟨702;1049)	⟨1049;1549)	≥ 1549
Skośność	Poniżej -6	⟨-6,0;-4.0)	⟨-4;-1.5)	⟨-1.5;0)	≥ 0
Kurtoza	Poniżej 4	⟨4;9.5)	⟨9.5;24)	⟨24;40)	≥ 40
Energia histogramu	Poniżej 0,015	⟨0,015; 0,028)	⟨0,028; 0,05)	⟨0,05;0,011)	≥ 0,011
Energia macierzy zdarzeń	Poniżej 0,0011	⟨0,0011; 0,004)	⟨0,004; 0,014)	⟨0,014;0,055)	≥ 0,055
Kontrast	Poniżej 300	⟨300;750)	⟨750;1200)	⟨1200;1900)	≥ 1900
Jednorodność	Poniżej 0,18	⟨0,18;0,35)	⟨0,35;0,52)	⟨0,52;0,73)	≥ 0,73

4.3.3.2. Analiza z wykorzystaniem teorii zbiorów przybliżonych

Wykonano analizę z wykorzystaniem teorii zbiorów przybliżonych dla określenia możliwości wykorzystania znormalizowanej funkcji czułości kontrastu CSF oraz parametrów obrazu do wyznaczania zróżnicowania bloków obrazów.

Wyznaczono liczbę zbiorów elementarnych dla pełnego zbioru atrybutów warunkowych otrzymując wyniki:

- **Liczba zbiorów elementarnych**: 10421
- **Liczba atomowych reguł użytecznych**: 8413

- **Sumaryczne prawdopodobieństwo bezwzględne atomowych reguł użytecznych**: 7818,405762
- **Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych**: 0,750255

Wyniki analizy dla zredukowanego zbioru atrybutów warunkowych przedstawia tabela 12.

Tabela 12. Wyniki analizy redukcji atrybutów

Redukowany atrybut	**Liczba zbiorów elementarnych zredukowanych**	**Liczba atomowych reguł użytecznych zredukowanych**	**Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych zredukowanych**	**Istotność atrybutu**
Liczba odcieni czerwieni	5141	3939	0,685204	0,086705
Średnia	7512	5843	0,709718	0,054031
Wariancja	7133	5597	0,716627	0,044822
Skośność	7731	6116	0,724501	0,034326
Kurtoza	7369	5785	0,716442	0,045068
Energia_hist	6843	5348	0,714092	0,048201
Energia macierzy zdarzeń	7557	5864	0,712264	0,050637
Kontrast	6836	5174	0,687726	0,083343
Jednorodność	6460	4849	0,687481	0,083670

Jak wynika z obliczeń, największą liczbę reguł użytecznych zachowuje się poprzez redukcję atrybutu skośności histogramu kolorów. Atrybutami o niskiej istotności są także wariancja i kurtoza histogramu kolorów. Najwyższą istotnością cechuje się liczba odcieni czerwieni, kontrast i jednorodność macierzy zdarzeń. Wyniki te zostaną porównane w dalszej kolejności z analizą istotności atrybutów dla obrazów z wprowadzoną dodatkową informacją.

4.3.3.3. Analiza istotności atrybutów obrazu, pod kątem określenia widoczności zmian zachodzących w obrazach cyfrowych po wprowadzeniu dodatkowej informacji

Steganograficzne ukrywanie informacji w obrazach cyfrowych nie powinno powodować widocznych zmian w obrazie wynikowym. Dlatego ważne jest opracowanie metody oceny zniekształceń jakie powoduje wybrany algorytm steganograficzny. Uwidocznienie zmian dokonywanych poprzez ukrywanie wiadomości metodą steganograficzną dyskwalifikuje samą metodę.

W pracy przeprowadzono analizę istotności atrybutów obrazu wpływających na ilość zmian jakie powoduje steganograficzne ukrywanie informacji, gdzie jako miarę stopnia zniekształceń wykorzystano znormalizowaną funkcję czułości kontrastu CSF. W miejsce użycia algorytmu steganograficznego użyto dodawania szumu do obrazu wynikowego, zaś jako miarę zniekształceń funkcję poczucia kontrastu CSF.

Analiza istotności atrybutów warunkowych została przeprowadzona z wykorzystaniem miękkiej redukcji atrybutów warunkowych w oparciu o względne prawdopodobieństwo reguł użytecznych w teorii zbiorów przybliżonych [80] na próbie 100800 obrazów.

Analizowano istotność atrybutów decyzyjnych:

a). liczba odcieni barwy czerwonej,

b). dla histogramu kolorów: średnia arytmetyczna, wariancja, dyspersja, kurtoza, energia,

c). dla macierzy zdarzeń: kontrast, energia oraz jednorodność.

Zastosowana miękka redukcja atrybutów została wybrana ze względu na to, że pozwala ona na odrzucanie tych atrybutów, których usunięcie nie zmniejsza znacząco liczby przykładów generujących reguły pewne. W badaniach reguła była uznawana za użyteczną, jeżeli jej prawdopodobieństwo jest większe od 0,5

Wykonano analizę istotności dla czterech przypadków dla szumu Gaussa o losowej wariancji w przedziałach $\langle 0{,}00001;0{,}00006\rangle$, $\langle 0{,}00001;0{,}00008\rangle$, $\langle 0{,}00001;0{,}0001\rangle$ oraz $\langle 0{,}00001;0{,}00012\rangle$. Rosnący zakres przedziałów symulował stosowanie algorytmu stegangraficznego o rosnącej sile wstawiania wiadomości, gdzie rosnąca siła odpowiada za powstawanie większej ilości zniekształceń. Zastosowano wariancję losową, aby uzyskać różne poziomu szumu i uzyskać losowość dla symulacji wstawiania wiadomości. Wartość maksymalna wariancji na poziomie 0,00012 była tak

dobrana, aby w jej przypadku uzyskiwać maksymalny poziom zmian dla wybranego rozmiaru bloku 47x47 pikseli.

Dla szumu Gaussa o rozkładzie ⟨0,00001;0,00006⟩ zastosowano kodowanie atrybutu decyzyjnego zgodne z tabelą 13.

Tabela 13. Kodowanie atrybutu decyzyjnego dla szumu Gaussa ⟨0,00001;0,00006⟩

Atrybut decyzyjny	⟨0;0,09)	⟨0,09;0,103)	⟨0,103;0,13)	⟨0,13;0,18)	⟨0,18;1⟩
Kodowanie	1	2	3	4	5

Zastosowano równy podział próbek w przedziałach. Poprzez tak przyjęte kodowanie otrzymano rozkład próbek zgodny z tabelą 14.

Tabela 14. Rozkład liczby próbek w przedziałach dla szumu Gaussa ⟨0,00001;0,00006⟩

Atrybut decyzyjny	⟨0;0,09)	⟨0,09;0,103)	⟨0,103;0,13)	⟨0,13;0,18)	⟨0,18;1⟩
Liczba próbek	23097	17361	21532	18653	20157

Dla atrybutów warunkowych zastosowano kodowanie z wykorzystaniem dyskretyzacji metodą równej liczby próbek w przedziałach taką samą jak w rozdziale 4.3.3.1. Otrzymano następujące wyniki analizy:

- **Liczba zbiorów elementarnych**: 10421
- **Liczba atomowych reguł użytecznych**: 5563
- **Sumaryczne prawdopodobieństwo bezwzględne atomowych reguł użytecznych**: 5305,637207
- **Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych**: 0,509129

Wyniki analizy dla zredukowanego zbioru atrybutów warunkowych z szumem Gaussa z wariancją ⟨0,00001;0,00006⟩, przedstawia tabela 15.

Tabela 15. Wyniki analizy obrazów z szumem Gaussa z wariancją ⟨0,00001;0,00006⟩

Redukowany atrybut	**Liczba zbiorów elementarnych zredukowanych**	**Liczba atomowych reguł użytecznych zredukowanych**	**Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych zredukowanych**	**Istotność atrybutu**
Liczba odcieni czerwieni	5141	2177	0,394888	0,224386
Średnia	7512	3494	0,454965	0,106385
Wariancja	7133	5597	0,462971	0,090661
Skośność	7731	3806	0,464935	0,086803
Kurtoza	7369	3562	0,455266	0,105796
Energia_hist	6843	3131	0,430990	0,153476
Energia macierzy zdarzeń	7557	3627	0,453150	0,109951
Kontrast	6836	3207	0,441215	0,133393
Jednorodność	6460	2981	0,435270	0,145069

W przypadku niewielkich zniekształceń jakie są dodawane do obrazu źródłowego z wykorzystaniem szumu Gaussa najwyższą istotnością cechuje się liczba odcieni czerwieni podobnie jak to było w rozdziale 4.3.3.2. Podobnie także, wysoką istotność posiadają nadal parametry energii histogramu oraz jednorodność macierzy zdarzeń i kontrast macierzy zdarzeń. Najniższą istotność wykazuje skośność histogramu podobnie jak w przypadku wyznaczania istotności atrybutów dla analizy jakości obrazu (Tabela 7). Także i tutaj niskim poziomem istotności cechuje się wariancja histogramu. Poziom istotności bliski 10 procentom nie pozwala na redukcję tych atrybutów.

Następnie wykonano analizę istotności przypadku z szumem Gaussa o wariancji ⟨0,00001;0,00008⟩. Dla szumu Gaussa o rozkładzie ⟨0,00001;0,00008⟩ zastosowano kodowanie atrybutu decyzyjnego wg tabeli 16.

Tabela 16. Kodowanie atrybutu decyzyjnego dla szumu Gaussa ⟨0,00001;0,00008⟩

Atrybut decyzyjny	⟨0;0,076)	⟨0,076;0,088)	⟨0,088;0,11)	⟨0,11;0,16)	⟨0,16;1⟩
Kodowanie	1	2	3	4	5

Dla atrybutu decyzyjnego zastosowano kodowanie z wykorzystaniem dyskretyzacji metodą równej liczby próbek w przedziałach. Poprzez tak przyjęte kodowanie otrzymano rozkład próbek zgodny z tabelą 17.

Tabela 17. Rozkład liczby próbek w przedziałach dla szumu Gaussa ⟨0,00001;0,00008⟩

Atrybut decyzyjny	⟨0;0,076)	⟨0,076;0,088)	⟨0,088;0,11)	⟨0,11;0,16)	⟨0,16;1⟩
Liczba próbek	21073	19857	20528	20256	19086

Dla atrybutów warunkowych zastosowano kodowanie z wykorzystaniem dyskretyzacji metodą równej liczby próbek w przedziałach taką samą jak w rozdziale 4.3.3.1.

Otrzymano następujące wyniki analizy po zastosowaniu szumu Gaussa z wariancją 0,005:

- **Liczba zbiorów elementarnych**: 10421
- **Liczba atomowych reguł użytecznych**: 5610
- **Sumaryczne prawdopodobieństwo bezwzględne atomowych reguł użytecznych**: 5333,909180
- **Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych**: 0,511842

Wyniki analizy dla zredukowanego zbioru atrybutów warunkowych po dodaniu szumu Gaussa z wariancją ⟨0,00001;0,00008⟩ przedstawia tabela 18.

Tabela 18. Wyniki analizy obrazów z szumem Gaussa z wariancją ⟨0,00001;0,00008⟩

Redukowany atrybut	**Liczba zbiorów elementarnych zredukowanych**	**Liczba atomowych reguł użytecznych zredukowanych**	**Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych zredukowanych**	**Istotność atrybutu**
Liczba odcieni czerwieni	5141	2164	0,392287	0,233579
Średnia	7512	3658	0,458252	0,104700
Wariancja	7133	3498	0,461860	0,097651
Skośność	7731	3817	0,466173	0,089226
Kurtoza	7369	3540	0,452447	0,116042
Energia_hist	6843	3182	0,435175	0,149787
Energia macierzy zdarzeń	7557	3623	0,453081	0,114804
Kontrast	6836	3214	0,441790	0,136864
Jednorodność	6460	2958	0,431336	0,157287

Dla obrazów, w których dodano większe zniekształcenia z wykorzystaniem szumu Gaussa zauważa się zwiększoną istotność wszystkich atrybutów. Jedynie dla energii histogramu istotność spadła. Nadal najwyższą istotnością cechuje się liczba odcieni czerwieni, a także jednorodność macierzy zdarzeń i energia histogramu kolorów. Najniższym poziomem istotności cechuje się ponownie skośność i wariancja histogramu kolorów przy czym większe zniekształcenia powodują wzrost ich istotności.

Wykonano analizę istotności kolejnego poziomu zmiany wariancji dla szumu Gaussa do poziomu ⟨0,00001;0,0001⟩. Dla szumu Gaussa o rozkładzie ⟨0,00001;0,0001⟩ zastosowano kodowanie atrybutu decyzyjnego zgodne z tabelą 19.

Tabela 19. Kodowanie atrybutu decyzyjnego dla szumu Gaussa ⟨0,00001;0,0001⟩

Atrybut decyzyjny	⟨0;0,068)	⟨0,068;0, 078)	⟨0,078;0, 096)	⟨0,096;0,14)	⟨0, 14;1⟩
Kodowanie	1	2	3	4	5

Dla atrybutu decyzyjnego zastosowano kodowanie z wykorzystaniem dyskretyzacji metodą równej liczby próbek w przedziałach. Poprzez tak przyjęte kodowanie otrzymano rozkład próbek zgodny z tabelą 20.

Tabela 20. Rozkład liczby próbek w przedziałach dla szumu Gaussa ⟨0,00001;0,0001⟩

Atrybut decyzyjny	⟨0;0,068)	⟨0,068;0, 078)	⟨0,078;0, 096)	⟨0,096;0,14)	⟨0, 14;1⟩
Liczba próbek	20329	19828	20293	20486	19864

Dla atrybutów warunkowych zastosowano kodowanie z wykorzystaniem dyskretyzacji metodą równej liczby próbek w przedziałach taką samą jak rozdziale 4.3.3.1.

Otrzymano następujące wyniki analizy.

- Liczba zbiorów elementarnych: 10421

- Liczba atomowych reguł użytecznych: 5590

- Sumaryczne prawdopodobieństwo bezwzględne atomowych reguł użytecznych: 5320,323242

- Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych: 0,510539

Wyniki analizy dla zredukowanego zbioru atrybutów warunkowych przy szumie Gaussa ⟨0,00001;0,0001⟩ przedstawia tabela 21.

Tabela 21. Wyniki analizy obrazów z szumem Gaussa z wariancją ⟨0,00001;0,0001⟩

Redukowany atrybut	**Liczba zbiorów elementarnych zredukowanych**	**Liczba atomowych reguł użytecznych zredukowanych**	**Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych zredukowanych**	**Istotność atrybutu**
Liczba odcieni czerwieni	5141	2151	0,391795	0,232584
Średnia	7512	3647	0,456764	0,105330
Wariancja	7133	3500	0,463276	0,092574
Skośność	7731	3827	0,467775	0,083762
Kurtoza	7369	3594	0,458483	0,101963
Energia_hist	6843	3174	0,434943	0,148071
Energia macierzy zdarzeń	7557	3619	0,452431	0,113817
Kontrast	6836	3209	0,441838	0,134566
Jednorodność	6460	3003	0,436852	0,144331

Ponowne podniesienie poziomu zniekształceń wprowadzanych do obrazu źródłowego nie powoduje dalszego wzrostu istotności atrybutów, a delikatny spadek. Nadal najwyższym poziomem cechują się liczba odcieni czerwieni, jednorodność i kontrast macierzy zdarzeń, a także energia histogramu. Najniższy poziom istotności dotyczy parametru skośności i wariancji histogramu.

W końcowym etapie wykonano analizę istotności szumu o rozkładzie Gaussa ⟨0,00001;0,00012⟩. Dla szumu Gaussa ⟨0,00001;0,00012⟩ zastosowano kodowanie atrybutu decyzyjnego zgodne z tabelą 22.

Tabela 22. Kodowanie atrybutu decyzyjnego dla szumu Gaussa ⟨0,00001;0,00012⟩

Atrybut decyzyjny	⟨0;0,063)	⟨0,063;0,072)	⟨0,072;0,088)	⟨0,088;0,13)	⟨0,13;1⟩
Kodowanie	1	2	3	4	5

Dla atrybutu decyzyjnego zastosowano kodowanie z wykorzystaniem dyskretyzacji metodą równej liczby próbek w przedziałach. Poprzez tak przyjęte kodowanie otrzymano rozkład próbek zgodny z tabelą 23.

Tabela 23. Rozkład liczby próbek w przedziałach dla szumu Gaussa ⟨0,00001;0,00012⟩

Atrybut decyzyjny	⟨0;0,063)	⟨0,063;0,072)	⟨0,072;0,088)	⟨0,088;0,13)	⟨0,13;1⟩
Liczba próbek	21146	19978	19703	20501	19472

Dla atrybutów warunkowych zastosowano kodowanie z wykorzystaniem dyskretyzacji metodą równej liczby próbek w przedziałach taką samą jak w rozdziale 4.3.3.1.

Otrzymano następujące wyniki analizy przy użyciu szumu Poissona.

- Liczba zbiorów elementarnych: 10421

- Liczba atomowych reguł użytecznych: 5577

-Sumaryczne prawdopodobieństwo bezwzględne atomowych reguł użytecznych: 5309,774902

- Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych: 0,509526

Wyniki analizy dla zredukowanego zbioru atrybutów warunkowych przedstawia tabela 24.

Tabela 24. Wyniki analizy obrazów z szumem Gaussa ⟨0,00001;0,00012⟩

Redukowany atrybut	**Liczba zbiorów elementarnych zredukowanych**	**Liczba atomowych reguł użytecznych zredukowanych**	**Względne prawdopodobieństwo wszystkich atomowych reguł użytecznych zredukowanych**	**Istotność atrybutu**
Liczba odcieni czerwieni	5141	2179	0,394883	0,225000
Średnia	7512	3592	0,451276	0,114323
Wariancja	7133	3492	0,461612	0,094038
Skośność	7731	3824	0,466890	0,083678
Kurtoza	7369	3532	0,451916	0,113067
Energia_hist	6843	3164	0,434410	0,147423
Energia macierzy zdarzeń	7557	3622	0,452559	0,111805
Kontrast	6836	3191	0,438649	0,139104
Jednorodność	6460	2972	0,434989	0,146287

W końcowym etapie przeprowadzono analizę dla najsilniejszych zakłóceń jakie można wprowadzić do bloku 47x47 pikseli, gdzie w przy szumie o wariancji 0,00012 wprowadza się zniekształcenia do pełnego bloku. Niemniej przy dużym szumie o losowej wariancji obserwuje się te same poziomy istotności dla poszczególnych atrybutów jak w poprzednich analizach. Wyniki potwierdzają otrzymane wnioski dla zamieszczonych wcześniej w tym rozdziale analiz. Także i tutaj najwyższy poziom istotności dotyczy atrybutu liczby odcieni czerwieni oraz energii histogramu i jednorodności macierzy zdarzeń. Wysoki poziom zachowują także kontrast i energia macierzy zdarzeń oraz średnia i kurtoza histogramu kolorów. Najniższy poziom istotności dotyczy atrybutów skośności i wariancji histogramu kolorów. Nie jest to jednak istotność niska przez co atrybutów tych nie powinno się redukować.

4.3.4. Przeniesienie obliczeń do dziedziny transformaty falkowej

W tej części pracy zaproponowano wykorzystanie możliwości przeniesienia obliczeń do dziedziny transformaty falkowej w celu ich ujednolicenia dla wszystkich kroków opracowanego dalej algorytmu steganograficznego opartego na tej transformacie. Wybór reprezentacji falkowej został podyktowany tym, że zmian wprowadzanych w dziedzinie tej transformaty dokonywać można na różnych poziomach szczegółowości pomijając istotne elementy obrazu opisane ich aproksymacją. W tej części dla eksperymentalnie wybranej funkcji falkowej Daubechies oraz różnych poziomów dekompozycji, przedstawiono sposób transformacji miar charakterystycznych obrazu [81] wyznaczanych dla dziedziny przestrzennej na miary liczone w dziedzinie transformaty falkowej. Do klasyfikacji obrazów pod kątem ich przydatności do ukrywania określonej porcji danych wykorzystano omawiane już istotne [62][80] parametry obrazów według, których dokonywana jest ich klasyfikacja oraz kryterium poziomu niewidoczności oparte na funkcji CSF [62][73].

Nowoczesne algorytmy steganograficznego ukrywania wiadomości w kolorowych obrazach cyfrowych przetwarzają obrazy w dziedzinie transformat w tym falkowej. Podpasma transformaty falkowej zawierają dwa rodzaje informacji: o częstotliwości oraz przestrzenne. Przechowywanie informacji przestrzennych odróżnia ją od innych jak kosinusowa DCT, która przechowuje same dane o częstotliwościach. Dzięki temu można ukrywać dane rozpraszając bity wiadomości po całym obrazie jednocześnie posiadając informacje o przestrzennym zróżnicowaniu obrazu.

Dekompozycja falkowa stosowana jest do steganograficznego ukrywania informacji oraz do analizy obrazów pod kątem jego przydatności do ukrywania określonej porcji danych. Przejście pomiędzy istotnymi atrybutami obrazu z dziedziny przestrzennej do dziedziny transformaty upraszcza implementację algorytmu steganograficznego opartego na transformacie DWT, gdyż wszystkie obliczenia są wykonywane w jednej dziedzinie.

4.3.5. Reprezentacja falkowa obrazów

Analiza falkowa opiera się na wykorzystaniu zmiennej wielkości okna. Pozwala ona na różne poziomy próbkowania. Wykonując rzadsze próbkowanie

uzyskuje się informacje o niskich częstotliwościach zaś wykonując gęstsze, uzyskiwane są informacji o wyższych częstotliwościach. Dokonywany jest tutaj podział sygnału na sygnały składowe powstające w wyniku odwzorowania falki podstawowej z przeprowadzeniem jej przesunięcia i skalowania na sygnał poddawany analizie [82, 83].

Poprzez użycie tej transformaty, otrzymuje się obraz czteroczęściowy podzielony według [82]:

- część *LL* (aproksymacja) powstaje poprzez użycie dwuwymiarowej funkcji skalującej,
- część *LH* (detale wertykalne) powstaje poprzez użycie horyzontalnej funkcji falkowej,
- część *HL* (detale horyzontalne) powstaje poprzez użycie wertykalnej funkcji falkowej,
- część *HH* (detale diagonalne) powstaje poprzez użycie diagonalnej funkcji falkowej.

Najmniejszą informację niesie ze sobą dekompozycja wertykalna, zaś największą dekompozycje horyzontalne. Dzięki zastosowaniu dwuwymiarowej transformaty falkowej istnieje możliwość wykonania analizy obrazu w różnych rozdzielczościach.

Dekompozycja falkowa może być stosowana do ukrywania w niej informacji poprzez modyfikowanie jej współczynników oraz do analizy obrazów pod kątem ich przydatności do ukrywania określonej porcji danych. Przejście pomiędzy istotnymi atrybutami obrazu, które pozwalają klasyfikować obrazy jako przydatne do ukrycia wiadomości.

Funkcja reprezentująca obraz ma postać $F(x, y)$, która należy do przestrzeni $L^2(R^2)$. Wszystkie główne aksjomaty analizy wielorozdzielczej są takie same jak dla funkcji jednowymiarowych, z tym, że aproksymacja wykonywana jest w tej właśnie przestrzeni. Aproksymacja na poziomie j jest jego rzutem ortogonalnym na przestrzeń wektorową $\mathbf{V}_j$:

1. $\boldsymbol{V}_0 = V_0 \otimes V_0$;

2. $F(x, y) \in V_j <=> F(2^j x, 2^j y) \in \boldsymbol{V}_0$;

Spełnienie punktów 1 i 2 pozwala przestrzeniom V_j tworzyć w przestrzeni $L^2(R^2)$ ciąg o następujących właściwościach:

3. $\ldots \boldsymbol{V}_2 \subset \boldsymbol{V}_1 \subset \boldsymbol{V}_0 \subset \boldsymbol{V}_{-1} \subset \boldsymbol{V}_{-2} \subset \ldots$;

Przestrzenie wektorowe zawierają się kolejno wzajemnie w sobie, a zatem przestrzeń V_{i-1} zawiera w sobie wszystkie kolejne przestrzenie V_i.

4. $\bigcap_{j\in Z} V_j = \{0\}$;

5. $\overline{\bigcup_{j\in Z} V_j} = L^2(R^2)$;

Spełnienie aksjomatów 4 i 5 świadczy o tym, że nie istnieje żadna funkcja, która należałaby do wszystkich przestrzeni. Przestrzenie są zawarte w sobie i każda przestrzeń V_{i-1} może zawierać dodatkowe funkcje, których V_i nie posiada.

W przestrzeni $\boldsymbol{V_0}$ bazą ortonormalną jest:

$$\Phi_{0;nm}(x, y)=\varphi(x-n)\varphi(x-m), \quad n,m\in Z \tag{21}$$

Baza ortonormalna jest generowana przez przesunięcia funkcji Φ względem zmiennych x i y.

Dla dowolnej przestrzeni $\mathbf{V}_j$ jest to funkcja skalująca:

$$\Phi_{j;nm}(x, y)=2^{-j}\Phi(2^{-j}x-n, 2^{-j}y-m), \quad n,m\in Z \tag{23}$$

Bazę w przestrzeni $\boldsymbol{W_j}$ stanowi:

$$\boldsymbol{V_{j-1}}=\boldsymbol{V_j}\oplus\boldsymbol{W_j} \tag{24}$$

Przejście z przestrzeni szczegółowej V_{j-1} do przestrzeni szczegółowej V_j powoduje odrzucenie części informacji zdefiniowanej w przestrzeni W_j, która jest dopełnieniem przestrzeni V_{j-1} do V_j. Przestrzeń $\boldsymbol{W_j}$ składa się z trzech członów z bazami ortonormalnymi definiujących trzy falki:

1. $\Psi^h(x, y)=\varphi(x)\psi(y)$ – falka pozioma
2. $\Psi^v(x, y)=\psi(x)\varphi(y)$ – falka pionowa
3. $\Psi^d(x, y)=\psi(x)\psi(y)$ – falka diagonalna

Daje to bazę ortonormalną w $\boldsymbol{W_j}$ w postaci $\{\Psi^{\lambda}_{j;nm};\ n, m\in Z,\ \lambda=h, v, d\}$,

zaś $\{\Psi^{\lambda}_{j;nm};j\in Z;\ (n, m)\in Z^2,\ \lambda=h, v, d\}$ jest bazą w $\overline{\bigoplus_{j\in Z} W_j} = L^2(R^2)$.

Zdefiniowane falki pozwalają na uzyskanie detali poziomych, pionowych oraz diagonalnych badanego obrazu.

Jeżeli φ i ψ mają zwarty nośnik to wygenerowane na ich podstawie Φ oraz Ψ^{λ} mają też zwarty nośnik.

Filtracja dolno- i górnoprzepustowa jest określona zależnościami (25) i (26).

$$d^{(1,\lambda)}{}_{nm}=(F, \Psi^{\lambda}{}_{1;nm}), \tag{25}$$

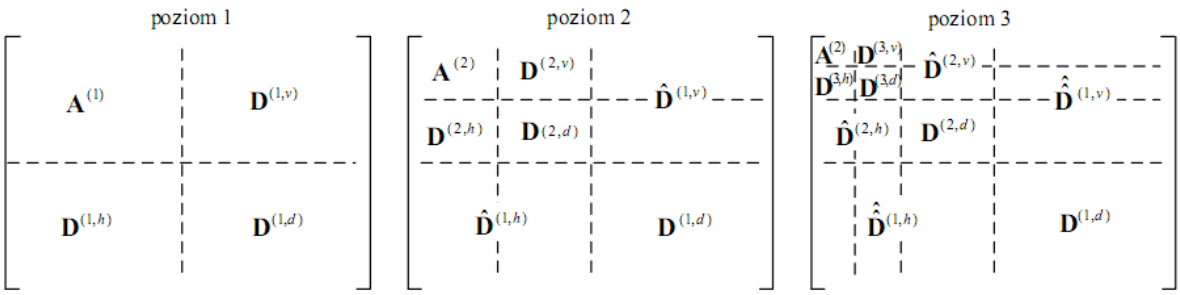
$$F = \sum_{n,m} f^{(0)}_{nm} \Phi_{0;nm} \tag{26}$$

W równaniach tych $d^{(1,\ \lambda)}{}_{nm}$ określają współczynniki rozwinięcia falkowego pierwszego poziomu i stanowią jego detale (są to rzuty ortogonalne na $\boldsymbol{W}_1$). Współczynniki $f^{(1)}{}_{nm}$ stanowią pierwszą aproksymację (rzuty ortogonalne na $\boldsymbol{V}_1$). Działania te są kolejno powtarzane na wierszach i kolumnach, tworząc następne aproksymacje i wyznaczają detale poziome, pionowe i diagonalne.

Kolejne aproksymacje j są zapisywane w blokach $f^{(j)}{}_{n,m.}$, Obraz stanowi ¼ obrazu stanowiącego aproksymację poziomu poprzedniego. Można, więc stwierdzić, że rozdzielczość jest związana z poziomem reprezentacji j zależnością $r_j=2^{-j}$, czyli maleje dwukrotnie ze wzrostem poziomu reprezentacji o jeden.

Detale $d^{(j,\ \lambda)}{}_{nm}$, stanowiące reprezentację szczegółową, zawierać będą informacje o krawędziach analizowanego obrazu. W składowej poziomej $d^{(1,\ h)}{}_{nm}$ widoczne będą krawędzie poziome obrazu oryginalnego, w $d^{(1,\ v)}{}_{nm}$ pionowe, a w diagonalnej $d^{(1,\ d)}{}_{nm}$ skośne.

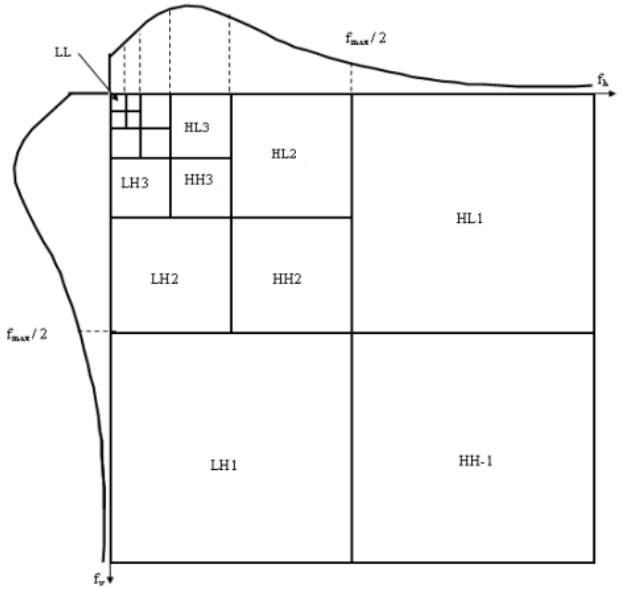
Schemat rozwinięcia falkowego sygnału dwuwymiarowego przedstawia rysunek 24.



Rys. 24. Dwuwymiarowa dekompozycja falkowa obrazu [84]

W pracy [85] przedstawiono możliwość przejścia między znormalizowaną funkcją czułości kontrastu, a dziedziną transformaty falkowej. Współczynniki CSF dla pasm biorą swoje wartości bezpośrednio z krzywej CSF dla znormalizowanej funkcji

czułości kontrastu z dziedziny przestrzennej. Rysunek 25 przedstawia relacje między funkcją CSF a transformatą falkową [86].



Rys.25. Relacja transformaty falkowej do funkcji CSF [86]

Rysunek 25 ten pokazuje, że odnosząc funkcję CSF na dekompozycję falkową obrazu, najbardziej zauważalne zmiany występują w aproksymacji niskopoziomowej, zaś najmniejsze na poziomie detali. Z tego też powodu, budując algorytm steganograficzny oparty na transformacie DWT należy brać pod uwagę, aby dane ukrywać na poziomie detali, szczególnie pierwszej aproksymacji, której częstotliwość zmian jest najmniej zauważalna.

Zgodnie z tym rysunkiem, najmniej widoczne zniekształcenia znajdują się w dekompozycji diagonalnej obrazu pierwszej dekompozycji. Potwierdza to fakt, że detale dekompozycji diagonalnej niosą ze sobą najmniejszą ilość informacji.

Funkcję czułości kontrastu określa zależność Manosa i Sakrisona [73] wyrażona wzorem (27).

$$H(f) = 2{,}6 * (0{,}192 + 0{,}114 * f) * e^{[-(0{,}114*f)^{1{,}1}} \tag{27}$$

We wzorze (27), $f=f_n*f_s$ i jest to środkowa częstotliwości dla danego pasma wyrażona w cyklach na stopień, f_n jest to znormalizowaną częstotliwością przestrzenną wyrażoną w cyklach na stopień, a f_s częstotliwością próbkowania wyrażoną w pikselach na stopień. Parametr f_s wyznacza się ze wzoru (28).

$$f_s = \frac{2v * \tan(0{,}5^\circ) * r}{0{,}0254} \tag{28}$$

We wzorze (28), parametr v wyznacza odległość obserwacji (zazwyczaj około 0,8 metra od monitora), zaś *r* to rozdzielczość monitora wyrażona w pikselach na cal. Przykładowo dla 19 calowego ekranu o rozdzielczości 1280x1024 pikseli parametr *r* wynosi:

$$r = \frac{\sqrt{1280^2 + 1024^2}}{19} = 102{,}44$$

Zgodnie z kryterium Nyquista maksymalna częstotliwość f_{max} wynosi połowę częstotliwości próbkowania, a zatem dla przedstawionego monitora 28,15 cykli/stopień.

4.3.6. Wyznaczenie przejścia pomiędzy istotnymi atrybutami obrazu a dziedziną transformaty falkowej

Do analizy przyjęto dziesięć obrazów kolorowych o rozdzielczości 1024x768 pikseli. W sposób eksperymentalny wybrano i zastosowano funkcję falkową o zwartym nośniku Daubechies pierwszego rzędu (Db1) dla czterech poziomów dekompozycji. Wyniki dla aproksymacji 4 poziomów dekompozycji, trzech wybranych do testów obrazów, prezentują tabele 25-28.

Tabela 25. Dekompozycja falkowa pierwszego poziomu dla falki Db1

Atrybut	**Obraz 1 Oryginał**	**Obraz 1 Przetworzony**	**Obraz 2 Oryginał**	**Obraz 2 Przetworzony**	**Obraz 3 Oryginał**	**Obraz 3 Przetworzony**
Liczba odcieni czerwieni	98	98	59	59	112	117
Średnia	95,30798	94,973495	82,3427	82,02296	94,65889	94,29889
Wariancja	7141,442	7004,94043	7791,189	7718,493	7085,302	6955,432
Skośność	0,488099	0,484995	0,781264	0,77902	0,542942	0,550236
Kurtoza	2,017253	2,027307	2,170373	2,167084	2,010148	2,036604
Energia_hist	0,073833	0,071305	0,067958	0,067362	0,066105	0,066194
Energia	0,068657	0,066059	0,064921	0,06386	0,063392	0,063255

macierzy zdarzeń						
Kontrast	0,067994	0,065054	0,064715	0,06325	0,062916	0,062392
Jednorodność	192,0398	288,059723	41,64256	127,2019	163,6349	122,8231

Tabela 26. Dekompozycja falkowa drugiego poziomu dla falki Db1

Atrybut	**Obraz 1 Oryginał**	**Obraz 1 Przetworzony**	**Obraz 2 Oryginał**	**Obraz 2 Przetworzony**	**Obraz 3 Oryginał**	**Obraz 3 Przetworzony**
Liczba odcieni czerwieni	98	97	59	57	112	116
Średnia	95,30798	94,942986	82,3427	82,0203	94,65889	94,28635
Wariancja	7141,442	6870,683594	7791,189	7665,822	7085,302	6893,906
Skośność	0,488099	0,479069	0,781264	0,771497	0,542942	0,554672
Kurtoza	2,017253	2,045178	2,170373	2,156449	2,010148	2,056276
Energia_hist	0,073833	0,069675	0,067958	0,06639	0,066105	0,066256
Energia macierzy zdarzeń	0,068657	0,064757	0,064921	0,063077	0,063392	0,063164
Kontrast	0,067994	0,063167	0,064715	0,061653	0,062916	0,061555
Jednorodność	192,0398	434,142426	41,64256	330,1153	163,6349	133,832

Tabela 27. Dekompozycja falkowa trzeciego poziomu dla falki Db1

Atrybut	**Obraz 1 Oryginał**	**Obraz 1 Przetworzony**	**Obraz 2 Oryginał**	**Obraz 2 Przetworzony**	**Obraz 3 Oryginał**	**Obraz 3 Przetworzony**
Liczba odcieni czerwieni	98	96	59	56	112	125
Średnia	95,30798	94,939049	82,3427	82,01926	94,65889	94,29127
Wariancja	7141,442	6675,947266	7791,189	7522,303	7085,302	6829,525
Skośność	0,488099	0,456656	0,781264	0,754141	0,542942	0,558328
Kurtoza	2,017253	2,057568	2,170373	2,141394	2,010148	2,077197
Energia_hist	0,073833	0,068755	0,067958	0,066209	0,066105	0,066349

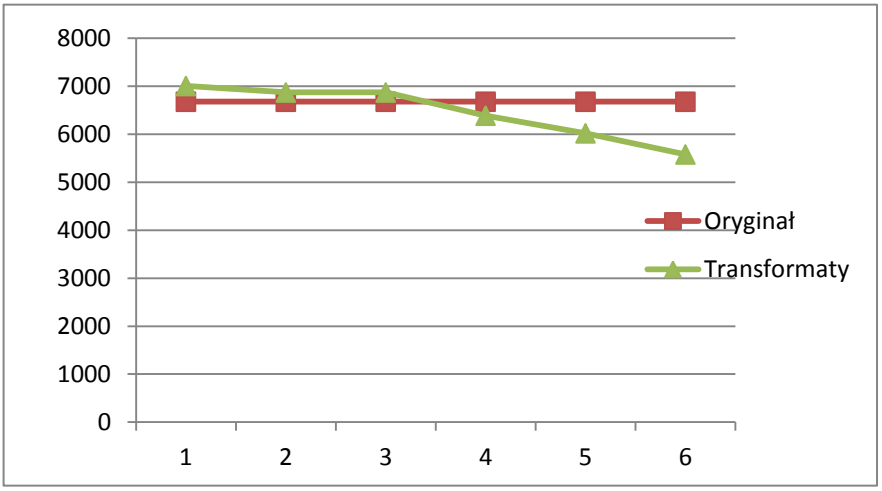
Energia macierzy zdarzeń	0,068657	0,063839	0,064921	0,062973	0,063392	0,063102
Kontrast	0,067994	0,060901	0,064715	0,060055	0,062916	0,060009
Jednorodność	192,0398	614,384033	41,64256	654,9199	163,6349	173,5446

Tabela 28. Dekompozycja falkowa czwartego poziomu dla falki Db1

Atrybut	**Obraz 1 Oryginał**	**Obraz 1 Przetworzony**	**Obraz 2 Oryginał**	**Obraz 2 Przetworzony**	**Obraz 3 Oryginał**	**Obraz 3 Przetworzony**
Liczba odcieni czerwieni	98	95	59	58	112	124
Średnia	95,30798	94,936203	82,3427	82,01855	94,65889	94,2858
Wariancja	7141,442	6383,765137	7791,189	7253,151	7085,302	6731,882
Skośność	0,488099	0,419007	0,781264	0,720222	0,542942	0,559247
Kurtoza	2,017253	2,067542	2,170373	2,112888	2,010148	2,10155
Energia_hist	0,073833	0,067451	0,067958	0,065924	0,066105	0,066537
Energia macierzy zdarzeń	0,068657	0,063065	0,064921	0,062917	0,063392	0,063072
Kontrast	0,067994	0,057187	0,064715	0,057068	0,062916	0,057077
Jednorodność	192,0398	790,146057	41,64256	1078,342	163,6349	208,0947

Parametrem przenośnym do dziedziny transformaty falkowej jest parametr liczby odcieni barwy czerwonej liczony z aproksymacji w dziedzinie transformaty. Dzieje się tak na pierwszym poziomie dekompozycji, gdzie w aproksymacji zachowywana jest największa część danych sprzed procesu dekompozycji. Zmniejszoną przenośność odnotowuje się także dla poziomów 2, 3 i 4. Bardzo dobrą przenośność zauważa się dla parametru średniej histogramu, w tym na wyższych poziomach dekompozycji. Przenośność obserwuje się także dla wariancji liczonej dla pierwszego i w mniejszym stopniu dla drugiego oraz trzeciego poziomu dekompozycji. Przykładowy wykresu dla zależności między wariancją dla obrazu oryginalnego (obraz 1) oraz

aproksymacji dla sześciu poziomów dekompozycji Falkowej z zastosowaniem funkcji Db1 przedstawia rysunek 26.



Rys.26. Przykład zmian wariancji dla sześciopoziomowej dekompozycji Falkowej

Na rysunku 26 widać zbieżność wariancji liczonej dla obrazu oryginalnego oraz uzyskanej z aproksymacji dla 6 poziomów dekompozycji. Wartości wariancji zachowują swoje zbliżone wartości do czterech poziomów dekompozycji falkowej, dzięki czemu można je wyliczać bazując na aproksymacji falkowej obrazu.

Przenośność skośności obserwuje się do drugiego poziomu dekompozycji. Dla parametrów kurtozy i energii histogramu oraz energii macierzy zdarzeń przenoszalność występuje tylko na pierwszym poziomie dekompozycji. Przy wyższych poziomach przenośność ulega pogorszeniu.

Do trzeciego poziomu dekompozycji dobrą przenośnością charakteryzuje się także kontrast macierzy zdarzeń.

Do parametru częściowo przenoszalnego należy jednorodność macierzy zdarzeń dla niskiego poziomu dekompozycji.

Eksperymentalnie, do dalszej analizy wzięto falki Daubechies wyższego rzędu. Wyniki dla falki czwartego i dziewiątego rzędu przedstawiają tabele 29 i 30.

Tabela 29. Dekompozycja falkowa czwartego poziomu dla falki Db4

Atrybut	**Obraz 1 Oryginał**	**Obraz 1 Przetworzony**	**Obraz 2 Oryginał**	**Obraz 2 Przetworzony**	**Obraz 3 Oryginał**	**Obraz 3 Przetworzony**
Liczba odcieni czerwieni	98	97	59	58	112	108
Średnia	95,30798	91,422974	82,3427	59,4614	94,65889	108,5335
Wariancja	7141,442	6182,77050	7791,189	6417,955	7085,302	8394,15
Skośność	0,488099	0,559143	0,781264	1,29162	0,542942	0,297643
Kurtoza	2,017253	2,306765	2,170373	3,328999	2,010148	1,633867
Energia_hist	0,073833	0,069882	0,067958	0,072757	0,066105	0,068815
Energia macierzy zdarzeń	0,068657	0,063415	0,064921	0,068206	0,063392	0,063932
Kontrast	0,067994	0,062079	0,064715	0,066921	0,062916	0,062601
Jednorodność	192,0398	279,958099	41,64256	122,4964	163,6349	276,394

Tabela 30. Dekompozycja falkowa czwartego poziomu dla falki Db9

Atrybut	**Obraz 1 Oryginał**	**Obraz 1 Przetworzony**	**Obraz 2 Oryginał**	**Obraz 2 Przetworzony**	**Obraz 3 Oryginał**	**Obraz 3 Przetworzony**
Liczba odcieni czerwieni	98	94	59	55	112	130
Średnia	95,30798	96,435478	82,3427	82,52491	94,65889	96,00864
Wariancja	7141,442	7127,97607	7791,189	7698,15	7085,302	7076,116
Skośność	0,488099	0,465173	0,781264	0,769986	0,542942	0,516482
Kurtoza	2,017253	1,984872	2,170373	2,155702	2,010148	1,974165
Energia_hist	0,073833	0,069907	0,067958	0,064455	0,066105	0,064362
Energia macierzy zdarzeń	0,068657	0,06364	0,064921	0,061373	0,063392	0,061294
Kontrast	0,067994	0,062639	0,064715	0,060711	0,062916	0,060468
Jednorodność	192,0398	296,606079	41,64256	136,1093	163,6349	131,3281

Dla falek wyższych rzędów pozostała niezmieniona przenośność liczby odcieni barwy wybieranej do ukrywania informacji. Przy wzroście rzędu do czterech istnieje przenośność średniej i energii histogramu dla dekompozycji pierwszego poziomu. Stosując kodowanie, o którym mówi rozdział 4 uzyskuje się całkowitą przenośność. Przenośność pogorszyła się dla wariancji, kurtozy, skośności histogramu, a także energii macierzy zdarzeń. Pogorszyła się przenośność kontrastu macierzy zdarzeń, zwłaszcza dla falek wyższego poziomu i wyższego rzędu. Niemniej przy kodowaniu nadal przenośność pozostaje zachowana. Pogorszyła się przenoszalność jednorodności macierzy zdarzeń. Problem nieprzenoszalności rośnie zwłaszcza dla dziewiątego rzędu falek.

A zatem wnioskując z przeprowadzanych obliczeń, wzrost rzędu falek w ujęciu ogólnym pogarsza możliwość uzyskiwania takich samych wartości dla obrazów aproksymowanych w porównaniu do wartości jakie uzyskuje się dla obrazów oryginalnych.

4.3.7. Ujednolicenie funkcji falkowych

Dla celów realizacji algorytmu steganograficznego wykorzystującego do ukrywania transformatę falkową autor proponuje ujednolicenie obliczeń opartych na różnych falkach bazowych, poprzez przejście do reprezentacji Pollena, która pozwala na generowanie baz falkowych o różnych stopniach regularności. Reprezentacja Pollena umożliwia konstruowanie rodzin falkowych zawierających różne bazy falkowe. Dzięki takiemu rozwiązaniu istnieje możliwość realizowania wszystkich obliczeń w jednej dziedzinie w miejsce dwóch: przestrzennej i falkowej, co ułatwia realizację sprzętową algorytmu steganograficznego.

Pollen wykazał, że dla filtru falkowego h o długości $2N$ istnieje ciągłe odwzorowanie z $[0, 2\pi]^{N-1}$ do wyznaczenia falkowego rozwiązania w postaci sekwencji $h=\{h_0, h_1, \ldots, h_{2N-1}\}$.

Przykładowo w pracy [87] przedstawiono reprezentację dla wszystkich rozwiązań falkowych o długościach 4 $(N=2)$, $N=2n-1$. Parametryzację dla $N=2$ (dla n równego 4 i mniej) tą przedstawia tabela 32.

Tabela 31. Parametryzacja Pollena dla *N=2* ($s = 2\sqrt{2}$)

n	**h_n dla N=2**
0	(1+cosφ-sinφ)/s
1	(1+cosφ+sinφ)/s
2	(1-cosφ+sinφ)/s
3	(1-cosφ-sinφ)/s

Różnica między $h_1(\varphi)$ oraz $h_2(\varphi)$ wyrażona jest poprzez $sin\varphi=h_1(\varphi)-h_2(\varphi)$. Przykładem zastosowania tej parametryzacji jest wzięcie jako parametrów $\varphi= л/6$ i $N=2$ dzięki którym uzyskuje się filtr Db2 (Daubechies #2).

Pollen w pracy [88] udowodnił, że parametryzację współczynników funkcji skalującej można rozszerzyć na dowolnie długą sekwencję. Przykład parametryzacji dla $N=3$ można znaleźć w pracy [89]. Wartość funkcji skalującej w punkcie oraz funkcji falkowej można w szybki sposób obliczać z algorytmu Daubechies-Lagariasa będącego alternatywą dla algorytmu Mallata [89].

W niniejszej pracy autor przeprowadził próbę przeniesienia istotnych parametrów obrazu z dziedziny przestrzennej do dziedziny transformaty falkowej wykorzystując do tego celu podobrazy aproksymacji obrazów falkowych dla falek Haara (haar), Daubechies (db1-9), Symlets (sym 2-8), Coiflets (coif 1-5) i DMeyera (dmey). Testowano 10 obrazów o rozmiarze 1024x768 pikseli na trzech poziomach aproksymacji. Licząc średnie odchylenie pomiędzy wartościami istotnych atrybutów dla obrazu oryginalnego i podobrazów aproksymacji otrzymano zestawienie proponowanych falek i poziomów aproksymacji, gdzie odchylenia były najmniejsze. Zestawienie to przedstawia tabela 32.

Tabela 32. Zestawienie proponowanych falek dla przenoszenia miar obrazów z dziedziny przestrzeni do transformaty

Miara	**Falka**	**Filtr korespondujący**
Odcieni czerwieni	Sym2	hn[0] = 0,48296291;hn[1] = 0,83651630; hn[2] = 0,22414386;hn[3] = -0,1294095;

Średnia	Sym5	hn[0] = 0,0195388;hn[1] = -0,0211018;
		hn[2] = -0,1753280;hn[3] = 0,01660210;
		hn[4] = 0,63397896;hn[5] = 0,72340769;
		hn[6] = 0,19939753;hn[7] = -0,0391342;
		hn[8] = 0,02951949;hn[9] = 0,02733306;

Wariancja	Db9	hn[0] = 0,0380779;hn[1] = 0,2438346;
		hn[2] = 0,6048231;hn[3] = 0,6572880;
		hn[4] = 0,1331973;hn[5] = -0,293273;
		hn[6] = -0,096840;hn[7] = 0,1485407;
		hn[8] = 0,0307256;hn[9] = -0,0676328;

		hn[10] = 0,0002509;hn[11] = 0,0223616;
		hn[12] = -0,0047232;hn[13] = -0,004281;
		hn[14] = 0,0018476;hn[15] = 0,0002303;
		hn[16] = -0,0002519;hn[17] = 0,0000393;

Skośność	Db1 (lub Sym1)	hn[0] = 0,7071067;hn[1] = 0,7071067;

Kurtoza	Sym5	hn[0] = 0,0195388;hn[1] = -0,0211018;
		hn[2] = -0,1753280;hn[3] = 0,01660210;
		hn[4] = 0,63397896;hn[5] = 0,72340769;
		hn[6] = 0,19939753;hn[7] = -0,0391342;
		hn[8] = 0,02951949;hn[9] = 0,02733306;

Energia_hist **Energia_MZ_v** **Energia_MZ_h** **Kontrast_MZ_h** **Jednorodność_MZ_h**	Db1 (lub Sym1)	hn[0] = 0,7071067;hn[1] = 0,7071067;

Kontrast_MZ_v	Sym3	hn[0] = 0,332670;hn[1] = 0,806891;
		hn[2] = 0,459877;hn[3] = -0,135011;
		hn[4] = -0,0854412;hn[5] = 0,035226;

Jednorodność_MZ_v	Sym2	hn[0] = 0,48296291;hn[1] = 0,83651630; hn[2] = 0,22414386;hn[3] = -0,1294095;

4.3.8. Podsumowanie rozdziału

W powyższym rozdziale zaprezentowane zostały badania nad niewidocznością zmian jakie występują pomiędzy obrazem wejściowym, a wyjściowym w wyniku działania algorytmów przetwarzania obrazów, ze szczególnym uwzględnieniem algorytmów steganograficznych.

Przedstawiona metoda oparta na funkcji czułości kontrastu CSF pozwala wyznaczać miejsca, których ukrycie wiadomości nie powoduje występowanie widocznych zmian w obrazach cyfrowych. Miejsca takie posłużą jako podbloki, w których ukryta zostanie wiadomość proponowanym w dalszej części pracy algorytmem steganograficznym.

W rozdziale tym zostały także zaprezentowane charakterystyczne miary statystyczne wyliczane dla obrazów cyfrowych oraz zbadana ich istotność. Miary te posłużą w proponowanym algorytmie jako opis obrazu, który przechowywany w bazie posłuży do szybkiego wyszukiwania obrazów przydatnych do ukrywania określonych porcji danych.

Na koniec zaproponowano ujednolicenie wszystkich obliczeń poprzez przeniesienie wszystkich ich do jednej dziedziny. Ponieważ zaproponowany w dalszej części pracy bazuje na transformacie falkowej, a zatem celowe było przeniesienie wszystkich obliczeń do tej dziedziny transformaty.

5. Propozycja algorytmu klucza oraz systemu steganograficznego

W pracy zaproponowano realizację algorytmu steganograficznego z kluczem opartego na dyskretnej transformacie falkowej DWT połączonego z wyborem miejsc ukrywania informacji.

5.1. Algorytm wyboru obrazów z bazy

Przedstawione w pracy metody oparte na parametrach obrazu pozwalają na opracowanie bazy reguł, które wykorzystane zostaną do wyboru przydatnych obrazów pod kątem ukrycia w nich określonej porcji danych. Zastosowane kodowanie atrybutów warunkowych oraz decyzyjne pozwala na wyznaczenie szeregu reguł, które następnie po zredukowaniu powtarzających się dają reguły mówiące w których przypadkach wprowadzenie danych do obrazu spowoduje zniekształcenia i w jakim stopniu. Przy przykładowo kodowaniu z rozdziału 4.3.3. atrybutu decyzyjnego wyznaczono zasadę kodowania zgodnie z tabelą 33.

Tabela 33. Przykładowe kodowanie atrybut decyzyjnego

Atrybut decyzyjny	⟨0; 0,03)	⟨0,03;0,036)	⟨0,036; 0,041)	⟨0,041; 0,087)	⟨0,087-1⟩
Kodowanie	1	2	3	4	5

Poszczególne wartości kodowe opisuje się wartościami lingwistycznymi, kolejno niech to będą: bardzo małe, małe, średnie, duże, bardzo duże. Podobnie opisuje się atrybuty warunkowe. Dzięki temu, podczas badania obrazów generuje się reguły określające stopień zmian kontrastu w danym obrazie. Po zredukowaniu powtarzalnych uzyskuje się reguły unikalne wyznaczające jednocześnie reguły wyboru obrazów z bazy. W celach badawczych w pracy realizowany był program działający na bazie danych, gdzie do bazy trafiały zapytania typu:

INSERT INTO tabela VALUES (‘1.bmp’, 4, 3,2,4,5, 3,3,5,3,3);

Przyjmując, że na pierwszej pozycji znajduje się nazwa obrazu, na drugiej zakodowany atrybut decyzyjny liczby zmian kontrastu, a na pozostałych zakodowane

atrybuty warunkowe, tworzona jest baza reguł wyboru obrazów z bazy. Atrybuty te można przechowywać zgodnie z zaproponowaną w rozdziale 4.3.7. reprezentacją Pollena. Osoba wybierająca obraz w celach steganograficznych, chcąc otrzymać listę obrazów przydatnych pod kątem ukrywania wiadomości z określoną niewidocznością, otrzymuje listę na podstawie klucza i wydanego zapytania do bazy o interesujących go parametrach. Ponieważ obraz jest dzielony na bloki pikseli w których badana jest niewidoczność (w pracy używano rozmiaru bloku 47x47 pikseli), a zatem dla każdego obrazu w bazie zapisywane są kolejne rekordy dotyczące każdego bloku. Użytkownik wydając zapytanie dotyczące zadanego parametru otrzymuje informacje ile bloków obrazu spełnia dany wymóg.

Przygotowanie takiej bazy danych na temat obrazów przeznaczonych do ukrywania informacji uzyskuje się szybki dostęp do informacji o obrazach bez konieczności na bieżąco wyszukiwania obrazów w przypadku chęci pozyskania odpowiedniego obrazu do ukrycia w nim wiadomości w sposób steganograficzny. Wybór obrazu jest uzależniany od klucza określającego z jakim poziomem niewidoczności wiadomość będzie ukrywana. Na tej podstawie generowana jest lista obrazów do dalszych operacji. Końcowy wybór zależy od klucza.

Wybór z bazy odbywa się poprzez wydanie odpowiedniego zapytania SQL do bazy o zwrócenie listy obrazów spełniających określone kryteria. Wszystkie reguły muszą zostać tam umieszczone na podstawie zakodowanych charakterystycznych parametrów obrazu.

5.2. Wybór obszarów ukrywania informacji w obrazach

W uzyskanym obrazie należy wyznaczyć miejsca ukrywania informacji. W tym celu proponuje się wykorzystanie funkcji czułości kontrastu. Jeżeli stopień zmian w bloku widzenia o kącie 1 stopnia jest powyżej progu widzialności, to taki blok klasyfikuje się jako przydatny pod kątem ukrycia w nim bitów wiadomości. Na podstawie tego buduje się mapę bloków przydatnych do ukrycia w nim wiadomości.

5.3. Dekompozycja falkowa obrazu źródłowego

W proponowanym algorytmie istnieje możliwość wykorzystania dowolnych funkcji falkowych. W pracy wykorzystano falki z rodziny Daubechies, Coiflets oraz Symlets na pierwszym poziomie dekompozycji. W przypadku poziomów wyższych należy zastosować odpowiednie filtry korespondujące oraz rozszerzyć klucz o wybór poziomu dekompozycji. W tabeli przedstawiono odpowiednie filtry korespondujące dla falki Daubechies (tabela 34).

Tabela 34. Filtry korespondujące dla falek Daubechies

Lp	**Nazwa**	**Filtr**
1	Db1	hn[0] = 0,70710678118654757; hn[1] = 0,70710678118654757;

2	Db2	hn[0] = 0,48296291314469025;
		hn[1] = 0,83651630373746899;
		hn[2] = 0,22414386804185735;
		hn[3] = -0,12940952255092145;

3	Db3	hn[0] = 0,332670552950;
		hn[1] = 0,806891509311;
		hn[2] = 0,459877502118;
		hn[3] = -0,135011020010;
		hn[4] = -0,085441273882;
		hn[5] = 0,035226291882;

4	Db4	hn[0] = 0,23037781330885523;
		hn[1] = 0,71484657055254153;
		hn[2] = 0,63088076792959036;
		hn[3] = -0,027983769416983849;
		hn[4] = -0,18703481171888114;
		hn[5] = 0,030841381835986965;
		hn[6] = 0,032883011666982945;
		hn[7] = -0,010597401784997278;

5	Db5	hn[0] = 0,16010239797412501;
		hn[1] = 0,60382926979747287;
		hn[2] = 0,72430852843857441;
		hn[3] = 0,13842814590110342;
		hn[4] = -0,24229488706619015;
		hn[5] = -0,032244869585029520;
		hn[6] = 0,077571493840065148;
		hn[7] = -0,0062414902130117052;
		hn[8] = -0,012580751999015526;
		hn[9] = 0,0033357252850015492;

6	Db6	hn[0] = 0,11154074335008017;
		hn[1] = 0,49462389039838539;
		hn[2] = 0,75113390802157753;
		hn[3] = 0,3152503517092432;
		hn[4] = -0,22626469396516913;
		hn[5] = -0,12976686756709563;
		hn[6] = 0,097501605587079362;
		hn[7] = 0,027522865530016288;

		hn[8] = -0,031582039318031156;
		hn[9] = 0,0005538422009938016;
		hn[10] = 0,0047772575110106514;
		hn[11] = -0,0010773010849955799;

7	Db7	hn[0] = 0,077852054085062364;
		hn[1] = 0,39653931948230575;
		hn[2] = 0,72913209084655506;
		hn[3] = 0,4697822874053586;
		hn[4] = -0,14390600392910627;
		hn[5] = -0,22403618499416572;
		hn[6] = 0,071309219267050042;
		hn[7] = 0,080612609151065898;
		hn[8] = -0,038029936935034633;
		hn[9] = -0,01657454163101562;
		hn[10] = 0,012550998556013784;
		hn[11] = 0,0004295779730047027 4;
		hn[12] = -0,0018016407039998328;
		hn[13] = 0,00035371380000103988;

8	Db8	hn[0] = 0,054415842243081609;
		hn[1] = 0,31287159091446592;
		hn[2] = 0,67563073629801285;
		hn[3] = 0,585354683654869093;
		hn[4] = -0,015829105256023893;
		hn[5] = -0,28401554296242809;
		hn[6] = 0,00047248457399797254;
		hn[7] = 0,12874742662018601;
		hn[8] = -0,017369301002022108;
		hn[9] = -0,044088253931064719;
		hn[10] = 0,013981027917015516;
		hn[11] = 0,0087460940470156547;
		hn[12] = -0,0048703529930106603;
		hn[13] = -0,00039174037299597711;
		hn[14] = 0,0006754494059985567 7;
		hn[15] = -0,00011747678400228192;

9	Db9	hn[0] = 0,038077947363167282;
		hn[1] = 0,24383467463766728;
		hn[2] = 0,6048231236767786;
		hn[3] = 0,65728807803663891;
		hn[4] = 0,13319738582208895;
		hn[5] = -0,29327378327258685;
		hn[6] = -0,096840783220879037;
		hn[7] = 0,14854074933476008;
		hn[8] = 0,030725681478322865;
		hn[9] = -0,067632829059523988;
		hn[10] = 0,00025094711499193845;
		hn[11] = 0,022361662123515244;
		hn[12] = -0,004723204757894831;
		hn[13] = -0,0042815036819047227;
		hn[14] = 0,0018476468829611268;
		hn[15] = 0,00023038576399541288;
		hn[16] = -0,00025196318899817888;
		hn[17] = 0,00003934731999502612 4;

W tabeli 35 przedstawiono odpowiednie filtry korespondujące dla falki Coiflets.

Tabela 35. Filtry korespondujące dla falek Coiflets

Lp	**Nazwa**	**Filtr**

10	Coif1	hn[0] = -0,072732619512853897;
		hn[1] = 0,33789766245780922;
		hn[2] = 0,85257202021225542;
		hn[3] = 0,38486484686420286;
		hn[4] = -0,072732619512853897;
		hn[5] = -0,01565572813546454;

11	Coif 2	hn[0] = 0,016387336463522112;
		hn[1] = -0,041464936781759151;
		hn[2] = -0,067372554721963018;
		hn[3] = 0,38611006682116222;
		hn[4] = 0,81272363544554227;
		hn[5] = 0,41700518442169254;
		hn[6] = -0,076488599078306393;
		hn[7] = -0,059434418646456898;
		hn[8] = 0,023680171946334084;
		hn[9] = 0,0056114348193944995;
		hn[10] = -0,0018232088707029932;
		hn[11] = -0,00072054944536451221;

12	Coif 3	hn[0] = -0,0037935128644910141;
		hn[1] = 0,0077825964273254182;
		hn[2] = 0,023452696141836267;
		hn[3] = -0,0657719112818555;
		hn[4] = -0,061123390002672869;
		hn[5] = 0,4051769024096169;
		hn[6] = 0,79377722262562056;
		hn[7] = 0,42848347637761874;
		hn[8] = -0,071799821619312018;
		hn[9] = -0,082301927106885983;
		hn[10] = 0,034555027573061628;
		hn[11] = 0,015880544863615904;
		hn[12] = -0,0090079761366615805;
		hn[13] = -0,0025745176887502236;
		hn[14] = 0,0011175187708906016;
		hn[15] = 0,00046621696011288631;
		hn[16] = -0,000070983303138141252;
		hn[17] = -0,000034599772836212559 05;

14	Coif 4	hn[0] = 0,00089231366858231456;
		hn[1] = -0,0016294920126017326;
		hn[2] = -0,0073461663276420935;
		hn[3] = 0,016068943964776348;
		hn[4] = 0,026682300156053072;
		hn[5] = -0,081266699680878754;
		hn[6] = -0,056077313316754807;
		hn[7] = 0,41530840703043026;
		hn[8] = 0,78223893092049901;
		hn[9] = 0,4343860564914685;
		hn[10] = -0,066627474263425038;
		hn[11] = -0,096220442033987982;
		hn[12] = 0,039334427123337491;
		hn[13] = 0,025082261844864097;
		hn[14] = -0,015211731527946259;
		hn[15] = -0,0056582866866107199;
		hn[16] = 0,0037514361572784571;
		hn[17] = 0,0012665619292989445;
		hn[18] = -0,00058902075624433831;

		hn[19] = -0,00025997455248771324;
		hn[20] = 0,00006233903446100 7128;
		hn[21] = 0,00003122987586534 5646;
		hn[22] = -0,00000325968023688336 75;
		hn[23] = -0,00000178498500308826 14;

15	Coif 5	hn[0] = -0,00021208083980379827;
		hn[1] = 0,00035858968789573785;
		hn[2] = 0,0021782363581090178;
		hn[3] = -0,004159358781386048;
		hn[4] = -0,010131117519849788;
		hn[5] = 0,023408156785839195;
		hn[6] = 0,02816802897093635;
		hn[7] = -0,091920010559696244;
		hn[8] = -0,052043163176243773;
		hn[9] = 0,42156620669085149;
		hn[10] = 0,77428960365295618;
		hn[11] = 0,43799162617183712;
		hn[12] = -0,062035963962903569;
		hn[13] = -0,10557420870333893;
		hn[14] = 0,041289208750181702;
		hn[15] = 0,032683574267111833;
		hn[16] = -0,019761778942572639;
		hn[17] = -0,0091642311624818458;
		hn[18] = 0,0067641854480530832;
		hn[19] = 0,0024333732126576722;
		hn[20] = -0,0016628637020130838;
		hn[21] = -0,00063813134304511142;
		hn[22] = 0,00030225958181306315;
		hn[23] = 0,00014054114970203437;
		hn[24] = -0,00004134043227251 2511;
		hn[25] = -0,00002131502680995 5787;
		hn[26] = 0,00000373465517514 14047;
		hn[27] = 0,00000206376185136 46814;
		hn[28] = -0,00000167442885768 23017;
		hn[29] = -0,00000095176572738 19165;

W tabeli 36 przedstawiono odpowiednie filtry korespondujące dla falki Symlets.

Tabela 36. Filtry korespondujące dla falek Symlets

Lp	**Nazwa**	**Filtr**

16	Sym2	hn[0] = 0,48296291314469025;
		hn[1] = 0,83651630373746899;
		hn[2] = 0,22414386804185735;
		hn[3] = -0,12940952255092145;

17	Sym3	hn[0] = 0,332670552950;
		hn[1] = 0,806891509311;
		hn[2] = 0,459877502118;
		hn[3] = -0,135011020010;
		hn[4] = -0,085441273882;
		hn[5] = 0,035226291882;

18	Sym4	hn[0] = 0,032223100604042702;
		hn[1] = -0,012603967262037833;
		hn[2] = -0,099219543576847216;
		hn[3] = 0,29785779560527736;

		hn[4] = 0,80373875180591614;
		hn[5] = 0,49761866763201545;
		hn[6] = -0,02963552764599851;
		hn[7] = -0,075765714789273325;

19	Sym5	hn[0] = 0,019538882735286728;
		hn[1] = -0,021101834024758855;
		hn[2] = -0,17532808990845047;
		hn[3] = 0,016602105764522319;
		hn[4] = 0,63397896345821192;
		hn[5] = 0,72340769040242059;
		hn[6] = 0,1993975339773936;
		hn[7] = -0,039134249302383094;
		hn[8] = 0,029519490925774643;
		hn[9] = 0,027333068345077982;

20	Sym6	hn[0] = -0,007800708325034148;
		hn[1] = 0,0017677118642428036;
		hn[2] = 0,044724901770665779;
		hn[3] = -0,021060292512300564;
		hn[4] = -0,072637522786462516;
		hn[5] = 0,3379294217276218;
		hn[6] = 0,787641141030194;
		hn[7] = 0,49105594192674662;
		hn[8] = -0,048311742585632998;
		hn[9] = -0,11799011114819057;
		hn[10] = 0,0034907120842174702;
		hn[11] = 0,015404109327027373;

21	Sym7	hn[0] = 0,010268176708511255;
		hn[1] = 0,0040102448715336634;
		hn[2] = -0,10780823770381774;
		hn[3] = -0,14004724044296152;
		hn[4] = 0,28862963175151463;
		hn[5] = 0,76776431700316405;
		hn[6] = 0,5361019170917628;
		hn[7] = 0,017441255086855827;
		hn[8] = -0,049552834937127255;
		hn[9] = 0,067892693501372697;
		hn[10] = 0,03051551316596357;
		hn[11] = -0,01263630340325193;
		hn[12] = -0,0010473848886829163;
		hn[13] = 0,0026818145682578781;

22	Sym7	hn[0] = 0,0018897950332759 4609;
		hn[1] = -0,000302920514213668;
		hn[2] = -0,014952258337048231;
		hn[3] = 0,0038087520138906151;
		hn[4] = 0,049137179673607506;
		hn[5] = -0,027219029917056003;
		hn[6] = -0,051945838107709037;
		hn[7] = 0,3644418948353314;
		hn[8] = 0,77718575170052351;
		hn[9] = 0,48135965125837221;
		hn[10] = -0,061273359067658524;
		hn[11] = -0,14329423835080971;
		hn[12] = 0,0076074873249176054;
		hn[13] = 0,031695087811492981;
		hn[14] = -0,00054213233179114812;
		hn[15] = -0,0033824159510061256;

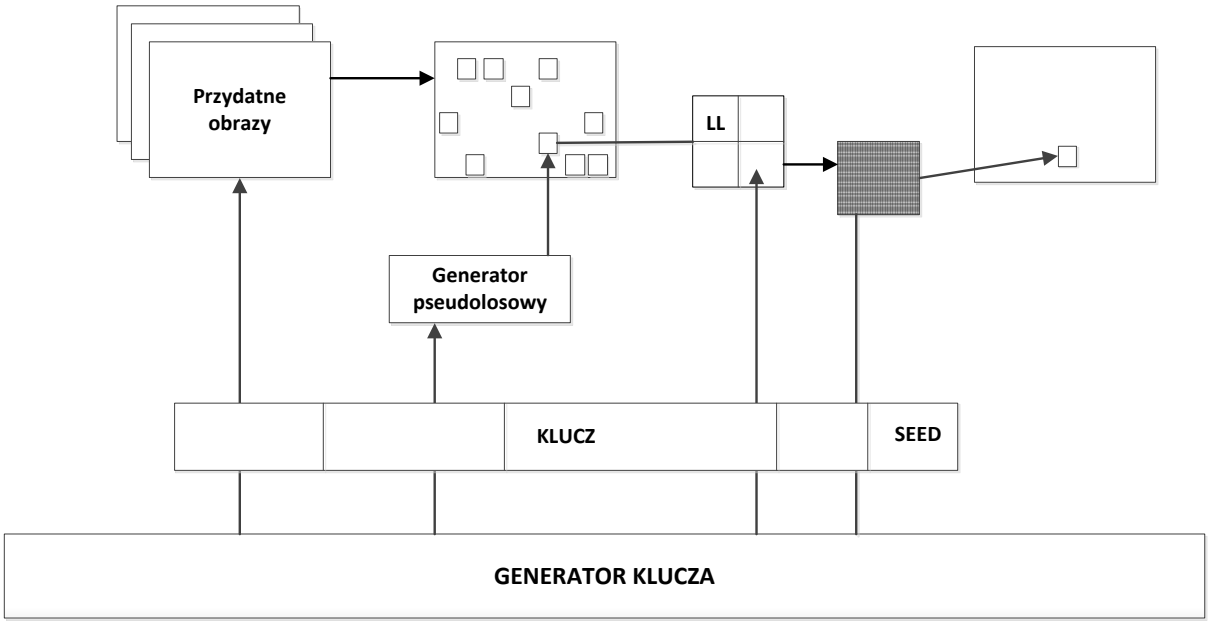
Przed ukryciem wiadomości, obraz źródłowy jest dzielony na bloki wielkości zbliżonej jednemu stopniowi patrzenia jaki definiuje się dla funkcji CSF, która dla monitora 19 cali wynosi 47 pikseli. Dla ujednolicenia tej wartości dla innych rodzajów monitorów przyjęto standardową wielkość 64 pikseli.

Na każdym bloku 64x64 piksele wykonywana jest następnie dekompozycja falkowa zależna od klucza.

Klucz wykorzystywany jest do algorytmu losowego wybierającego kolejne przydatne podbloki obrazu z wygenerowanej mapy przydatności. Kolejna część klucza określa id falki jaka zostanie użyta do dekompozycji. Na końcu przy pomocy klucza wybierana jest ćwiartka ukrywania (nie brany jest pod uwagę blok *LL*) oraz numery wierszy i kolumn modyfikowanych współczynników. Po modyfikacji współczynników poprzez podmianę wartości bitów dokonywana jest dekompozycja odwrotna.

5.4. Ogólny schemat proponowanego algorytmu

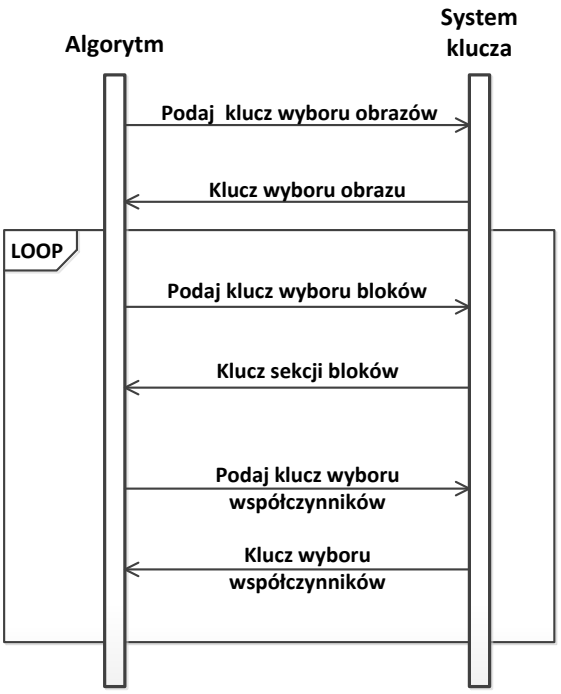
Dla realizacji postawionego w celu pracy autor proponuje przyjęcie następującego uogólnionego algorytmu steganograficznego opartego na kluczu. Algorytm ten zaprezentowano na rysunku 27.



Rys. 27. Proponowany algorytm steganograficzny z kluczem.

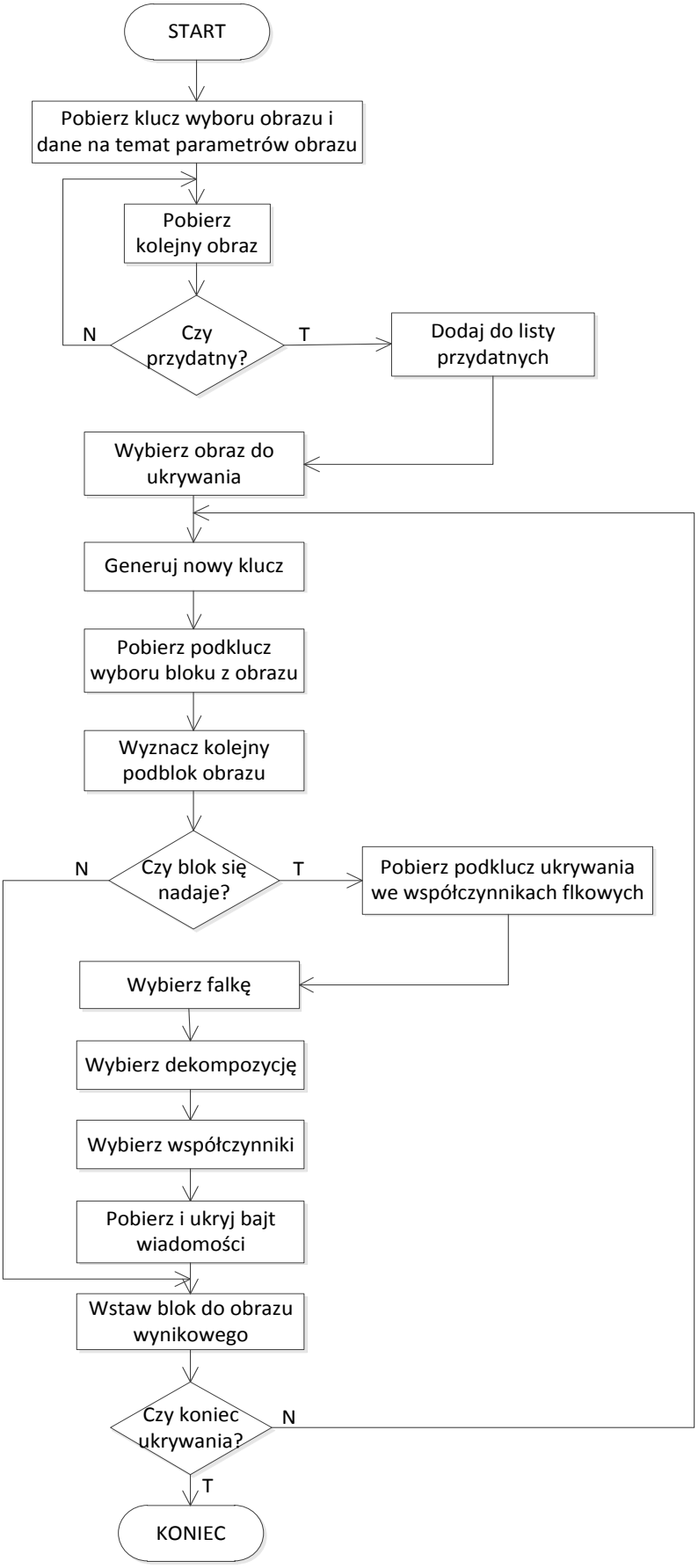
W algorytmie tym przed każdym użyciem głównego klucza, a więc przed każdym ukryciem bitu wiadomości proponuje się wyliczenie na nowo klucza. Obliczenia nowego klucza wykonuje się na podstawie obecnego klucza z częścią *SEED*, która jako ziarno nie jest nigdzie wykorzystywana w algorytmie, więc nie jest ujawniana. Poprzez taką budowę klucza uzyskuje się losowość w nowym kluczu, gdzie przy założeniu użycia bezpiecznego generatora hasła, uzyskuje się klucz niemożliwy do obliczenia na podstawie innych kroków algorytmu steganograficznego.

Wygenerowany klucz jest następnie dzielony na pięć części. Pierwsza część wyboru obrazu wykorzystywana jest tylko w pierwszym etapie działania algorytmu , czyli wyborze obrazu. Druga część wykorzystywana jest także jednokrotnie do generatora pseudolosowego wyznaczającego ścieżkę przechodzenia po przydatnych blokach obrazu. Trzecia część określa ćwiartkę, w której modyfikowane będą współczynniki. Czwarta część odpowiada za określenie wierszy i kolumn modyfikowanych współczynników, natomiast piąta część staje się nową wartością *SEED*. Diagram sekwencji dla tego algorytmu przedstawia rysunek 28



Rys. 28. Diagram sekwencyjny proponowanego algorytmu

Prezentowany algorytm jest algorytmem klucza rozproszonego, gdzie klucz działa na każdym etapie ukrywania wiadomości. Bezpieczeństwo tego algorytmu zwiększa użycie generatora pseudolosowego, który buduje graf przejść. Na rysunku 29 przedstawiono ogólny algorytm proponowanej metody.



Rys. 29. Proponowany algorytm steganograficzny z kluczem

Zgodnie z prezentowanym na rysunku 29 algorytmem, w pierwszej kolejności dokonywany jest wybór obrazu do ukrycia w nim wiadomości. Wybór dokonywany jest na podstawie fragmentu klucza, który określa jakie parametry musi spełnić obraz, aby ukryć w nim wiadomość.

Początkowo użytkownik decyduje się poprzez podanie klucza, jakie parametry obrazu muszą być spełnione, aby uzyskać dany poziom niewidoczności. Na podstawie zadanych parametrów obrazu wykonuje się zapytania do bazy danych w celu uzyskania informacji dla każdego obrazu, ile bloków w obrazie spełnia zadane parametry. Dzięki tym danym uzyskuje się informacje na temat tego, ile w danym obrazie można ukryć bitów wiadomości na danym poziomie niewidoczności. Kolejny fragment klucza określa bezpośrednio, który obraz zostanie wybrany do ukrycia w nim wiadomości. Klucz określa dokładny identyfikator obrazu.

W dalszej kolejności w wybranym obrazie wykonywane jest ukrywanie informacji. Przy wykorzystaniu funkcji czułości kontrastu określane są miejsca (bloki), w których stopień zmian w obrazie jest powyżej progu widzenia wzroku ludzkiego. Każdy taki blok klasyfikowany jest jako przydatny do ukrycia w nim wiadomości. Wszystkie pozytywne podbloki są zbierane razem w mapę pozwoleń, po której przejście odbywa się przy pomocy algorytmu pseudolosowego uzależnionym od klucza. Blok taki jest dekomponowany przy pomocy pojedynczej dekompozycji falkowej na cztery podobrazy: jeden aproksymacji i trzy detali. Dekompozycji falkowej dokonuje się z wykorzystaniem falki określonej przez fragment klucza, który podaje identyfikator falki. Ze względu na percepcję ludzkiego wzroku, wykorzystywana jest tylko barwa czerwona.

W uzyskanym obrazie dekompozycji falkowej przy pomocy fragmentu klucza wybiera się podobraz detali, w którym wykonana zostanie modyfikacja współczynników w celu ukrycia w nich danych. Podklucz jest identyfikatorem podobrazu.

Na wybranym podobrazie detali wykonywana jest modyfikacja współczynników falkowych w celu ukrycia w nich wiadomości. Ukrywanie wiadomości odbywa się poprzez zamianę najmniej znaczącego bitu współczynnika wartością ukrywanego bitu wiadomości. Wybór współczynników odbywa się przy pomocy fragmentu klucza, który określa wiersz i kolumnę w której znajduje się dany współczynnik. Zakłada się, że w jednym bloku zostanie ukryty bajt wiadomości. Po

ukryciu wiadomości blok jest przetwarzany przez odwrotną transformatę falkową i zapisywany do obrazu wynikowego.

W celu odtworzenia wiadomości, odbiorca musi posiadać bazę danych informacji na temat obrazów oraz cały klucz, które jednocześnie pozwalają na czytanie wiadomości.

5.5. Przykład działania proponowanego algorytmu

Przeprowadzono eksperyment zastosowania proponowanego algorytmu steganograficznego dla przykładowego obrazu, który przedstawiony został na rysunku 30.

Rys. 30. Przykładowy rysunek dla prowadzenia eksperymentu.

Jest to obraz mapy bitowej o 24 bitowej głębi kolorów w rozdzielczości 1024x768 pikseli. Rozmiar fizyczny wynosi 2 359 296 bajtów. Natężenie barwy czerwonej dla tego obrazu wynosi 147.

Parametry ogólne dla tego obrazu przedstawia tabela 37.

Tabela 37. Parametry ogólne badanego obrazu.

		Histogram					Macierz zdarzeń		
Parametr	**Odcieni**	**średnia**	**wariancja**	**skośność**	**kurtoza**	**energia**	**energia**	**kontrast**	**Jednor.**
Wartość	147	116,75	8354,22	91,401	1,397	0,067	0,063	0,54	0,54

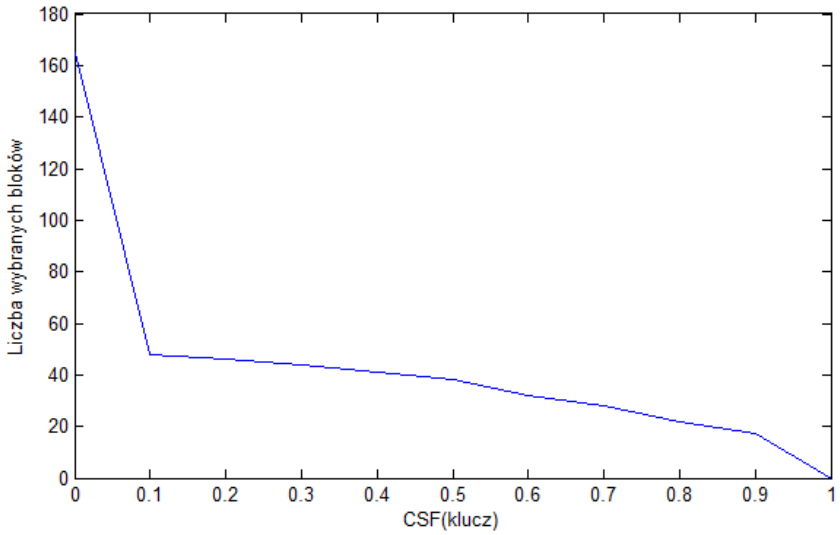
Baza danych dla tego obrazu posiada 336 rekordów. Charakteryzuje się ona średnimi wartościami przedstawionymi w tabeli 38

Tabela 38. Średnie wartości parametrów dla podbloków badanego obrazu

		Histogram					Macierz zdarzeń		
Parametr	**Odcieni**	**średnia**	**wariancja**	**skośność**	**kurtoza**	**energia**	**energia**	**kontrast**	**Jednor**
Wartość	3,49	3,57	1,22	2,26	4,76	2,21	2,28	2,288	2,288

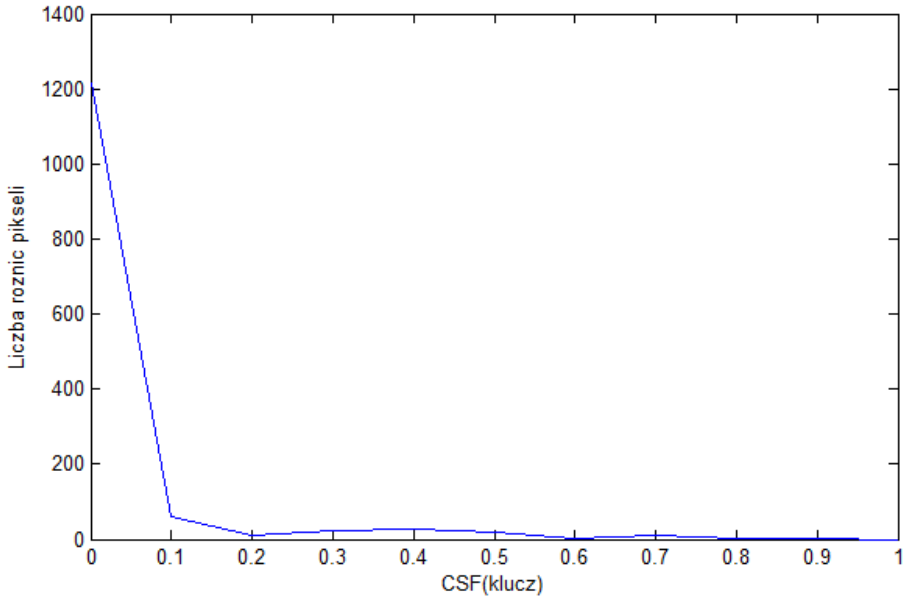
Dla tego obrazu, przy założeniu, że bajt wiadomości jest ukrywany jednokrotnie w jednym bloku obrazu uzyskano maksymalną pojemność kontenera wynoszącą 165 bajtów.

Dla testowanego obrazu istnieje 80 unikalnych reguł zapisanych w bazie danych. Dla takiego obrazu ukrywanie wiadomości dla ustalonej zmiany progu widoczności rosnącej od 0 do 1 funkcji CSF uzyskuje się możliwość ukrywania na poziomie do 165 bloków. Zależność, w jaki sposób maleje liczba klasyfikowanych pozytywnie bloków przedstawia rysunek 31.



Rys. 31. Liczba wybranych bloków zależna od progu niewidoczności

Dla progu funkcji CSF do poziomu 0,1 ukrywanych było powyżej 40 bajtów wiadomości. Wraz ze wzrostem niewidoczności (zależność CSF) można było ukrywać od 20 do 40 bajtów wiadomości. Powyżej progu, przy którym człowiek przestaje widzieć jakiekolwiek zmiany, czyli 0,6 możliwe było ukrywanie do 30 do 40 bajtów wiadomości.



Rys. 32. Liczba różnic wartości pikseli w zależności od progu niewidoczności

Na rysunku 32 przedstawiono wykres zależności pomiędzy poziomem niewidoczności, a poziomem zmian pomiędzy obrazem wynikowym, a źródłowym dla badanego obrazu.

5.6. Test efektywności proponowanego algorytmu steganograficznego

Do testów wykorzystano bazę danych obrazów UCID [90], w której umieszczono 1320 kolorowych obrazów w rozmiarze 512x384 piksele (obrazy o orientacji poziomej) lub 384x512 pikseli (obrazy o orientacji pionowej) o mocno zróżnicowanej treści. Znajdują się w niej obrazy TIFF w formie nieskompresowanej. Na obrazach tych umieszczono zarówno obiekty fotografowane na dworze jak i w pomieszczeniach, Do budowy bazy wykorzystano aparat fotograficzny Minolta Dimage 5, który pozwala na zapisywanie zdjęć w postaci nieskompresowanej [91].

Zdjęcia były wykonywane na ustawieniach automatycznych, dzięki czemu otrzymano bazę obrazów składającą się ze zdjęć jakie wykonuje przeciętny użytkownik aparatu. Ustawieniami automatycznymi objęte były takie parametry jak ekspozycja, kontrast czy balans kolorów.

Baza ta została przygotowana z myślą o [91]:

1. zapewnieniu standardowego zestawu danych do badań efektywności kompresji obrazów,
2. zapewnieniu standardowego zestawu danych dla oceny stopnia kompresji [92],
3. zapewnienia trudnego zbioru danych do oceny algorytmów wyszukiwania obrazów,
4. zapewnienia zbioru danych do oceny technik kompresji obrazów i kwantyzacji kolorów,
5. dostarczenie sprawdzonego zestawu danych dostępnych dla badań naukowych.

Przykładowe obrazy z bazy UCID pokazuje rysunek 33.

Rys. 33. Przykładowe obrazy z bazy UCID

Dla bazy UCID wyliczono średnie wartości wszystkich istotnych parametrów obrazów, które zaprezentowano w tabeli 39.

