AUTOMATYKA • 2008 • Tom 12 • Zeszyt 2

Piotr Kopniak*

Steganograficzne wykorzystanie piramid filtrów kierunkowych

1. Wprowadzenie

Steganografia jest nauką zajmującą się ukrywaniem cennych informacji przed „okiem" niepowołanego odbiorcy. Wiadomość zabezpieczona steganograficznie, może zostać odczytana jedynie przez osobę dysponującą wiedzą o jej istnieniu oraz odpowiednim kluczem steganograficznym.

Zastosowanie technik ukrywania informacji powoduje podniesienie poziomu bezpieczeństwa informacji znacznie bardziej niż w przypadku zastosowania kryptografii, zwłaszcza, jeśli wiadomość zawierająca cenną informację przesyłana jest przez publiczny kanał komunikacyjny. Wynika to z tego, że wiadomość poufna jest ukrywana wewnątrz innej informacji, która jest jawnie przesyłana otwartym kanałem komunikacyjnym. Przeciwnik widząc jedynie niewinnie wyglądający przekaz i nie mając świadomości istnienia poufnej wiadomości, nie będzie próbował jej odczytu lub zniszczenia.

Współczesna steganografia zwana jest steganografią techniczną, ponieważ wykorzystuje różne możliwości urządzeń technicznych do ukrywania informacji [7]. Najczęściej wykorzystywane są w tym celu komputery, dlatego można nazwać ją także komputerową. Nośnikami poufnych danych w przypadku steganografii komputerowej w większości przypadków są różnego rodzaju pliki multimedialne [5]. Charakteryzują się one dużą redundancją danych wynikającą z wysokiej jakości zapisu cyfrowego, znacznie przekraczającej wrażliwość zmysłów człowieka. W związku z tym duża ilość danych w plikach tego typu może zostać zastąpiona poprzez poufne dane w procesie steganograficznym, bez zauważalnej dla człowieka utraty jakości nośnika.

Metody steganograficzne rozwijają się w różnych kierunkach. Istniejące algorytmy można podzielić ze względu na rodzaj wykorzystywanego nośnika informacji, np. ukrywające dane w plikach dźwiękowych lub obrazach cyfrowych oraz ze względu na sposób ukrywania informacji. Drugi typ podziału wyróżnia między innymi: metody substytucyjne,

* Politechnika Lubelska w Lublinie

których przykładem jest metoda ukrywająca dane w najmniej znaczących bitach poszczególnych bajtów informacji nośnej, metody generacji nośnika na podstawie poufnego przekazu oraz metody statystyczne modyfikujące wskaźniki statystyczne danych nośnika [5]. Najnowsze metody steganograficzne opierają się na transformacji danych nośnika do innej przestrzeni, np. przestrzeni częstotliwościowej za pomocą transformacji Fouriera [15] lub czasowo-częstotliwowej za pomocą transformacji falkowej [2].

2. Nowe podejście do ukrywania informacji

Niniejsza praca zawiera najważniejsze wyniki przeprowadzonych badań, mających na celu wykorzystanie teorii cyfrowego przetwarzania sygnałów na potrzeby steganograficznego zabezpieczania informacji. Badania te przeprowadzono na potrzeby rozprawy doktorskiej [16], których skutkiem było opracowanie nowego algorytmu ukrywania informacji.

Przeprowadzona krytyczna analiza obecnego dorobku przetwarzania sygnałów oraz wcześniejsze prace badawcze opisane w publikacjach [10–17] wykazały, że możliwe jest wykorzystanie właściwości sterowalności kierunkowej dwuwymiarowych filtrów cyfrowych oraz przetwarzania wielorozdzielczego sygnałów do ukrycia informacji w obrazie cyfrowym.

Przetwarzanie wielorozdzielcze (*multirate processing*) wykorzystuje modyfikację częstotliwości próbkowania sygnału, dzięki technikom decymacji i interpolacji i wykorzystywane jest m.in. do analizy sygnałów medycznych, radarowych, zdjęć satelitarnych, kompresji sygnałów oraz w systemach widzenia maszynowego do dopasowywania obrazów stereoskopowych [6]. Najczęściej obecnie stosowanym przekształceniem umożliwiającym analizę wielorozdzielczą, zarówno w przypadku sygnałów jedno jak i wielowymiarowych, jest transformacja falkowa [1].

Z punktu widzenia steganografii popularność metody przetwarzania sygnału nie jest jednak cechą korzystną, ponieważ im bardziej znana jest metoda dołączania poufnych danych, tym większa jest możliwość ich wykrycia i odczytu, uszkodzenia lub podmiany. Ze względu na to, do opracowania metody steganograficznej, wykorzystującej przetwarzanie sygnałów, zostały wybrane mniej znane piramidy dwuwymiarowych filtrów sterowalnych [3, 20].

Transformacja pasmowa, zwana *sterowalną*, wykorzystująca piramidy kierunkowych filtrów cyfrowych, została opracowana m.in. w celu usprawnienia metod poprawy jakości obrazu, detekcji krawędzi oraz dopasowywania obrazów w stereoskopii [21]. Wykorzystanie steganograficzne tego typu przekształcenia jest podejściem nowatorskim.

Transformacja sterowalna umożliwia analizę danych graficznych nie tylko zlokalizowaną w przestrzeni i częstotliwości, tak jak jest to w przypadku transformacji falkowych

obrazu, ale także zlokalizowaną w wybranym kierunku geometrycznym. Możliwe jest to dzięki zastosowaniu podczas transformacji pasmowych filtrów cyfrowych, umożliwiających sterowanie kierunkiem ich filtrowania.

Zastosowanie odpowiedniej filtracji podczas budowy wielorozdzielczej piramidy przetwarzania eliminuje także zjawisko aliasingu występujące np. w przypadku podpasm transformaty falkowej. Inną różnicą w stosunku do transformacji falkowej jest nadkompletność transformaty otrzymanej w wyniku przekształcenia sterowalnego, tzn. ilość współczynników transformaty jest większa od ilości danych obrazu wejściowego. Powoduje to, że przestrzeń, którą można wykorzystać do ukrycia danych, jest większa. Wymienione zalety wskazują na większą atrakcyjność wykorzystania steganograficznego tego typu przetwarzania sygnału niż np. transformacji falkowej [20].

Przeprowadzone badania teoretyczne umożliwiły stworzenie modelu nowego stegosystemu. Opracowany stegosystem ukrywa dane poprzez modyfikacje wartości średnich bloków współczynników podpasma transformaty obrazu, otrzymanej w wyniku transformacji za pomocą piramidy filtrów sterowalnych.

Metoda dołączania danych oparta została na algorytmie steganograficznym Lee i Chena [18]. Wybrane elementy algorytmu, oryginalnie opracowanego dla obrazów monochromatycznych w reprezentacji przestrzennej, wykorzystano do współczynników transformaty obrazu barwnego.

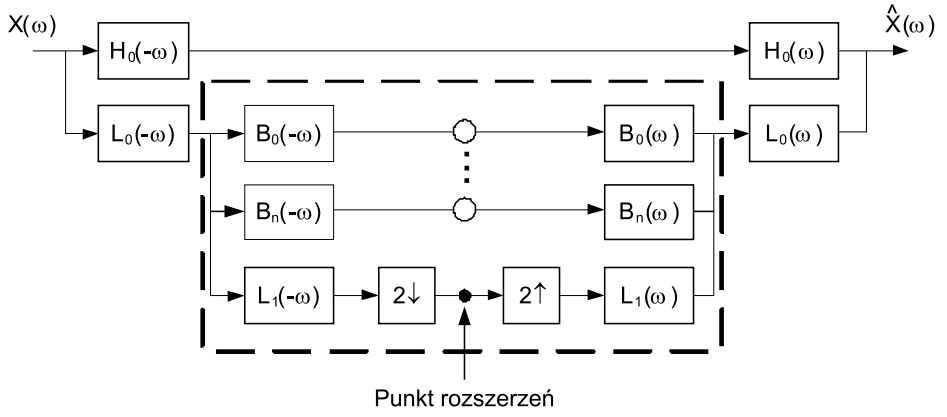
3. Piramidy filtrów kierunkowych

Piramida sterowalna opracowana przez Freemana, Adelsona i Simoncelliego [3, 20, 21] umożliwia wykonanie liniowej wielorozdzielczej i wielokierunkowej dekompozycji obrazu. Transformacja ta jest także samoodwracalna, co oznacza, że macierz transformacji odwrotnej jest transpozycją macierzy transformacji prostej.

W odróżnieniu od transformacji falkowych jest to dekompozycja nieortogonalna, tzn. funkcje bazowe są liniowo zależne, i nadkompletna, tzn. liczba współczynników powstałej dekompozycji przewyższa liczbę pikseli obrazu wejściowego.

W tej dekompozycji obraz jest przekształcany do zbioru podpasm zlokalizowanych jednocześnie w skali i orientacji oraz niezależnych od translacji (*shift invariant*) i obrotu (*rotation invariant*). Podpasma pozbawione są także efektu aliasingu występującego w podpasmach transformacji falkowej. Jednak podstawową cechą tej transformacji jest sterowalność, czyli możliwość wyboru dowolnego kierunku filtrowania obrazu, czego nie posiadają inne transformacje przestrzenno-częstotliwościowe, tzn. transformacja Gabora, Laplace'a czy transformacja falkowa.

Schematycznie jeden poziom piramidy filtrów sterowalnych wykorzystywanej do transformacji sterowalnej przedstawia rysunek 1.



Rys. 1. Piramida filtrów sterowalnych o jednym poziomie rozdzielczości
Objaśnienia w tekście

Na schemacie (rys. 1) filtr $H_0(\omega)$ jest niezorientowanym filtrem górnoprzepustowym, a $L_0(\omega)$ wąskopasmowym filtrem dolnoprzepustowym, które wstępnie przygotowują sygnał do przetwarzania poprzez kolejne poziomy piramidy filtrów. Filtry $B_0(\omega) - B_n(\omega)$ są filtrami pasmowymi, stanowiącymi sterowalną bazę, gdzie każdy filtr jest taki sam, tylko jego maska współczynników obrócona jest pod innym kątem względem jej środka.

Filtry bazowe spełniają warunek sterowalności, czyli są minimalną liczbą funkcji umożliwiającą interpolację filtru pasmowego w dowolnym kierunku geometrycznym. Najprostszym przykładem sterowalnej bazy jest zestaw $N+1$ pochodnych kierunkowych N-tego rzędu.

Odpowiedź częstotliwościową filtru pasmowego zorientowanego w określonym kierunku k, czyli pochodnej kierunkowej N-tego rzędu, można zapisać jako iloczyn składnika radialnego i kątowego:

$$B_k(\omega) = B(\omega)[-j\omega\cos(\theta - \theta_k)]^N \tag{1}$$

gdzie:
$$\theta = \tan^{-1}(\omega_y / \omega_x), \quad \theta_k = \frac{k\pi}{N+1}, \text{ dla } k \in [0, 1, ..., N] \tag{2}$$

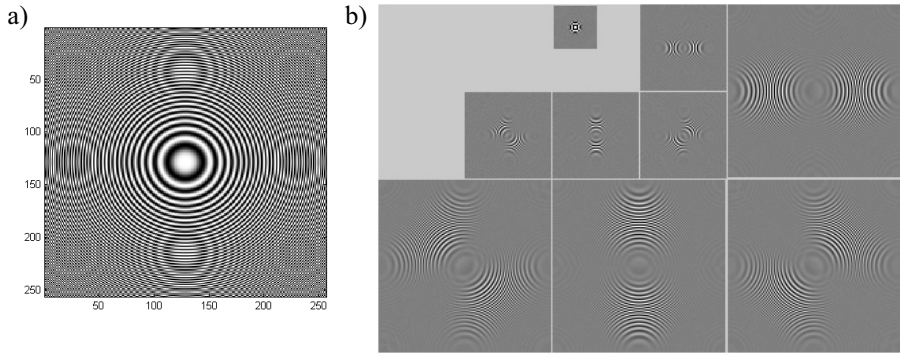
i
$$B(\omega) = \sqrt{\sum_{k=0}^{N} |B_k(\omega)|^2} \tag{3}$$

W wyniku filtrowania poprzez filtry pasmowe powstają podpasma kierunkowe na danym poziomie rozdzielczości, oznaczone na schemacie rysunku 1 za pomocą kółek. Ze względu na brak decymacji przed filtrowaniem pasmowym nie występuje tu zjawisko

aliasingu. Poziom rozdzielczości podpasma określa poziom piramidy, na którym położony jest dany zespół filtrów.

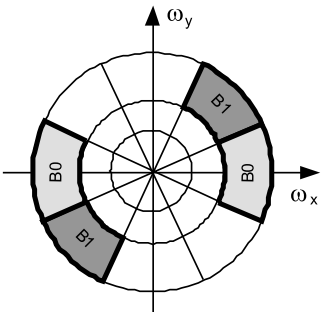
Kolejne poziomy niższych rozdzielczości uzyskuje się poprzez rekursywne rozwinięcie piramidy w punkcie rozszerzeń, poprzez umieszczenie w nim całego bloku filtrów otoczonych przerywaną linią. Sygnał wejściowy każdego kolejnego poziomu poddany jest decymacji powodujące dwukrotne zmniejszenie jego częstotliwości i filtrowaniu dolnoprzepustowemu.

Piramidę obrazów powstałą w wyniku dekompozycji poprzez transformację sterowalną, gdzie filtrami bazowymi są pochodne trzeciego rzędu, a piramida posiada trzy poziomy rozdzielczości, przedstawia rysunek 2.



Rys. 2. Obraz testowy (a) i jego dekompozycja wielorozdzielcza za pomocą piramidy sterowalnej o trzech poziomach i czterech filtrach bazowych (b)

Analizę sygnału w dziedzinie częstotliwości za pomocą dwupoziomowej piramidy sterowalnej o bazie składającej się z czterech filtrów pasmowych przedstawiono na rysunku 3. Widma Fouriera czterech filtrów bazowych dzielą kąt półpełny przestrzeni Fouriera na cztery części i są symetryczne względem środka układu współrzędnych.



Rys. 3. Idealna spektralna dekompozycja obrazu przy wykorzystaniu piramidy filtrów kierunkowych

Jeżeli poprzez $X(\omega)$ oznaczymy transformatę Fouriera obrazu oryginalnego, podanego na wejście piramidy sterowalnej, to transformatę obrazu zrekonstruowanego na wyjściu definiuje formuła:

$$\hat{X}(\omega) = \left\{ |H_0(\omega)|^2 + |L_0(\omega)|^2 \left(|L_1(\omega)|^2 + \sum_{k=0}^{n} |B_k(\omega)|^2 \right) \right\} X(\omega) + a \quad (4)$$

gdzie a – eliminowany podczas dekompozycji składnik związany z występowaniem aliasingu.

