Marek R. OGIELA, Katarzyna KOPTYRA
AGH AKADEMIA GÓRNICZO-HUTNICZA W KRAKOWIE
30-059 Kraków, Al. Mickiewicza 30

Porównanie wybranych algorytmów steganografii cyfrowej

Prof. dr hab. Marek R. OGIELA

Profesor zwyczajny na Akademii Górniczo – Hutniczej w Krakowie. Prowadzi badania nad kognitywnymi systemami informacyjnymi nowej generacji, a także kryptografią i podziałem sekretów. Jest członkiem wielu renomowanych towarzystw naukowych, a także autorem ponad 250 publikacji o zakresie międzynarodowym.

e-mail: mogiela@agh.edu.pl

Mgr inż. Katarzyna KOPTYRA

Doktorantka na kierunku informatyka na AGH i pracownik naukowo-dydaktyczny UP w Krakowie. Specjalista w zakresie technik steganografii cyfrowej. Ponadto prowadzi badania nad bezpieczeństwem systemów komputerowych.

e-mail: kkoptyra@agh.edu.pl

Streszczenie

W artykule opisano techniki steganografii cyfrowej służące do ukrywania informacji w plikach obrazowych i dźwiękowych. Porównano najważniejsze cechy wpływające na bezpieczeństwo oraz praktyczne wykorzystanie tych metod. Przedstawione algorytmy znajdują zastosowanie przede wszystkim w tajnej komunikacji. Wskazano jednak na potencjał łączenia steganografii z kryptografią i innymi metodami ochrony danych.

Słowa kluczowe: steganografia cyfrowa, ukrywanie informacji, tajna komunikacja.

Comparison of selected methods of digital steganography

Abstract

Information security plays significant role in personal and business data exchange. Digital steganography is appropriate solution in the case where undetectability of communication is required. This paper presents selected methods of image and audio steganography. First, the general schema of steganographic system and its most important properties are outlined. Next section, which describes image steganography techniques, is split into algorithms hiding data in particular pixels and in image colour palettes. This categorization is determined by file format, e.g. palettes are present only in indexed images. Audio steganography section contains a detailed description of methods dedicated to embedding data in audio samples or file structure. In the summary the main features of selected algorithms are compared to show differences in security level, usefulness and complexity of implementation. Steganography has many practical applications and can be used with cryptography or separately. The paper suggests possible directions of future studies, including combining steganography with biometric techniques in order to provide additional layer of data protection.

Keywords: digital steganography, information hiding, secret communication.

1. Wstęp

Bezpieczeństwo informacji jest ważnym zagadnieniem, które ma wpływ na funkcjonowanie nie tylko pojedynczych osób, ale całych instytucji, przedsiębiorstw, a nawet krajów. Niemal od zawsze istniała potrzeba ukrywania danych lub ich ochrony przed nieuprawnionym dostępem, do czego wykorzystywano techniki nie tylko kryptografii, ale także steganografii. Na przestrzeni wieków opracowano wiele metod tajnej komunikacji, które ewoluowały i były doskonalone wraz z rozwojem technologii komputerowych, a obecnie umożliwiają niewidoczny przekaz danych w postaci cyfrowej [9].

Ponieważ rozmaite treści i dane są obecnie przechowywane cyfrowo, zatem właśnie ta forma zabezpieczania informacji stała się niezwykle popularna i jest nawet przedmiotem badań naukowych [3]. Proponowane są coraz to nowsze techniki stenograficzne mogące często być stosowane wspólnie z kryptografią (kanał podprogowy w podpisach cyfrowych, podział sekretu wizualnego etc.). Wiele powstających algorytmów steganograficznych wykorzystuje pliki multimedialne, co ze względu na ich dużą objętość stwarza możliwość ukrywania danych o znacznej objętości informacyjnej.

Gwałtowny wzrost zainteresowania omawianą dziedziną nastąpił z dwóch powodów. Pierwszym z nich było zwrócenie uwagi na cyfrowe znaki wodne, które w praktycznych zastosowaniach mogą posłużyć do oznaczenia autorstwa plików multimedialnych lub umieszczenia w nim konkretnych informacji autorskich. Drugą przyczyną były próby ograniczania stosowania kryptografii przez niektóre rządy. Zmotywowało to osoby dbające o własną prywatność do poszukiwania innych metod ochrony danych. Dawne ograniczenia w używaniu steganografii głównie do ukrywania informacji strategicznej uległy zmianie i obecnie można spotkać wiele zastosowań komercyjnych dla takich metod.

Niniejsza publikacja ma przybliżyć, czym jest nowoczesna steganografia, zaprezentować różne metody ukrywania danych w nośnikach cyfrowych, a także przedstawić dokładną analizę wybranych metod.

2. Charakterystyka metod steganografii cyfrowej

Steganografia jest nauką zajmującą się ukrywaniem informacji przed osobami postronnymi. Jej głównym celem jest zapewnienie bezpieczeństwa komunikacji między nadawcą i odbiorcą w taki sposób, aby sam fakt porozumiewania się nie został wykryty. Odbywa się to najczęściej poprzez przesłanie sekretnej treści umieszczonej w innej, nie wzbudzającej podejrzeń wiadomości.

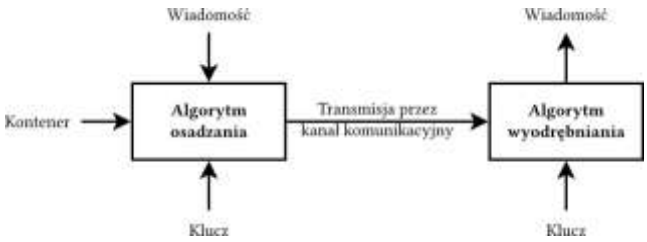
Stosowanie steganografii nie chroni przed odczytaniem tajnej treści, ale ukrywa jej istnienie. W niektórych zastosowaniach ma to ogromne znaczenie. Przechwycenie zaszyfrowanej wiadomości, nawet w przypadku braku możliwości złamania szyfru, daje wiedzę o tym, że komunikacja ma miejsce, co samo w sobie jest cenną informacją. Z tego względu użycie steganografii może chronić przed pewnymi zagrożeniami, jak np. próby wymuszenia wyjawienia kluczy kryptograficznych lub sposoby rekonstrukcji sekretu. Zatem naukę tę można traktować jako narzędzie służące ochronie informacji i prywatności.

Obecnie powstaje wiele nowoczesnych algorytmów, jednak wszystkie oparte są na wspólnym założeniu zwanym problemem więźniów. Ten najbardziej znany problem steganograficzny został opisany przez Simmonsa [8].

Podstawowymi elementami każdego systemu steganograficznego są:
1. Wybór kontenera (medium służącego do komunikacji),
2. Algorytmy osadzania i wyodrębniania tajnej informacji,
3. Zarządzanie kluczami steganograficznymi (informacje niezbędne do osadzenia danych w kontenerze jak również ich odzyskania).

W skład systemu steganograficznego wchodzą algorytmy osadzania i wyodrębniania. Pierwszy z nich przyjmuje na wejściu wiadomość, kontener oraz klucz i na ich podstawie generuje obiekt z ukrytą treścią. Jest on następnie transmitowany do odbiorcy, który podaje klucz oraz otrzymany plik na wejście algo-

rytmu wyodrębniania. W rezultacie otrzymuje wiadomość wysłaną przez nadawcę. Ogólny schemat systemu steganograficznego został przedstawiony na rysunku 1.



Rys. 1. Schemat systemu steganograficznego [3]
Fig. 1. General schema of steganographic system

Algorytm można uznać za bezpieczny, jeśli nie można odróżnić czystego kontenera od takiego, w którym została osadzona wiadomość. Na jakość systemu steganograficznego składa się kilka cech:

- ilość przenoszonych informacji (pojemność),
- niewykrywalność steganogramu określana za pomocą:
  - *niewykrywalności sensorycznej* (trudność rozpoznania zmian kontenera za pomocą ludzkich zmysłów),
  - *niewykrywalności statystycznej* (możliwość detekcji steganogramu poprzez analizę statystycznych własności przesyłanych treści),
- odporność na modyfikację.

Do najpopularniejszych mediów steganograficznych należą: tekst, obraz, dźwięk, sekwencje wideo oraz pakiety transmisji sieciowych. Trzeba jednak podkreślić, że każdy plik może być potencjalnym nośnikiem sekretnej wiadomości, w związku z czym wiele metod ukrywania danych wykorzystuje mniej typowe kontenery takie jak dokumenty HTML, TeX, metapliki torrent, a nawet pliki wykonywalne programów.

3. Techniki steganografii obrazowej

Ze wszystkich rodzajów steganografii cyfrowej najpopularniejsza jest steganografia obrazowa. Dzieje się tak, ponieważ pliki graficzne stanowią dużą część ogółu wymienianych w Internecie informacji oraz są relatywnie duże, przez co łatwiej w nich ukryć dowolne dane nawet o dużym rozmiarze. Poniżej zostaną opisane dwie podstawowe kategorie steganografii obrazowej: techniki ukrywające informacje w pikselach oraz w paletach kolorów.

3.1. Metody operujące na pikselach

Najpowszechniejszym sposobem ukrywania informacji w obrazach cyfrowych jest osadzenie przekazu bezpośrednio w pikselach. W obrazach kolorowych korzystających z modelu RGB każda barwa jest kombinacją trzech składowych: czerwonej (red), zielonej (green) i niebieskiej (blue). Najczęściej piksel zapisywany jest jako liczba 24-bitowa, po 8 bitów na każdą składową. Fakt ten jest wykorzystywany w wielu technikach steganograficznych. Podstawowym algorytmem należącym do tej grupy jest LSB (leastsignificant bit) ukrywający sekretną informację w najmniej znaczących bitach.

W metodzie tej statystycznie w 50% przypadków (pikseli) konieczna jest modyfikacja wartości. Ponieważ nowa i stara wartość różnią się tylko na ostatniej pozycji, każda ze składowych może zostać zmieniona maksymalnie o 1, co jest niemożliwe do wykrycia dla ludzkiego oka.

Wyodrębnianie przekazu jest realizowane poprzez odczytanie najmniej znaczących bitów, a następnie przekształceniu otrzymanego ciągu do pożądanej reprezentacji.

Pojemność tej metody to 12,5% rozmiaru nośnika. W niektórych przypadkach do ukrycia informacji można użyć większej liczby bitów z każdego bajtu barwy składowej, co zwiększa dopuszczalny maksymalny rozmiar ukrywanej wiadomości. Sprawia to jednak, że konieczny jest dobór obrazu o odpowiednio zróżnicowanej kolorystyce. Na rysunku 2 przedstawiono przykład oryginalnego kontenera (2a) oraz rezultat działania algorytmu przy wykorzystaniu jednego bitu (2b) oraz dwóch bitów (2c).

a) czysty kontener

b) LSB z użyciem 1 bitu

c) LSB z użyciem 2 bitów

Rys. 2. Przykład algorytmu LSB
Fig. 2. Example of LSB techniqueapplication

Oczywiście nie każdy nośnik jest odpowiedni dla techniki LSB. Wynika to z faktu, że po osadzeniu wiadomości, najmniej znaczące bity w sposób przypadkowy przyjmują wartości 0 i 1. Tymczasem w rzeczywistych obrazach zdarzają się sytuacje, gdy duże obszary występują w jednolitym kolorze. Jest to dobrze widoczne w bardziej znaczących bitach, ale niektóre obrazy wykazują takie własności dla wszystkich bitów, również najmniej znaczących. Przykład kontenera, w którym nastąpiła znaczna zmiana w stosunku do stanu początkowego został zaprezentowany na rysunku 3.

Do zalet opisywanej metody należą prostota implementacji, małe zniekształcenia wprowadzane do nośnika oraz brak zmiany rozmiaru pliku – żadne dodatkowe informacje nie są wprowadzane do obrazu, a jedynie następuje modyfikacja istniejących pikseli. Najpoważniejszą wadą jest łatwość wykrycia. Programy służące do steganalizy są w stanie odkryć statystyczne anomalie objawiające się zmianą kształtu histogramu obrazu, czego przykład zaprezentowano na rysunku 4.

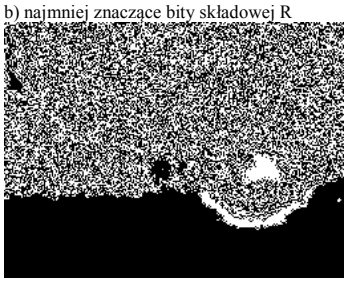
Algorytm ±1 [2] jest rozszerzeniem poprzednio omawianej metody próbującym ograniczyć jej wady. Aby zaradzić powstawaniu anomalii w histogramie, proces osadzania wiadomości przebiega następująco:

$$p_s = \begin{cases} p_c + 1, & gdy \quad b \neq LSB(p_c)\ i\ (\kappa > 0 \text{ lub } p_c = 0) \\ p_c - 1, & gdy \quad b \neq LSB(p_c)\ i\ (\kappa < 0 \text{ lub } p_c = 255) \\ p_c, & gdy \quad b = LSB(p_c) \end{cases} \quad (1)$$

gdzie p_s i p_c oznaczają wartość piksela w wynikowym obrazie i w kontenerze, b to bit wiadomości, a κ jest zmienną losową ze zbioru $\{-1, +1\}$.

a) oryginalny obraz

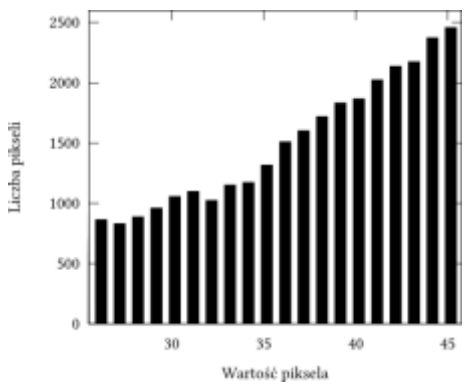
b) najmniej znaczące bity składowej R



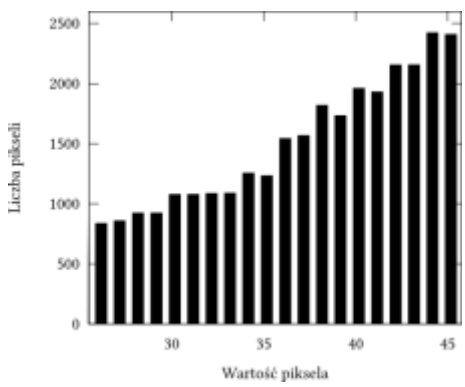
c) LSB składowej R po osadzeniu wiadomości

Rys. 3. Algorytm LSB
Fig. 3. LSB technique

a) czysty kontener



b) obraz z wiadomością osadzoną metodą LSB



Rys. 4. Fragment histogramu składowej R obrazu z rysunku 2
Fig. 4. Histogram of Red component of image presented in Fig. 2

Zatem jeśli wymagana jest modyfikacja najmniej znaczącego bitu, jego wartość jest losowo zmieniana o 1. W rezultacie parzysty piksel zostanie przekształcony w nieparzysty większy lub mniejszy o 1. Analogiczne postępowanie zostanie przeprowadzone dla piksela nieparzystego. Wyjątkiem od tej reguły są wartości graniczne, tj. 0 i 255, które nie mogą przekroczyć zakresu wartości jednego bajtu. Są więc one taktowane następująco. Jedyne dopuszczalne przekształcenia to $0 \rightarrow 1$ i $255 \rightarrow 254$ i jeśli zajdzie konieczność, są one wykonywane niezależnie od wartości κ. Ponieważ nie występuje tu asymetria z algorytmu LSB, zmiany w histogramie są znacznie łagodniejsze. Z drugiej strony możliwa jest modyfikacja innych niż ostatnia pozycji w bajcie (np. $127 \rightarrow 128$, czyli $01111111 \rightarrow 10000000$).

Wyodrębnianie wiadomości jest identyczne jak w metodzie LSB. Przykład obrazu z informacją ukrytą za pomocą techniki ±1 został zaprezentowany na rysunku 5.

a) oryginalny obraz

b) obraz z ukrytą wiadomością

Rys. 5. Przykład działania algorytmu ±1
Fig. 5. Example of algorithm ±1

Omawiany algorytm charakteryzuje się podobnymi cechami co LSB – ma identyczną pojemność i podobną złożoność. Rozmiar obrazu również jest niezmienny, a wprowadzane zmiany nie są widoczne gołym okiem. Wykrycie sekretnego przekazu jest trudniejsze, ale są opracowywane metody steganalizy radzące sobie z tym zadaniem, na przykład w pracy [2].

Poważną słabością przedstawionych algorytmów jest zapis tajnej informacji w sposób sekwencyjny. W dużym stopniu ułatwia to steganalizę i nawet gdy wiadomość jest zaszyfrowana, często można oszacować jej rozmiar. Użycie współdzielonego klucza rozwiązuje ten problem, ale wymusza ustalenie wspólnego sekretu, co nie zawsze jest możliwe. Z tego względu zaproponowana została metoda, która bazuje na LSB i ukrywa dane tylko w niektórych pikselach [6].

Przedstawiana technika znajduje piksel, który występuje najczęściej bez uwzględnienia najmniej znaczącego bitu. Oznacza to, że podczas przeszukiwania branych jest pod uwagę tylko 7 pierwszych bitów każdej składowej. Wydzielone piksele służą następnie do osadzania wiadomości w identyczny sposób jak w metodzie LSB. Aby wyodrębnić przekaz, ponownie należy zlokalizować piksele występujące z największą częstotliwością i odczytać z nich ostatnie bity. Jest to możliwe, ponieważ wyszukiwanie nie uwzględnia fragmentów modyfikowanych w procesie osadzania.

Dostępną pojemność i niewykrywalność trudno jest oszacować, ponieważ te cechy są zależne od wybranego nośnika. Obrazy bardzo zróżnicowane, gdzie najczęstszy piksel występuje niewielką ilość razy, cechują się znacznie ograniczonym maksymalnym rozmiarem wiadomości. Natomiast w przypadku, gdy jeden kolor

jest ulokowany na dużym obszarze, rezultat jest podobny jak w algorytmie LSB.

Możliwe są modyfikacje prezentowanej techniki zwiększające jej praktyczność, jak np. wykorzystanie dwóch najczęściej pojawiających się kolorów lub wyznaczenie liczby n i ukrywanie danych w co n pikselu. Wpływa to pozytywnie na bezpieczeństwo, gdyż rozmieszczenie takich pikseli jest przeważnie zbliżone do losowego.

Odmiennym podejściem wykorzystywanym w steganografii obrazowej jest tworzenie fraktali (obiektów samopodobnych) [10]. Ponieważ takie metody są metodami generacyjnymi, nie jest potrzebny żaden zewnętrzny kontener. Proces osadzania jest zdefiniowany w poniższy sposób.

Algorytm 1. Algorytm osadzania

Wejście: a, b – wymiary obrazu, p, q – parametry wejściowe, R – maksymalny promień, T – maksymalny czas
Wyjście: obraz o wymiarach $a * b$

1. $x_{min} = -1.5$, $y_{min} = -1.5$, $x_{max} = 1.5$, $y_{max} = 1.5$
   $\Delta x = (x_{max} - x_{min}) / (a - 1)$
   $\Delta y = (y_{max} - y_{min}) / (b - 1)$
   Wykonaj kroki 2–4 dla wszystkich punktów (n_x, n_y),
   gdzie $n_x = 0,1,..., a-1$ i $n_y = 0,1,..., -1$.
2. $x_0 = x_{min} + n_x \, x \, \Delta x$,
   $y_0 = y_{min} + n_y \, x \, \Delta y$,
   $t = 0$.
3. $x_{t+1} = x_t^2 - y_t^2 + p$,
   $y_{t+1} = 2x_t y_t + q$,
   $t = t + 1$.
4. $r = x^2 + y^2$
   a. Jeżeli $r > R$ i $t < T$, pobierz jeden bit wiadomości.
      Jeśli jest on równy 0, ustaw wartość piksela (n_x, n_y)
      na kolor pierwszoplanowy.
      W przeciwnym razie piksel przyjmuje kolor tła.
      Przejdź do kroku 2.
   b. Jeżeli $t = T$, piksel (n_x, n_y) przyjmuje kolor tła.
      Przejdź do kroku 2.
   c. Jeżeli $r < R$ i $t < T$, przejdź do kroku 3.

Wyodrębnianie jest realizowane podobnie do osadzania. Zostało ono opisane algorytmem 2.

Algorytm 2. Algorytm wyodrębniania

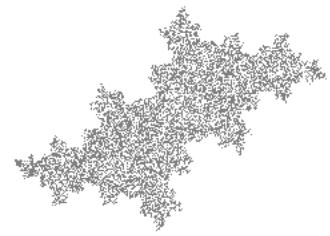
Wejście: obraz o wymiarach a, b, p, q – parametry wejściowe, R – maksymalny promień, T – maksymalny czas
Wyjście: tajna wiadomość

1. Wykonaj kroki 1–3 algorytmu 1.
2. $r = x^2 + y^2$
   a) Jeżeli $r > R$ i $t < T$, pobierz kolor punktu (n_x, n_y)
      i porównaj z wartością piksela obrazu.
      Jeśli są równe, bit wiadomości wynosi 0;
      w przypadku, gdy się różnią, bit sekretu wynosi 1.
   b) Jeżeli $t = T$, kolor punktu (n_x, n_y) jest ignorowany.

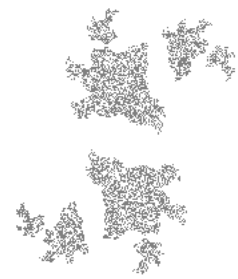
Odbiorca może więc odczytać wiadomość poprzez porównanie różnic między otrzymanym obrazem a fraktalem wygenerowanym z takimi samymi warunkami początkowymi. Ponieważ niezbędne jest podanie identycznych parametrów jak przy osadzaniu, są one traktowane jako klucz, który musi być współdzielony między uczestnikami. Przykład obrazów wygenerowanych z zastosowaniem opisywanej techniki został przedstawiony na rysunku 6.

Pojemność takich metod jest zależna od rozmiaru fraktala, a tym samym od warunków początkowych. Z tego względu nie można oszacować jej szczegółowo bez znajomości tych parametrów. Wiadome jest natomiast, że każdy piksel należący do fraktala koduje 1 bit informacji. Metoda bardzo dobrze sprawdza się do ukrywania losowych danych. Jeśli sekretna wiadomość jest krótsza niż maksymalna pojemność, pozostałe obszary zostaną zapełnione w sposób przypadkowy. Napastnik nie jest więc w stanie określić, czy w danym obrazie ukryta jest losowa treść, czy też nie. Na wysoką niewykrywalność tej techniki składa się również spełnienie zasady Kerckhoffsa mówiącej, że bezpieczeństwo powinno opierać się na kluczu. Bez znajomości parametrów startowych nie można wygenerować fraktala o takich samych własnościach, zatem praktycznie eliminuje to próby ataku ze stegosystemem.

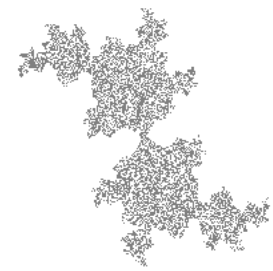
a) $p = -0.394$, $q = 0.606$



b) $p = 0.394$, $q = 0.406$



c) $p = 0.192$, $q = -0.606$



Rys. 6. Fraktale z osadzoną tajną wiadomością ($R = 400$, $T = 15$)
Fig. 6. Fractals with hidden message ($R = 400$, $T = 15$)

3.2. Metody operujące na paletach kolorów

Jako nośnik steganograficzny mogą posłużyć także obrazy indeksowane, np. gif. Zawierają one paletę kolorów o maksymalnym rozmiarze 256. Piksele nie przechowują informacji o swojej barwie, tylko indeks odwołujący się do pozycji w palecie. Dzięki temu możliwe jest zmniejszenie wielkości pliku, jednak kosztem ograniczenia dostępnych kolorów.

Obrazy w innych trybach mogą zostać przekształcone do indeksowanych bez straty jakości, jeśli mają nie więcej niż 256 kolorów. W przeciwnym razie konieczna jest redukcja polegająca na usunięciu niektórych barw z palety. Do pikseli, które zawierały skasowane indeksy, powinny zostać przypisane kolory najbardziej zbliżone znajdujące się w palecie. Operacja ta może znacząco wpłynąć na jakość obrazu, dlatego bardzo ważny jest właściwy dobór kontenera.

Algorytm redukcji działa w następujący sposób. Dopóki rozmiar palety jest większy od zadanego, są wykonywane poniższe kroki.

1. Oblicz odległości między kolorami (każdy z każdym).
2. Usuń z palety dwa kolory o najmniejszym dystansie.
3. Dodaj do palety kolor będący średnią dwóch usuniętych.

Do obliczania odległości między kolorami używa się następującej metryki:

$$d = \sqrt{(R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2}\ , \qquad (2)$$

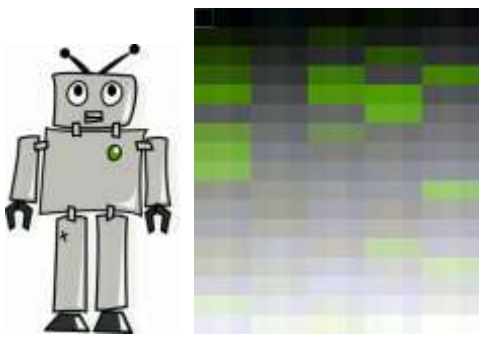
gdzie R_x, G_x, B_x to składowe czerwona, zielona i niebieska danej barwy.

Pierwsza z omawianych metod steganograficznych polega na powieleniu każdej pozycji palety. W konsekwencji dowolny piksel może odwoływać się do więcej niż jednego indeksu bez zmiany swojego koloru. Przykładowo jeśli paleta zostanie podwojona, to każdą barwę można zapisać na dwa sposoby, zatem pojedynczy piksel może kodować jeden bit informacji. Wymaga to startowego rozmiaru palety nie większego niż 128 lub zredukowania nadmiarowych pozycji.

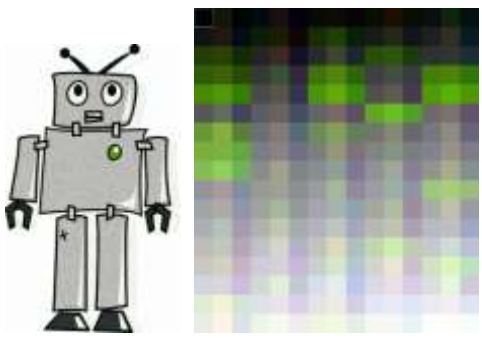
Jeżeli jest konieczna redukcja, do kontenera zostają wprowadzone niewielkie modyfikacje barw, których widoczność zależy od kolorystyki. W przeciwnym wypadku technika ta nie powoduje żadnych widzialnych zmian w nośniku. Zwiększa się natomiast rozmiar pliku ze względu na podwojenie wielkości palety.

Inna metoda operująca na obrazach indeksowanych dodaje do palety nowe kolory różniące się nieznacznie od początkowych [7]. Pierwszym krokiem w osadzaniu jest rozszerzenie palety poprzez wprowadzenie dla każdej barwy dwóch podobnych (ale nieidentycznych), z których jedna będzie jaśniejsza, a druga ciemniejsza. Dla odróżnienia składowa niebieska oryginalnego koloru jest ustawiana na wartość parzystą, a dodanych – na nieparzystą.

a) 256-elementowa paleta kolorów, maks. różnica 5



b) 256-elementowa paleta kolorów, maksymalna różnica 19



Rys. 7. Obrazy i palety kolorów po osadzeniu wiadomości
Fig. 7. Images and colour palette after message embedding

Rozmiar otrzymanej palety jest więc trzykrotnością początkowej wielkości. Proces ukrywania wiadomości polega na następującym przypisaniu indeksów pikseli: jeśli bit przekazu jest równy 1, indeks powinien odwoływać się do pierwotnego koloru; dla bitu 0 powinien wskazywać na jedną z barw włączonych do palety podczas rozszerzania.

W zależności od akceptowalnej maksymalnej różnicy dodawanych kolorów, do obrazu zostają wprowadzone mniejsze lub większe zakłócenia. Wynik działania algorytmu został zaprezentowany na rysunku 7. Widać, że im bliższe są nowe i bazowe kolory, tym mniej zaburzeń występuje w otrzymanym obrazie. Odbywa się to jednak kosztem wprowadzenia do palety wzorców, które mogą być wykryte podczas steganalizy, a które są mniej wyraźne w przypadku bardziej odległych wartości. Aby zwiększyć bezpieczeństwo metody, elementy palety można wymieszać, aby podobne kolory nie występowały obok siebie.

4. Techniki steganografii dźwiękowej

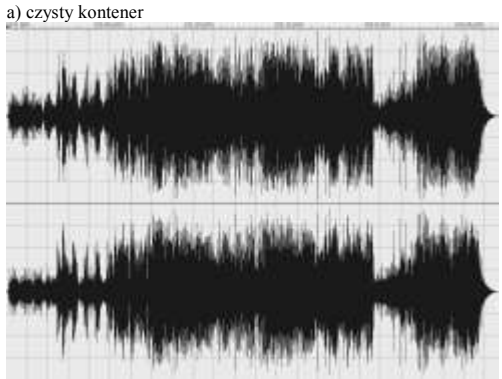
Podobnie jak obrazy dźwięk cyfrowy stanowi znakomity nośnik do ukrywanych danych. Pojemność steganograficzna plików audio jest bardzo wysoka, przez co stały się one obiektem zainteresowania wielu badaczy. Techniki steganograficzne wykorzystują niedoskonałości ludzkiego układu słuchu, takie jak niska czułość na zmiany siły tonu czy zjawisko maskowania niektórych dźwięków przez inne.

4.1. Metody operujące na próbkach dźwięku

Ukrywanie informacji w próbkach dźwięku jest często praktykowane ze względu na dużą pojemność plików muzycznych. Najpopularniejszą metodą (podobnie jak dla obrazów 5) jest LSB, której zasada działania jest zbliżona do algorytmu steganografii obrazowej. W nieskompresowanym formacie WAV, który jest odpowiedni dla tej techniki, próbki mogą być reprezentowane między innymi przez liczby całkowite.

Osadzanie polega na zastępowaniu najmniej znaczących bitów próbki bitami sekretnej wiadomości. Powinno być jednak przeprowadzone ostrożnie z uwagi na pewne cechy ludzkiego słuchu. Czułość na biały szum powoduje, że ilość zmienionych bitów nie może być zbyt duża – wprowadzanie informacji na warstwy LSB wyższe niż 4 powoduje znaczną utratę jakości i jest już dobrze słyszalne [4].

a) czysty kontener



b) kontener z ukrytą wiadomością

Rys. 8. Przykład działania algorytmu LSB na plikach audio
Fig. 8. Example of LSB hiding method in audio file

Wyodrębnianie przekazu odbywa się poprzez odczyt najmniej znaczących bitów próbek dźwięku. W ten sposób mogą być ukrywane i odczytywane dowolne dane, między innymi pliki binarne, tekst jawny lub zaszyfrowany. Metoda LSB z użyciem jednego bitu nie wprowadza słyszalnych zniekształceń, nie zmienia się również rozmiar nośnika. Przykład kontenerów przed i po osadzaniu wiadomości został zaprezentowany na rysunku 8.

Pomimo wielu zalet, omawiana technika posiada znaczną słabość – nie zapewnia wystarczającego poziomu bezpieczeństwa. Możliwe jest odkrycie osadzonych informacji lub ich zniszczenie, np. poprzez losową modyfikację najmniej znaczących bitów w całym pliku. Z tego względu opracowano kilka ulepszeń algorytmu LSB. Jedno z nich przewiduje ukrycie danych w kilku warstwach LSB i zakłada zmianę wartości próbki na najbardziej zbliżoną do oryginalnej. Ma to na celu mniejszą modyfikację sygnału, a co za tym idzie – podniesienie bezpieczeństwa [4].

4.2. Metody operujące na strukturze pliku

Dane mogą być ukrywane nie tylko w próbkach dźwięku, ale również w strukturze pliku. Sytuacja taka występuje, gdy pewien format zezwala na zapis tej samej informacji na różne sposoby. Przykładem mogą być pliki MIDI, dla których opracowano kilka algorytmów steganograficznych [1].

Standard MIDI (Musical Instrument Digital Interface) opisuje komunikację między instrumentami elektronicznymi. Pliki tego typu nie zawierają żadnych dźwięków, a jedynie komendy sterujące. Z tego powodu ich rozmiar jest stosunkowo niewielki w porównaniu do innych popularnych formatów.

Każdy z plików MIDI rozpoczyna się nagłówkiem, po którym następuje jedna lub więcej ścieżek. Ścieżka może zawierać wiele zdarzeń, a każde z nich składa się z różnicy czasu pomiędzy aktualnym zdarzeniem i następnym (Δt) oraz wiadomości. Standard definiuje trzy typy wiadomości: komunikaty kanałowe, systemowe oraz meta-komunikaty.

Opisywana metoda steganograficzna dotyczy pierwszego rodzaju wiadomości. Zawiera ona kod komendy oraz parametry. Według specyfikacji, jeżeli w dwóch kolejnych zdarzeniach występuje komunikat kanałowy o identycznym kodzie komendy, kod ten może zostać pominięty. W takiej sytuacji wiadomość będzie zawierała jedynie parametry, a za obowiązujący uznaje się poprzedni kod. Zjawisko takie nosi nazwę running status.

Rozpatrzmy następujący strumień danych składający się z czterech zdarzeń:

00 90 23 23 00 90 13 42 01 80 23 00 01 80 13 00

Pierwsza wartość każdego zdarzenia to opóźnienie Δt, następna to kod komendy, a ostatnie dwa – parametry.

Może on zostać zapisany jako

00 90 23 23 00 13 42 01 80 23 00 01 13 00

Ponieważ skrócony zapis jest dopuszczalny, ale nie jest konieczny, może zostać wykorzystany do ukrycia przekazu. Przedstawiana technika zakłada, że kod komendy pomijany jest wtedy, gdy bit wiadomości jest równy 0, w odwrotnej sytuacji jest zachowywany. Kolejne bity mogą być osadzane tylko w dozwolonych miejscach, tj. w następujących po sobie komunikatach z jednakowymi kodami. Zatem pojemność jest ściśle powiązana z typami zdarzeń oraz ich kolejnością.

Dla przedstawionego powyżej przykładu można wskazać, jak będzie wyglądał strumień po ukryciu w nim informacji „01”:

00 90 23 23 00 13 42 01 80 23 00 01 80 13 00
0 1

Algorytm zapewnia wysoki poziom bezpieczeństwa i nie zmienia komend, a jedynie zapisuje je w innej formie. Z tego powodu muzyka stworzona na podstawie czystego kontenera nie będzie się różniła od tej pochodzącej z nośnika tajnej informacji. Jedynym widocznym śladem jest zmiana rozmiaru pliku – może być on większy lub mniejszy od oryginalnego w zależności od stosowanego w nim zapisu.

Wadę prezentowanej metody stanowi fakt, że łatwo jest usunąć ukryte w ten sposób dane. Zazwyczaj większość aplikacji domyślnie pomija powtarzające się kody komend, zatem otwarcie pliku w edytorze MIDI i ponowny zapis zniszczy tajny przekaz.

Praca [1] prezentuje również technikę ukrywania informacji w rozszerzonych komunikatach systemowych (SysEx). Jest to specjalny typ komend nie zawartych w standardzie, ale stosowanych przez niektórych producentów. Są one ignorowane przez większość instrumentów. W tej metodzie do ścieżki dołączane jest zdarzenie z komunikatem SysEx, którego dane stanowi sekretna wiadomość. Charakteryzuje się nieograniczoną pojemnością, ale jest łatwa do wykrycia i w niektórych przypadkach może wpływać w sposób nieprzewidywalny na brzmienie.