Tabela 39. Średnie miary charakterystyczne bazy UCID

Atrybut	**Obraz Oryginał**
Liczba odcieni czerwieni	85,5643
Średnia	86,9698
Wariancja	5949,47
Skośność	0,4659
Kurtoza	2,2488
Energia_hist	0,0682

Energia macierzy zdarzeń	0,06390
Kontrast	304,8777
Jednorodność	0,4220

Poziom parametrów pozostał niezmieniony w porównaniu do wcześniej przyjętego w pracy założenia co do kodowania atrybutów.

Obrazy umieszczone w bazie UCID charakteryzują się mniejszą liczbą barw czerwieni pomimo, że obrazy zostały w niej zapisane w kodowaniu 24 bitowym. Ponadto wszystkie obrazy posiadają podobne poziomy liczby odcieni barw oraz średniej histogramu kolorów dla wszystkich barw, tj czerwonej, zielonej oraz niebieskiej. Potwierdza to fakt, że obrazy te nie były wcześniej kompresowane przez co nie doszło do utraty w zróżnicowaniu barw jaka zachodzi podczas np. kompresji JPEG, gdzie najmocniej kompresowana jest barwa niebieska.

W celu zbadania możliwości ukrywania wiadomości w obrazach z pomocą proponowanego algorytmu zastosowano następującą metodę:

1. wybierane były wszystkie obrazy z bazy, przy czym obrazy robione aparatem zorientowanym pionowo były obracane dla potrzeb ukrywania, a następnie ponownie odwracane,
2. miejsca ukrycia wiadomości były wybierane poprzez użycie losowego klucza,
3. ukrywanie wiadomości w obrazach było realizowane z wykorzystaniem wybieranej falki na podstawie losowego klucza na pierwszym poziomie dekompozycji,
4. podpasmo dekompozycji falkowej, w którym ukrywano wiadomość, było wybierane w zależności od losowego klucza,
5. przeprowadzono następujące próby ukrywania:

   a) z wykorzystaniem maksymalnej pojemności obrazu, tj próbie ukrywania wiadomości we wszystkich możliwych współczynnikach falkowych obrazu,

   b) z wykorzystaniem losowego klucza określającego minimalny poziom zmian kontrastu jaki musi istnieć w podbloku obrazu, aby ukrywać w nim wiadomość, przy czym liczba wprowadzonych zmian była tak dobierana, aby zniekształcenia pozostawały niewidoczne dla ludzkiego oka.

W obrazach testowych z bazy UCID o rozdzielczości 512x384 piksele znajduje się 196 608 pikseli. W obrazach takich podczas ukrywania informacji na pierwszym poziomie dekompozycji należy pamiętać, że następuje redukcja rozmiarów subpasm do rozdzielczości 256x192 piksele. Odrzucane było podpasmo aproksymacji jako, że niesie ono największą porcję informacji na temat obrazu oryginalnego. W pozostałych podpasmach wiadomość była ukrywana na danej pozycji współczynnika tylko w jednym podpaśmie, tak aby zmiany wprowadzone w tym samym miejscu ale w innych podpasmach po dekompozycji się nie sumowały.

Stosując możliwość ukrywania wiadomości w maksymalnej liczbie miejsc, w których zmiany nie wprowadzą widocznych zniekształceń otrzymano następujące wyniki:

a) dla wyboru wszystkich możliwych miejsc ukrycia wiadomości bez względu na stosowany klucz:

- średnia liczba miejsc ukrycia wiadomości wyniosła 49 152 współczynników,
- średnia liczba zmian kontrastu wyniosła 14026,5;

b) dla zastosowania klucza określającego poziom niewidoczności w danym miejscu obrazu hosta:

- średnia liczba miejsc ukrycia wiadomości wyniosła 555 współczynników,
- średnia liczba zmian kontrastu wyniosła 2779,3.

Oznacza to, że w najlepszym przypadku ukrywanych jest około 49 KB dodatkowych informacji. W typowej realizacji algorytmu ukrywanych jest około 550 bajtów wiadomości. Zakłada się, że w jednym współczynniku ukrywany jest bajt wiadomości.

5.7. Przyspieszenie pracy działania proponowanego algorytmu

Proponowany algorytm składa się z kilku kroków, które w połączeniu z brakiem optymalizacji mogą spowolnić proces ukrywania informacji w obrazach cyfrowych.

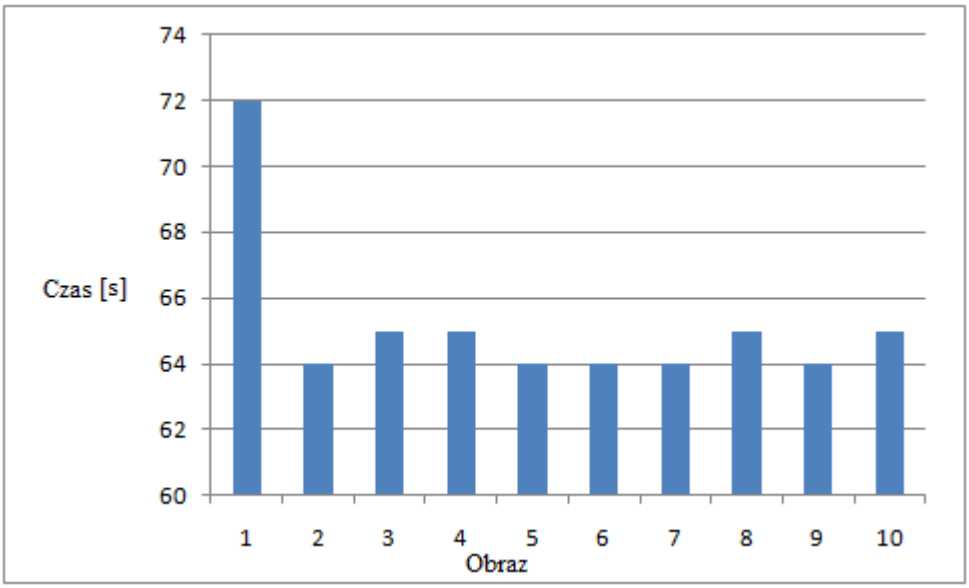
Najważniejszym elementem tego algorytmu jest zapewnienie szybkich realizacji działania algorytmów losowań i wyszukiwania pozycji oraz zastosowanej transformaty Falkowej.

Dla przyspieszenie czasu realizacji procesu ukrywania obrazu proponowanym algorytmem zaproponowano:

Wygenerowanie jednokrotne grafu przejść algorytmu steganograficznego po obrazie cyfrowym, czyli po miejscach ukrycia wiadomości. Graf ten generowany jest przed ukryciem wiadomości, zaś algorytm przechodzi po nim pobierając kolejne pozycje współczynników,

1. Do generowania użyto metody losowania z odrzucaniem, która zastąpiła stosowaną wcześniej metodę sprawdzającą za każdym razem czy losowane współrzędne były już używane. Etap ten jest przydatny w momencie, gdy zastosowany algorytm losowania zależny od klucza generuje powtarzające się wartości.
2. W celu przyspieszenia obliczeń, macierz prostokątną o rozmiarze obrazu, gdzie trzymane są kolejne koordynaty do przejścia, rozwinięto do macierzy jednowymiarowej, gdzie kolejne elementy przechowują następną współrzędną do przejścia. Ułatwia to proces wyszukiwania następnych współrzędnych.
3. W celu uproszczenia generowane są dwie macierze - jedna dla kolejnego koordynatu współrzędnej poziomej i jeden dla pionowej.

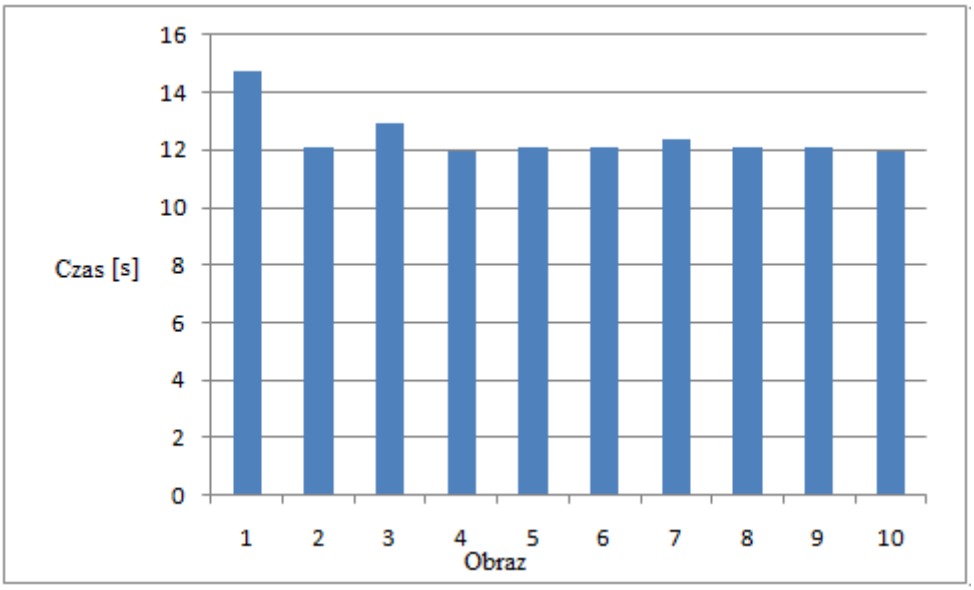
Średnie czasy realizacji algorytmu z wykorzystaniem proponowanego algorytmu steganograficznego bez optymalizacji przedstawia wykres na rysunku 34.



Rys. 34. Średnie czasy działania algorytmu bez optymalizacji [90]

Średni czas algorytmu steganograficznego, gdzie na każdym etapie ukrywania następuje wyszukanie następnych współrzędnych do ukrycia wiadomości wynosi około 65 sekund.

Czas realizacji dla 10 obrazów algorytmu ukrywania po optymalizacji przedstawia wykres na rysunku 35.

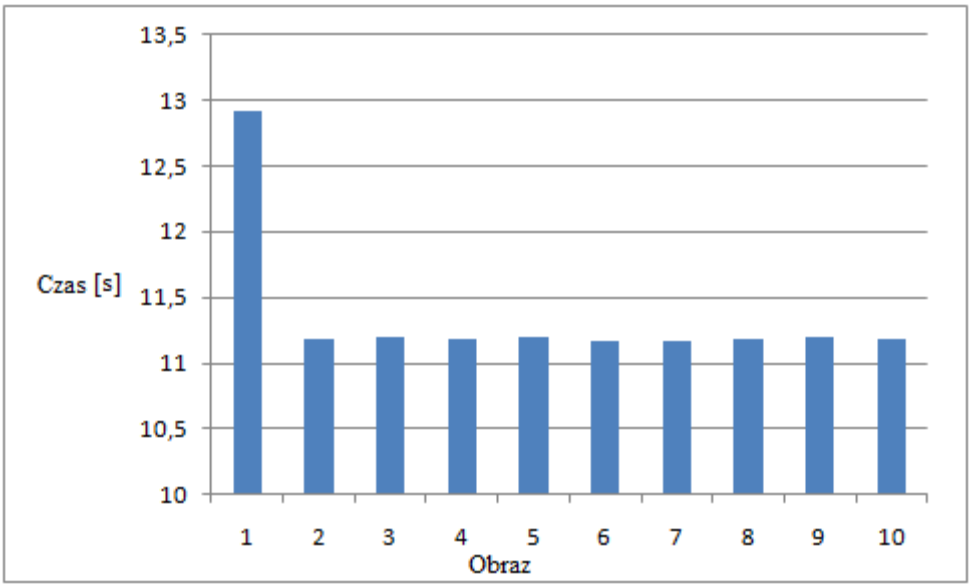


Rys. 35. Czasy ukrywania wiadomości proponowanym algorytmem po optymalizacji

Średni czas realizowania procesu ukrywania dla bazy UCID wynosi około 12,1 sekundy. Zaobserwowana anomalia dla pierwszych obliczeń we wszystkich wykresach wiąże się z początkowym przydzielaniem pamięci dla wszystkich macierzy pośrednich

zastosowanych w procesie ukrywania. W celu przyspieszenia warto zastosować tablice statyczne o dostosowanych do obrazu rozmiarach.

Sam proces wyszukiwania zajmuje największą część czasu, co pokazuje wykres na rysunku 36.



Rys.36. Czasy wyszukiwania miejsc ukrycia wiadomości

Średni czas samej operacji wyszukiwania wyniósł 11,3 sekundy, a zatem wyliczając różnicę pomiędzy obydwoma rezultatami można zauważyć, że sam proces ukrywania trwa średnio 0,6 sekundy. Przy czym jest to czas ukrywania z wykorzystaniem kompletnego algorytmu steganograficznego, dla którego wybór obszarów ukrycia wiadomości, wybór falki oraz podpasma dekompozycji Falkowej jest zależny losowo od zastosowanego klucza steganograficznego. W tym przypadku prędkość algorytmu ukrywania wiadomości bez wyszukiwania pozycji jest już optymalna.

Wnioskując, należy w trakcie realizacji tego algorytmu zadbać o dobór szybkich metod wyszukiwania i przechodzenia po grafach.

Dla prezentowanego w rozdziale 2 serwisu Hotfix.pl przedstawiono w tabeli 40, średnie czasy wyrażone w sekundach, sprawdzania wiadomości przy założeniu, że atakujący zna klucze.

Tabela 40. Średnie czasy wyszukiwania wiadomości dla przykładowego serwisu WWW.

Typ obrazu	**Liczba**	**Bez wyszukiwania [s]**	**Z wyszukiwaniem optymalnym [s]**	**Bez optymalizacji [s]**
JPG	16815	10089	203461,5	1092975
PNG	53249	31949,4	644312,9	3461185
Łącznie	70064	42038,4	847774,4	4554160

W przypadku gdyby atakujący znał klucz i chciał sprawdzać wszystkie obrazy oraz udałoby mu się sprowadzić proces wyszukiwania do czasu zerowego, mógłby on poszukiwać wiadomości w czasie około 11,6 godziny wykorzystując do tego komputer domowy z procesorem Intel Core2Duo E8200.

W momencie zastosowania przedstawionego wyszukiwania optymalnego, chcąc zbadać kolejno wszystkie wiadomości potrzebowałby już 235,4 godziny. Przy założeniu, że w jednym obrazie każdego dnia wysyłana byłaby jedna wiadomość, proces ten stałby się niemożliwy do zrealizowania przy użyciu domowego komputera. Bez optymalizacji, atakujący poszukiwałby wiadomości w czasie 1265 godzin. Dane te byłyby realne przy założeniu, że na witrynie internetowej znajdowałyby się obrazy o rozmiarze takim samym jaki te, które posiadają obrazy w bazie UCID. Dla większych obrazów złożoność ta rośnie.

5.8. Porównanie proponowanego algorytmu z innymi algorytmami steganograficznymi

Do badań porównawczych skuteczności proponowanego algorytmy wybrano dostępne następujące programy: Invisible Secret, Silent Eye, Stegomagic, OpenPuff, QuickStego, S-Tools, Steganography Studio oraz Virtual Steganographic Laboratory for Digital Images.

Invisible Secret to oprogramowanie zdolne do ukrywania danych algorytmem steganograficznym oraz przesłania dalej kontenera z ukrytymi danymi. Dane przed ukryciem można w nim dodatkowo zaszyfrować przy użyciu algorytmu blokowego AES z użyciem hasła. Program ten oferuje także pomoc przy tworzeniu silnego hasła. W najnowszej wersji oferowane są także narzędzia czyszczenia informacji na temat

działalności w Internecie, jak czyszczenie pamięci cache czy cookie przeglądarki. Jako kontener dla danych ukrywanych algorytmem steganograficznym zastosować można pliki JPEG, PNG, BMP, a także muzyczne WAV i stron HTML. Wiadomość ukrywana jest w dziedzinie przestrzennej z wykorzystaniem hasła metodą LSB. Sam program pozwala sprawdzić pojemność informacji nośnej zanim zostanie ukryta wiadomość oraz porównywać wiadomości bit po bicie w celu sprawdzenia czy pliki się różnią. Do badań porównawczych wykorzystano wersję 2.1 tej aplikacji.

Kolejną wykorzystaną w badaniach aplikacją jest Silent Eye. Rozpowszechniana na licencji GNU GPL v3 aplikacja oferuje ukrywanie informacji z wykorzystaniem algorytmu steganograficznego w plikach JPEG, BMP oraz Wave. Dane mogą być dodatkowo szyfrowane algorytmem AES128 lub AES 256 i kompresowane. Wszystkie dane są ukrywane przy pomocy algorytmu LSB. Ukrywanie odbywa się z możliwością wyboru dowolnej liczby barw z przestrzeni RGB oraz wykorzystaniu od 1 do 6 najmniej znaczących bitów dla każdej z barw.

Trzecim programem był Stegomagic pozwalający na ukrywanie wiadomości tekstowej lub pliku w trzech rodzajach wiadomości nośnych. Jako nośnik wykorzystuje się pliki tekstowe, WAV, BMP 256 kolorów lub BMP 24 bit. Ukrywanie nie zwiększa wielkości pliku, wykorzystywane są tylko barwy obrazu za wyjątkiem, gdy wiadomość zostanie ukryta w innym pliku tekstowym. Do szyfrowania używa się algorytmu DES. Do ukrywania wykorzystuje się metodę LSB z losowym mieszaniem bitów. Losowość sprawdzana jest zgodnie z testem częstotliwości (equidistribution test).

Czwartym programem jest OpenPuff. Jest to oprogramowanie ukrywające dane w kolejnych informacjach nośnych. Tylko właściwie podana kolejność nośników ma gwarantować poprawne odczytanie ukrytej wiadomości. Dane przed ukryciem są szyfrowane, mieszane, wybielane oraz kodowane. Wykorzystywane są podwójne klucze 256 bit w algorytmach takich jak AES, Anubis, Cast-256, FROG, Idea-NXT, MARS, RC6, Safer+ czy Twofish. Po zaszyfrowaniu, wiadomość jest mieszana aby usunąć wszelkie wzorce. Wykorzystywany jest generator liczb pseudolosowych CSPRNG z wykorzystaniem trzeciego klucza o długości 256 bit. Następnie następuje wybielanie z wykorzystaniem szumu generowanego przez CSPRNG i kodowane funkcją nieliniową. Obsługiwane wiadomości nośne: pliki graficzne (BMP, JPG, PCX, PNG, TGA), audio (AIFF, MP3, NEXT/SUN, WAV), wideo (3GP, MP4, MPG, VOB) oraz Adobe Flash (FLV, SWF, PDF).

