Rozdział 1

Steganografia

Steganografia jest dziedziną nauki poświęconą ukrywaniu informacji w jawnych kanałach komunikacji. Nazwa nauki wywodzi się z języka greckiego, i może być tłumaczona jako „ukryte pismo" (*steganós* - ukryty, *graphia* - pismo).

W celu podkreślenia cech oraz charakteru metod steganograficznych często przytaczane jest również pojęcie kryptografii. Obiektem zainteresowań kryptografii jest uniemożliwienie zrozumienia treści wiadomości przez osoby postronne, pozbawione do niej dostępu. Współcześnie jest to osiągane poprzez stosowanie klucza dzielonego przez osoby zaufane (kryptografia symetryczna) lub par kluczy publicznych i prywatnych (kryptografia asymetryczna). Dzięki ich zastosowaniu, osoba postronna pomimo dostępu do szyfrogramu nie jest w stanie wydobyć tekstu jawnego.

W odróżnieniu od kryptografii, celem technik steganograficznych jest umożliwienie uczestnikom komunikacji przesyłania informacji bez ujawniania faktu istnienia samego przekazu.

1.1 Zastosowania steganografii

Pierwszych przykładów zastosowania steganografii można doszukiwać się już w czasach starożytnych[14]. Herodotus, w swoim dziele *Dzieje* opisuje historię greckiego polityka Histiajosa, który w celu przekazania poufnej informacji wytatuował ją na skalpie zaufanego niewolnika. Gdy jego włosy odrosły, został on wysłany w

celu doręczenia listu oraz ukrytej wiadomości. Do innych przykładów steganografii można zaliczyć również ukrywanie wiadomości w zapisach nutowych, stosowanie atramentów sympatycznych lub technikę mikrokropek[14], która przeżyła swój renesans w czasach zimnej i drugiej wojny światowej.

Warto również podkreślić, że kolejnym z zastosowań steganografii są znaki wodne oraz symbole pozwalające na identyfikację źródła informacji. Za równo w przypadku multimediów objętych prawami autorskimi jak i poufnych dokumentów, ich producent lub organizacja strzegąca ich tajności może umieścić ukryte informacje pozwalające wskazać źródło wycieku[12]. Podobną technikę stosują producenci drukarek - seria oraz model drukarki może być odzwierciedlona w drukowanym dokumencie poprzez układ niewidocznych gołym okiem żółtych kropek. Takie działania mają na celu ułatwienia walki z przestępczością polegającą na fałszowaniu dokumentów i banknotów[18].

1.2 Steganografia cyfrowa

Wraz z wzrostem wykorzystania komputerów do celach multimedialnych oraz rozpowszechnieniu szerokopasmowego internetu coraz popularniejsza i bardziej opłacalna staje się steganografia cyfrowa. Jej ideą jest wykorzystanie jako medium nośnego różnych rodzajów plików komputerowych lub protokołów komunikacji cyfrowej. Przykładem wykorzystania protokołów do celów steganograficznych może być ukrywanie danych w polach kontrolnych ramek TCP/IP, kontrolowanie opóźnień między poszczególnymi pakietami lub nawet umyślne powodowanie utrat wybranych pakietów[16].

Znacznie prostszą, lecz bardzo rozwiniętą techniką jest wykorzystanie plików multimedialnych takich jak zdjęcia, pliki muzyczne i filmy. Do ich szczególnej atrakcyjności jako medium służące do ukrywania informacji przyczynia się między innymi ich wszechobecność, duże rozmiary oraz wysoka nadmiarowość[9, 15]. Ostatni aspekt w kontekście steganografii ma szczególne znaczenie, gdyż oznacza że modyfikacja pewnej części informacji bitowej zawartej w pliku ma niski wpływ na jego końcową treść. Przykładowo, zmiana wartości jednego z kanałów konkretnego piksela będzie miało mało zauważalny wpływ na końcowy obraz nawet przez uważnego obserwatora. Podobne prawidłowości można również dostrzec w plikach

muzycznych - manipulacja zawartością częstotliwości składowych będących poza granicą percepcji, czyli poniżej 20Hz i powyżej 20kHz również będzie trudna w detekcji przez subiektywnego odbiorcę[21]. Innym przykładem ukrywania informacji w muzyce jest tzw. *backmasking*, polegający na ukrywaniu wiadomości możliwych w odbiorze tylko i wyłącznie po odtworzeniu utworu od tyłu. Jednym z pierwszych zespołów przyczyniających się do wzrostu popularności powyższych eksperymentów jest *The Beatles*.

1.3 Steganografia z wykorzystaniem obrazów cyfrowych

Mimo tego, że jako medium steganograficzne można wykorzystać każdy plik binarny, szczególnie dużo uwagi zostało poświęcone cyfrowym obrazom i zdjęciom. Pomimo pozornej prostoty powyższego zadania powstało wiele wyrafinowanych metod i technik, różniących się za równo pod kątem założeń jak i rezultatów. Pierwszym parametrem mogącym służyć do podziału zaproponowanych metod jest dziedzina w której obraz zostaje poddany analizie.

1.3.1 Techniki przestrzenne

W technikach przestrzennych, obraz jest traktowany jak zbiór punktów (pikseli) umieszczonych w dwuwymiarowym układzie współrzędnych. Zaletą tych metod jest ich intuicyjność oraz przystępność, lecz są to również metody bardziej podatne na ataki polegające na wykryciu lub zniszczeniu ukrytej wiadomości[19].

Najbardziej powszechną techniką przestrzenną jest metoda *Least Significant Bit (LSB)*. Jej zastosowanie sprowadza się do zastąpienia najmniej znaczącego bitu obrazu będącego nośnikiem informacji bitem wiadomości ukrywanej. W zależności od spadku jakości który uznajemy za akceptowalny, możemy wykorzystać n najmniej znaczących bitów każdego z kanałów *RGB*. Pewnym uszczegółowieniem *LSB* jest metoda *4LSB*. Zakłada ona wykorzystanie dokładnie 4 bitów z każdego bajtu obrazu maskującego, co przekłada się na wykorzystanie 50% pojemności nośnika. Kosztem tak znacznej pojemności jest znaczący spadek jakości obrazu oraz ułatwiona steganoanaliza.

W celu zmniejszenia wykrywalności manipulacji obrazu przy jednoczesnym zachowaniu względnie dużej pojemności steganogramu, zaproponowano technikę *Variable Least Significant Bit (VLSB)*[7]. W przeciwieństwie do *LSB* podczas ukrywania danych wykorzystywana jest różna ilość bitów obrazu w zależności od położenia piksela. Nośnik zostaje podzielony na zadaną ilość sekcji, a następnie dla każdej z nich wyznaczana jest ilość bitów które zostaną zastąpione tekstem jawnym. Twórcy metody zaproponowali algorytm *Decreasing Distance Decreasing Bits Algorithm (DDDBA)*, który na podstawie odległości sektora względem piksela referencyjnego, którym najczęściej jest środkowy piksel obrazu, wyznacza proporcjonalną ilość ukrywanych bitów. Wynikiem działania algorytmu *VLSB* jest obraz, którego środkowa część jest mniej zniekształcona, co obniża subiektywne odczucie spadku jakości i pozwala na ukrycie większej ilości danych[7].

Dalszym udoskonaleniem, za równo pod kątem bezpieczeństwa ukrywanej informacji jak i utrudnienia wykrywalności ukrytego przekazu jest metoda o nazwie *Varying Index Varying Bits Substitution (VIVBS)* zaproponowana przez Sahib Khan, N. Ahmad i M. Wahid[6]. Podobnie jak w metodzie *VLSB*, ilość wykorzystanych bitów obrazu nośnego jest zmienna. W przeciwieństwie do wariantu *VLSB* opartego o algorytm *DDDBA*, ilość bitów ukrywanych w danym pikselu nie jest wyznaczana podczas działania algorytmu, lecz jest zależna od dodatkowego klucza będącego parametrem jego działania. Klucz przyjmuje postać tablicy przypisującej indeksowi każdego z pikseli ilość bitów które należy zastąpić bitami tekstu jawnego. Ponieważ ilość możliwych kombinacji rozmieszczenia bitów informacji w obrazie jest znacząca, odczytanie przekazu poprzez wykorzystanie przeszukiwania wyczerpującego poprzez osobę postronną nieposiadającą klucza będzie praktycznie niemożliwe. Główną wadą, powyższej metody jest jej również największa zaleta - klucz definiujący rozmieszczenie informacji w pikselach obrazu. Każdorazowe kodowanie informacji wymaga utworzenia klucza, od którego będzie również zależeć wpływ procesu na jakość obrazu - arbitralny wybór wysokiej ilości wykorzystanych bitów w nieodpowiednich sekcjach obrazu może przykuć uwagę osób postronnych i zdradzić fakt istnienia ukrytego przekazu. Dodatkową wadę metody jest również rozmiar klucza - w minimalnym przypadku, w którym wykorzystujemy 0 lub 1 bit każdego piksela klucz ma rozmiar $w * h$ bitów, gdzie w i h to odpowiednio szerokość i wysokość obrazu. Wraz z wzrostem ilości wykorzystywanych bitów, rozmiar

klucza również będzie się powiększał[6].

W celu poprawy subiektywnej oceny jakości obrazów oraz zmniejszenia ryzyka przekazu w roku 2003, Da-Chun Wu oraz W. Tsai zaproponowali metodę *Value Pixel Differencing (VPD)*. Jednym z jej założeń jest uzależnienie ilości wykorzystanych bitów obrazu nośnego od różnicy pomiędzy poziomami intensywności kolejnych pikseli[22]. W metodzie *VPD* piksele są odczytywane parami sekwencyjnie, zakreślając ciągły, łamany kształt. Dla każdej napotkanej pary pikseli obliczana jest ich różnica jasności, a następnie na jej podstawie wyznaczana jest ilość bitów które zostaną podmienione na treść ukrywanej wartości. Ilość ukrytych bitów jest proporcjonalna do zmiany wartości pikseli. W ten sposób możliwe jest osiągnięcie obrazów mniej podatnych na steganoanalizę przy jednoczesnym zachowaniu znacznej pojemności[22].

1.3.2 Techniki częstotliwościowe

Alternatywnym podejściem do steganografii wykorzystującej cyfrowe obrazy, są techniki oparte o częstotliwościową reprezentację obrazów. Metody te polegają na transformacji obrazu w postaci bitmapy do macierzy współczynników określających amplitudę lub natężenie fal o konkretnych częstotliwościach występujących w obrazie[2, 17].

Analiza obrazów w dziedzinie częstotliwości daje alternatywną perspektywę na treść obrazu i pozawala na rozpoznawanie, ekstrakcję i manipulację poszczególnych cech które mają odmienny wpływ na jego percepcję. Pasma niskich częstotliwości przekładają się na percepcję ogólnych kształtów i barw obiektów oraz ich kompozycję i wzajemne umiejscowienie. Pasma wysokie pozwalają na rozróżnianie ostrych krawędzi obrazów, rozpoznawanie detali oraz reprezentują wszelkie złożone tekstury[1].

Metody częstotliwościowe zyskały również na popularności w pokrewnej dziedzinie do steganografii, jaką jest oznaczanie (ang. *watermarking*) produktów cyfrowych. Za równo ukrywając dane poufne, jak i cyfrowe podpisy chroniące praw autorskich, celem metod działających w dziedzinie częstotliwościowej jest nie tylko zachowanie możliwie najwyższej jakości medium w którym zawarto dodatkowe informacje, lecz również uodpornienie ukrytego przekazu na jego manipulację i znisz-

czenie przez kompresję[20].

Jedną z transformat pozwalających na wyznaczenie częstotliwościowej reprezentacji obrazu jest *Dyskretna transformata kosinusowa (DCT)*[2]. Polega ona na podziale obrazu na bloki, najczęściej rozmiaru 8x8 pikseli. Następnie wyznaczana jest macierz współczynników $T_{i,j}$ za pomocą poniższego wzoru 1.1. N oznacza rozmiar bloku, w powszechnych zastosowaniach wynosi 8.

$$T_{i,j} = \left\{ \begin{array}{ll} \frac{1}{\sqrt{N}} & \text{if } i = 0 \\ \sqrt{\frac{2}{N}} \cos\left[\frac{(2j+1)i\pi}{2N}\right] & \text{if } i > 0 \end{array} \right\} \tag{1.1}$$

W kontekście złożoności obliczeniowej istotny jest fakt, że macierz transformacji T można wyznaczyć jednokrotnie i ponownie wykorzystać dla każdego z bloków obrazu. W tym przypadku stosowane jest równanie 1.2, w którym wyznacza się macierz współczynników D korzystając z macierzy transformacji T oraz bloku wartości pikseli M przeskalowanych do zakresu $[-128, 127]$.

$$D = TMT' \tag{1.2}$$

Jednym z zastosowań dyskretnej transformacji kosinusowej jest stratna kompresja danych, przykładowo w formacie JPEG. Po wyznaczeniu współczynników odpowiadających kolejnym częstotliwościom następuje proces kwantyzacji - macierz współczynników zostaje skalarnie przemnożona przez macierz kwantyzacji a następnie zaokrąglana. Zadaniem macierzy kwantyzacji jest przeskalowanie współczynników odpowiadających zakresom częstotliwości w taki sposób, aby pasma których zmiany mają najmniejszy wpływ na subiektywną percepcję przyjęły wartości bliskie zeru. Ostatnim krokiem kompresji jest zaokrąglenie uzyskanych współczynników. Poprzez odrzucenie miejsc po przecinku wszystkich współczynników końcowy obraz charakteryzuje się dużo mniejszym rozmiarem. W celu rekonstrukcji wykonuje się transformację odwrotną (*IDCT*).

Przykładem algorytmu steganograficznego korzystającego z *DCT* jest praca „Reversible Data Hiding in JPEG Images"[3, 8]. Wyznaczone współczynniki częstotliwości służą za nośnik tekstu jawnego - współczynnikom z eksperymentalnie dobranych pasm częstotliwości zostają podmienione najmniej znaczące bity, podobnie jak w przestrzennych metodach *LSB*. W celu osiągnięcia dużo większej

odporności steganogramu na kompresję, Zhiqiang Zhu, N. Zheng, Tong Qiao oraz Ming Xu zaproponowali metodę opartą o manipulację znaków współczynników, w odróżnieniu do manipulacji ich wartościami[24].

Inną transformacją wykorzystywaną w steganografii jest *Dyskretna transformata falkowa* (ang. *Discrete wavelet transform (DWT)*) oraz jej odpowiednik pozwalający na bezstratną transformację odwrotną - *Całkowitoliczbowa transformata falkowa* (ang. *Integer wavelet transform (IWT)*)[23].

Jedną z możliwości transformaty falkowej jest wyodrębnienie części obrazu w której skład wchodzą osobno wysokie i niskie pasma częstotliwości. Obraz zostaje kolejno przekształcany wierszami i kolumnami przez filtr dolnoprzepustowy (wykonujący operację uśredniania) i górnoprzepustowy (obliczający różnicę).

Po pierwszej iteracji oryginalny obraz zostaje podzielony na sekcje:

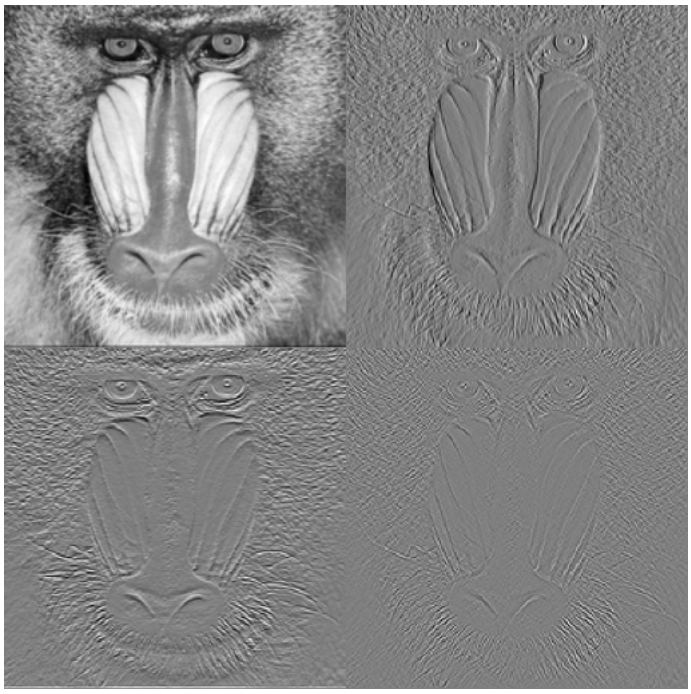
- LL - filter dolnoprzepustowy zaaplikowany do wierszy i kolumn,
- LH - filter dolnoprzepustowy zaaplikowany do wierszy, górnoprzepustowy dla kolumn,
- HL - filter górnoprzepustowy zaaplikowany do wierszy, dolnoprzepustowy dla kolumn,
- HH - filter górnoprzepustowy zaaplikowany do wierszy i kolumn.

Przykład działania *IWT* przedstawia rysunek 1.1.

W artykule „Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique" opisano metodę ukrywania bitów wiadomości w najmniej znaczących bitach współczynników odpowiadających pasmom wysokiej częstotliwości. Wyniki eksperymentalne, względem innych metod, wykazały znaczący wzrost pojemności obrazu przy zachowaniu tego samego współczynnika szczytowego stosunku sygnału do szumu[23].

1.3.3 Podsumowanie

Na podstawie przytoczonej literatury oraz opisanych metod, można zauważyć pewną tendencję sugerującą istotność doboru regionów obrazu w których są ukrywane dane. W opisanych pracach korzystających z transformat częstotliwościo-



Rysunek 1.1: Wynik działania *IWT* na przykładowym obrazie. Kolejno sekcje LL, HL, LH, HH. Do wykonania rysunku wykorzystano narzędzie Image Processing Online Demonstration, http://bigwww.epfl.ch/demo/ip/demos/wavelets/

wych, dokonywano wyboru pomiędzy ukrywaniem danych w niskich-średnich[4, 11, 8] lub wysokich pasmach częstotliwości[23, 10].

Główną motywacją autorów decydujących się na dobór niskich bądź średnich pasm w celach ukrywania informacji jest uzyskanie obrazu o większej odporności na manipulacje i zniekształcenia. W pracach opisujących metody wykorzystujące wysokie pasma częstotliwości, wybór jest argumentowany niższą percepcyjną wykrywalnością przez osobę postronną.

Mechanizm ludzkiej percepcji obrazów jest niezmiernie złożony a nauki z nią związane pozostają dziedzinami w których pozostaje jeszcze wiele do odkrycia i wyjaśnienia. Na postrzeganie i rozróżnianie obrazów wpływa nie tylko udział poszczególnych składowych częstotliwości, lecz również stosunek kontrastu pasm oraz sposoby uprzedniego przetwarzania obrazu[13]. Niemniej jednak, eksperymentalne badania przeprowadzane na grupie uczestników sugerują większe znaczenie niższych i średnich pasm częstotliwości przy percepcji jakości oraz zniekształceń obrazów. Dowodem tego mogą być powszechnie stosowane tablice kwantyzacji wykorzystywane w formatach stratnej kompresji, które faworyzują pasma o średniej lub niższej częstotliwości[2]. Oznacza to, że istnieje większy potencjał w manipulacjach obrazem w zakresie pasm wysokich, przy jednoczesnej zachowaniu jak najwyższej subiektywnej jakości obrazu. Istnieją prace związane z steganografią popierające powyższą tezę. Należą do nich już przytoczona w kontekście metody *PVD* „A steganographic method for images by pixel-value differencing"[22], oraz praca„Edge-based image steganography" oparta na wykrywaniu krawędzi obrazu[5].

Bibliografia

[1] American Psyhological Association. Perception of high and low spatial frequency information in pigeons and people, 2015.

[2] K. Cabeen, P. Gent. image compression and the discrete cosine transform. College of Redwoods.

[3] Fangjun Huang, Xiaochao Qu, H. J. Kim, J. Huang. Reversible data hiding in jpeg images. *IEEE Transactions on Circuits and Systems for Video Technology*, 26:1610–1621, 2016.

[4] J. Huang, Y. Shi. Embedding image watermarks in dc components. *IEEE Trans. Circuits Syst. Video Technol.*, 10:974–979, 2000.

[5] S. Islam, Mangat Rai Modi, P. Gupta. Edge-based image steganography. *EURASIP Journal on Information Security*, 2014:1–14, 2014.

[6] Sahib Khan, N. Ahmad, M. Wahid. Varying index varying bits substitution algorithm for the implementation of vlsb steganography. *Journal of the Chinese Institute of Engineers*, 39:101 – 109, 2016.

[7] Sahib Khan, M. Yousaf, Jamal Akram. Implementation of variable least significant bits stegnography using dddb algorithm. 2011.

[8] X. Li, J. Wang. A steganographic method based upon jpeg and particle swarm optimization algorithm. *Inf. Sci.*, 177:3099–3109, 2007.

[9] Scott Mitchell. H.264 encoded digital video protection using temporal redundancy lsb steganography. 2018.

[10] P. Muhuri, Z. Ashraf, Swati Goel. A novel image steganographic method based on integer wavelet transformation and particle swarm optimization. *Appl. Soft Comput.*, 92:106257, 2020.

[11] Sunil Muttoo, Sushil Kumar. Data hiding in jpeg images. *International Journal of Information Technology (IJIT)*, 1, 07 2009.

[12] Hebah H. O. Nasereddin. Digital watermarking a technology overview. 2011.

[13] Sabrina Perfetto, John D. Wilder, Dirk B. Walther. Effects of spatial frequency filtering choices on the perception of filtered images. *Vision*, 4, 2020.

[14] F. Petitcolas, R. Anderson, M. Kuhn. Information hiding-a survey. 1999.

[15] M. Pope, M. Warkentin, E. Bekkering, M. B. Schmidt. Digital steganography - an introduction to techniques and tools. *Commun. Assoc. Inf. Syst.*, 30:22, 2012.

[16] Roshan Poudél. *Covert Channel and Data Hiding in TCP/IP*. 11 2019.

[17] J. Reichel, G. Menegaz, M. Nadenau, M. Kunt. Integer wavelet transform for embedded lossy to lossless image compression. *IEEE transactions on image processing : a publication of the IEEE Signal Processing Society*, 10 3:383–92, 2001.

[18] T. Richter, S. Escher, D. Schönfeld, Thorsten Strufe. Forensic analysis and anonymisation of printed documents. *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, 2018.

[19] N. Sharma, Usha Batra. An inclusive study and analysis of steganographic methodologies for data security. 2020.

[20] Hai Tao, Li Chongmin, J. Zain, A. Abdalla. Robust image watermarking theories and techniques: A review. *Journal of Applied Research and Technology*, 12:122–138, 2014.

[21] David Wheeler, Daryl Johnson, Bo Yuan, P. Lutz. Audio steganography using high frequency noise introduction. 2012.

[22] Da-Chun Wu, W. Tsai. A steganographic method for images by pixel-value differencing. *Pattern Recognit. Lett.*, 24:1613–1626, 2003.

[23] G. Xuan, Y. Shi, Chengyun Yang, Yizhan Zhen, D. Zou, P. Chai. Lossless data hiding using integer wavelet transform and threshold embedding technique. *2005 IEEE International Conference on Multimedia and Expo*, strony 1520–1523, 2005.

[24] Zhiqiang Zhu, N. Zheng, Tong Qiao, Ming Xu. Robust steganography by modifying sign of dct coefficients. *IEEE Access*, 7:168613–168628, 2019.

Spis rysunków

Spis tablic