JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 8 (2018) 292-297
Wysłane: 2018-06-17
Przyjęte: 2018-06-27

Analiza właściwości metod steganografii odwracalnej

Piotr Zimnicki*, Grzegorz Kozieł
Politechnika Lubelska, Instytut Informatyki, Nadbystrzycka 36B, 20-618 Lublin, Polska

Streszczenie. Steganografia, czyli nauka zajmująca się ukrywaniem informacji w informacji, zyskuje na popularności wraz ze wzrostem znaczenia internetu. Mwtody steganografii odwracalnej, będącej jej częścią, umożliwiają bezstratne odzyskanie zarówno ukrytej wiadomości jak i oryginału jej nośnika. Mają one jednak różne zastosowania i możliwości. Niniejszy artykuł poświęcony jest teoretycznej i praktycznej analizie różnych metod steganografii odwracalnej opracowanych przez badaczy.

Słowa kluczowe: steganografia odwracalna; grafika; dziedzina przestrzenna

*Autor do korespondencji.

Adres e-mail: zimnickipm@gmail.com

Analysis of properties of reversible steganography methods

Piotr Zimnicki*, Grzegorz Kozieł
Institute of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract. Steganography is a science that deals with hiding information in other information, and it's becoming increasingly popular with rapid growth of Internet utilization. Reversible steganography methods allow lossless recovery of not only the message, but the cover image as well. Different methods have different characteristics, and thus different applications. This paper aims to deepen the understanding of selected reversible methods, their strong and weak point, through both theoretical and practical analysis. The comparison of chosen methods is presented in the paper.

Keywords: reversible steganography; graphics; spatial domain

*Corresponding author.

E-mail address: zimnickipm@gmail.com

1. Wstęp

Wraz z postępem informatyzacji, zagadnienie ochrony danych staje się coraz istotniejsze. Choć korzenie steganografii sięgają znacznie głębiej, to jest ona jedną z odpowiedzi na ten problem. Z uwagi na ogromną popularność plików graficznych, metody steganograficzne wykorzystujące obrazy cyfrowe są zdecydowanie najpopularniejsze. Metody steganografii odwracalnej stanowią jedynie część wszystkich metod steganograficznych. Ich cechą charakterystyczną jest możliwość bezstratnego odzyskania nie tylko ukrytej wiadomości, ale również pliku, w którym była ona ukryta. Znajdują one zastosowanie w przypadku danych medycznych, dowodów sądowych, jako kanał ukrytej komunikacji lub jako jedna z metod uwierzytelnienia.

Mnogość potencjalnych zastosowań przyczyniła się, i przyczynia się nadal, do powstania znacznej ilości różnych metod steganografii odwracalnej. Niniejszy artykuł poświęcony jest teoretycznej i praktycznej analizie części tych metod. Ma on na celu umożliwienie ich lepszego zrozumienia, oraz poznania słabych i mocnych stron.

2. Dotychczasowe badania

Steganografia jest nauką stale rozwijaną przez badaczy z całego świata. Każdego roku publikowane są artykuły naukowe, opisujące nowe, bądź udoskonalone, metody ukrywania informacji. Trudno jednak odnaleźć publikację zestawiającąze sobą takie metody. Jedną z nielicznych jest praca Yun Q. Shi zatytuowana *Reversible Data Hiding* [1]. Autor dokonuje podziału metod steganograficznych ze względu na zastosowanie, przy czym wyróżnia trzy kategorie:

a) Uwierzytelnianie wrażliwe, gdzie nawet najmniejsza modyfikacja obrazu jest niedopuszczalna
b) Uwierzytelnianie mniej wrażliwe, enigmatyczne sformułowanie oznaczające uwierzytelnianie, gdzie pewne modyfikacje obrazu, jak na przykład kompresja, są akceptowalne
c) Wymagające wysokiej pojemności informacyjnej, to znaczy umożliwiające ukrycie dużych ilości informacji w obrazie

Tego typu podział jest oczywiście merytorycznie poprawny, jednak nie jest całkowicie wyczerpujący. Autor porusza tutaj temat metod steganograficznych działających na obrazach skompresowanych, co prowadzi nas do innego, bardziej technicznego podziału metod steganografii odwracalnej:

a) Operujące w dziedzinie przestrzennej (*ang. spatial domain*), ukrywające sekretne informacje bezpośrednio w obrazie. Jest to najprostsza, a zarazem najczęściej spotykana technika.

b) Operujące w dziedzinie transformacji (*ang. transform domain*), ukrywające treść wiadomości w częstotliwościach występujących w obrazie. W przypadku obrazów poddanych kompresji JPEG większość metod steganograficznych opiera się na manipulowaniu wartościami współczynników dyskretnej transformaty kosinusowej nośnika.

Interesującym przykładem metod operujących w dziedzinie przestrzennej, są metody oparte o modyfikację histogramu. Na podstawie obrazu-nośnika budowany jest histogram wartości pikseli, w którym to właśnie ukrywana jest wiadomość steganograficzna. Sposób ukrycia wiadomości zależny jest od metody – może opierać się o wartości ekstremalne [2] czy zmiany wartości sąsiadujących pikseli [3]. Jeśli natomiast chodzi o metody operujące w dziedzinie transformacji, to warta wspomnienia jest metoda opracowana przez badaczy z Tajwanu [4]. Używa ona transformaty falkowej do dekompozycji obrazu na poszczególne pasma, ukrywając sekretną wiadomość zarówno w wysokich jak i niskich częstotliwościach. Umożliwia ukrycie dużych ilości informacji i jest wysoce odporna na kompresję, jednak jej słabą stroną jest podatność na zmiany w dziedzinie przestrzennej - drobne manipulacje wartościami pikseli mogą uniemożliwić odczyt wiadomości, jak również odzyskanie oryginalnego medium. Studiując literaturę tematyczną można natknąć się również na inne, bardziej egzotyczne kryteria klasyfikacji metod steganograficznych [5][6]:

a) Techniki rozproszonego widma (*ang. spread spectrum*), stosujące techniki zapożyczone z szerokopasmowych systemów komunikacji. Sekretna wiadomość jest tu kodowana w szerokim spektrum częstotliwości, znacznie utrudniając jej wykrycie, lecz także odzyskanie oryginalnego obrazu.
b) Techniki statystyczne, kodujące informacje poprzez zmianę właściwości statystycznych obrazu, a wykorzystujące proces weryfikacji hipotez do ich odczytania.
c) Techniki oparte o zakłócenia, wstrzykujące w nośnik pewne zniekształcenia, których późniejsze wykrycie i pomiar umożliwia odczytanie wiadomości.

W pewnych sytuacjach bezstratne odzyskanie całego obrazu-nośnika może nie być wymagane. W takich przypadkach pomocne są metody oparte o tak zwany obszar zainteresowania (*ang. region of interest*). Za ich pomocą można odzyskać tylko ten obszar obrazu, który został odpowiednio oznaczony na etapie kodowania. Pozostała część może zostać nieodwracalnie zniekształcona, o czym należy pamiętać używając takich metod. Znajdują one zastosowanie m.in. w obrazach medycznych - z uwagi na charakter takich obrazów oraz wysoką pojemność informacyjną, oferowaną przez te metody [7].

Użycie metod steganograficznych nie oznacza jednak konieczności rezygnacji z innego sposobu zabezpieczania informacji – kryptografii. Metody steganograficzne w żaden sposób nie konfliktują z metodami kryptograficznymi. Część z nich stosuje wręcz szyfrowanie obrazu jako jeden z kroków działania, jeszcze mocniej zabezpieczając ukrytą informację.

3. Algorytmy metod steganografii odwracalnej

Badaniom porównawczym poddane zostały trzy metody, wybrane na podstawie analizy literatury tematycznej. Są one mocno zróżnicowane, dzięki czemu otrzymane wyniki powinny znacznie różnić się od siebie, uwypuklając mocne i słabe strony tych metod.

3.1. Rozszerzanie różnic

Metoda ta została opracowana z myślą o umożliwieniu ukrycia dużych ilości informacji w obrazie[8]. Opiera się ona o pary pikseli *(x, y)*, ich wartość średnią l oraz różnicę ich wartości h.

$$\begin{aligned} l &= \lfloor 0{,}5 \cdot (x + y) \rfloor \\ h &= x - y \\ x &= l + \lfloor 0{,}5 \cdot (h + 1) \rfloor \\ y &= l - \lfloor 0{,}5 \cdot h \rfloor \end{aligned} \tag{1}$$

Wartość h przesuwana jest o jeden bit w lewo (mnożona przez dwa), a najmniej znaczący bit nowej wartości używany jest do ukrycia kolejnego bitu sekretnej wiadomości. Ostatecznie, nowe wartości pikseli obliczane są przy użyciu rozszerzonej różnicy oraz (niezmienionej) wartości średniej. Rozwiązaniem problemu przepełnienia jest w tym wypadku ukrywanie danych tylko w takich parach pikseli, których zmiana nie spowoduje przepełnienia wartości. Macierz wartości binarnych, kodujących informację o ukryciu bitu wiadomości w danej parze, poddawana jest kompresji bezstratnej i ukrywana wraz z właściwą treścią wiadomości. Przykładowy obraz poddany działaniu metody, oraz błędy odczytu po etapie kodowania (t.j. pary ukrywające wiadomość) przedstawia rysunek 1. Sposób doboru par jest właściwie dowolny, o ile jest powtarzalny. Podczas badań pary tworzone będą z następujących po sobie pikseli.

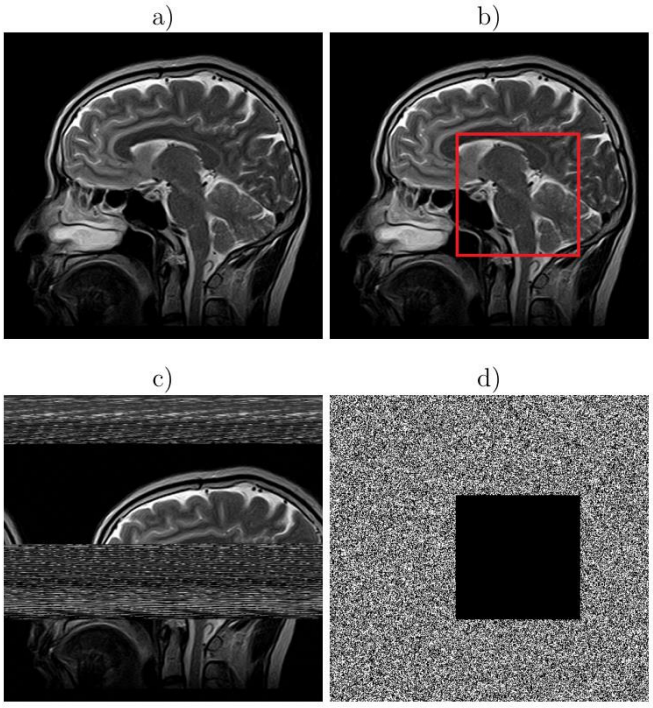
Rys 1 Obraz *clown* oraz błędy odczytu obrazu wynikowego względem oryginalnego po etapie ukrycia wiadomości

Odwracalność modyfikacji obrazu stosowanych w metodzie nie jest na pierwszy rzut oka oczywista – funkcja *podłoga* oznacza bowiem bezpowrotną utratę informacji o części dziesiętnej poddawanych niej liczb. Problem ten występuje jednak tylko pozornie. Zgodnie z falką Haara, działanie to jest odwracalne w obrębie takich par liczb całkowitych [8]. Odwracalność ta, eliminująca błąd zaokrąglenia, wraz z wspomnianą wcześniej macierzą kodującą informację o ukryciu wiadomości gwarantuje odwracalność metody.

3.2. Obszar zainteresowania

Metoda ta została opracowana z myślą o ukrywaniu danych pacjentów w obrazach stworzonych za pomocą rezonansu magnetycznego lub tomografii komputerowej [7]. Nie oznacza to jednak, że jest to jej jedyne możliwe zastosowanie. Fragment obrazu jest tutaj oznaczany jako ROI (*ang. region of interest, obszar zainteresowania*) i tylko tą część będzie można bezstratnie odzyskać. Pozostała część obrazu (*RONI, ang. region of non-interest, obszar braku zainteresowania*) posłuży do ukrycia zakodowanej wiadomości za pomocą algorytmu GLSB [9]. Warto wspomnieć o specjalnym wycinku obszaru RONI, oznaczonym jako krawędź (*ang. border*), znajdującym się na końcu pliku i posiadającym z góry określony rozmiar. Obszar ten zostanie użyty do ukrycia informacji pozwalających na odczytanie zakodowanej wiadomości. Wizualizacja działania algorytmu przedstawiona jest na rysunku 2.

Interesujący jest tu również fakt, że obraz może zostać zaszyfrowany dowolnym kluczem kryptograficznym w sposób niezależny i nie wpływający na możliwość ukrycia czy odczytu wiadomości steganograficznej. Klucz steganograficzny może zostać użyty do odczytania danych steganograficznych bez znajomości klucza kryptograficznego i *vice versa*.



Rys. 2. Wizualizacja algorytmu metody obszaru zainteresowania *a) Przykładowy obraz b) Obraz z wyznaczonym ROI c) Obraz zawierający ukrytą wiadomość d) Błędy odczytu*

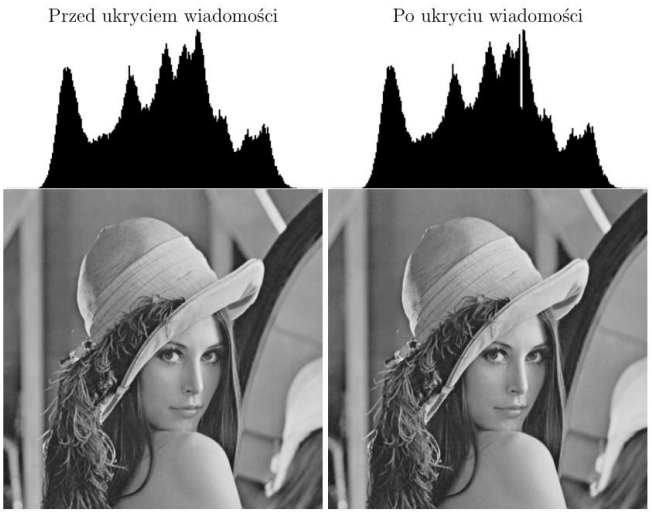
Pierwszym krokiem algorytmu jest określenie obszarów ROI, RONI oraz krawędzi. Należy również wyznaczyć sumę kontrolną ROI, umożliwiającą późniejszą weryfikację poprawności odczytanych danych. Po podziale obrazu następuje jego reorganizacja. Dane dotyczące ROI są usuwane ze swojego oryginalnego miejsca w obrazie i umieszczane na samym początku pliku. Tak przygotowany obraz jest szyfrowany z użyciem szyfru strumieniowego, na przykład za pomocą operacji XOR.

Zaszyfrowany obraz może już posłużyć do ukrycia wiadomości steganograficznej za pomocą metody GLSB [9]. Jest to metoda stratna, ponieważ jednek dane ukryte zostaną jedynie w obszarze RONI - ROI nie zostanie poddane modyfikacji, a więc obszar ten można będzie w całości odzyskać. Wspomniany wcześniej obszar krawędzi nie jest używany do ukrycia treści wiadomości, a do przechowania informacji o położeniu i rozmiarze ROI oraz jego sumie kontrolnej.

3.3. Modyfikacja histogramu

Jest to jedna z pierwszych metod opierających się na histogramie obrazu [2]. Jest kompatybilna z wieloma formatami i typami plików oraz zapewnia dobrą jakość obrazu wynikowego. Umożliwia jednak ukrycie jedynie stosunkowo niewielkich ilości danych.

Warto zaznaczyć, że wszelkie operacje dotyczące modyfikacji wartości histogramu przeprowadzane są bezpośrednio na obrazie. Histogram jest jedynie cechą charakterystyczną obrazu, więc niemożliwa jest jego bezpośrednia modyfikacja. Przykładowo, operacja przesunięcia histogramu w prawo o jedną jednostkę, oznacza zwiększenie wartości każdego piksela obrazu o jeden – po wykonaniu tej operacji histogram obrazu wynikowego będzie przesunięty w prawo, zgodnie z oczekiwaniami.



Rys. 3 Wizualizacja działania metody opartej o modyfikację histogramu

Działanie algorytmu rozpoczyna stworzenie histogramu wartości pikseli obrazu wejściowego, oraz znalezienie występujących w nim ekstremów – minimum i maksimum. W przypadku obrazu *Lena*, widocznego powyżej, wartości te są równe odpowiednio $h(0) = 0$ oraz $h(154) = 2723$. Kolejnym krokiem jest przesunięcie fragmentu histogramu należącego do przedziału (0, 154) w lewo o jedną jednostkę. Spowoduje to powstanie pustej kolumny dla wartości 153, sąsiadującej z wartością maksymalną. Wiadomość steganograficzna może teraz zostać ukryta za pomocą tych

dwóch wartości – każdy kolejny piksel przyjmujący wartość 154 jest zestawiany z kolejnym bitem sekretnej wiadomości, i jeśli wartość bitu równa się jeden wartość piksela zmniejszana jest o jeden.

W przypadku, gdy wartość minimalna jest różna od zera należy zachować współrzędne pikseli osiągających wartość minimalną. Dane te należy później skompresować i dołączyć do ukrytej informacji jako narzut.

Odczyt ukrytej informacji odbywa się w sposób analogiczny, odwracając kierunek i kolejność kroków algorytmu. Aby jednak odczyt jakichkolwiek danych był możliwy adresat musi posiadać odpowiedni klucz steganograficzny. W przypadku tej metody składa się on z informacji o histogramie oryginalnego obrazu, a mianowicie wartości minimalnej i maksymalnej. Rysunek 3 przedstawia wizualizację działania tej metody.

4. Specyfika badań

Ponieważ treść wiadomości ukrywanej w obrazach jest bez znaczenia z punktu widzenia metody będącej obiektem analizy, wiadomość generowana będzie w sposób losowy. Weryfikacji poddana zostanie jedynie integralność danych odzyskanych bezpośrednio z obrazu. Kolejnym czynnikiem wymagającym uwagi jest sam obraz, służący za nośnik treści. Oczywiste jest, że większy obraz może umożliwić ukrycie większej ilości informacji. Aby wyniki były możliwie najbardziej miarodajne, wszystkie obrazy użyte do badań będą miały stałe wymiary, wynoszące 512x512 pikseli. Wszystkie będą również monochromatyczne, co oznacza, że na jeden piksel obrazu przypadać będzie zawsze dokładnie 8 bitów pamięci. Zawartość obrazu może również mieć znaczący wpływ na działanie algorytmów. Aby zniwelować potencjalne oddziaływanie tego czynnika próby prowadzone będą w dwojaki sposób: na pojedynczych, wybranych obrazach, oraz na zbiorze 109 obrazów, zgromadzonych specjalnie w tym celu.

Do badania wpływu metody na jakość obrazu wynikowego posłuży następujący zestaw miar:

- Błąd średniokwadratowy, wyrażony wzorem

$$MSE = \frac{1}{M \cdot N} \cdot \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \left[x_{i,j} - x'_{i,j} \right]^2 \quad (2)$$

- Znormalizowany błąd średniokwadratowy, wyrażony wzorem

$$NMSE = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \left[x_{i,j} - x\prime_{i,j} \right]^2}{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \left[x_{i,j} \right]^2} \quad (3)$$

- Szczytowy stosunej sygnału do szumu, wyrażony wzorem

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE} \quad (4)$$

- Ilość bitów wiadomości na jeden piksel obrazu, wyrażona wzorem

$$\text{bpp} = \frac{\text{Pojemność-Narzut}}{\text{N·M}} \quad (5)$$

Gdzie N oraz M oznaczają wymiary obrazu, natomiast $x_{i,j}$ oraz $x'_{i,j}$ oznaczają odpowiednio kolejne piksele obrazu wejściowego oraz wynikowego. *Pojemnością* z kolei nazywamy całkowitą ilość bitów, które można zakodować w obrazie, a *narzutem* jest ilość bitów które musimy dodatkowo ukryć, aby możliwe było poprawne odzyskanie danych i/lub obrazu. W pewnych sytuacjach może wystąpić sytuacja, że *Narzut* ≥ *Pojemność* – przypadki takie będą pomijane, gdyż nie będzie możliwe zastosowanie danej metody. Współczynnik *bpp* wynosi tutaj zero. Dodatkowej ocenie poddana zostanie również wizualna jakość obrazu. Będzie ona całkowicie subiektywna i nie podlegająca żadnej standaryzacji, a jednak niezbędna.