Kolejnym programem wykorzystanym jest QuickStego. Autorzy programu nie wyjaśniają jakim algorytmem ukrywają wiadomość. Wiadomość tekstowa ukrywana jest w plikach graficznych BMP.

S-Tools jest oprogramowaniem przygotowanym do ukrywania wiadomości w plikach graficznych BMP oraz GIF. Z jego wykorzystaniem ukrywane są wiadomości zapisane jako tekst oraz inne pliki graficzne. Ukrywanie wiadomości odbywa się z wykorzystaniem algorytmu LSB.

Steganography Studio oferuje ukrywanie wiadomości w plikach JPG, BMP oraz PNG z wykorzystaniem różnych algorytmów ukrywania. Algorytmami tymi są BattleSteg, BlindHide, DynamicBattleSteg, DynamicFilterFirst, FilterFirst, HideSeek oraz SLSB. Ponieważ program ten umożliwia także prowadzenie analiz steganoanalizy, a zatem wykorzystano go do przeprowadzenia badań nad bezpieczeństwem proponowanego w pracy algorytmu oraz przedstawionych wyżej programów.

Narzędzia steganoalityczne zawarte w programie Steganography Studio pozwalają na porównywanie kontenera wiadomości z obrazem wynikowym, w którym ukryta została wiadomość. Wyliczanymi parametrami są średnia różnica bezwzględna, błąd średniokwadratowy, Norma LP, Laplasjanowy błąd średniokwadratowy, SNR (Signal to Noise Ratio), PSNR (Peak Signal to Noise Ratio), znormalizowana korelacja wzajemna, jakość korelacji.

Virtual Steganographic Laboratory for Digital Images (VSL) jest to program przeznaczony do prowadzenia laboratoriów ze steganografii napisany w języku Java. Oprócz szeregu algorytmów ukrywających informacje, implementuje także narzędzia do prowadzenia steganoanalizy. Programem tym ukrywano wiadomość algorytmem F5.

Zestawienie wyliczonych miar statystycznych dla przykładowego obrazu z bazy UCID przedstawionego na rysunku 37 prezentuje tabela 28. Obraz ten stanowi kontener dla ukrywanej wiadomości.

Rys. 37. Przykładowy obraz z bazy UCID

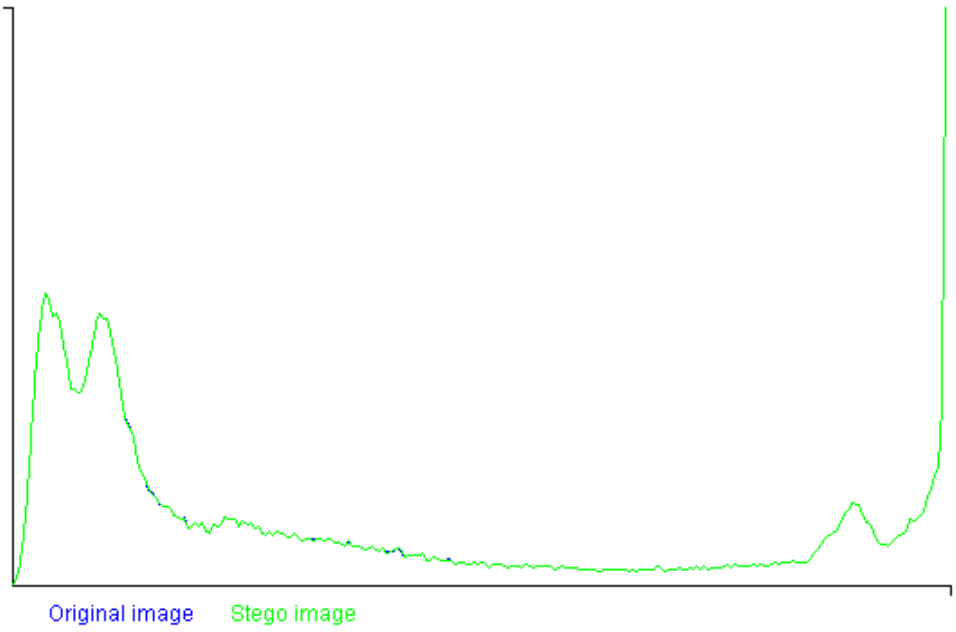
Tabela 41. Miary statystyczne wyliczane dla przykładowego obrazu

Program	**Średnia różnica bezwzględna**	**Błąd średniokwadratowy**	**Lp Norma**	**Laplasjanowy błąd średniokwadratowy**	**SNR**	**PSNR**	**Znormalizowana korelacja wzajemna**	**Jakość korelacji**
Invisible Secret	1,5777	3,2783	1,6391	5,4219E-4	46014	178512	0,99685	178,4244
SilentEye – 6 bit	0,08059	2,636	1,3180	0,00166	57227	222011	0,9998	178,95
SilentEye – 5 bit	0,0457	0,7268	0,3634	4,5863E-4	207532	805121	0,9999	178,979
SilentEye – 4 bit	0,030	0,249	0,1246	1,6230E-5	604880	2346629	0,9999	178,978
SilentEye – 3 bit	0,019	0,0764	0,0382	5,1305E-4	1971974	7650260	0,9999	178,983
SilentEye – 2 bit	0,0135	0,0261	0,01307	1,8149E-5	5766770	2,2372E-7	0,9999	178,9851
SilentEye – 1 bit	0,01084	0,0108	0,0054	7,791E-6	1,3911E7	5,3958E7	0,9999	178,9859
Stegomagic	0,01038	0,01044	0,00522	7,517E-6	1,4446	5,6044E7	0,9999	178,9864
OpenPuff 1/2	0,3459	0,39157	0,19578	2,5290E-4	385245	1494556	0,9999	178,9851
OpenPuff 1/3	0,34548	0,39127	0,19563	2,5271E-4	385540	1495702	0,9999	178,9861

OpenPuff 1/4	0,34559	0,39088	0,19544	2,5341E-4	385917	1497162	0,9999	178,9861
OpenPuff 1/5	0,3454	0,39157	0,19578	2,5249E-4	385245	1494556	0,9999	178,9857
OpenPuff 1/6	0,3448	0,3904	0,1952	2,526E-4	386369	1498917	0,9999	178,9859
OpenPuff 1/7	0,3451	0,3903	0,19515	2,5359E-4	386495	1499405	0,9999	178,985
OpenPuff 1/8	0,3447	0,38966	0,19483	2,5164E-4	387126	1501852	0,9999	178,9863
QuickStego	0,0109	0,0202	0,01013	6,0978E-6	7552534	2,8873E7	0,9999	178,9846
TheThirdEye	0,01102	0,01102	0,005109	7,7791E-6	1,3686E7	5,3096E7	0,9999	178,9841
S-Tools4	0,01206	0,01218	0,00609	8,7867E-6	1,2383E7	4,8041E7	0,99999	178,9862
Steganography Studio BattleSteg	0,00924	0,01088	0,00544	6,8449E-6	1,3852E7	5,3741E7	0,9999	178,9858
Steganography Studio BlindHide	0,01043	0,02252	0,01126	5,7958E-6	6696432	2,5978E7	0,9999	178,9821
Steganography Studio DynamicBattleSteg	0,0094	0,0109	0,00545	6,9965E-6	1,3833E7	5,3666E7	0,9999	178,9857
Steganography Studio Dynamic FilterFirst	0,0094	0,01899	0,00949	9,1696E-6	7942822	3,0814E7	0,9999	178,9854
Steganography Studio FilterFirst	0,00961	0,01961	0,00980	9,2315E-6	7689525	2,9831E7	0,9999	178,9854
Steganography Studio HideSeek	0,0094	0,0095	0,00475	6,8698E-6	1,5868E7	6,1562E7	0,9999	178,9858
Steganography Studio SLSB	0,00938	0,00941	0,00470	7,2664E-6	1,6022E7	6,2160E7	0,9999	178,9849
VSL (F5)	5,4824	65,1722	32,5861	0,006084	2214	8979,67	0,9996	178,9214
Proponowany algorytm	**0,01132**	**0,10438**	**0,05219**	**1,4142E-4**	**1445236**	**5606661**	**0,9999**	**178,985**

Prezentowane wyniki w układzie tabelarycznym w tabeli 41 dają podstawy do stwierdzenia, że proponowany algorytm wykazuje lepsze właściwości statystyczne od większości badanych algorytmów. Zgodnie z wartościami uzyskiwanymi dla miary średniej różnicy bezwzględnej algorytm ten zachowuje lepszą właściwość statystyczną od algorytmów bazujących na przekształceniach przestrzennych (algorytmy najmniej znaczących bitów) oraz algorytmu opartego o transformatę kosinusową, jakim jest algorytm F5. Gorsze wartości uzyskiwane są jednak w stosunku do algorytmów wbudowanych w program Steganography Studio. Dla Laplasjanowego błędu średniokwadratowego proponowany algorytm przyjmuje podobną zależność w stosunku do porównywanych programów. Większe wartości tego współczynnika oznaczają gorszą jakość obrazu. Proponowany algorytm zachowuje własności lepsze od algorytmu F5 i algorytmów działających w dziedzinie przestrzeni. Gorsze wyniki dla prezentowanego algorytmu uzyskuje się dla parametrów SNR oraz PSNR. Jeśli chodzi o parametry korelacji pozostają one podobne dla wszystkich algorytmów.

Gorsze wyniki dla współczynników SNR i PSNR są związane z ukrywaniem całych bajtów wiadomości we współczynnikach DWT danego bloku. Dodatkowo większość z programów używało przez ukrywaniem funkcji wybielających oraz kompresji, które znacząco wpływały na wyniki wyliczanych miar statystycznych. Niemniej histogram dla przykładowego obrazu z ukrytą wiadomością pozostaje niezmieniony w stosunku do nośnika wiadomości. Przedstawia to rysunek 38.



Rys. 38. Nałożone histogramy obrazu źródłowego i wynikowego

Na rysunku tym, obydwa histogramy dla barwy czerwonej pokrywają się, a zatem liczba odcieni pozostała praktycznie niezmieniona i kolorystyka pozostaje taka sama.

Wykazano, że proponowany algorytm steganograficzny zachowuje dobre właściwości statystyczne, zaś podejście do badania widoczności zniekształceń pozwala na sterowanie poziomem zniekształceń w obrazie wynikowym.

6. Podsumowanie

W pracy zostało przedstawionych wiele aspektów związanych z budowaniem algorytmu steganograficznego z kluczem. W rozdziale 2 przeprowadzono analizę ruchu w Internecie pod kątem wykorzystania jego jako medium transmisji cyfrowych obrazów graficznych z ukrytą w sposób steganograficzny wiadomością. Autor przedstawił dane statystyczne dotyczące liczby użytkowników na świecie, ilości stron internetowych jaka zarejestrowana jest w Internecie oraz liczby użytkowników Internetu w Polsce. Następnie wykonano analizę możliwości wykorzystania serwisów internetowych w celach steganograficznych. Przedstawiono propozycje wykorzystania dwóch rodzajów serwisów, w których można umieszczać obrazy z ukrytą w nich wiadomością. Pierwszym typem serwisów były tzw hostingi plików graficznych, natomiast drugim tradycyjny portal, w tym wypadku komputerowy. Przedstawiono także informacje na temat przeciętnej liczby występowania obrazów użytecznych do ukrywania wiadomości, spośród wszystkich obrazów graficznych jakie są przesyłane do użytkowników na prezentowanym portalu. Ilość danych jaka jest w nich przesyłana, świadczy o tym, że gdyby umieścić w nich obraz cyfrowy z ukrytą wiadomością w określonym przedziale czasowym, po czym usunąć go i zastąpić obrazem bez wiadomości (pod warunkiem, że odbiorca zdążyłby przechwycić właściwy obraz z wiadomością), to potencjalny agresor nie byłby w stanie przy użyciu zwykłego przeglądania tych obrazów wykryć faktu ukrycia wiadomości. W rozdziale tym przedstawiono czasy wykonywania wykrywania wiadomości z użyciem funkcji czułości kontrastu CSF.

W rozdziale 3 przedstawiono analizę systemów ochrony informacji. Omówiono zagadnienie teoretyczne związane z użytkowaniem kluczy w systemach ochrony informacji wraz z odpowiednimi definicjami pojęć. Przedstawiono wykorzystanie kluczy steganograficznych w podstawowych metodach ukrywania informacji, w tym metodach ukrywania danych w dziedzinie przestrzennej oraz transformaty DWT.

W rozdziale 4 autor przedstawił propozycję metody analizowania niewidoczności zmian jakie powoduje ukrywanie wiadomości metodami steganograficznymi. Zaproponowana metoda wykorzystuje funkcję czułości kontrastu CSF Mannosa i Sakrisona, która odpowiada sposobowi postrzegania obrazów przez

system ludzkiego wzroku. W tym rozdziale, aby uniezależnić się od wybranych metod steganograficznych autor zaproponował użycie szumu jako modelu symulacji faktu ukrycia wiadomości. Przedstawiona metoda wyznaczania niewidoczności zmian polega na określeniu liczby zmian kontrastu w kącie patrzenia na obraz i odniesieniu tej liczby na funkcję poczucia kontrastu. Liczba ta pozwala wnioskować na temat widoczności lub niewidoczności tych zmian dla systemu ludzkiego oka.

W rozdziale 4 zaproponowany został przez autora zbiór miar charakteryzujący obrazy cyfrowe pozwalający budować reguły dla zaprezentowanego w kolejnym rozdziale algorytmu steganograficznego pod kątem zabezpieczenia odpowiedniego poziomu niewidoczności ukrycia wiadomości. Zaprezentowano miary liczone na podstawie histogramu kolorów jak i znormalizowanej macierzy zdarzeń określającej relacje pomiędzy poszczególnymi parami par pikseli. Dla zaproponowanych do użycia miar charakteryzujących obrazy cyfrowe wykonano analizę istotności pod kątem określania widoczności zmian w poszczególnych obszarach obrazów. W analizie tej wykorzystano teorię zbiorów przybliżonych z miękką redukcją atrybutów warunkowych opartą o względne prawdopodobieństwo reguł użytecznych. Zaproponowano odpowiednie kodowanie atrybutów warunkowych i decyzyjnych w oparciu o równy podział próbek w przedziałach.

Rozdział 4 zawiera też wykonaną analizę możliwości przeniesienia wszystkich obliczeń do jednej dziedziny, w tym przypadku do dziedziny transformaty falkowej DWT, zastosowanej w dalszej kolejności w zaproponowanym w rozdziale numer 5 algorytmie steganograficznym. Omówiono sposób reprezentacji falkowej obrazów oraz przedstawiono możliwość przejścia znormalizowanej funkcji czułości kontrastu oraz proponowanych miar charakterystycznych obrazu z dziedziny przestrzennej do dziedziny transformaty. Dla celów ujednolicenia obliczeń zaproponowano także przeniesienie różnych funkcji falkowych do jednej reprezentacji Pollena.

W rozdziale 5 przedstawiono propozycję algorytmu steganograficznego z kluczem wykorzystującym do oceny przydatności bloków do ukrycia wiadomości w sposób niewidoczny dla ludzkiego oka, znormalizowaną funkcję czułości kontrastu oraz charakterystyczne miary obrazu w celu wyboru obrazów z bazy, w których możliwe jest ukrywanie określonych porcji danych. Przedstawiona propozycja algorytmu steganograficznego wykorzystuje do ukrywania wiadomości transformatę falkową DWT oraz zmianę wartości jej współczynników w zależności od zastosowanego klucza. Algorytm ten jest algorytmem steganograficznym klucza rozproszonego, gdzie klucz

działa we wszystkich etapach ukrywania wiadomości, od wyboru obrazu, po wybór miejsc ukrycia wiadomości i samo ukrywanie. W rozdziale tym przedstawiono analizę efektywności i bezpieczeństwa proponowanego algorytmu steganograficznego.

Wyniki przeprowadzonych badań w pełni udowodniły przyjętą tezę, że „**Zastosowanie metody kształtowania kluczy i połączenie jej z metodą steganograficzną opartą o badanie niewidoczności zmian w obrazach poprawia bezpieczeństwo ukrywanej informacji przed wykryciem**”.

6.1. Wnioski końcowe

Wyniki badań objętych tematyką prezentowanej rozprawy doktorskiej pozwoliły na sformułowanie następujących wniosków końcowych:

- udowodniono, że cyfrowe środowisko graficzne jest dobrym medium do ukrywania w nim dodatkowych porcji danych,
- opracowano metodę oceny niewidoczności zmian powodowanych działaniem algorytmów steganograficznych na kolorowych obrazach cyfrowych,
- opracowano metody doboru obrazów z bazy na podstawie charakterystycznych parametrów obrazu,
- opracowano metody wyboru miejsc ukrywania wiadomości,
- opracowano metodę kształtowania kluczy steganograficznych i wbudowanie jej w algorytm steganograficzny w celu zwiększenia bezpieczeństwa dla ukrywanej wiadomości.

W pracy opracowano nowy, oryginalny algorytm steganograficzny z kluczem rozproszonym, który to w przeciwieństwie do innych kluczy w obecnie stosowanych metodach steganograficznych, jest wykorzystywany w każdym etapie działania algorytmu. W połączeniu z zaproponowaną metodą oceny zniekształceń wprowadzanych w obrazach wynikowych oraz z metodą wyboru miejsc ukrywania informacji w tych obrazach, z dodatkowym wykorzystaniem miar charakterystycznych dla nich, zbudowano wydajny i bezpieczny algorytm steganograficzny porównywalny i w wielu przypadkach lepszy od powszechnie używanych algorytmów. Algorytm ten, w przeciwieństwie do wielu innych wykorzystuje złożony klucz steganograficzny zwiększający bezpieczeństwo ukrywanych danych. Dodatkowo, zaproponowana metodyka badań niewidoczności oraz budowy algorytmu posiadają charakter ogólny i mogą być zastosowane w budowie innych algorytmów steganograficznych.

6.2. Dalsze badania

W trakcie realizacji pracy natknięto się na wiele problemów w budowaniu pełnego modelu niewidoczności dla ukrywanej wiadomości. W przyszłości proponowaną metodę należałoby poszerzyć o kolejne sposoby określania niewidoczności i powiązać je z kluczem.

Kolejnym aspektem do rozwiązania jest rozbudowa proponowanego algorytmu o zaawansowane mechanizmy wzmacniające bezpieczeństwo wiadomości przed usunięciem.

W przyszłości warto proponowaną metodą rozbudować o mechanizm wyboru algorytmów wikłania bitów wiadomości w zależności od klucza.

Literatura

(publikacje własne zostały wyróżnione pogrubioną czcionką)

1. Indradip Banerjee, Souvik Bhattacharyya and Gautam Sanyal, An Approach of Quantum Steganography through Special SSCE Code, International Journal of Computer and Information Engineering, Volume 4, Issue 4, s.233-240, 2010
2. Saraju P. Mohanty, Digital Watermarking: A Tutorial Review, Department of Computer Science and Engineering, University of South Florida, http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/WMSurvey1999Mohanty.pdf (dostęp online: 2012)
3. M. F. Tolba, M. A. Ghonemy, I. A. Taha, A. S. Khalifa, Using Integer Wavelet Transforms In Colored Image-Steganography, IJICIS Vol. 4 No. 2, July 2004
4. M. Umamaheswari, S. Sivasubramanian, S. Pandiarajan, Analysis of Different Steganographic Algorithms for Secured Data Hiding, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010
5. http://news.netcraft.com/archives/2010/11/05/november-2010-web-server-survey.html
6. http://www.newwebsitebuilders.net/Astounding%20Internet%20World%20Stats%20and%20Online%20Growth%20Exposure.pdf
7. http://www.stat.gov.pl/cps/rde/xbcr/gus/rs_rocznik_statystyczny_rp_2011.pdf
8. http://www.stat.gov.pl/cps/rde/xbcr/gus/oz_maly_rocznik_statystyczny_2012.pdf
9. Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, Farnam Jahanian, Internet Inter-Domain Traffic, SIGCOMM'10, 2010
10. http://imgur.com/stats/
11. http://www.google.com/intl/pl_ALL/analytics/#utm_source=pl-ha-pl-google_brand_gen_analytics&utm_medium=ha&utm_campaign=pl&utm_term=google%20analytics
12. http://www.nedworks.org/~mark/reqstats//trafficstats-daily.png
13. http://support.cs.umu.se/stats/web/support.html
14. http://216.116.32.101/stats/files.htm
15. **Jerzy Korostil, Łukasz Nozdrzykowski, Impact analysis of the wavelet order on the visibility of the image, Pomiary, Automatyka, Kontrola, 12/2010**
16. Shuo-Zhong WANG, Xin-Peng ZHANG, Kai-Wen ZHANG, Steganographic Technique Capable of Withstanding RQP Analysis, Journal of Shanghai University (English Edition), No. 6(4), s. 273-277, 2002
17. V. Ahuja, Bezpieczeństwo w sieciach, Wydawnictwo Mikom, Warszawa 1997
18. R. Wobst, Kryptologia. Budowa i łamanie zabezpieczeń, Wydawnictwo RM, Warszawa 2002
19. Tomasz Bilski, Tadeusz Pankowski, Janusz Stokłosa, Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo PWN, 2001

20. A. Białecki, Wprowadzenie do technologii podwyższających bezpieczeństwo korzystania z sieci teleinformatycznych, I Krajowa Konferencja Zastosowań Kryptografii, Enigma 1997
21. A. Białecki, Biometryka i kryptografia – razem czy osobno? VII Krajowa Konferencja Zastosowań Kryptografii, Enigma 2003
22. M. Maćkowiak, Zastosowanie DNA w ochronie danych, VIII Krajowa Konferencja Zastosowań Kryptografii, Enigma 2004
23. Harshvardhan Tiwari, Krishna Asawa, Cryptographic Hash Function: An Elevated View, European Journal of Scientific Research, Vol.43 No.4, pp.452-465, 2010
24. Claude Shannon, Communication theory of secrecy systems, Bell Systems Technical Journal 28, 656 – 715, 1949
25. A. Zugaj, Zarządzanie kluczami w bankowości, I Krajowa Konferencja Zastosowań Kryptografii, Enigma 1997
26. Alfred J. Menzes, Paul C. von Oorschot, Scott A. Vanstone, Kryptografia Stosowana, Wydawnictwo WNT, Warszawa 2005
27. A. Zugaj, Zarządzanie kluczami w bankowości, I Krajowa Konferencja Zastosowań Kryptografii, Enigma 1997
28. Christof Paar, Jan Pelzl, Bart Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, Springer 2010
29. B. Schneier, Kryptografia dla praktyków, Wydawnictwo WNT, Warszawa 1995
30. S. Even and O. Goldreich, On the power of cascade ciphers, ACM Transactions on Computer Systems, vol. 3, s. 108–116, 1985
31. Matt J. B. Robshaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995
32. A. Paszkiewicz, Projektowanie szyfrów strumieniowych, IV Krajowa Konferencja Zastosowań Kryptografii, Enigma 2000
33. A. Paszkiewicz, Estetyczne aspekty generowania liczb pseudolosowych, VII Krajowa Konferencja Zastosowań Kryptografii, Enigma 2003
34. IEEE 1363: Standard Specifications for Public-Key Cryptography, dostęp online: http://grouper.ieee.org/groups/1363/
35. J. Katz, Y. Lindell, Introduction to Modern Cryptography, CRC Press 2007
36. A. Orłowski, Faktoryzacja dużych liczb przy użyciu komputerów kwantowych – algorytm Shora, III Krajowa Konferencja Zastosowań Kryptografii, Enigma 1999
37. Peter W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing archive, Volume 26 Issue 5, s. 1484-1509, 1997
38. Ł. Nozdrzykowski, Wbudowywanie wiadomości metodami steganograficznymi w środowisku graficznym na podstawie wykorzystania specjalnych parametrów obrazu, Praca magisterska, Politechnika Szczecińska, Wydział Informatyki, Szczecin 2006
39. Jonathan Watkins, Steganography - Messages Hidden in Bits, 2nd Annual CM316 Conference on Multimedia Systems, based at Southampton University, UK, 2002. dostęp online: http://mms.ecs.soton.ac.uk/mms2002/papers/6.pdf

40. Enrique Cauich, Roberto Gómez Cárdenas, Ryouske Watanabe, Data hiding in identification and offset IP fields, ISSADS'05 Proceedings of the 5th international conference on Advanced Distributed Systems, Pages 118-125, Springer-Verlag Berlin 2005
41. Jessica Fridrich, Miroslav Goljan, Dorin Hogea, David Soukal, Quantitative steganalysis of digital images: estimating the secret message length, Multimedia Systems 9: 288–302, Springer-Verlag, 2003
42. Dariusz Bogumił, Cyfrowe znaki wodne odporne na kompresję JPEG, Politechnika Warszawska, Instytut Informatyki, wrzesień 2001, dostęp online: www.ii.pw.edu.pl/~dbogumil/msc_thesis.pdf
43. H. S. Majunatha Reddy, K. B. Raja, High Capacity And Security Steganography Using Discrete Wavelet Transform, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6), s. 462-472, 2010
44. Johnnie Thomas, Digital steganography, dostęp online: www.seas.upenn.edu/~cse400/CSE400_2004_2005/04writeup.pdf
45. Ross Anderson, Stretching the Limits of Steganography, Proceedings of the First International Workshop on Information Hiding, s. 39-48, Springer-Verlag, 1996
46. Luis von Ahm, N. J. Hopper, Public-Key Steganography, Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques Interlaken, Switzerland, May 2-6, 2004, Proceedings, s.323-341, Springer, 2004
47. W. Diffie, M. Hellman, New Direction in Cryptography, IEEE Transactions on Informations Theory, vol. IT-22, No 6, 1976
48. Abdelkader H. Ouda, Mahmoud R. El-Sakka, A Step Towards Practical Steganography Systems, ICIAR 2005, LNCS 3656, s. 1158–1166, Springer-Verlag Berlin Heidelberg 2005
49. Andrew D. Ker, Resampling and the Detection of LSB Matching in Colour Bitmaps. Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose, California, USA, 17-20 January 2005, s. 1-15, SPIE 2005
50. Rastislav Hovančák, Peter Foriš, Dušan Levický, Steganography Based on DWT Transform, 16th International Conference Radioelektronika 2006, dostęp online: www.urel.feec.vutbr.cz/ra2007/archive/ra2006/abstracts/038.pdf
51. Harsh Vikram Singh, Digital Image Watermarking Algorithm Based on DCT and Spread Spectrum, Proc. Of International Conference on Advance Computing, Communication and Networks'11 (ICAdCN), s. 1124-1129, UACEE, 2011
52. I. Pitas, Digital Image Processing Algorithms and Applications, John Wiley & Sons, 2000
53. Lisa M. Marvel, Charles G. Boncelet, Jr., Charles T. Retter, Spread Spectrum Image Steganography, IEEE Transactions On Image Processing, Vol. 8, No. 8, August 1999
54. A. S. Abbass, E. A. Soleit, S. A. Ghoniemy, Blind Video Data Hiding Using Integer Wavelet Transforms, UBICC Journal - Volume 2 NO. 1, s. 11-25, 2008

55. Bo Yang and Beixing Deng. Steganography In Gray Images Using Wavelet, In Proceedings of the second International Symposium on Communication, Control and Signal Processing (ISCCSP), 2006, dostęp online: http://www.eurasip.org/Proceedings/Ext/ISCCSP2006/defevent/papers/cr1012.pdf
56. Siddharth Singh, Tanveer J. Siddiqui, A Security Enhanced Robust Steganography Algorithm for Data Hiding, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, 2012
57. Mohamed I. Mahmoud, Moawad I. M. Dessouky, Salah Deyab, and Fatma H. Elfouly, Wavelet Data Hiding using Achterbahn-128 on FPGA Technology, UbiCC Journal - Special Issue of IKE'07 Conference, IKE'07, 2008
58. Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering, 2006. 4, 3: 275-290
59. Dr. Jane J. Stephan, Image Watermarking Using Wavelet Transform, dostęp online: http://www.uop.edu.jo/download/research/members/CSIT2006/vol1%20pdf/pg157.pdf
60. Rastislav Hovančák, Peter Foriš, Dušan Levický, Steganography Based On Dwt Transform, dostęp online: http://www.urel.feec.vutbr.cz/ra2008/archive/ra2006/abstracts/038.pdf
61. Michiharu Niimi, Eiji Kawaguchi Jeremiah Spaulding, Hideki Noda Mahdad N. Shirazi, BPCS Steganography Using EZW Encoded Images, DICTA2002: Digital Image Computing Techniques and Applications, 21—22 January 2002, Melbourne, Australia, dostęp online: http://www.aprs.org.au/dicta2002/dicta2002_proceedings/Spaulding157.pdf
62. Łukasz Nozdrzykowski, Analiza istotności miar obrazu wpływających na zmniejszenie zniekształceń spowodowanych steganograficznym ukrywaniem wiadomości w obrazach w oparciu o funkcję CSF, Metody Informatyki Stosowanej, 3/2009 (Tom 20), s.159-167, 2009
63. Bailey Karen, Curran Kevin, An evaluation of image based steganography methods, Multimedia Tools and Applications Volume:30, Issue: 1, s. 55–88, July 2006
64. Conway Maura, Code wars: Steganography, signals intelligence, and terrorism Knowledge, Technology & Policy Volume: 16, Issue: 2, June 2003, s. 45 - 62
65. Jerzy Korostil, Łukasz Nozdrzykowski, Sposób budowania klucza steganograficznego w oparciu o progowe metody wyboru bloków obrazu, Metody Informatyki Stosowanej, vol. 10, s. 605-612, 2006
66. Jerzy Korostil, Łukasz Nozdrzykowski, Opracowanie rozproszonego klucza steganograficznego, XII Sesja Naukowa Informatyki, Metody Informatyki Stosowanej. Kwartalnik Komisji Informatyki PAN Oddział w Gdańsku, Nr 1/2008 (Tom 13), s.75-82, Szczecin 2008
67. Jerzy Korostil, Łukasz Nozdrzykowski, Metoda formowania struktury sprzętowej realizacji rozproszonego klucza steganograficznego na bazie FPGA, Pomiary Automatyka Kontrola, vol. 54, No. 8, s. 562-564, 2008
68. P. Dymarski, Obiektywne metody oceny jakości sygnału wideo, dostęp online: http://cygnus.tele.pw.edu.pl/dymarski/ptmt-old/video_quality.doc

69. Zając Marek, Funkcja wrażliwości na kontrast jako miara jakości widzenia, III Kongres Optyków zrzeszonych w Krajowej Rzemieślniczej Izbie Optycznej, Zakopane 2001
70. Jerzy Korostil, Łukasz Nozdrzykowski, The security level of a particular blind steganographic systems, Advanced Computer Science, Elektronika-konstrukcje, technologie, zastosowania, Nr 11/2009, s 41-44, 2009
71. Pyka Krystyna, Uwarunkowania fizjologiczne i techniczne wpływające na percepcję obrazu obserwowanego na ekranie monitora, Roczniki Geomatyki, Tom III, Zeszyt 1, Warszawa 2005
72. D. G. Pelli, J. G. Robson, The design of a New letter chart for measuring contrast sensitivity, Vlin Vision Sci, Vol. 2, No. 3, s. 187-199, 1988
73. J. Mannos, D. Sakrison, The Effects of a Visual Fidelity Criterion on the Encoding of Images, IEEE Transactions on Information Theory, Vol. 20, No 4, s. 525-535, 1974
74. Noureddine Moumkine, Ahmed Tamtaoui, Abdellah Ait Ouahman, Integration of the Contrast Sensitive Fumction into Wavelet Codec, ISCCSP 2006, Marrakech, Maroc 13-15 Mars 2006
75. Z. Rudnicki, Analiza sekwencji obrazów niejednorodnych, Informatyka w Technologii Materiałów, Numer 2, Tom 3, s. 86-96, 2003
76. J. Rumiński, Metody reprezentacji, przetwarzania i analizy obrazów w medycynie, http://astrophysics.fic.uni.lodz.pl/medtech/dodatki/metpo.html (dostęp: marzec 2009)
77. Z. Rudnicki, Wybrane metody przetwarzania i analizy cech obrazów teksturowych, Informatyka w Technologii Materiałów, Nr 1, Tom 2, 2002
78. http://www.netmarketshare.com/report.aspx?qprid=17&qpct=2
79. A. Mrózek, L. Płonka, Analiza danych metodą zbiorów przybliżonych. Akademicka Oficyba Wydawnicza PLJ, Wydanie 1, Warszawa 1999
80. Andrzej Piegat, Matematyka - zbiory przybliżone. Materiały do wykładów, Politechnika Szczecińska, Wydział Informatyki, Szczecin 2007
81. Jerzy Korostil, Łukasz Nozdrzykowski. The Analysis of the Importance of Image Attributes Affecting Visibility Fact of Steganographic Hide Messages in Digital Image, Polska Akademia Nauk Oddział w Gdańsku. Komisja Informatyki. Nr 2/2009 (Tom 19), s. 57-64, Szczecin 2009
82. Anna Zawada-Tomkiewic, Analiza obrazu powierzchni obrobionej do celów estymacji parametrów tej powierzchni, Acta mechanica et automatic, vol. 1 no. 2, 2007,
83. Krzysztof Nozdrzykowski, Łukasz Nozdrzykowski, Zastosowanie analizy Falkowej do oceny błędów kształtu, XXIII Sympozjon Podstaw Konstrukcji Maszyn, 17-21, wrzesień, Rzeszów-Przemyśl, s. 370-376, 2007
84. Dorota Majorkowska-Mech, Alexandr Ţariov, Algorytmy wielopoziomowej dekompozycji i rekonstrukcji falkowopodobnej danych 2D, Metody Informatyki Stosowanej, nr 1/2008, s.93-103, 2008
85. Jerzy Korostil, Łukasz Nozdrzykowski, Wyznaczenie zależności pomiędzy istotnymi parametrami obrazu dla zmniejszenia widoczności ukrycia

wiadomości w obrazach pomiędzy dziedziną przestrzenną a transformaty Falkowej, Metody Informatyki Stosowanej, nr 4/2009 (21), s. 55-62, 2009

86. Noureddine Moumkine, Ahmed Tamtaoui, Abdellah Ait Ouahman, Integration of the Contrast Sensitive Fumction into Wavelet Codec, ISCCSP 2006, Marrakech, Maroc 13-15 Mars 2006
87. Thomas Beth, Andreas Klappenecker, Armin N¨uckel, Construction of Algebraic Wavelet Coefficients, Proc. Int. Symp. on Information Theory and its Applications 1994, ISITA'94, Sydney, pages 341-344, 1994
88. D. POLLEN, Parametrization of compactly supported wavelets, Technical report, Aware Inc., 1989
89. Brani Vidakovic, Pollen Bases and Daubechies-Lagarias Algorithm in MATLAB, http://www2.isye.gatech.edu/~brani/datasoft/DL.pdf [dostęp online: luty 2010]
90. **Jerzy Korostil, Łukasz Nozdrzykowski, Propozycja algorytmu steganograficznego z kluczem rozproszonym opartego na funkcji CSF, SOFTSEC, Szczecin 2011, Pomiary, Automatyka, Kontrola, PAK 2012 nr 02, s. 214-217, 2012**
91. G. Schaefer, M. Stich, UCID - An Uncompressed Colour Image Database, Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia 2004, s. 472-480, 2004
92. R. Picard, Content access for image video coding, The fourth criterion, Tech. Rep. 195, MIT Media Lab, 1994

Spis rysunków:

Spis tabel: