STUDIA INFORMATICA 2014
Volume 35 Number 2 (116)

Grzegorz KOZIEŁ
Politechnika Lubelska, Instytut Informatyki

WSPÓŁCZESNE TECHNIKI STEGANOGRAFICZNE W DŹWIĘKU

Streszczenie. Artykuł prezentuje przegląd współczesnych metod steganograficznych stosowanych w różnych zastosowaniach steganografii, takich jak: znakowanie wodne, tajna komunikacja, odciski palca, tworzenie ukrytych wolumenów danych. Każda grupa zastosowań została scharakteryzowana pod kątem wymagań kluczowych ze względu na pełnione funkcje.

Słowa kluczowe: steganografia, znakowanie wodne, ukrywanie informacji

THE MODERN STEGANOGRAPHIC TECHNIQUES IN SOUND

Summary. Some modern steganographic techniques are presented in the article. These methods can be used for various purposes: hidden communication, watermarking, fingerprinting, hidden data volumes creation. The most important requirements for each of the above applications were examined and are presented.

Keywords: steganography, watermarking, information hiding, sound

1. Wstęp

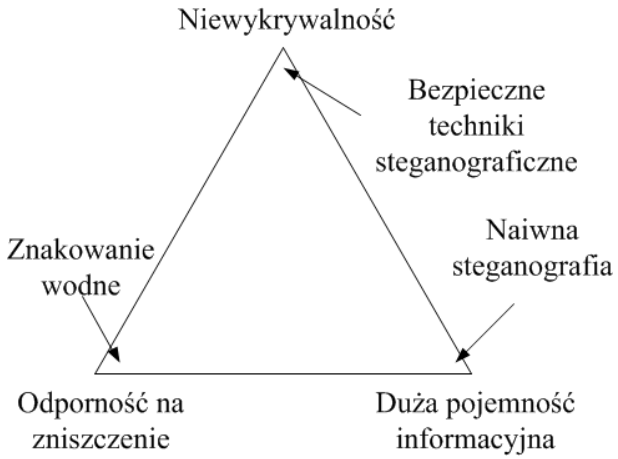
Steganografia jest nauką zajmującą się ukrywaniem jednej informacji w innej. Najczęściej definiujemy ją w kontekście ochrony informacji jako ukrywanie cennej informacji w innym zbiorze danych, niemającym szczególnej wartości. Jednak ta definicja sugeruje, że steganografia jest nauką zajmującą się ochroną informacji. W rzeczywistości jest to tylko jedno z jej zastosowań. Techniki steganograficzne są wykorzystywane do:

- realizowania tajnej komunikacji – tajne (chronione dane) są umieszczane w innym nośniku, a następnie przesyłane za pomocą publicznego medium do odbiorcy lub umieszczane w miejscu publicznym; utajnienie komunikacji jest możliwe przez dostatecznie dobre

ukrycie tajnych danych, uniemożliwiające osobom postronnym wykrycie istnienia dodatkowych ukrytych danych,

- znakowania wodnego (ang. *watermarking*) – do danych będących najczęściej utworem są dołączane dodatkowe dane stanowiące znak wodny twórcy lub osoby mającej prawa majątkowe do utworu; odpowiednio skonstruowany znak wodny pozwala na ustalenie osoby mającej prawa do utworu w momencie wystąpienia sporu na tym tle,
- umieszczania „odcisków palca" (ang. *fingerprinting*) – operacja podobna do znakowania wodnego, lecz mająca inny cel; w tym zastosowaniu do danych dodawana jest sygnatura oznaczająca osobę użytkownika lub nabywcy określonej kopii danych,
- tworzenia ukrytych nośników danych (steganograficznych systemów plików) – w ramach istniejącego nośnika danych tworzona jest przestrzeń ukryta, pozwalająca na dostęp i wykrycie jej istnienia tylko osobom posiadającym informacje o sposobie dostępu i stosowanym kluczu; przykładem może być użycie niewykorzystanych części klastrów systemu plików czy umieszczenie woluminu w specjalnie spreparowanym pliku,
- zabezpieczania nośników optycznych przed powielaniem – techniki zabezpieczające płyty CD, DVD, Blue-Ray przed nielegalnym powielaniem również zaliczane są do technik steganograficznych, najczęściej polegają na takim zmodyfikowaniu zapisu na płycie oryginalnej, by operacja jej kopiowania była niemożliwa lub przebiegała błędnie, tak by w rezultacie nie dało się uzyskać działającej kopii nośnika,
- wielu innych zastosowań wykorzystujących ukrywanie informacji – sposoby wykorzystania steganografii nie są w żaden sposób ograniczone i zależą od potrzeb i idei twórców; przykładem może być dodawanie przez drukarki żółtych kropek do wydruku, służących do identyfikacji drukarki, której użyto.

Oprócz różnorodności zastosowań należy zwrócić uwagę na możliwość wykorzystania w steganografii różnego rodzaju nośników ukrytej informacji, zwanych kontenerami. Dobre metody steganograficzne charakteryzują się tym, że dołączają dodatkową informację bezpośrednio do danych nośnika w taki sposób, by usunięcie lub zniszczenie ukrytych danych wiązało się z uszkodzeniem danych nośnika lub ich znaczną modyfikacją. Ponadto dołączana informacja musi być przezroczysta, czyli jej dołączenie nie może powodować zmian, które mogłyby być wykryte za pomocą zmysłów lub przez analizę statystyczną nośnika. W wielu zastosowaniach nie mniej istotna jest pojemność steganograficzna. Dotyczy to zwłaszcza steganograficznych systemów plików i tajnej komunikacji. W obydwu tych zastosowaniach niezbędna jest możliwość ukrycia dużej ilości danych. Niestety niemożliwe jest jednoczesne osiągnięcie doskonałych wartości tych trzech parametrów, tj. przezroczystości, odporności i pojemności. Ilustruje to trójkąt sprzeczności wymagań, który został przedstawiony na rys. 1.



Rys. 1. Trójkąt sprzeczności wymagań
Fig. 1. The triangle of requirements discrepancy

Zgodnie z zależnościami przedstawionymi na rysunku 1 właściwości każdej z metod są określone przez punkt znajdujący się wewnątrz trójkąta sprzeczności wymagań. Modyfikacja właściwości metody powoduje przesunięcie tego punktu. Oznacza to, że poprawa jednego z parametrów odbywa się kosztem pozostałych. Niemożliwa jest jednoczesna poprawa wszystkich właściwości. Stwierdzenie to jest prawdziwe, jeżeli zmieniamy jedynie parametry metody, nie zmieniając zasady jej działania. Możliwe jest bowiem zastosowanie doskonalszej metody, która będzie miała lepsze parametry, niemniej jednak ona też będzie podlegała tym samym ograniczeniom.

Jak zostało wspomniane, nośnik informacji steganograficznej podlega modyfikacjom podczas dołączania dodatkowych danych. Oznacza to, że nośnikiem może być dowolny rodzaj danych, które można poddać modyfikacji bez ich zniszczenia lub uszkodzenia. W praktyce najpopularniejszymi nośnikami informacji steganograficznej są dane multimedialne, takie jak obraz, dźwięk i film. Stosunkowo łatwo wprowadzić w nich nieznaczne zmiany, które nie wpłyną na postrzegalną zmianę jakości. Nie mniej popularne jest wykorzystywanie pakietów protokołu IP, każdy pakiet ma bowiem w nagłówku niewykorzystane pola, które mogą zostać użyte do przeniesienia dodatkowych danych. Popularna jest steganografia VoIP ze względu na powszechne zastosowanie tego typu połączeń. Wykorzystywane są tu zarówno techniki opierające się na modyfikowaniu nagłówków pakietów, jak również techniki ukrywania informacji w dźwięku oraz specyficzne rozwiązania projektowane specjalnie dla połączeń VoIP [17]. Znane są również algorytmy steganograficzne wykorzystujące tekst jako nośnik ukrytej informacji [6], jednak ich stosowanie jest ograniczone ze względu na niewielką pojemność steganograficzną, kłopotliwe ukrywanie oraz łatwość usunięcia dołączonych danych podczas przetwarzania we współczesnych edytorach tekstu, które często automatycznie modyfikują formatowanie tekstu oraz jego niektóre znaki.

Wymienione nośniki ukrytej informacji nie wyczerpują wszystkich możliwości, stanowią jednak najbardziej reprezentatywną grupę. O fakcie, że nośnikiem informacji steganograficznej może być niemalże dowolny nośnik danych, świadczy duża liczba publikacji omawiających tematykę dołączania ukrytych danych do takich nośników, jak: pliki wykonywalne *.exe [3], wiadomości MMS [29], różne języki [7, 8, 2], łańcuchy DNA [36], pakiety protokołów UDP oraz ICMP [9] oraz wiele innych.

2. Steganografia dźwięku

Dźwięk oferuje dwa typy kontenerów:

- ciągłe – przez to pojęcie rozumiemy sygnał trwający przez długi czas, niemający określonego końca; przykładem może być transmisja radiowa,
- o ograniczonej pojemności – tym mianem określamy wszystkie zapisy dźwięku, które mają określony początek i koniec.

Od typu kontenera zależą wymagania stawiane metodzie steganograficznej. W przypadku kontenerów ciągłych metody muszą pracować w czasie rzeczywistym, bez wprowadzania zauważalnego opóźnienia. Ponadto muszą zapewniać możliwość wstawiania i wykrywania znaczników początku i końca transmisji, gdyż ukrywana wiadomość jest transmitowana tylko przez pewien określony czas.

Najprostszą metodą i jednocześnie oferującą największą pojemność steganograficzną jest metoda najmniej znaczących bitów (ang. *Least Significant Bits* – LSB). Jej działanie polega na zamianie najmniej znaczących bitów wybranych próbek sygnału na bity ukrywanych danych. Metoda LSB może być stosowana zarówno w przypadku sygnałów mających reprezentację w dziedzinie czasu, jak i po ich przetransformowaniu do dziedziny częstotliwości lub innej oferowanej przez dowolną w pełni odwracalną transformatę [22, 1, 10, 13]. Technika LSB może być łączona z innymi, takimi jak: zamiana błędu minimalnego (ang. *minimum error replacement*) [11], rozpraszanie błędów (ang. *error dispersal*) [12] lub maskowanie [10]. Metoda LSB niezależnie od swoich modyfikacji nie jest odporna na uszkodzenia. Niewielki stopień odporności udało się osiągnąć autorom [12], lecz nie dorównuje on innym technikom. Metoda najmniej znaczących bitów zapewnia dużą pojemność steganograficzną i niski poziom wprowadzanych zakłóceń.

Metodę pozwalającą uniknąć wprowadzania zakłóceń przedstawiono w [21]. Twórcy wykorzystali operację usuwania zakłóceń do dołączania dodatkowych danych. Wynik naprawy jest zależny od danych, jakie mają zostać ukryte. W ten sposób ukrywają dane, jednocześnie polepszając jakość sygnału. Metoda również nie zapewnia odporności na uszkodzenia.

Aby osiągnąć odporność na uszkodzenia, opracowano metody operujące na sygnale przetransformowanym do dziedziny częstotliwości, które rozpraszają ukrywaną informację w dużym fragmencie sygnału. Wiele z metod operujących w dziedzinie częstotliwości wykorzystuje zjawisko maskowania do ukrywania wprowadzanych zmian. Jest to konieczne ze względu na dużą wrażliwość ludzkiego słuchu na zmiany częstotliwości. Metodę znakowania wodnego opartą na transformacie Fouriera i maskowaniu zaprezentowano w [30]. Metody komunikacji opierające się na transformacie Fouriera i maskowaniu, ukrywające informację przez modyfikację wartości współczynników widma częstotliwościowego, zaprezentowano w [21, 22]. Metody ukrywające przez kodowanie oraz modulację fazy przedstawiono w [18, 25]. Metodę znakowania wodnego wykorzystującą transformatę falkową jako przekształcenie bazowe opisano w [14]. W [27] zastosowano natomiast odmienne podejście. Znak wodny jest dołączany do sygnału reprezentowanego w dziedzinie czasu, natomiast modyfikacja współczynników transformaty cosinusowej jest wykorzystywana do zwiększenia przezroczystości dołączonych danych.

Innym podejściem pozwalającym uzyskać odporność na uszkodzenie są metody ukrywające dane przez dołączenie echa przenoszącego ukrytą informację do sygnału kontenera. Metody takie zostały zaprezentowane w [15, 16, 20].

W pracy [15] opisano również metodę filtracji podpasmowej, pozwalającą na osiągnięcie wysokiego poziomu odporności. Niestety jej wadą jest wprowadzanie w niektórych przypadkach słyszalnych zakłóceń.

Możliwe jest też uzyskanie dobrego poziomu odporności na zniszczenie dołączonej informacji przez modyfikację histogramu sygnału, jak to opisano w [33, 34], czy też modyfikację amplitudy tonów o niskich częstotliwościach [23].

3. Steganografia VoIP

Coraz częściej dźwięk jest przesyłany poprzez połączenia głosowe VoIP. Steganografia VoIP jest zupełnie inną formą steganografii, gdyż jest to operacja czasu rzeczywistego. Ponadto zachodzą tu zupełnie nowe zjawiska wynikające z charakteru wykorzystywanej usługi. Transmisja VoIP jest najczęściej dokonywana za pomocą protokołów bezpołączeniowych (np. UDP). Wiąże się to z utratą części pakietów przesyłanych przez sieć. W VoIP nie wykorzystuje się retransmisji utraconych pakietów, więc część danych traconych jest bezpowrotnie. Z punktu widzenia usługi nie ma to znaczenia, lecz może poważnie uszkodzić ukryte dane, gdyż zagubienie jednego bitu może zniszczyć całą dalszą część ukrytej transmisji. W transmisji VoIP występują zawsze co najmniej dwaj rozmówcy, czyli istnieją też dwa nie-

zależne kanały: jeden od rozmówcy A do B, drugi od rozmówcy B do A. Transmisja danych jest bowiem kierunkowa.

Korzystanie z transmisji VoIP jako kanału transmisji ukrytych danych stawia więc dodatkowe wyzwania [17]:

- konieczność radzenia sobie z porzucaniem i opóźnianiem pakietów w transmisji – ze względu na charakter usługi transmisja jest niewiarygodna, co może spowodować zniszczenie przesyłanej wiadomości, ponadto część pakietów dociera z opóźnieniem, co powoduje konieczność identyfikacji prawidłowej ich kolejności,
- ograniczenia w rozmiarze kontenera – nie jest znana całkowita długość rozmowy, nie można więc wyznaczyć pojemności steganograficznej nośnika,
- konieczność określania strumieni – w transmisji VoIP występują dwa niezależne strumienie danych – po jednym w każdą stronę; utrzymanie dwustronnej komunikacji wymaga właściwego zarządzania nimi,
- kompresja – dane głosowe często podlegają kompresji; w przypadku gdy zostanie zastosowana kompresja stratna, ukryta informacja może zostać uszkodzona podczas kompresowania danych kontenera,
- modyfikacje wprowadzane przez bramy VoIP oraz zmiany formatu – dane przesyłane przez sieć są przetwarzane przez szereg urządzeń sieciowych, które mogą wprowadzać do nich modyfikacje zarówno w budowie pakietu, jak i danych audio, a także mogą użyć innego formatu kompresji dźwięku.

Ze względu na przedstawione wyzwania pojawiają się dodatkowe wymagania dotyczące metod steganograficznych wykorzystujących transmisję VoIP jako kanału komunikacyjnego, takie jak: konieczność przetwarzania w czasie rzeczywistym, odporność na utratę części pakietów oraz potrzeba synchronizacji [17].

Miarami używanymi do określania jakości ukrytych kanałów w transmisji VoIP są [26]:

- przepustowość – określająca liczbę bitów możliwą do przesłania w jednostce czasu wyrażana w bitach na sekundę,
- całkowita liczba bitów ukrytej wiadomości – określająca ilość danych przesyłanych w jedną stronę podczas typowej rozmowy VoIP,
- przepływ ukrytych danych w trakcie połączenia – określenie ilości danych przesłanych w określonym momencie połączenia.

Spełnienie wymagań w stopniu zapewniającym możliwość tajnej komunikacji przy wykorzystaniu transmisji VoIP wymaga stosowania odpowiednio dobranych rozwiązań. Najprostsze techniki steganograficzne wykorzystywane w telefonii VoIP są oparte na zasadzie działania metody najmniej znaczących bitów (LSB) [31, 32]. Jest ona tak modyfikowana, by dostosować ją do określonych systemów kodowania i kompresji dźwięku przesyłanego przez VoIP [4, 5]. Metoda LSB jest podatna na ataki i zakłócanie transmisji [35]. W celu zwiększe-

nia odporności na te czynniki autorzy [35] zaproponowali adaptacyjną metodę steganografii VoIP polegającą na dynamicznym doborze fragmentów sygnału, w których ukrywane są dodatkowe dane. Fragmenty te są tak dobierane, by pokrywały się z czasem mowy ludzkiej. W momentach ciszy dodatkowe informacje nie są dołączane. Zaproponowane podejście umożliwiło redukcję prawdopodobieństwa wykrycia dołączonej informacji za pomocą miary stosunku sąsiadujących wektorów (ang. *neighbor vectors ratio*). W przypadku proponowanej metody prawdopodobieństwo to wynosi 8%. Autorzy dla porównania wskazują, że prawdopodobieństwo wykrycia informacji dołączonej za pomocą tradycyjnej metody LSB wynosi 80%. Proponowana metoda oferuje pojemność steganograficzną rzędu 114 bajtów na sekundę. Dołączanie informacji powoduje opóźnienie do 20 ms.

Ukryte dane mogą być przesyłane również w nagłówkach pakietów wykorzystywanych protokołów, takich jak TCP, UDP czy IP. Jest to możliwe ze względu na fakt, że pakiety są wyposażone w nagłówek o ustandaryzowanej strukturze, zawierającej szereg pól, które w wielu zastosowaniach nie są wykorzystywane lub ich wartość może zostać zamieniona bez uszkodzenia działania kanału transmisji VoIP [28, 26]. Wymienione protokoły sieciowe są wykorzystywane do przenoszenia danych protokołu czasu rzeczywistego, którego nagłówki stwarzają dodatkowe możliwości ukrycia informacji. One również zawierają pola, które mogą zostać użyte do przeniesienia dodatkowych danych [26]. Są to m.in.:

- błędne oktety – pakiet może zawierać pewną liczbę oktetów niebędących częścią przesyłanych danych, są one domyślnie wypełniane danymi losowymi,
- rozszerzenie nagłówka – nagłówek protokołu RTP może zawierać dodatkowe struktury, wewnątrz których część pól można dowolnie modyfikować,
- wartości pól znacznika czasu i numeru sekwencyjnego w pierwszym pakiecie – domyślnie są wypełniane wartościami losowymi, ich modyfikacja nie nastręcza żadnych trudności,
- najmniej znaczące bity znacznika czasu – ich modyfikacja w nieznacznym stopniu wpłynie na oznaczenie czasu używane do synchronizacji.

Użycie pól nagłówka nie jest jednak rozwiązaniem odpornym na ataki aktywne. Zawartość tych pól może bowiem łatwo zostać uszkodzona lub podmieniona.

Przykładem użycia nagłówka może być metoda zaprezentowana w [24], polegająca na podmienieniu zawartości znacznika autentykacji na zaszyfrowane bity ukrywanych danych. Zwykły odbiorca VoIP będzie traktował takie pakiety jako uszkodzone, jednak osoba mająca klucz będzie w stanie zidentyfikować je i odczytać ukryty przekaz.

W celu zapewnienia jakości usług (QoS) stosowane są dodatkowe protokoły kontroli protokołów czasu rzeczywistego (RTCP). One również przesyłają pakiety zawierające pola, które mogą zostać zmodyfikowane. W [26] przedstawiono listę pól dostępnych do modyfikacji, uzyskując pojemność steganograficzną 160 bitów w każdym pakiecie. Działanie metody od-

bywa się kosztem utraty części funkcjonalności protokołu RTCP. W [26] została zaprezentowana również inna metoda wykorzystująca do ukrywania informacji celowo opóźnione pakiety. Normalnie są one porzucane przez odbiorcę pomimo tego, że dotrą do niego. Metoda polega na celowym opóźnianiu wybranych pakietów zawierających ukrytą informację zamiast danych audio. Odbiorca mający odpowiednie narzędzia i wiedzę o zawartości ukrytych pakietów jest w stanie odebrać je i odczytać ukryty przekaz. Metoda ta została rozwinięta przez autorów [17] przez wykorzystanie metody interpolacji Lagrange'a dla wielomianów, co zwiększyło jej niezawodność oraz poziom oferowanego bezpieczeństwa.

Oprócz wymienionych, stosowane są techniki przeznaczone do ukrywania w dźwięku. Z powodzeniem używane są: metoda najmniej znaczących bitów, metoda echa czy metody operujące na widmie częstotliwościowym sygnału [26].

4. Podsumowanie

Techniki steganograficzne zyskują coraz większą popularność ze względu na oferowane możliwości. Pozwalają zarówno na ochronę własności intelektualnej przez znakowanie utworów, jak i na zabezpieczanie danych przesyłanych poprzez sieć internetową. Ponadto oferują dodatkowe cechy niemożliwe do osiągnięcia za pomocą innych rozwiązań, takie jak zachowanie anonimowości komunikujących się stron oraz ukrycie faktu transmisji danych. Dodatkowo techniki steganograficzne są niewrażliwe na algorytmy opracowane dla komputerów kwantowych w przeciwieństwie do algorytmów kryptograficznych, co ma duże znaczenie w związku z dynamicznym rozwojem komputerów kwantowych oraz ich dystrybucją komercyjną [37].

Autor publikacji jest uczestnikiem projektu „Kwalifikacje dla rynku pracy – Politechnika Lubelska przyjazna dla pracodawcy", współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

BIBLIOGRAFIA

1. Agaian S., Akopian D., Caglayan O., D'souza S.: Lossless adaptive digital audio steganography. Proc. IEEE Int. Conf. Signals, Systems and Computers. IEEE, 2005, s. 903÷906.
2. Alla K., Prasad R.: An Evolution of Hindi Text Steganography. Sixth International Conference Information Technology: New Generations, 2009.

3. Anckaert B., De Sutter B., Chanet D., De Bosschere K.: Steganography for Executables and Code Transformation Signatures. Lecture Notes in Computer Science, Vol. 3506, Springer, 2005, s. 425÷439.
4. Aoki N.: A band extension technique for G.711 speech using steganography. IEICE Transactions on Communications, Vol. E89-B, No.6, 2006, s. 1896÷1898.
5. Aoki N.: A technique of lossless steganography for g.711 telephony speech. Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, ser. IIH-MSP '08. IEEE Computer Society, Washington, DC, USA 2008, s. 608÷611.
6. Banerjee D.: Asymmetric key steganography. International Conference on Information and Electronics Engineering, IPCSIT, Vol. 6, 2011, http://www.ipcsit.com/vol6/47-E20010.pdf.
7. Changder S., Ghosh D., Debnath N. C.: LCS based text steganography through Indian Languages. Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference, 2010.
8. Changder S., Ghosh D., Debnath N. C.: A Greedy Approach to Text Steganography Using Properties of Sentences. Eighth International Conference Information Technology: New Generations (ITNG), 2011.
9. Ciobanu R.-I., Tirsa M., Lupu R., Stan S., Andreica M. I.: SCONeP: Steganography and Cryptography approach for UDP and ICMP. Roedunet International Conference (RoEduNet), 2011.
10. Cvejic N., Seppanen T.: A wavelet domain LSB insertion algorithm for high capacity audio steganography. Proc. IEEE Digital Signal Processing Workshop. IEEE, 2002, s. 53÷55.
11. Cvejic N., Seppanen T.: Increasing the capacity of LSB-based audio steganography. IEEE Workshop on Multimedia Signal Processing. IEEE, 2002, s. 336÷338.
12. Cvejic N., Seppanen T.: Increasing robustness of LSB audio steganography using a novel embedding method. Proc. IEEE Int. Conf. Info. Tech. Coding and Computing, 2. IEEE, 2004, s. 533÷537.
13. Delforouzi A., Pooyan M.: Adaptive Digital Audio Steganography Based on Integer Wavelet Transform. Circuits Syst. Signal Process., Vol. 27, 2008, s. 247÷259.
14. Ding F., Wang X., Shen Y., Lu Y., Hu J.: Non-embedded audio watermark based on wavelet transform. IEEE 3rd International Conference Software Engineering and Service Science (ICSESS), IEEE, 2012.
15. Dymarski P.: Filtracja sygnałów dźwiękowych jako metoda znakowania wodnego i steganografii. Krajowe Sympozjum Telekomunikacji, Bydgoszcz. Akademia Techniczno-Rolnicza w Bydgoszczy, 2006, s. 12÷23.

16. Dymarski P., Pobłocki A., Baras C., Moreau N.: Algorytmy znakowania wodnego sygnałów dźwiękowych. Krajowe Sympozjum Telekomunikacji, Bydgoszcz. Akademia Techniczno-Rolnicza w Bydgoszczy, 2003, s. 26÷34.
17. Hamdaqua M., Tahvildari L.: ReLACK: A Reliable VoIP Steganography Approach. Fifth International Conference Secure Software Integration and Reliability Improvement (SSIRI), 2011.
18. Johnson N., Katzenbeisser S.: A survey of steganographic techniques. Information hiding: Techniques for steganography and digital watermarking. Artech House, London 2000.
19. Katzenbeisser S., Petricolas A.: Information Hiding. Artech House, London 2000.
20. Kim S., Kwon H., Bae K.: Modification of polar echo kernel for performance improvement of audio watermarking. International Workshop on Digital Watermarking, No. 2, LNCS 2939, Springer, 2004, s. 456÷466.
21. Koziel G.: Increasing steganographic capacity of the MF method. Actual Problems of Economics, No. 6, Vol. 132, 2012, s. 367÷373.
22. Koziel G.: Steganographic algorithm of hiding information in sound based on Fourier transform and masking. Control and Cybernetics, No. 4, Vol. 40, 2011, s. 1231÷1247.
23. Lie W. N., Chang L. C.: Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification. IEEE Trans. on Multimedia, Vol. 8, No. 1, 2006, s. 46÷59.
24. Lucena N., Lewandowski G., Chapin S.: Covert Channels in IPv6. Proc. of 5th Privacy Enhancing Technologies Workshop, Lecture Notes in Computer Science, Vol. 3856, Springer, 2005, s. 147÷166.
25. Matsuka H.: Spread spectrum audio steganography using subband phase shifting. IEEE Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '06). IEEE, 2006, s. 3÷6.
26. Mazurski W., Szczypiorski K.: Steganography of VoIP Streams. Lecture Notes in Computer Science, Vol. 5332, Springer, 2008, s. 1001÷1018.
27. Murata H., Ogihara X., Iwata M, Shiozaki A.: Sound quality improvement of multiple audio watermarking by using DC component. IEICE(A), Vol. J93-A, No. 3, 2010, s. 171÷180.
28. Murdoch S., Lewis S.: Embedding Covert Channels into TCP/IP. Information Hiding, 2005, s. 247÷261.
29. Shirali-Shahreza M.: Steganography in MMS. Multitopic Conference, INMIC 2007. IEEE International Conference, 2007.

30. Tachibana R., Shimizu S., Nakamura T., Kobayashi S.: An audio watermarking method robust against time and frequency fluctuation. Proc. of SPIE Int. Conf. on Security and Watermarking of Multimedia Contents III, Security Professionals Information Exchange, Vol. 4314, 2001, s. 104÷115.
31. Tian H., Zhou K., Huang Y., Feng D., Liu J.: A covert communication model based on least significant bits steganography in voice over IP. Proceedings of the 9th International Conference for Young Computer Scientists, IEEE Computer Society, Washington, DC, USA 2008, s. 647÷652.
32. Tian H., Zhou K., Jiang H., Feng D.: Digital logic based encoding strategies for steganography on voice-over-ip. Proceedings of the 17th ACM international conference on Multimedia, ser. MM '09, New York, NY, USA 2009, s. 777÷780.
33. Xiang S., Huang J., Yang R.: Time-Scale Invariant Audio Watermarking Based on the Statistical Features in Time Domain. Artificial Intelligence and Lecture Notes in Bioinformatics, Springer 2007, s. 93÷108.
34. Xiang S., Kim H., Huang J.: Audio watermarking robust against time scale modification and MP3 compression. Signal Processing, Vol. 88, No. 10, 2008, s. 2372÷2387.
35. Xu E., Liu B., Xu L., Wei Z.: Adaptive VoIP Steganography for Information Hiding within Network Audio Streams. Proc. NBiS, Tirana, Albania 2011.
36. Wang Z., Zhao X., Wang H., Cui G.: Information hiding based on DNA steganography. 4th IEEE International Conference Software Engineering and Service Science (ICSESS), 2013.
37. Hollister S.: D-Wave sells first commercial quantum computer to Lockheed Martin, http://www.engadget.com/2011/05/29/d-wave-sells-first-commercial-quantum-computer-to-lockheed-marti/.

Wpłynęło do Redakcji 9 stycznia 2014 r.

Abstract

Steganography is a science that deals with hiding some information in another. Of course this definition concerns the digital version of steganography. Digital steganography has a wide spectrum of applications: watermarking, hidden communication, fingerprinting, hidden data volumes and others. Depending on the application the various features of the used method are required. The basic features that characterize each method are: capacity, transparency and robustness against hidden data damage.

Watermarking consists of adding the signatures to the watermarked content to proof the copyright or authorship. The most important aspect in this type of application is to obtain good level of transparency and robustness. In fingerprinting we want to let the receiver know that the content was not modified. It is only possible when included fingerprint is destroyed after any modification of the fingerprinted data. To obtain this effect, it is necessary to apply a method characterized by low robustness. In both of the above applications the capacity does not have to be very big, because the amount of added data is insignificant. This feature is important in secret communication, whose main task is to hide as big a portion of data as it is possible. In secret communication the transparency is also important; the hidden data should be impossible to detect by unauthorized parties. Robustness in this application is rather not important unless it is a noisy channel that is used to send the stegocontainer with secret data inside.

In the article the review of various applications is shown. In each application the currently popular algorithms having the desired features are presented.

Adres

Grzegorz KOZIEŁ: Politechnika Lubelska, Instytut Informatyki, ul. Nadbystrzycka 36b, 20-618 Lublin, Polska, g.koziel@pollub.pl.