5. Podsumowanie

W niniejszym artykule zaprezentowano szereg najważniejszych zagadnień związanych z nowoczesnymi technikami steganografii cyfrowej, oraz omówiono kilka wybranych algorytmów. Publikacja dostarcza wiedzy o technologiach steganograficznych, które mogą być wykorzystane w praktyce. W tabeli 1 zestawiono najważniejsze cechy przedstawionych metod.

Tab. 1. Porównanie poszczególnych algorytmów steganograficznych
Tab. 1. Features of selected steganography methods

	Algorytm	Detekcja	Pojemność	Wprowadzane modyfikacje	Zmiana rozmiaru pliku	Złożoność
Steganografia obrazowa	LSB	Łatwa	Duża	Niewielkie	Nie	Niska
	±1	Średnia	Duża	Niewielkie	Nie	Niska
	Najczęstsze piksele	Średnia	Zazwyczaj mała	Niewielkie	Nie	Niska
	Fraktale	Trudna	Zależna od parametrów	Nie dotyczy	Nie dotyczy	Średnia
	Powielenie kolorów palety	Łatwa/ Średnia	Duża	Czasami	Czasami	Średnia
	Modyfikacja kolorów palety	Średnia	Duża	Tak, zależnie od progu	Czasami	Średnia
Steganografia dźwiękowa	LSB	Łatwa	Duża	Niewielkie	Nie	Niska
	Powtarzanie kodów komend	Trudna	Mała	Brak	Tak	Wysoka
	SysEx	Bardzo łatwa	Nieograniczona	Tak	Tak	Niska

Obecnie steganografia znajduje zastosowanie w wielu dziedzinach życia i służy najczęściej do ochrony prywatności. Nauka ta nie stoi w sprzeczności z innymi gałęziami bezpieczeństwa informacji ani nie próbuje ich zastąpić, lecz stanowi ich uzupełnienie. W sytuacji, gdy zastosowanie kryptografii jest niemożliwe lub utrudnione, rola steganografii będzie nieoceniona. Zazwyczaj w takim przypadku ukrycie wiadomości jest jedyną możliwością jej bezpiecznego przekazania.

Potrzeba zwiększania poufności komunikacji jest przyczyną ciągłego postępu, jaki można zaobserwować w steganografii. Opracowywane są coraz lepsze metody pozwalające przekazywać duże ilości informacji oraz takie, których głównym zadaniem jest osiągnięcie jak największej niewykrywalności. Z drugiej strony doskonalone są również techniki steganalizy służące do wykrywania i usuwania sekretnej wymiany danych. Stanowi to dodatkowy bodziec do rozwoju tej ciekawej dziedziny.

Jako przyszłe kierunki badawcze można wskazać nie tylko dalsze ulepszanie i optymalizację istniejących metod, ale także połączenie steganografii z technikami biometrycznymi. Za potrzebą opracowywania takich rozwiązań przemawia fakt, że współcześnie wiele wartościowych informacji przechowywanych jest cyfrowo i przy łatwości ich przesyłania i powielania konieczne jest stosowanie dodatkowych zabezpieczeń mających charakter personalny. Dalszy rozwój tych technik pozwoli lepiej chronić ważne dane przed ujawnieniem i może przyczynić się do postępu w dziedzinie spersonalizowanej kryptografii. Może także umożliwić wprowadzenie dodatkowych zabezpieczeń do protokołów wymiany gotówki elektronicznej, a tym samym umożliwić wykrywanie nieprawidłowych transakcji prowadzonych z użyciem pieniądza elektronicznego [5].

6. Literatura

[1] Adli A., Nakao Z.: Three steganography algorithms for midi files. Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on, vol. 4, pp. 2401–2404, 2005.

[2] Cancelli G., Doerr G., Cox I., Barni M.: Detection of ±1 lsb steganography based on the amplitude of histogram local extrema. Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on, pp. 1288–1291, 2008.

[3] Cox I., Miller M., Bloom J., Fridrich J., Kalker T.: Digital Watermarking and Steganography. Morgan Kaufmann Publishers, 2008.

[4] Cvejic N., Seppanen T.: Increasing robustness of lsb audio steganography by reduced distortion lsb coding. Journal of Universal Computer Science, vol. 11(1), pp. 56–65, 2005.

[5] Ogiela M.R. Sułkowski P.: Wykrywanie wielokrotnych nieprawidłowych transakcji w protokołach wymiany elektronicznej gotówki PAK, Vol. 60(4), pp. 257-261, 2014.

[6] Saha A., Halder S., Kollya S.: Image steganography using 24-bit bitmap images. Computer and Information Technology (ICCIT), 2011 14th International Conference on, pp. 56–60, 2011.

[7] Samaratunge S.: New steganography technique for palette based images. Industrial and Information Systems, 2007. ICIIS 2007. International Conference on, pp. 335–340, 2007.

[8] Simmons G.: The prisoners' problem and the subliminal channel. Advances in Cryptology, pp. 51–67. Springer US, 1984.

[9] Singh S.: The code book. Anchor Books, New York, 1999.

[10] Zhang H., Hu J., Wang G., Zhang Y.: A steganography scheme based on fractal images. Networking and Distributed Computing (ICNDC), 2011 Second International Conference on, pp. 28–31, 2011.

otrzymano / received: 26.09.2014
przyjęto do druku / accepted: 03.11.2014 *artykuł recenzowany / revised paper*

INFORMACJE