Piramida sterowalna zapewnia perfekcyjną rekonstrukcję obrazu na wyjściu, czyli:

$$\hat{X}(\omega) = X(\omega),$$

jeżeli spełnione są następujące warunki:

– Amplituda odpowiedzi systemu jest jednostkowa, tzn. nie występuje zniekształcenie amplitudowe systemu:

$$|H_0(\omega)|^2 + |L_0(\omega)|^2 \left(|L_1(\omega)|^2 + \sum_{k=0}^{N} |B_k(\omega)|^2 \right) = 1 \quad (5)$$

– Występuje zależność rekursywna, tzn. niskoczęstotliwościowa gałąź diagramu nie zmienia się po dołączeniu rekursywnego bloku systemu:

$$|L_1(\omega/2)|^2 \left(|L_1(\omega)|^2 + \sum_{k=0}^{N} |B_k(\omega)|^2 \right) = |L_1(\omega/2)|^2 \quad (6)$$

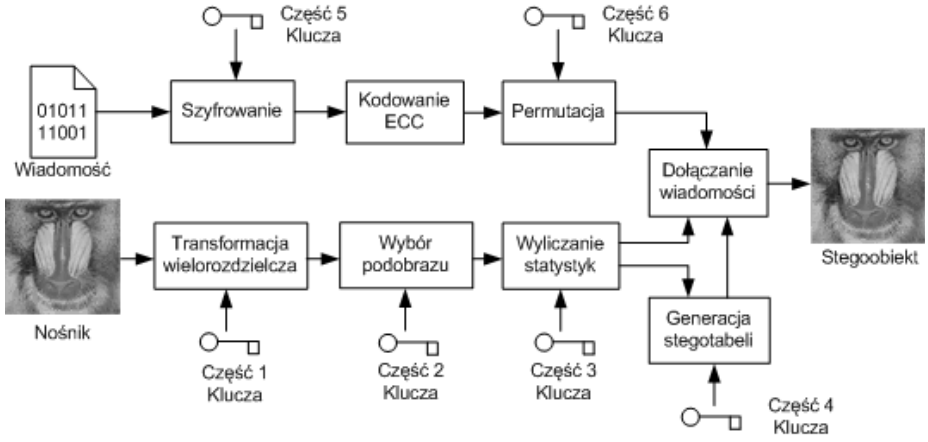
– Filtr $L_1(\omega)$ powoduje eliminację aliasingu (składnika a we wzorze (4)), który mógłby się pojawić po decymacji na kolejnym poziomie piramidy:

$$L_1(\omega) = 0 \quad \text{dla} \quad |\omega| > \frac{\pi}{2} \quad (7)$$

Analiza wielorozdzielcza za pomocą piramidy sterowalnej umożliwia zastosowanie w wielu różnych dziedzinach przetwarzania i rozpoznawania obrazów, o czym wspomniano na początku paragrafu. Dzięki cechom takim jak: samoodwracalność, nadkompletność i perfekcyjna rekonstrukcja może być także skutecznie wykorzystana w steganografii.

4. Model stegosystemu opartego na transformacji sterowalnej

Zaproponowany model stegosystemu umożliwia ukrywanie poufnych informacji z wykorzystaniem nośnika będącego cyfrowo zapisanym obrazem barwnym. Schemat blokowy opracowanego systemu ukrywania informacji przedstawia rysunek 4.



Rys. 4. Schemat ukrywania informacji opracowanego stegosystemu

W procesie ukrywania informacji można wyróżnić dwie ścieżki przetwarzania, które mogą być wykonywane niezależnie od siebie. Pierwsza z nich to wstępne przygotowanie obrazu, do którego wiadomość będzie dołączana, a druga to przygotowanie wiadomości poprzedzające jej dołączenie do nośnika.

Przygotowanie wstępne obrazu stanowią następujące operacje:

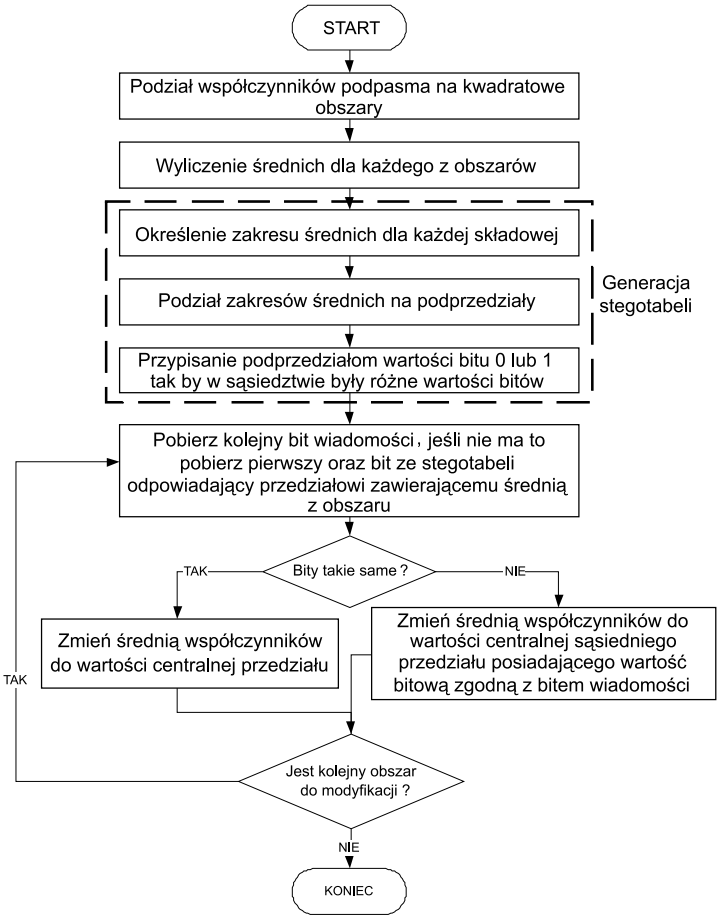
1. **Transformacja wielorozdzielcza** – przekształcenie wielorozdzielcze każdej składowej barwnej obrazu RGB osobno za pomocą piramidy sterowalnej, gdzie filtrami bazowymi są pochodne kierunkowe. Etap ten wymaga wyboru parametrów dekompozycji, tzn. określenia liczby poziomów piramidy oraz liczby podpasm kierunkowych, które stanowią pierwszą część klucza steganograficznego.
2. **Wybór podobrazu** – wybór jednego lub wielu podpasm transformaty, w których będzie ukryta informacja. Określenie podpasma polega na wskazaniu poziomu piramidy oraz indeksu popdpasma na wybranym poziomie. Te dwa zmienne parametry stanowią drugą część klucza steganograficznego.

Przygotowanie wstępne wiadomości przed jej ukryciem ma na celu jej dodatkowe zabezpieczenie przed próbą odczytu lub uszkodzenia i składa się za następujących etapów:

1. **Szyfrowanie** – wstępne szyfrowanie wiadomości, zwiększające bezpieczeństwo informacji w przypadku próby jej odczytu, niezmieniające jednak poziomu bezpieczeństwa steganograficznego. Z tego powodu etap ten może zostać pominięty na etapie badań. Klucz kryptograficzny stanowi piątą część klucza steganograficznego.
2. **Kodowanie ECC** – wykorzystanie kodu korekcji błędów – ECC (*Error Correcting Code*), polegające na uzupełnieniu informacji o dane korekcyjne według wybranego algorytmu korekcji. Etap ten umożliwia wyeliminowanie części błędnych bitów wiadomości uszkodzonej w wyniku przetwarzania stegoobrazu.

3. **Permutacja** – jest etapem zwiększającym odporność ukrytej informacji poprzez wykonanie jej pseudolosowej permutacji, co odpowiada losowemu wyborowi bloków współczynników, do których informacja dodawana byłaby sekwencyjnie. Permutacja wykonywana jest pseudolosowo, więc wymaga podania wartości startowej generatora liczb losowych. Wartość ta jest szóstą częścią klucza steganograficznego.

Metodę dołączania danych do nośnika oparto na algorytmie steganograficznym opracowanym przez Lee i Chena (nazywanym dalej skrótowo LC). Wybrane jego elementy, tzn. generacja stegotabeli i sposób dołączania bitów wiadomości poprzez modyfikację właściwości statystycznych nośnika, zostały wykorzystane do ukrywania informacji w podpasmach transformaty obrazu barwnego w przestrzeni transformacji sterowalnej. Schemat zaimplementowanego algorytmu ukrywania informacji przedstawia rysunek 5.



Rys. 5. Schemat algorytmu steganograficznego

Danymi wejściowymi procesu ukrywania informacji jest wstępnie przetworzona wiadomość oraz wybrane podpasmo transformaty. Proces dołączania informacji rozpoczyna się od podziału współczynników podpasma P na kwadratowe, rozłączne bloki B_i, tzn.:

$$P = \{B_1, B_2, ..., B_M\} \tag{8}$$

o jednakowym rozmiarze $n \times n$ podanym jako część składowa klucza steganograficznego.

Następnie dla każdego bloku B_i wyliczana jest wartość wybranej miary statystycznej. Miarą statystyczną może być wartość średnia, co ma miejsce w przypadku algorytmu LC, lub inna miara jak: wariancja, odchylenie standardowe czy mediana. Jak wykazały przeprowadzone badania, najlepsze rezultaty uzyskuje się dla wartości średnich, więc jako statystykę modyfikowaną przyjęto wartość średnią S_i współczynników w_j bloku:

$$S_i = \sum_{j=1}^{n^2} w_j / n^2 \tag{9}$$

Korzystając z wyliczonych statystyk, tworzy się stegotabelę, która jest podstawowym elementem procesu dołączania i odczytu wiadomości. Na jej podstawie modyfikowane są wartości statystyczne bloku współczynników transformaty, w celu ukrycia w nim określonej wartości bitu informacji.

Stegotabela jest zbiorem podprzedziałów o równych długościach, których suma jest przedziałem o granicach wyznaczonych przez minimalną i maksymalną wartość wyliczonych statystyk. W stegotabeli każdy podprzedział posiada przypisaną mu wartość bitową „0" lub „1". Ukrycie określonego bitu informacji w danym bloku współczynników wymaga dostosowania jego statystyki w taki sposób, aby jej wartość zawierała się w przedziale stegotabeli z przypisaną wymaganą wartością bitową.

Generacja stegotabeli rozpoczyna się od wyznaczenia wartości ekstremalnych statystyk, czyli:

$$S_{\min} = \min\{S_i\} \quad \text{oraz} \quad S_{\max} = \max\{S_i\}, \quad i = 0, 1, ..., M \tag{10}$$

stanowiących granice stegotabeli. Przedział wartości $\langle S_{\min}, S_{\max} \rangle$ dzielony jest następnie na k podprzedziałów p_k. Wartość k jest parametrem metody, będącym czwartą częścią klucza steganograficznego (rys. 4). Utworzona stegotabela ST wygląda następująco:

$$ST = \{p_0, p_1, ..., p_{k-1}\}^T \tag{11}$$

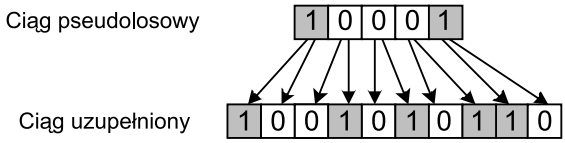
gdzie:

$$p_i = S_{\min} + i(S_{\max} - S_{\min}) / k \tag{12}$$

Kolejnym krokiem jest wygenerowanie binarnego ciągu pseudolosowego, którego poszczególne elementy zostaną przypisane do kolejnych podprzedziałów stegotabeli. War-

tość startowa generatora liczb pseudolosowych jest elementem klucza steganograficznego i zawiera się w jego czwartej części (rys. 4).

Wygenerowany ciąg przed dołączeniem do stegotabeli jest rozszerzany, według sposobu zaproponowanego w algorytmie *LC*. Rozszerzenie polega na tym, że każda wartość „0" zastępowana jest ciągiem bitowym „01", a wartość „1" ciągiem „10", co przedstawiono na rysunku 6. Dzięki temu w otoczeniu każdej wartości „1" w ciągu bitowym znajduje się wartość „0" i na odwrót.



Rys. 6. Rozszerzanie binarnego ciągu pseudolosowego

Taki układ bitów zapewnia mniejsze modyfikacje nośnika podczas dołączania bitów wiadomości, ponieważ odpowiednie dostosowanie statystyki wymaga mniejszych zmian wartości współczynników bloku.

Rozszerzony ciąg przypisywany jest następnie sekwencyjnie do kolejnych przedziałów stegotabeli:

$$ST = \begin{Bmatrix} p_0 & p_1 & \cdots & p_{k-1} \\ b_0 & b_1 & \cdots & b_{k-1} \end{Bmatrix}^T \tag{13}$$

W identyczny sposób generowane są stegotabele dla wszystkich składowych barwnych nośnika.

Po wygenerowaniu stegotabel możliwe jest dołączenie bitów wiadomości do nośnika. Dołączanie przebiega cyklicznie, tzn. pobierane są kolejne wartości S_i oraz kolejne bity wiadomości m_i, a następnie wykonywane jest poszukiwanie w stegotabeli przedziału p, takiego, że:

$$p_j \le S_i < p_{j+1} \tag{14}$$

Jeżeli bit wiadomości m_i i bit b_i przypisany do wybranego przedziału są równe, to wartość statystyki S_i zmieniana jest w taki sposób, aby osiągnęła środek przedziału stegotabeli, w którym się znajduje. Jeżeli wartości bitów się nie zgadzają, to wykonywane są dwa inne porównania z bitami w sąsiednich przedziałach stegotabeli, tzn.: czy $m_i = b_{j-1}$ oraz czy $m_i = b_{j+1}$. Przynajmniej jedna z tych dwóch równości będzie zachodzić zawsze, dzięki rozszerzeniu pseudolosowego ciągu bitowego dołączanego do stegotabeli (rys. 6). W takim przypadku wartość S_i zmieniana jest w taki sposób, aby osiągnęła środek przedziału p_{j-1} lub p_{j+1} w zależności od wyniku porównań. Przesunięcie wartości statystycznej do środka

przedziału powoduje zwiększenie odporności ukrytej wiadomości na uszkodzenie, ponieważ ukryty bit danych będzie odczytany przez odbiorcę posługującego się taką samą stegotabelą prawidłowo, w każdym przypadku, gdy wartość statystyki nie przekroczy granicy przedziału, w którym się pierwotnie znajdowała.

Modyfikacja danych może być przeprowadzona na różne sposoby, np. poprzez zmianę wartości wszystkich współczynników bloku lub tylko wybranej grupy. Ze względu na to, że modyfikacje wybranych współczynników mogłyby spowodować duże różnice ich wartości w stosunku do otoczenia, powodujące zauważalne zmiany, narażające ukryty przekaz na wykrycie, przyjęto modyfikację wszystkich współczynników bloku jednocześnie. Dla wartości średniej można wykonać to na dwa sposoby.

Pierwszy sposób to modyfikacja regularna, w której wszystkie współczynniki bloku zmieniają się o taką samą wartość:

$$w_j = w_j + R \tag{15}$$

będącą różnicą pomiędzy wyliczoną wartością S_i i wartością środka przedziału:

$$R = S_i - (p_{j+1} - p_j)/2 \tag{16}$$

Drugi sposób polega na modyfikacji proporcjonalnej, tzn. każdy współczynnik zmienia się o wartość proporcjonalną do jego wartości wyjściowej:

$$w_j = w_j(1 + n^2 R / \sum_{j=1}^{n^2} w_j) = w_j(1 + R/S_i) \tag{17}$$

Wiadomość podczas dołączania do nośnika powtarzana jest wielokrotnie, w celu wykorzystania wszystkich bloków współczynników, co przedstawiono na schemacie algorytmu na rysunku 5. W przypadku wykorzystania jedynie części nośnika, dołączona informacja mogłaby być łatwiej wykryta przez stegoanalityka [19].

Odczyt wiadomości z podpasma przetransformowanego stegoobrazu polega na porównaniu wartości statystycznych bloków współczynników z przedziałami w stegotabeli. Stegotabela musi być identyczna ze stegotabelą zastosowaną przez nadawcę wiadomości, co zapewnia klucz steganograficzny określający liczbę przedziałów zakresu wartości statystyk.

Dzięki zastosowaniu podczas procesu ukrywania informacji powtórzeń wiadomości, mających na celu wykorzystanie całej powierzchni nośnika, ukryta wiadomość może być z większym prawdopodobieństwem prawidłowo odczytana przez odbiorcę. Poszczególne wystąpienia ukrytej wiadomości o długości L odczytywane są ze stegoobrazu, a następnie ich bity są uśredniane w sposób następujący:

$$m_i = \left[\sum_{1}^{M/L} m_i \right] / (M/L) \tag{18}$$

gdzie M/L – liczba wystąpień wiadomości na obszarze nośnika.

