Grzegorz KOZIEŁ

MOŻLIWOŚCI WYKORZYSTANIA TRANSFORMATY FOURIERA W STEGANOGRAFII DŹWIĘKU

STRESZCZENIE *Niniejszy artykuł prezentuje możliwości wykorzystania transformaty Fouriera jako przekształcenia bazowego do opracowania metody steganograficznej wykorzystującej dźwięk jako kontener. Pokazuje możliwości rozwiązania problemu wprowadzania słyszalnych zakłóceń podczas wykonywania operacji w dziedzinie częstotliwości.*

Słowa kluczowe: *steganografia, ochrona informacji.*

1. WSTĘP

Istnieje wiele metod steganograficznych wykorzystujących dźwięk jako nośnik ukrytej informacji [23]. Największą pojemnością charakteryzują się metody najmniej znaczących bitów (LSB). Polegają one na zamienianiu najmniej znaczących bitów kontenera bitami ukrywanej informacji. Mogą operować w dziedzinie

mgr inż. Grzegorz KOZIEŁ
e-mail: grzes@pluton.pol.lublin.pl

Zakład Ochrony Informacji,
Instytut Informatyki,
Wydział Elektrotechniki i Informatyki,
Politechnika Lubelska

PRACE INSTYTUTU ELEKTROTECHNIKI, zeszyt 247, 2010

czasu, częstotliwości czy też innej pozwalającej na pełną odwracalność operacji [1, 8, 4, 5]. Często łączy się również tą technikę z innymi takimi jak minimum error replacement [5], rozpraszania błędów [6] czy wykorzystuje efekt maskowania [4]. Metody te nie są odporne na uszkodzenia ukrytych danych. