STUDIA INFORMATICA 2011
Volume 32 Number 2A (96)

Grzegorz KOZIEŁ
Politechnika Lubelska, Instytut Informatyki

ZASTOSOWANIE TRANSFORMATY FOURIERA W STEGANOGRAFII DŹWIĘKU

Streszczenie. W artykule przedstawiono zastosowanie transformaty Fouriera w steganografii sygnałów dźwiękowych. Zaproponowano nową metodę ukrywania informacji w dźwięku, bazującą na zmodyfikowanej transformacie Fouriera. Prezentowana metoda wykorzystuje zjawisko maskowania do określenia optymalnego miejsca ukrycia informacji. Informacja ukrywana jest poprzez modyfikację wartości prążków widma częstotliwościowego sygnału.

Słowa kluczowe: steganografia, transformata Fouriera, ochrona informacji

USING FOURIER TRANSFORM IN SOUND STEGANOGRAPHY

Summary. Various use of the Fourier transform in steganogtraphy is presented in the article. A new method of information hiding in sound is proposed. This method employs modified Fourier transform to hide data. The masking phenomenon is used to determine the optimal hiding place. Information is hidden by modifying spectrum stripes values.

Keywords: steganography, Fourier transform, information protection

1. Wstęp

Steganografia jest nauką zajmującą się ochroną informacji. Jej działanie polega na ukrywaniu ważnej (chronionej) informacji w innej, niemającej wartości, zwanej *kontenerem*. Nośnik wynikowy zawierający ukryte dane nazywamy *stegokontenerem*. Wbrew przekonaniom steganografia nie jest nową nauką. Powszechnie znane są jej wcześniejsze postaci takie, jak choćby użycie atramentu sympatycznego czy technika mikrokropek. Jednak obecnie rozwój steganografii skupia się na jej postaci cyfrowej, która pojawiła się stosunkowo

niedawno wraz z rozwojem techniki cyfrowej. Diametralnie zmieniło to również sposób działania steganografii, ze względu na uniezależnienie danych od nośnika. Ilekroć w dalszej części artykułu mowa będzie o steganografii, to będzie to dotyczyło steganografii cyfrowej. Jej zasada działania pozostała taka sama, jak w przypadku wersji analogowej, jednak zmianie uległa technika ukrywania. Steganografia cyfrowa ukrywa dane poprzez wprowadzenie drobnych, niezauważalnych zmian do innych danych cyfrowych. Może to zostać wykonane za pomocą wielu istniejących metod. Najprostsze z nich bazują na technice najmniej znaczących bitów (LSB), polegającej na zastępowaniu najmniej znaczących bitów oryginalnego sygnału bitami ukrywanej informacji[19]. Pozwala to na uzyskanie bardzo dużej pojemności steganograficznej. Niestety metody LSB nie wykazują żadnej odporności na modyfikację nośnika. Ponadto, przy modyfikacji zbyt dużej liczby najmniej znaczących bitów w sygnale pojawiają się słyszalne zakłócenia. W celu ograniczenia ich poziomu często uwzględnia się zjawisko maskowania [1]. Technika LSB łączona jest również z innymi takimi, jak minimum error replacement [4] lub też wykorzystuje rozpraszanie błędów [5].

Niektórzy autorzy w swoich algorytmach implementują rozwiązania pozwalające na zwiększenie odporności na uszkodzenia, lecz ze względu na dużą pojemność steganograficzną i wykorzystanie najbardziej nieodpornej na zmiany części nośnika udaje się osiągnąć tylko niewielki wzrost odporności [11, 12].

Metody LSB spotykane są w wersjach działających w różnych dziedzinach zarówno czasu czy częstotliwości, jak i wybranej ortogonalnej lub biortogonalnej bazy [1, 6, 7, 11, 12]. Istotne jest by przekształcenie wykorzystywane przy przejściu do wybranej reprezentacji sygnału było w pełni odwracalne.

Istnieją również metody steganograficzne poprawiające jakość sygnału. Wykorzystywane są do tego zmodyfikowane algorytmy usuwania zakłóceń [15, 20].

Za pomocą przedstawionych metod nie udało się uzyskać dobrego poziomu odporności. Udało się to natomiast przy użyciu metod dołączania echa [14, 3, 8, 13, 10, 16, 9], filtracji subpasmowej [16], kodowania lub modulacji fazy dźwięku [14, 3, 18], modyfikacji histogramu [22, 23], a nawet za pomocą metod ukrywania w obrazie [21, 2].

Przegląd metod steganograficznych pokazuje, że trudno jest uzyskać wysoki poziom odporności za pomocą metod operujących w dziedzinie czasu. Na tym polu o wiele lepiej radzą sobie metody wykorzystujące transformację sygnału, jednak często powodują wprowadzanie słyszalnych zakłóceń.

2. Metody wykorzystujące transformację Fouriera

W wyniku transformaty Fouriera uzyskujemy reprezentację częstotliwościową analizowanego sygnału. Modyfikacja wartości poszczególnych prążków lub też fazy sygnału umożliwia wprowadzenie trwałych zmian w sygnale. Może to zostać wykorzystane do ukrycia dodatkowej informacji. Istniejące techniki steganograficzne bazują na zmianie wartości poszczególnych prążków modułu widma lub modyfikują fazę sygnału. Wśród nich możemy wyróżnić kilka grup.

- Techniki najmniej znaczących bitów – metody polegające na zamianie najmniej znaczących bitów modułu widma sygnału na bity ukrywanej informacji. Działają na identycznej zasadzie, jak tradycyjne metody najmniej znaczących bitów. Różnica polega jedynie na wykorzystaniu reprezentacji sygnału w dziedzinie częstotliwości, a nie czasu. W wyniku wykorzystania widma częstotliwościowego uzyskujemy jednak większą odporność na uszkodzenia ukrytych danych.
- Techniki modyfikujące wartości prążków modułu widma, mające na celu uzyskanie wysokiej odporności na uszkodzenia. Wprowadzają one znaczące modyfikacje wartości niewielkiej liczby prążków. Duża wartość zmiany gwarantuje, że w wyniku niewielkich modyfikacji nośnika nie zostanie ona usunięta. Niewielka liczba modyfikowanych prążków sprawia, że zmiana w skali całego sygnału jest niewielka i trudna do wykrycia. Metody te wykazują dużą odporność na uszkodzenia i zniszczenie dołączonej informacji. Odbywa się to jednak kosztem znacznego zmniejszenia pojemności steganograficznej i możliwości wprowadzenia słyszalnych zakłóceń. Do zapisu informacji może zostać wykorzystany tylko jeden prążek. Odczyt możliwy jest wówczas poprzez porównanie widma stegokontenera z oryginalnym. Metoda ta jednak nie zyskała popularności, ze względu na konieczność zapewnienia bezpiecznego kanału do wymiany oryginalnych nośników. Wady tej pozbawione są metody wykorzystujące większą liczbę prążków do zapisu informacji. Najczęściej używane są dwa prążki. W przypadku wykorzystania dwóch częstotliwości, modyfikacji podlega stosunek ich wartości. Jeśli większy udział ma częstotliwość f1, to jest to równoznaczne z zakodowaniem jedynki, a jeśli f2, to ukryte jest zero. Na potrzeby niniejszego artykułu metoda ta została oznaczona symbolem TF. W niektórych metodach wykorzystywane są trzy prążki widma. Osiągnięcie stosunku wartości $f1<f2<f3$ jest interpretowane jako dołączenie zera, $f1>f2>f3$ jako dołączenie jedynki binarnej. Niespełnienie żadnej z dwóch powyższych nierówności oznacza, że w danym fragmencie nie została dołączona żadna informacja. Takie podejście pozwala na zwiększenie pewności odczytu oraz zmniejszenie poziomu wprowadzanych zniekształceń, poprzez zapewnienie

możliwości uniknięcia wprowadzania modyfikacji we fragmentach, które zostałyby w znacznym stopniu zniekształcone.

- Techniki modyfikujące prążki widma o największej energii zostały przedstawione w [4]. Zaproponowano tam wykorzystanie k największych współczynników transformaty do ukrycia znaku wodnego, wprowadzanego za pomocą DFT. Zaletą tego podejścia jest uzyskanie dużej odporności na uszkodzenia oraz zniszczenie. Aby usunąć tak dołączone dane, trzeba w znacznym stopniu uszkodzić sygnał, co spowoduje utratę jego wartości. Jednak modyfikacja największych współczynników transformaty wprowadza znaczne zmiany do sygnału. O ile oko ludzkie ma niewielką wrażliwość na zmiany częstotliwości i można zaimplementować proponowaną metodę do znakowania obrazów, to w dźwięku nie znajduje ona zastosowania ze względu na dużą wrażliwość ludzkiego słuchu na zmiany częstotliwości. Do zidentyfikowania dołączonego znaku wodnego niezbędne jest porównanie z oryginałem.
- Metody wykorzystujące znaczące punkty sygnału. W [17] przedstawiono metodę opracowaną przez Mansour i Tewfik. Autorzy wskazują, że jest ona w stanie uzyskać bardzo wysoką odporność na różne przekształcenia sygnału. Osiągają tak wysoką odporność przez wielokrotne umieszczenie tej samej sekwencji w utworze. Odbywa się to kosztem znacznego zmniejszenia pojemności steganograficznej, co czyni tę metodę przydatną jedynie do znakowania wodnego utworów.
- Techniki zmiany fazy sygnału ukrywające informację poprzez wprowadzanie modyfikacji w przebiegu fazy sygnału. Metody te również charakteryzują się wysoką odpornością na uszkodzenia oraz mają małą pojemność steganograficzną, ze względu na konieczność modyfikacji fazy w całym przetwarzanym fragmencie.

W metodach wykorzystujących cały przetwarzany sygnał do ukrycia bitu informacji konieczne jest podzielenie sygnału na bloki. Każdy z bloków przenosi wówczas jeden bit informacji. Najpierw blok przekształcany jest za pomocą DFT do reprezentacji częstotliwościowej i określane są wartości wybranych prążków widma. Następnie wykonywana jest modyfikacja tych wartości, zgodnie z przyjętym algorytmem. Tak przygotowane widmo transformowane jest z powrotem za pomocą IDFT do postaci przebiegu czasowego. Przetworzone bloki łączone są w jeden sygnał.

Metody bazujące na transformacie Fouriera są z powodzeniem wykorzystywane w steganografii obrazu. W przypadku sygnałów audio ich zastosowanie w technikach anonimowej komunikacji ma marginalne znaczenie, ze względu na wprowadzanie słyszalnych zakłóceń przy dołączaniu dużych ilości informacji. Sygnał dołączany za pomocą zaprezentowanych metod musiałby mieć bardzo małą moc, co spowodowałoby jego nieodporność na zakłócenia. Wykorzystanie częstotliwości większych niż 16 kHz pozwala uniknąć słyszalnych zakłóceń, jednak to pasmo częstotliwości jest pomijane podczas kompresji stratnej czy

zmniejszeniu częstotliwości próbkowania. Ponadto, zakres częstotliwości dźwięku najczęściej zawiera się w przedziale od 20 Hz do 10 kHz. Pojawienie się podczas analizy częstotliwościowej sygnału wyższych częstotliwości jest bardzo łatwe do zauważenia. W efekcie obecność dołączonej informacji jest łatwa do wykrycia.

3. Proponowane rozwiązanie – metoda MF

Na bazie metody TF opracowana została jej modyfikacja (MF) wykorzystująca, podobnie jak poprzedniczka, dwa prążki do ukrycia bitu dodatkowej informacji. Wprowadzone zmiany polegają na:

- wykorzystaniu zjawiska maskowania do określenia częstotliwości maskowanych,
- adaptacyjnym dobieraniu częstotliwości do zmodyfikowania, tak by wprowadzane zmiany znajdowały się w sąsiedztwie prążka widma częstotliwościowego, który ma największą wartość,
- adaptacyjnym dopasowywaniu wartości wprowadzanych zmian do parametrów sygnału w przetwarzanym fragmencie sygnału,
- zmienionym kodowaniu binarnych wartości ukrywanej informacji: ukrycie binarnego zera polega na doprowadzeniu do sytuacji, w której wartości obydwu wybranych prążków będą sobie równe; ukrycie binarnej jedynki jest równoznaczne z uzyskaniem określonej różnicy wartości (R) pomiędzy wybranymi prążkami.

Działanie proponowanego algorytmu steganograficznego przebiega w 5 etapach:

1. Podziału na bloki – polega na podzieleniu sygnału na fragmenty, które zostaną użyte do ukrycia informacji. Wielkość oraz położenie fragmentów zależą od klucza steganograficznego.
2. Przetworzenia bloków dyskretną transformatą Fouriera (DFT) – pozwalającego na przejście do dziedziny częstotliwości.
3. Dołączenia bitu informacji – wykonywanego poprzez wybór pary prążków i odpowiednią modyfikację ich wartości.
4. Przetworzenia bloków odwrotną transformatą Fouriera (IDFT) – gwarantującego powrót do dziedziny czasu.
5. Złożeniu przetworzonych bloków – mającego na celu złączenie wszystkich fragmentów sygnału.

Rozwinięcie punktu 3 stanowi pełny przebieg algorytmu ukrywania bitu informacji b=1 we fragmencie sygnału, który zaprezentowany został poniżej.

1) Sygnał przetwarzany jest za pomocą DFT – w wyniku uzyskujemy wektor Y_c,
2) wyliczamy wartość bezwzględną z wartości wektora $Y_r=|Y_c|$,
3) w Y_r wyszukujemy wartość maksymalną $W_{max}=max(Y_r)$,
4) obliczamy oczekiwaną różnicę $R= W_{max} \bullet R_p$ (R_p – wartość pochodząca z klucza steganograficznego, określająca siłę ukrywania),
5) określamy położenie f_{max} prążka widma o wartości maksymalnej p_{max} oraz prążków spełniających wymogi stawiane prążkom przenoszącym dołączoną informację,
6) wybieramy prążki widm p_1 i p_2, przeznaczone do dołączenia dodatkowej informacji oraz określamy ich wartości w_1 i w_2,
7) dla każdego z nich na podstawie klucza określamy maksymalną dopuszczalną wartość prążka: $W_{1\_dopuszczalna}$ i $W_{2\_dopuszczalna}$,
8) jeśli $|w_2-w_1|\geq R$, to koniec algorytmu (prążki widma mają odpowiednią wartość),
9) jeśli $|w_2-w_1|\leq R$, to sprawdzamy, który prążek jest mniejszy, a który większy, oznaczamy odpowiednio ich wartości: w_m, w_w. Następnie obliczamy docelowe wartości prążków widma:
   - jeśli $w_m/\theta_{max}+R\leq w_w$, to $w_m=w_w-R-rnd(\beta)$, ($rnd(\beta)$ – funkcja zwracająca liczbę losową z przedziału $<-\beta, \beta>$, θ_{max} – określona w kluczu steganograficznym maksymalna wartość przez jaką można podzielić wartość prążka widma podczas jego zmniejszania),
   - jeśli $w_m/\theta_{max}+R>w_w$, to $w_m=w_m/\theta_{max}$, $w_w=w_m+R+rnd(\beta)$,
10) na podstawie wyliczonych wartości aktualizujemy wektor Y_c,
11) za pomocą IDFT zaktualizowany wektor Y_c zmieniamy na sygnał w funkcji czasu.

4. Przezroczystość dołączonych danych

W celu weryfikacji jakości opracowanej metody, za jej pomocą utworzono zestaw stegokontenerów. Porównywalny zestaw stegokontenerów został utworzony za pomocą metody TF. Ze względu na różne właściwości, uzyskiwane podczas ukrywania metodą TF w pasmach słyszalnym i niesłyszalnym, utworzone zostały dwa zestawy stegokontenerów – jeden dla metody TF, wykorzystującej pasmo 330-360 Hz, oznaczony TF_{aud} oraz drugi oznaczony TF_{inaud}, powstały w wyniku użycia pasma powyżej 20 kHz.

Porównanie przezroczystości wprowadzanych zakłóceń przeprowadzono w zakresie następujących miar numerycznych:

1) błędu średniokwadratowego, zdefiniowanego wzorem:

$$MSE = \frac{1}{N}\sum (S_n - S'_n)^2 \tag{1}$$

2) odległości sygnału od szumu, według:

$$SNR = 10\log(\sum_{\mathrm{n}} \mathrm{S}_{\mathrm{n}}^2 / \sum_{n} (S_n - S'_n)^2) \tag{2}$$

3) szczytowej wartości odległości sygnału od szumu, zdefiniowanego wzorem:

$$PSNR = 10\log(\mathrm{R}^2 / MSE) \tag{3}$$

4) średniej bezwzględnej różnicy pomiędzy sygnałami, opisanej równaniem:

$$AD = \frac{1}{N} \sum_{n} |S_n - S'_n| \tag{4}$$

5) przezroczystości znaku wodnego, opisanej równaniem:

$$AF = 1 - \sum_{n} (S_n - S'_n)^2 / \sum_{\mathrm{n}} \mathrm{S}_{\mathrm{n}}^2 \tag{5}$$

Wyniki przeprowadzonego porównania przedstawione zostały w tabeli 1.

Tabela 1

Zniekształcenia wprowadzane przez porównywane metody

Metoda	MSE	SNR [dB]	PSNR [dB]	AD	AF
MF	2E-4	24,1	85,2	0,008	1
TF_{aud}	2,8E-4	15,3	75,4	0,018	0,97
TF_{inaud}	3E-4	22,3	83,3	0,015	0,99

Analiza wyników umieszczonych w tabeli pozwala zauważyć, że metoda MF osiąga przewagę nad metodą TF. Uwidacznia się to zwłaszcza w wynikach osiąganych w mierze AF, która jako jedyna uwzględnia zjawisko maskowania.

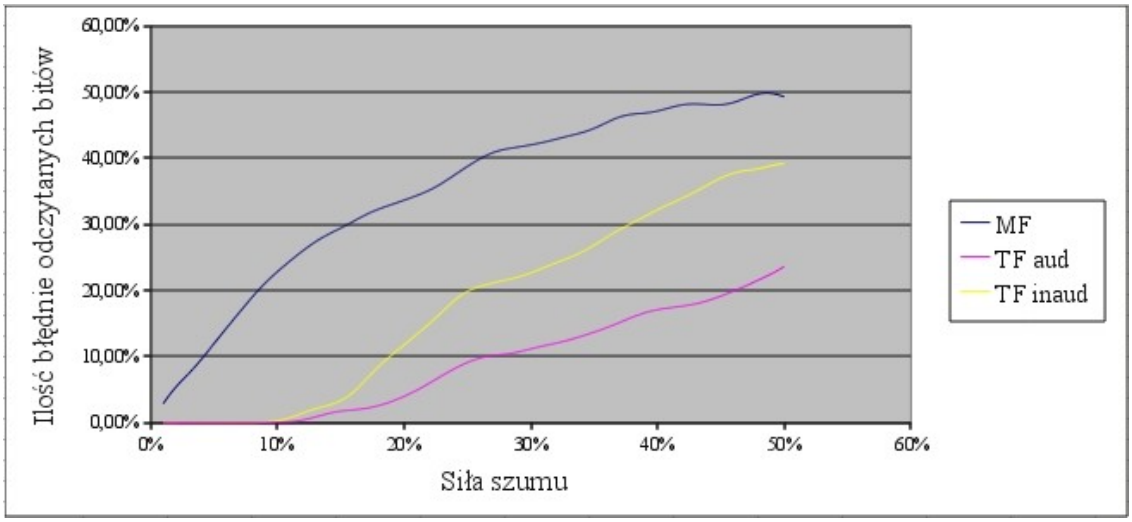
5. Odporność dołączonych danych na uszkodzenia

W przypadku gdy konieczne jest zastosowanie steganografii w kanałach komunikacyjnych wprowadzających zmiany do nośnika, konieczne jest korzystanie z metod zapewniających odporność na uszkodzenia ukrytej informacji.

Stegokontenery utworzone za pomocą porównywanych metod poddane zostały różnym przekształceniom. Po ich wykonaniu przeprowadzany był proces odczytywania ukrytej informacji, która podlegała ocenie, w celu określenia liczby błędnie odczytanych bitów (BER). Wyniki odporności na dołączanie szumu przedstawione zostały na rys. 1.

Jak widać na rys. 1 metoda TF (w obu przypadkach) wykazuje lepszą odporność na dołączanie szumu. Metoda MF wykazuje niewielki poziom odporności na tego typu operację, niemniej jednak dla szumu o niezbyt dużej sile poziom błędów jest na tyle niski, że z powodzeniem może zostać skorygowany przy zastosowaniu algorytmu korekcji błędów.

Zupełnie inaczej przedstawiają się wyniki odporności na przekształcenia dynamiczne, zaprezentowane w tabeli 2.

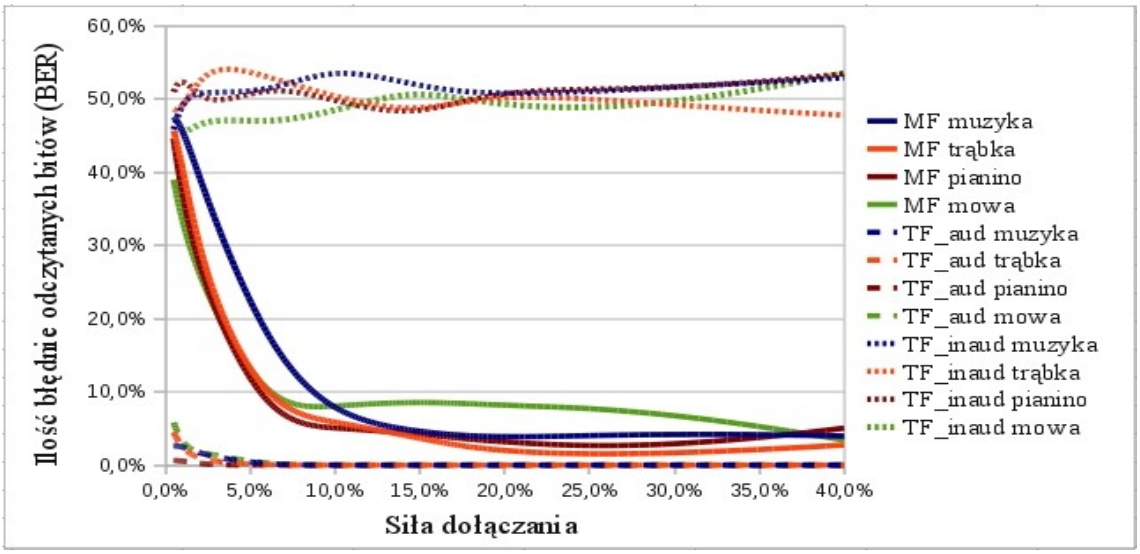


Rys. 1. Odporność porównywanych metod na dołączanie szumu
Fig. 1. Resistance compared methods for attaching noise

Tabela 2

Liczba błędów wprowadzana przez przekształcenia dynamiczne

metoda	wyciszanie				normalizacja			
	muzyka	mowa	pianino	trąbka	muzyka	mowa	pianino	trąbka
MF	**4,4%**	**4,6%**	**2,1%**	**1,3%**	**4,4%**	**5,3%**	**2,1%**	**0%**
TF_{aud}	56,6%	50%	58,3%	48,9%	47,7%	49,4%	60,8%	49,7%
TF_{inaud}	0%	0%	0%	0%	0%	0%	0%	0%



Rys. 2. Odporność porównywanych metod na kompresję mp3
Fig. 2. Resistance compared methods for mp3 compressing

Analiza wyników przedstawionych w tabeli 2 pozwala zauważyć, że metoda MF osiąga dobre wyniki odporności na przekształcenia dynamiczne. W przypadku obu badanych przekształceń poziom błędów nie przekracza kilku procent. Ciekawe zjawisko daje się zauważyć

w przypadku metody TF. Okazuje się bowiem, że odporność tej metody zależy od wykorzystywanego pasma częstotliwości – w paśmie słyszalnym metoda TF nie jest odporna na badane przekształcenia. Mogłoby się wydawać, że metoda TF działająca w paśmie niesłyszalnym wykazuje przewagę nad pozostałymi, jednak analiza wyników odporności na kompresję mp3 o przepływności 64 kbit/s pokazuje, że wcale tak nie jest. Tak silna kompresja usuwa częstotliwości niesłyszalne z sygnału, a wraz z nimi ukryta informację. Metoda MF, również w tym przypadku, pozwala na uzyskanie dobrego poziomu odporności na uszkodzenie ukrytej informacji – przy zastosowaniu odpowiednio dużej siły ukrywania (R_p) liczba błędów jest tak mała, że z powodzeniem może zostać naprawiona przez algorytm korekcji błędów. Uzyskane rezultaty odporności na kompresję mp3 zostały zaprezentowane na rys. 2.

6. Wnioski

Zaproponowane w artykule podejście do problemu steganografii komputerowej, polegające na połączeniu zjawiska maskowania częstotliwościowego sygnału dźwiękowego z dyskretną transformatą Fouriera, pozwoliło uzyskać skuteczną i efektywną metodę ukrywania informacji w kontenerach dźwiękowych. Zastosowane podejście polega na odnalezieniu w widmie prążka zdolnego zamaskować zmiany wprowadzone w innych prążkach o zbliżonej częstotliwości (maskera), a następnie na określeniu skutecznie maskowanych prążków widma częstotliwościowego. Dodatkową zaletą tego rozwiązania jest uzależnienie położenia wykorzystywanych prążków widma częstotliwościowego sygnału od położenia maskera, skutkujące niezależnym wyborem prążków w każdym z fragmentów sygnału. Powoduje to rozproszenie dołączanej informacji w szerokim spektrum częstotliwości, znacząco utrudniając celowe uszkodzenie ukrytych danych – zwłaszcza, że modyfikowane częstotliwości prawie zawsze znajdują się w paśmie słyszalnym.

Wielkość wprowadzanych zmian wartości prążków widma uzależniona jest od wartości największego prążka w widmie. Pozwala to na uzyskanie optymalnego rozwiązania zarówno pod kątem odporności, jak i adaptacji wartości wprowadzanych zmian do amplitudy sygnału w danym fragmencie tego sygnału oraz na wykorzystanie wszystkich fragmentów do ukrycia, niezależnie od ich głośności. Ponadto, rozwiązanie to pozwala uzyskać wysoką odporność na przekształcenia dynamiczne sygnału, gdyż fragmenty przetwarzane są niezależnie, a dodatkowa informacja ukryta jest w proporcjach pomiędzy prążkami widma. Zmiany w krótkim przedziale czasu są praktycznie jednakowe dla całego fragmentu, więc nie modyfikują wykorzystywanych proporcji wartości prążków widma.

Wyniki uzyskane podczas porównań z metodą TF pokazują, że zastosowane rozwiązania pozwoliły na uzyskanie większej przezroczystości ukrywanych danych pomimo dołączania ich w paśmie słyszalnym. Jednocześnie pozwoliły na uzyskanie odporności na przekształcenia, które niszczą informację ukrytą za pomocą metody TF, operującej na paśmie słyszalnym.

BIBLIOGRAFIA

1. Agaian S. S., Akopian D., Caglayan O., D'Souza S. A.: Lossless adaptive digital audio steganography. Proc. IEEE Int. Conf. Signals, Systems and Computers, 2005, s. 903÷906.
2. Bao P., Ma X.: MP3-resistant music steganography based on dynamic range transform. IEEE Int. Sym. Intelligent Signal Proc. and Communication Systems, 2004, s. 266÷271.
3. Bender W., Gruhl D., Morimoto N., Lu A.: Techniques for data hiding. IBM Systems Journal, Vol.35, No. 3&4, 1996, s. 313÷336.
4. Cox I., Kilian J., Leighton T., Shamon T.: A secure, robust watermark for multimedia. Information hiding, Lect. Notes of Comp. Science(1147), Springer-Verlag, 1996, s. 185÷206.
5. Cvejic N., Seppanen T.: Increasing robustness of LSB audio steganography using a novel embedding method. Proc. IEEE Int. Conf. Info. Tech. Coding and Computing, Vol. 2, 2004, s. 533÷537.
6. Cvejic N., Seppanen T.: A wavelet domain LSB insertion algorithm for high capacity audio steganography. Proc. IEEE Digital Signal Processing Workshop, 2002, s. 53÷55.
7. Delforouzi A., Pooyan M.: Adaptive Digital Audio Steganography Based on Integer Wavelet Transform. Circuits Syst Signal Process Vol. 27, 2008, s. 247÷259.
8. Dymarski P., Poblocki A., Baras C., Moreau N.: Algorytmy znakowania wodnego sygnałów dźwiękowych. Krajowe Sympozjum Telekomunikacji, Bydgoszcz 2003.
9. Dymarski P.: Filtracja sygnałów dźwiękowych jako metoda znakowania wodnego i steganografii. Bydgoszcz 2006.
10. Garay A.: Measuring and evaluating digital watermarks in audio files. Washington 2002.
11. Gopalan K.: Audio steganography using bit modification. Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Vol. 2, 2003, s. 421÷424.
12. Gopalan K.: Audio steganography by cepstrum modification. Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 5, 2005, s. 481÷484.
13. Gruhl D., Lu A.: Echo Hiding. Information Hiding Workshop. Cambridge University, UK 1996, s. 295÷315.
14. Johnson N. F., Katzenbeisser S. C.: A survey of steganographic techniques, Information hiding: Techniques for steganography and digital watermarking. Boston 2000, s. 43÷48.

15. Katzenbeisser S., Petricolas A.P.: Information Hiding, Artech House, 2000.
16. Kim S., Kwon H., Bae K.: Modification of polar echo kernel for performance improvement of audio watermarking. Lecture notes in computer science: international workshop on digital watermarking, No. 2, Vol. 2939, Seoul, Coree, Republique De (22/10/2003) 2004, s. 456÷466.
17. Mansour M., Tewfik A.: Audio Watermarking by Time-Scale Modification. IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings 3, 2001, s. 1353÷1356.
18. Matsuka H.: Spread spectrum audio steganography using sub-band phase shifting. IEEE Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), 2006, s. 3÷6.
19. Petitcolas F. A. P., Ross J., Kuhn G.: Information Hiding—A Survey. Proceedings of the IEEE, special issue on protection of multimedia content 87(7), 1999, s. 1062÷1078.
20. RLE, Massachusetts 1999, http://rleweb.mit.edu/Publications/currents/cur111/11-1watermark.htm.
21. Santosa R. A., Bao P.: Audio-to-image wavelet transform based audio steganography. IEEE Int. Symp., 2005, s. 209÷212.
22. 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 2007, s. 93÷108.
23. Xiang S., Kim H., Huang J.: Audio watermarking robust against timescale modification and MP3 compression. http://ieeexplore.ieee.org.

Recenzenci: Dr hab. inż. Andrzej Chydziński, prof. Pol. Śląskiej
Dr inż. Jerzy Respondek

Wpłynęło do Redakcji 31 stycznia 2011 r.

Abstract

Developed steganographic methods that deal with hidden communication are focused on high capacity. It is not always enough. In some areas it may be more important to achieve hidden data robustness too, especially, when using a noisy communication channel. It is worthy to use methods that have enough steganographic capacity and at the same time ensure hidden data robustness. Good results in this field can be obtained by using the Fourier trans-

form. An overview of steganographic methods which use the Fourier transform as a base operation is presented in the article. A new steganographic method is presented too. This method introduces modifications into a choosen spectrum stripes to hide additional data inside an audio signal. The presented method uses the masking phenomenon to determine the best places to introduce modifications. Additionally, the value of introduced changes is adaptively adjusted if the signal parameters change. Research results show that the presented approach allows to obtain good robustness and transparency of hidden data at the same time. The steganographic capacity is about 42 bits per second in each channel of recording. It is enough to allow for hidden communication.

Adres

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