5. Wyniki

Tabela 1. Średnie wyniki pomiarów po zastosowaniu metody rozszerzania różnic dla dużej próby

Mierzony parametr	**Wartość**
MSE	41,0115
NMSE	0,288%
PSNR	33,825
Pojemność	124939
Narzut	12000
Bpp	0,43083

Metoda oparta o rozszerzanie różnic umożliwia ukrycie znaczących ilości danych, osiągając średni poziom *bpp = 0,43083*, co jest wynikiem bardzo dobrym. Niestety, okazała się też najgorsza pod względem jakości obrazu. Jakość jest tu bowiem mocno powiązana z charakterystyką danego nośnika informacji. Rozszerzanie różnic może wprowadzić znaczne zakłócenia w przypadku par o dużym gradiencie wartości pikseli. Problem ten pojawia się zwłaszcza w obrazach, zawierających zmiany wysokiej częstotliwości. Rozwiązaniem pozwalającym na jego zniwelowanie może być inny sposób tworzenia par, oparty na przykład o generator liczb pseudolosowych zainicjowany znanym ziarnem,. Każdy przypadek należy jednak rozpatrywać indywidualnie. Wizualna jakość obrazu jest dobra, choć różnice między obrazem początkowym a steganograficznym są czasami zauważalne. Wyniki pomiarów dla tej metody przedstawia tabela 1.

Tabela 2. Średnie wyniki pomiarów po zastosowaniu metody modyfikacji histogramu dla dużej próby

Mierzony parametr	**Wartość**
MSE	0,5105
NMSE	0,006%
PSNR	52,258
Pojemność	16011
Narzut	223
Bpp	0,06023

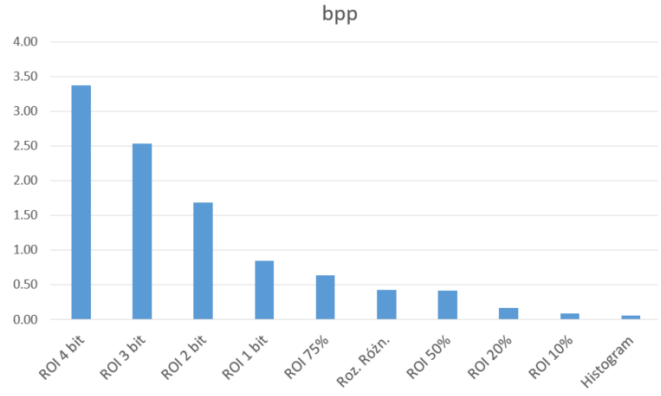
Metoda modyfikacji histogramu, której wyniki przedstawia tabela 2, osiągnęła najmniejszą pojemność spośród badanych metod, jednak jest to zgodne z oczekiwaniami. Powstała ona z myślą o ukrywaniu niewielkich ilości informacji, zachowując przy tym wysoką jakość obrazu wynikowego. Rzeczywiście, metoda ta zapewnia najlepszą spośród badanych metod jakość obrazu, w tym również wizualną. Jakość ta jest jednak zależna od

charakterystyki obrazu, t.j. od odległości dzielącej minimalną oraz maksymalną wartość histogramu. Minimalizacja tej odległości, o ile w danym przypadku jest to możliwe, zmniejszy ilość zakłóceń wprowadzanych przez algorytm, co zaowocuje poprawą jakości. Problem niskiej pojemności zapewnianej przez metodę można częściowo zniwelować poprzez wielokrotne kodowanie informacji w tym samym obrazie. Każda kolejna iteracja zwiększy długość ukrytej wiadomości, jednak za cenę jakości obrazu.

Tabela 3. Średnie wyniki pomiarów po zastosowaniu metody ROI dla dużej próby

Mierzony parametr	**Wartość**
MSE	0,4221
NMSE	0,004 %
PSNR	51,876
Pojemność	221120
Narzut	0
Bpp	0,84351

Metoda oparta o obszar zainteresowania osiąga niemal tak wysoką jakość, co metoda modyfikacji histogramu, zapewniając jednocześnie znacznie wyższą pojemność. Ceną za to jest brak całkowitej odwracalności – odzyskać można tu bowiem jedynie wskazany uprzednio fragment nośnika.

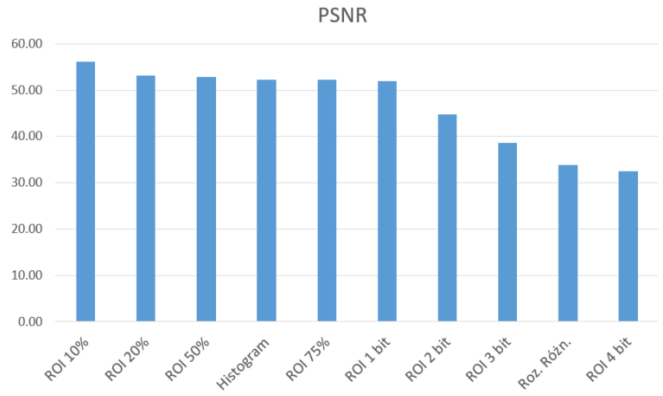


Rys. 4 Średnie wyniki *bpp* osiągane przez poszczególne metody i ich warianty

Metoda okazała się całkowicie niewrażliwa na obraz i jego cechy charakterystyczne. Dodatkowo, użycie krótszej niż jest to możliwe wiadomości (t.j. niewykorzystanie całego dostępnego miejsca) pozytywnie wpłynie na jakość. Dzięki zmianie liczby najmniej znaczących bitów odpowiedzialnych za zapis informacji przez algorytm GLSB, o który opiera się metoda obszaru zainteresowania, można umożliwić ukrycie jeszcze dłuższej wiadomości steganograficznej. Każdy kolejny bit użyty do zapisu informacji spowoduje liniowy wzrost pojemności. Dla badanych obrazów, zapisujących wartość pikseli za pomocą 8 bitów, użycie dwóch najmłodszych bitów nie wpłynie znacząco na pogorszenie jakości obrazu wynikowego. Użycie każdego kolejnego bitu znacząco wpłynie na jakość, przy czym zastosowanie więcej niż czterech okazuje się wysoce niepraktyczne, powodując zbyt duże zniekształcenia.

Zestawienie średnich wyników pomiarów dla poszczególnych metod i ich wariantów przedstawia tablea 4.

Jeśli chodzi o maksymalną długość wiadomości, przedstawioną na rysunku 4, metoda oparta o obszar zainteresowania okazała się bezkonkurencyjna. Co więcej, umożliwia ona dalsze zwiększenie pojemności poprzez zwiększenie liczby bitów, użytych do ukrycia wiadomości steganograficznej. Najgorsza okazała się metoda modyfikacji histogramu, przy czym jest to wynik zgodny z oczekiwaniami.



Rys. 5. Średnie wyniki *PSNR* osiągane przez poszczególne metody i ich warianty

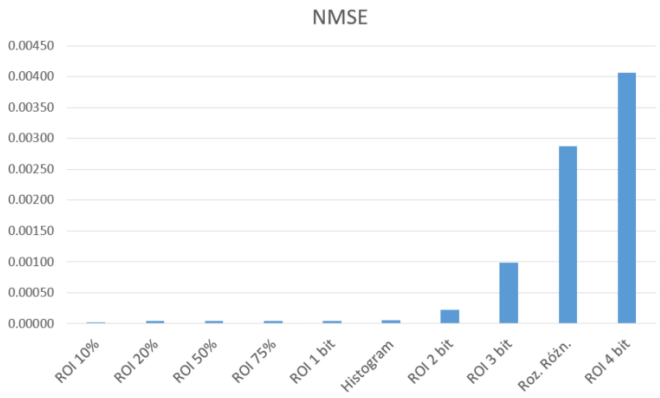
Tabela 4. Średnie wartości pomiarów dla poszczególnych metod i ich wariantów

Metoda	**bpp**	**PSNR**	**NMSE**
Roz. Różn.	0,43083	33,825	0,288%
Histogram	0,06023	52,258	0,006%
ROI 10%	0,08435	56,258	0,002%
ROI 20%	0,16870	53,107	0,004%
ROI 50%	0,42175	52,878	0,004%
ROI 75%	0,63263	52,247	0,004%
ROI 1 bit	0,84351	51,876	0,004%
ROI 2 bit	1,68701	44,831	0,023%
ROI 3 bit	2,53052	38,606	0,098%
ROI 4 bit	3,37402	32,508	0,406%

Szczytowy stosunek sygnału do szumu, przedstawiony na rysunku 5, okazał się najwyższy dla metody modyfikacji histogramu. Jednak w przypadku, gdy za pomocą metody obszaru zainteresowania ukryjemy wiadomość krótszą niż jest to możliwe, wykorzystując jedynie część dostępnego miejsca, możliwe jest osiągnięcie lepszych rezultatów. Przyjmując wykorzystanie dostępnego miejsca na poziomie 10%, co daje średni poziom *bpp* zbliżony do wyniku metody modyfikacji histogramu, metoda ROI osiąga lepszą jakość. Metoda oparta o rozszerzanie różnic osiągnęła tu najgorsze wyniki.

W przypadku znormalizowanego błędu średniokwadratowego, przedstawionego na rysunku 6, metoda modyfikacji histogramu oraz metoda obszaru zainteresowania osiągnęły bardzo zbliżone rezultaty. Wynika to bezpośrednio ze sposobu ich działania – wartość dowolnego piksela nośnika jest tu bowiem modyfikowana co najwyżej o 1. Użycie więcej niż jednego najmniej znaczącego bitu przez metodę ROI drastycznie zwiększa poziom błędu średniokwadratowego. Ponownie, najgorsza okazała się metoda rozszerzania różnic - może ona bowiem wprowadzać

duże zakłócenia w obrębie dobranych par, co znacznie zwiększa błąd.



Rys. 6. Średnie wyniki *NMSE* osiągane przez poszczególne metody i ich warianty

6. Podsumowanie

Wszystkie trzy wybrane metody udało się skutecznie zaimplementować. Zgodnie z oczekiwaniami każda z nich umożliwia ukrycie sekretnej wiadomości steganograficznej we wskazanym obrazie, oraz późniejszy bezbłędny odczyt zarówno wiadomości jak i jej nośnika – zgodnie z charakterystyką metody. Otrzymane wyniki różnią się od siebie nie tylko pomiędzy metodami, ale nawet w obrębie jednej metody. Okazuje się, że poszczególne metody są w różnym stopniu wrażliwe na cechy charakterystyczne samego obrazu, będącego nośnikiem informacji.

Na podstawie przeprowadzonych badań można wnioskować, że metoda oparta o obszar zainteresowania umożliwia ukrycie największej ilości informacji. Jeśli chodzi o jakość obrazu, metoda modyfikacji histogramu uzyskała najlepsze wyniki, przy czym metoda ROI nie pozostaje daleko w tyle. Wizualna jakość obrazów otrzymanych za pomocą wszystkich trzech metod jest bardzo dobra.

Metoda oparta o obszar zainteresowania okazała się najciekawsza pod względem badawczym, umożliwiając uzyskanie drastycznie różnych wyników poprzez modyfikację odpowiednich parametrów. Użycie więcej niż jednego bitu do zapisu treści wiadomości steganograficznej skutkuje liniowym wzrostem pojemności informacyjnej.

Metoda oparta o rozszerzanie różnic okazała się niezwykle wrażliwa na pewne cechy charakterystyczne obrazu, a mianowicie na zmiany wysokiej częstotliwości. Problem ten można jednak zniwelować stosując alternatywny sposób tworzenia par – na przykład w oparciu o algorytm generujący ciąg liczb pseudolosowych. Występuje on jednak stosunowo rzadko, a każdy taki przypadek wymaga indywidualnego podejścia.

Literatura

[1] Y. Shi. Reversible data hiding, *Department of Electrical and Computer Engineering, New Jersey Institute of Technology*, 2005.

[2] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari. Reversible data hiding, *IEEE Transaction on Circuits and Systems for Video Technology*, 16, 2006.

[3] Chia-Chen Lin, Wei-Liang Tai, Chin-Chen Chang. Multilevel reversible data hiding based on histogram modification of difference images, *Pattern Recognition*, 41, 2008.

[4] Ching-yu Yang, Chih-Hung Lin, Wu-Chih Hu. Reversible data hiding for high quality images based on integer wavelet transform, *Journal of Information Hiding and Multimedia Signal Processing*, 2, 2012.

[5] C.P. Sumathi, T. Santanam, G. Umamaheswari. A study of various steganographic techniques used for information hiding, *International Journal of Computer Science and Engineering Survey*, 4, 2013.

[6] Divya .A, S. Thenmozhi. Steganography: Various techniques in spatial and transform domain, *International Journal of Advanced Scientific Research and Management*, 1, 2016.

[7] Yuling Liu, Xinxin Qu, Goujiang Xin. A ROI-based reversible data hiding scheme in encrypted medical images, *Journal of Visual Communication and Image Representation*, 39, 2016

[8] J. Tian. Reversible data embedding using a difference expansion, *IEEE Transaction on Circuits and Systems for Video Technology*, 13, 2003

[9] Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp. Reversible data hiding, *International Conference on Image Processing*, 2, 2002