Dzięki tej operacji eliminowany jest wpływ błędnych bitów na ostateczną postać odczytanej wiadomości. Błędne bity pochodzą z bloków współczynników, w przypadku których wartość statystyczna przekroczyła granice przedziału stegotabeli, do którego była zakwalifikowana podczas ukrywania informacji. Takie zmiany wartości statystycznych mogą wystąpić podczas celowych zniekształceń stegoobrazu przez przeciwnika, ale także podczas procesu rekonstrukcji obrazu na podstawie jego transformaty.

Proces odczytu wiadomości ze stegoobrazu wymaga znajomości wszystkich części klucza steganograficznego, ponieważ wykonuje takie same operacje jak podczas ukrywania informacji tylko w odwrotnej kolejności.

5. Badania doświadczalne opracowanej metody steganograficznej

Nowy algorytm steganograficzny został poddany weryfikacji doświadczalnej mającej na celu określenie i dobór odpowiednich wartości parametrów metody, dla których wiadomość jest prawidłowo dołączana do nośnika i możliwy jest jej prawidłowy odczyt.

Weryfikowanymi parametrami były:

- rodzaj modyfikowanej miary statystycznej,
- sposób modyfikacji wartości współczynników transformaty,
- składowa barwna obrazu, która najlepiej nadaje się do ukrycia danych,
- liczba poziomów i podpasm kierunkowych dekompozycji obrazu,
- liczba podpasm, które mogą być wykorzystane jednocześnie,
- rozmiar bloku współczynników,
- liczba przedziałów całego zakresu wartości średnich obliczonych z bloków współczynników podpasma.

Zweryfikowanie dopuszczalnych wartości wyżej wymienionych parametrów umożliwiło dalsze badania charakteryzujące metodę, tzn. dotyczące określenia długości klucza steganograficznego, co jest istotne z punktu widzenia bezpieczeństwa informacji oraz pojemności informacyjnej.

Wielkością statystyczną, która podlega najmniejszym zniekształceniom podczas kompozycji stegoobrazu na podstawie podpasm transformaty spośród trzech zbadanych, tzn. wartości średniej, wariancji oraz mediany, jest wartość średnia współczynników. W związku z tym, w przypadku zaproponowanego stegosystemu, najlepiej ukrywać wiadomości poprzez modyfikacje wartości średniej bloku współczynników transformaty.

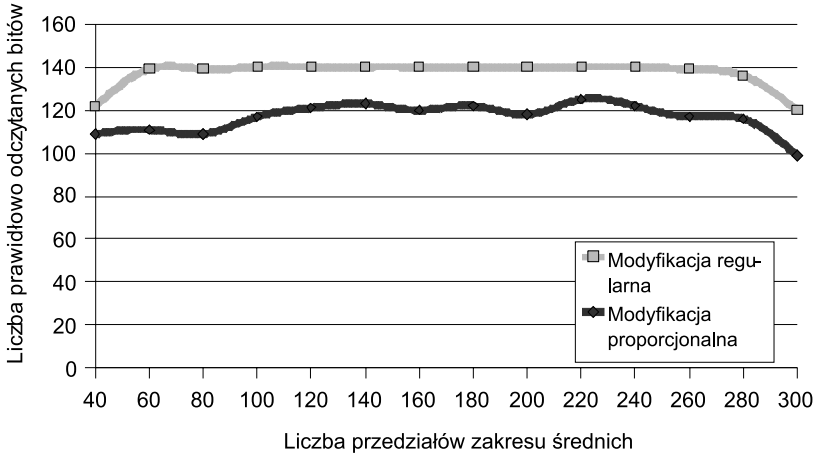
Porównanie skuteczności odczytu 140-bitowej informacji ukrytej w obrazach testowych RGB o rozdzielczości 256 × 256 punktów poprzez modyfikacje średniej i wariancji współczynników w bloku przedstawia tabela 1.

Modyfikacja wartości współczynników transformaty może być przeprowadzona w sposób regularny lub proporcjonalny. Na podstawie badań można stwierdzić, że ukryta wiadomość jest w mniejszym stopniu zniekształcana podczas procesu rekonstrukcji obrazu

wyjściowego, kiedy wykorzystuje się regularne zmiany wartości współczynników podpasma. W tym przypadku skuteczność odczytu ukrytej wiadomości jest większa, co obrazuje dla wiadomości o długości 140 bitów rysunek 7.

Tabela 1
Liczba prawidłowo odczytanych bitów 140-bitowej wiadomości
przy modyfikacji wartości średniej i wariancji bloków współczynników

Obraz	Miara	Liczba przedziałów zakresu wielkości modyfikowanej															
		100	110	120	130	140	150	160	170	180	190	200	210	220	230	240	250
Pawian	Waria.	138	139	140	138	138	139	140	140	138	140	140	138	139	138	139	138
	Śred.	140	140	140	140	140	140	140	140	140	140	139	140	140	140	140	140
Kwiat	Waria.	115	121	112	120	94	96	119	118	94	126	125	125	101	121	127	101
	Śred.	129	129	134	139	140	140	139	140	140	140	140	140	140	140	140	140
Lena	Waria.	121	115	114	119	82	83	120	122	94	127	117	129	92	127	132	98
	Śred.	140	130	139	140	140	140	140	140	139	140	139	140	140	140	140	140



Rys. 7. Wpływ wyboru metody modyfikacji wartości średniej obszarów pasma na liczbę prawidłowo odczytanych bitów 140-bitowej wiadomości dla obrazu Pawian i liczbie podziałów zakresu średnich od 40 do 300

Prawdopodobieństwo prawidłowego odczytu informacji wzrasta wraz z liczbą jej powtórzeń na obszarze nośnika, ponieważ odczytywane wartości bitowe są wynikiem uśredniania wszystkich wystąpień wiadomości, w związku z tym najlepiej dołączać wiadomość do wszystkich składowych barwnych obrazu jednocześnie i powtarzać krótszą wiadomość

tak, aby wykorzystać wszystkie bloki współczynników. Wykorzystanie wszystkich bloków współczynników eliminuje także możliwość wykonania przez przeciwnika trywialnej stegoanalizy statystycznej polegającej na rozróżnieniu obszarów modyfikowanych i niemodyfikowanych o różnych właściwościach statystycznych.

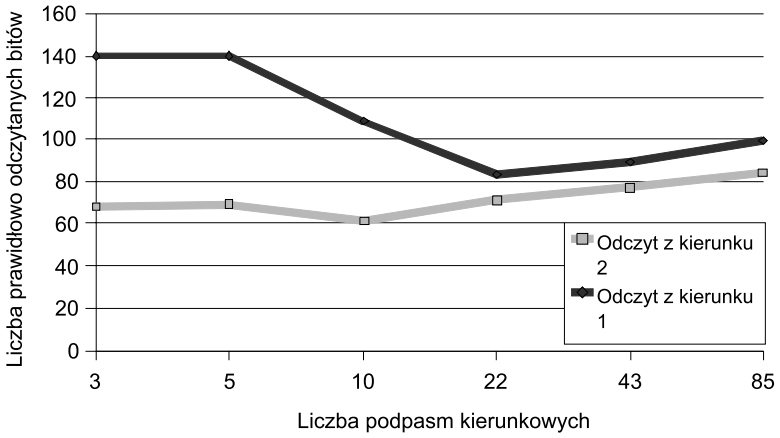
Wykorzystany algorytm dekompozycji obrazu umożliwia uzyskanie do 85 podpasm kierunkowych na każdym z poziomów piramidy w przypadku obrazów o rozdzielczości 256 × 256 punktów, jednak tylko w przedziale od 2 do 10 podpasm można za pomocą opracowanego algorytmu ukryć i odczytać prawidłowo wiadomość. Przykładową skuteczność odczytu 140-bitowej wiadomości przedstawia tabela 2.

Tabela 2
Liczby prawidłowo odczytanych bitów 140-bitowej wiadomości ukrytej w różnych obrazach przy dekompozycji o różnych liczbach podpasm kierunkowych

Obraz	Maksymalna liczba prawidłowo odczytanych bitów					
	3 podpasma	5 podpasm	10 podpasm	22 podpasma	43 podpasma	85 podpasm
Pawian	**140**	**140**	139	138	133	116
Samolot	**140**	**140**	138	135	129	116
Kwiat	**140**	**140**	138	135	125	116
Lena	**140**	139	137	119	122	120
Papryki	**140**	139	139	133	124	116

W przypadku obrazu 256 × 256 punktów możliwe jest utworzenie piramidy wielorozdzielczej o sześciu poziomach, a informacje mogą być dołączane na dowolnym poziomie, jednak im wyższy poziom piramidy, tym mniejsza jest rozdzielczość podpasma, a co za tym idzie – mniejsza pojemność informacyjna. Ilość informacji, którą można ukryć i prawidłowo odczytać, maleje około dwukrotnie przy przejściu na wyższy poziom piramidy.

Zweryfikowano także możliwość prawidłowej ekstrakcji wiadomości w przypadku, gdy przeciwnik nie zna dokładnych wartości składników klucza steganograficznego. Badania wykazały, że nie jest możliwy prawidłowy odczyt wiadomości z podpasma innego niż to, w którym ją ukryto – nie występuje przeciek informacji do pasm sąsiednich, nawet w przypadku 85 podpasm kierunkowych. Co oznacza, że wiadomość może zostać odczytana prawidłowo tylko w przypadku znajomości klucza. Wyniki skuteczności odczytu wiadomości z podpasma, w którym rzeczywiście została ona ukryta oraz podpasma sąsiedniego dla różnej liczby podpasm kierunkowych, przedstawia rysunek 8. Jak widać na wykresie, w przypadku 22 i większej liczby podpasm kierunkowych wiadomość w obu przypadkach jest całkowicie zniszczona. Obrazuje to skuteczność odczytu na poziomie niewiele wyższym niż 50%, który odpowiada statystycznie porównaniu wiadomości ukrytej z dowolnym ciągiem bitowym.



Rys. 8. Liczba prawidłowych bitów wiadomości 140-bitowej odczytanych z podpasma, w którym ukryto wiadomość (kierunku 1), oraz podpasma sąsiedniego (kierunku 2), w zależności od liczby podpasm na jednym poziomie piramidy dla obrazu Pawian

Opracowana metoda wymaga doboru wielkości bloku współczynników, w którym ukrywany jest jeden bit informacji, oraz liczby podprzedziałów, na które dzielony jest cały zakres zmienności wartości średnich wyliczonych z bloków współczynników transformaty. Najlepsze rezultaty uzyskano dla bloków o rozmiarach od 2×2 do 10×10 punktów oraz liczby przedziałów od 50 do 300.

Przeprowadzone badania umożliwiły określenie parametrów nowej metody oraz realnych zakresów ich zmienności, co z kolei umożliwiło określenie składników i długości klucza steganograficznego niezbędnego do odczytu ukrytej informacji. Składniki klucza przedstawia tabela 3.

Tabela 3
Zestawienie składników klucza steganograficznego

Lp.	Składnik klucza	Dopuszczalne wartości	Długość [bit]
1	Liczba poziomów piramidy	1–6	3
2	Liczba podpasm kierunkowych	1–10	4
3	Wybrany poziom piramidy	1–6	3
4	Wybrane podpasmo kierunkowe	1–10	4
5	Rozmiar bloku współczynników	2–10	4
6	Liczba przedziałów zakresu średnich	50–300	8
7	Długość wiadomości	1 -50 znaków	6
8	Ziarno PRNG do generacji stegotabeli	Przyjęto 3 * 0–255 (RGB)	24
9	Ziarno PRNG do permutacji wiadomości	Przyjęto 0–255	8
W sumie			64

W zależności od wymaganego poziomu bezpieczeństwa długość klucza może być różna. Dla zadanej rozdzielczości obrazu i przy wykorzystaniu zmienności wszystkich parametrów wyniosła ona 64 bity. Długość klucza może być dodatkowo zwiększona o długość klucza kryptograficznego, wykorzystanego do zaszyfrowania treści wiadomości ukrywanej.

Pojemność informacyjna metody zależy od danych nośnika i dla obrazu 256 × 256 punktów wynosi około 300 bitów.

6. Ocena jakości nowego algorytmu

Jakość steganograficzna nowego algorytmu (oznaczanego dalej symbolem PS – skrótem od piramidy sterowalne) została zweryfikowana podczas testów porównawczych z innymi znanymi aplikacjami steganograficznymi. Aplikacje porównawcze dobrano w taki sposób, aby stanowiły implementacje różnych technik steganograficznych. Pierwszą z nich był program Hide4PGP wykorzystujący do ukrycia informacji metodę substytucji najmniej znaczących bitów, każdego z trzech bajtów opisujących punkt obrazu RGB. Drugą implementacją była aplikacja EzStego wykorzystująca nośnik będący obrazem skompresowanym w formacie GIF, która do ukrycia informacji wykorzystywała sortowanie palety kolorów i substytucję najmniej znaczących bitów indeksów kolorów. Ostatnią z aplikacji porównawczych była implementacja algorytmu F5, który ukrywa informacje poprzez modyfikacje wartości współczynników transformaty kosinusowej obrazu, podczas kompresji stratnej JPEG.

Aspektami weryfikowanymi podczas testów porównawczych były:

- pojemność informacyjna oferowana przez poszczególne algorytmy,
- wielkość zniekształceń nośnika wprowadzanych podczas dołączenia wiadomości,
- wpływ celowego zniekształcania stegoobrazu na uszkodzenia wiadomości ukrytej,
- wpływ kompresji stratnej stegoobrazu na uszkodzenia wiadomości,
- odporność stegoobrazu na stegoanalizę.

Zmiany jakości stegoobrazów, czyli obrazów z ukrytą informacją, w stosunku do obrazów źródłowych, oceniono na podstawie miar jakości obrazu przedstawionych w tabeli 4.

Badania porównawcze algorytmu steganograficznego opartego na piramidach filtrów oraz algorytmów wykorzystywanych przez aplikacje: Hide4PGP, EzStego i F5 wykazały, że opracowana metoda dorównuje jakością ukrywania danych aplikacjom porównawczym, a w niektórych przypadkach je przewyższa.

Modyfikacje danych obrazu wprowadzane przez metodę PS są niewielkie i mniejsze niż wprowadzane przez aplikacje EzStego i F5. Lepsze rezultaty daje tylko wykorzystanie aplikacji Hide4PGP, która zmienia dane minimalnie, ale jednocześnie wykorzystuje metodę, która powoduje, że ukryte informacje są bardzo podatne na uszkodzenie.

Okazało się także, że wielkość zniekształceń nie zależy od wartości parametrów metody, tj. liczby poziomów i podpasm piramidy, liczby przedziałów i wielkości bloków współ-

czynników, z wyjątkiem przypadków, dla których liczba przedziałów zakresu wartości średnich była mniejsza od 40, czyli przypadków nieużytecznych, ponieważ niezapewniających prawidłowego odczytu wiadomości ukrytej.

Tabela 4
Zestawienie miar zniekształceń obrazu

Nazwa miary	Równanie
Maksymalna różnica wartości pikseli	$\max DF = \max_{x,y}(p_{x,y} - \hat{p}_{x,y})$
Minimalna różnica wartości pikseli	$\min DF = \min_{x,y}(p_{x,y} - \hat{p}_{x,y})$
Średnia różnica wartości pikseli	$AD = \frac{1}{XY}\sum_{x,y}\left\|p_{x,y} - \hat{p}_{x,y}\right\|$
Odchylenie standardowe różnicy wartości pikseli	$STD = \sqrt{\frac{1}{XY}\sum_{x,y}\left\|\left(p_{x,y} - \hat{p}_{x,y}\right) - AD\right\|^2}$
Odstęp sygnału od szumu [dB]	$SNR = 10\log_{10}\frac{\sigma^2(p_{x,y})}{STD^2}$
Relatywna entropia – zmienność pojemności informacyjnej	$D(P_C \parallel P_S) = \sum_{q\in Q} P_C(q)\log_2\frac{P_C(q)}{P_S(q)}$

Zestawienie wielkości zniekształceń poszczególnych aplikacji dla jednego z obrazów testowych przedstawia tabela 5.

Tabela 5
Wartości zniekształceń obrazu wprowadzanych przez metodę PS i aplikacje porównawcze

Obraz	Aplikacja	minDF	maxDF	AD	STD	SNR	D
Kwiat	PS	0,00	1,00	0,5030	0,5000	42,10	0,0090
	Hide4PGP	–1,00	1,00	0,0000	0,0221	69,17	0,0000
	EzStego	–0,20	0,20	0,0000	0.0041	36,21	0,0000
	F5	–4,00	6,00	0,5422	0,9722	36,41	0,0350

Wielkość możliwej do ukrycia informacji z wykorzystaniem metody PS jest w prawdzie mniejsza, ale wiadomość jest bardziej odporna na uszkodzenia podczas przekształcania stegoobrazu.

Informacja ukryta metodą PS była prawidłowo odczytana przy kompresji stratnej obrazu JPEG o współczynniku jakości 100%, powodującej kilkukrotne zmniejszenie wielkości pliku w stosunku do obrazu wejściowego. W przypadku aplikacji porównawczych wyniki były gorsze. Przeprowadzona kompresja powodowała, że dane ukryte za pomocą aplikacji Hide4PGP i F5 nie nadawały się do odczytu, zaś ukryte za pomocą aplikacji EzStego były całkowicie zakłócone, a liczba prawidłowo odczytanych bitów wynosiła około 50%, co odpowiada losowo wygenerowanemu ciągowi bitów.

Testy polegające na dodaniu do obrazu z wiadomością szumu także pokazały wyższość metody PS. Dane ukryte w ten sposób są bardziej odporne na: losowe modyfikacje pikseli za pomocą szumu typu „sól i pieprz", wprowadzanie szumu Gaussa oraz filtrowanie górnoprzepustowe obrazu, co pokazują wartości procentowe skuteczności odczytu wiadomości o długości 5 znaków ASCII przedstawione w tabeli 6. W przypadku algorytmów dołączających do nośnika informację o długości wiadomości podczas procesu ukrywania danych niemożliwe było nawet prawidłowe określenie ilości znaków ukrytych znaków podczas odczytu. Tabela nie zawiera wyników testów dla algorytmu F5 ze względu na to, że każda modyfikacja stegoobrazu w przypadku tego algorytmu uniemożliwiała odczyt ukrytych danych.

Stegoanaliza przeprowadzona na stegoobrazach utworzonych metodą PS i za pomocą aplikacji porównawczych wykazała, że wszystkie badane algorytmy w nieznacznym stopniu modyfikują właściwości statystyczne nośnika podczas ukrywania danych, co uniemożliwia skuteczne wykrycie istnienia informacji ukrytej.

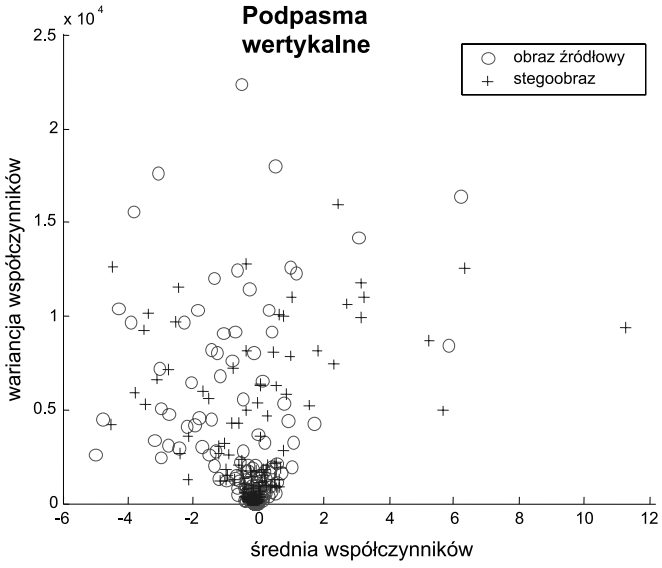
Wykorzystana do stegoanalizy liniowa dyskryminacja Fishera (FLD) nie umożliwiła wykrycia modyfikacji steganograficznych. Badano zmiany w statystykach obrazów, tzn.: zmiany wartości średnich, wariancji, współczynników asymetrii oraz skupienia wyznaczonych na podstawie współczynników transformat falkowych oraz ich liniowej predykcji.

Potwierdza to fakt, że opracowana metoda charakteryzuje się dobrą jakością ukrywania danych porównywalną do pozostałych badanych aplikacji. Badania stegoanalityczne przeprowadzono na dwóch grupach obrazów RGB o rozdzielczości 256 × 256 punktów pochodzących ze zbiorów autorskich oraz z witryny FreeFoto.com. Mimo wykorzystania 400 obrazów z ukrytą informacją i 400 obrazów niemodyfikowanych stanowiących zbiór obrazów uczących algorytmu FLD niemożliwe było prawidłowe sklasyfikowanie obrazów testowych. Z grupy obrazów niemodyfikowanych 98,67% obrazów zostało sklasyfikowanych jako obrazy niemodyfikowane, a 99,33% obrazów z grupy obrazów z ukrytą informacją zostało sklasyfikowanych jako obrazy niemodyfikowane. Wynika to z tego, że wartości cech statystycznych współczynników transformat dla obrazów źródłowych i stegoobrazów pokrywały się, co uniemożliwiało wyznaczenie jednoznacznej granicy pomiędzy klasami cech obrazów źródłowych i stegoobrazów.

Pokrywające się wartości cech klasy obrazów źródłowych i klasy stegoobrazów dla dwóch wybranych cech, tzn. wariancji i wartości średniej współczynników przedstawia wykres rozrzutu na rysunku 9.

Tabela 6
Wartości zniekształceń stegoobrazu na uszkodzenia wiadomości

Obraz (metoda)	Typ uszkodzenia	Wartość parametru	Bity prawidłowe [%]	Odczytane znaki
Pawian (PS)	Szum „sól i pieprz” (parametr: wsp. gęstości szumu)	0,005	100	5
		0,01	100	5
	Szum Gaussa (parametr: wariancja)	0,0001	100	5
		0,0002	100	5
	Filtr dolnoprzepustowy	–	66	5
	Filtr górnoprzepustowy	–	63	5
Pawian (Hide4PGP)	Szum „sól i pieprz”	0,005	100	5
		0,01	91	5
	Szum Gaussa	0,0001	46	40 916
		0,0002	57	32 682
	Filtr dolnoprzepustowy	–	54	7
	Filtr górnoprzepustowy	–	37	30 362
Pawian (EzStego)	Szum „sól i pieprz”	0,005	100	8 192
		0,01	97	8 192
	Szum Gaussa	0,0001	100	8 192
		0,0002	94	8 192
	Filtr dolnoprzepustowy	–	57	8 192
	Filtr górnoprzepustowy	–	34	8 192



Rys. 9. Wykres rozrzutu wartości wariancji i średniej wyliczonej ze współczynników transformat falkowych obrazów źródłowych i stegoobrazów uzyskanych metodą PS, pochodzących ze zbioru 100 obrazów testowych

7. Wnioski

Piramidy filtrów kierunkowych opracowane zostały głównie na potrzeby analizy obrazu i poprawy jego jakości. Jednak jak wykazały przeprowadzone badania, mogą być także z powodzeniem wykorzystane w steganografii.

Opracowana metoda steganograficzna wykorzystująca analizę wielorozdzielczą poprzez zastosowanie filtrów kierunkowych oraz algorytm dołączania do nośnika poufnych danych poprzez dostosowany do przestrzeni transformacji algorytm statystyczny Lee i Chena jest rozwiązaniem nowatorskim i nie stosowanym wcześniej.

Podczas przeprowadzonych badań określono parametry nowej metody steganograficznej i zbadano doświadczalnie dopuszczalne zakresy ich zmienności, co umożliwiło optymalizację ukrywania danych. Wyznaczono m.in. zakres optymalnych wartości rozmiarów bloków współczynników, na które dzielone były podpasma transformaty oraz optymalne liczby podprzedziałów zakresu wartości średnich.

Badania doświadczalne wykazały, że informacje mogą być ukrywane w dowolnie wybranym podpaśmie kierunkowym na dowolnie wybranym poziomie rozdzielczości, dla różnych rozmiarów piramidy, określonych poprzez liczbę poziomów i liczbę podpasm kierunkowych na każdym z nich.

Parametry ukrywania informacji za pomocą opracowanej metody opisuje klucz steganograficzny, bez którego znajomości, jak wykazały przeprowadzone testy, odczyt wiadomości nie jest możliwy. W przypadku badawczym, niewykorzystującym szyfrowania dołączanych informacji, długość klucza określono na 64 bity. Długość ta może zostać jednak zwiększona w przypadku zastosowania wstępnego szyfrowania wiadomości i dodatkowej parametryzacji metody.

Nowa metoda charakteryzuje się wysokim poziomem jakości obrazu wyjściowego określonym m.in. poprzez odstęp sygnału od szumu na poziomie 38 dB. Jakość opracowanej metody steganograficznej została zweryfikowana także na podstawie analizy porównawczej z istniejącymi aplikacjami steganograficznymi.

Badania porównawcze wykazały także przewagę opracowanej metody w przypadku ataków aktywnych na stegoobraz. Ataki polegały na filtrowaniu oraz wprowadzaniu celowych zniekształceń poprzez dodawanie szumu i kompresję stratną JPEG stegoobrazu.

Specyfika opracowanej metody steganograficznej ukrywającej poszczególne bity danych w większych obszarach nośnika uniemożliwiała ukrycie tak dużych ilości informacji, jakie mogły być ukryte za pomocą pozostałych aplikacji porównawczych. Maksymalne długości wiadomości, które mogły być ukryte za pomocą nowej metody w obrazach o rozdzielczości 256 × 256 punktów były różne dla różnych obrazów i wahały się w granicach 300 bitów.

Opracowany algorytm steganograficzny zapewnia także wysoki poziom bezpieczeństwa ukrytej informacji w przypadku stegoanalizy statystycznej. Analiza dyskryminacyjna Fishera pomimo zbioru uczącego składającego się z 800 obrazów nie umożliwia prawidłowego sklasyfikowania obrazów testowych jako modyfikowanych steganograficznie.

Dalsze prace kontynuujące przeprowadzone badania powinny zmierzać w kierunkach:

- wykorzystania opracowanej metody steganografiicznej do obrazów w innych przestrzeniach kolorów,
- zwiększenia pojemności informacyjnej oferowanej przez opracowany,
- wykorzystania innych funkcji posiadających właściwość sterowalności jako cyfrowych filtrów bazowych transformacji sterowalnej,
- weryfikacji możliwości wykorzystania obrazu dynamicznego jako nośnika ukrywanych informacji dla opracowanej metody.

Literatura

[1] Białasiewicz J.T., *Falki i aproksymacje.* Warszawa, Wydawnictwa Naukowo-Techniczne 2004.

[2] Chang L., *Issues in Information Hiding Transform Techniques*. NRL/MR/5540-02-8621, Center for High Assurance Computer Systems (CHACS), Naval Research, 2002.

[3] Freeman W.T., Adelson E.H., *The Design and Use of Steerable Filters.* IEEE Trans. Patt. Anal. and Machine Intell., Vol. 13, No. 9, 1991, 891–906.

[4] Garbarczuk W., Kopniak P., *Steganologia: współczesne metody ochrony informacji (przegląd).* Pomiary Automatyka Kontrola, wydanie specjalne 3/2005, Warszawa, 2005, 21–25.

[5] Garbarczuk W., Świć A. (Kopniak P. – współautor rozdziału III): *Podstawy ochrony informacji.* Lublin, Politechnika Lubelska 2005, 247–307.

[6] Ifeachor E.C., Jervis B.W., *Digital Signal Processing. A Practical Approach.* Second Edition, Pearson Education Limited, 2002.

[7] Katzenbeisser S., Petitcolas F. (eds), *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, 2000.

[8] Kopniak P., *Evaluation of Possibilities of Java Cryptography Architecture and Java Mail Libraries Usage to Encrypt E-Mail Massages.* Annales Universitatis Mariae Curie-Skłodowska, Sectio AI Informatica, vol. II, Lublin, Wydawnictwo UMCS 2004, 379–389.

[9] Kopniak P., *Porównanie odporności na zniekształcenia danych ukrytych w obrazie metodą LSB i metodą modyfikacji widma.* Algorytmy, metody i programy naukowe, redakcja S. Grzegórski, M. Miłosz, P. Muryjas, Lublin, PTI 2004, 101–108.

[10] Kopniak P., *Wykorzystanie transformacji obrazu do przestrzeni częstotliwościowej w steganografi.* VI Międzynarodowe Warsztaty Doktoranckie, OWD 2004 – Wisła, 16–19 października 2004, Archiwum Konferencji PTETiS, vol. 19, 2004, 263–268.

[11] Kopniak P., *Aproksymacja obrazów za pomocą funkcji prostokątnych. Transformacje: Walsha, Hadamarda i Haara.* Varia Informatica. Obliczenia i technologie, Lublin, Polskie Towarzystwo Informatyczne 2005, 33–42.

[12] Kopniak P., *Influence of Lossy Compression on the Data Encoded Using Image Frequency Domain*. Scientific-theoretical magazine "Artificial Intelligence.", No. 2/2005, Donetsk, Ukraine, 2005.

[13] Kopniak P., *The Quantitive Measurement of the Image Distortions.* Actual Problems of Economics, Information Technology in Economics and Management, No. 10(52), Kiev, Ukraine, 2005, 133–140.

[14] Kopniak P., *Zabezpieczenie informacji poprzez jej ukrycie – steganografia i jej narzędzia.* Bezpieczeństwo Informacji – od teorii do praktyki, red. M. Miłosz, MIKOM, 2005, 145–156.

[15] Kopniak P., *Robustness of Data Hidding in Image Fourier Spectrum.* Annales Universitatis Mariae Curie-Skłodowska, Sectio AI Informatica, vol. V, Lublin, Wydawnictwo UMCS 2006, 181–190.

[16] Kopniak P., *Metody cyfrowego przetwarzania sygnałów na potrzeby steganologii komputerowej.* Politechnika Lubelska, 2007 (Rozprawa doktorska).
[17] Kopniak P.: *Steganograficzne wykorzystanie piramid kierowalnych filtrów cyfrowych.* Informatyka Stosowana – Planowanie, Katowice, Polskie Towarzystwo Informatyczne 2007, 47–54.
[18] Lee Y.K., Chen L.H., *A Secure Robust Image Steganographic Model.* Tenth National Conference of Information Security, Hualien, Taiwan, 2000, 275–284.
[19] Pejas M., *Zastosowanie metod odkrywania wiedzy w stegoanalizie.* ENIGMA 2004 – VIII Krajowa Konferencja Zastosowań Kryptografii, Warszawa, 2004.
[20] Simoncelli E.P., Freeman W.T., *The Steerable Pyramid: A Flexible Architecture For Multi-Scale Derivative Computation.* 2nd IEEE International Conference on Image Processing, Washington, DC. vol. III, 1995, 444–447.
[21] Simoncelli E.P., Freeman W.T., Adelson E.H., Heeger D.J., *Shiftable Multi-scale Transforms.* IEEE Trans. Information Theory, vol. 38(2), 1992, 587–607.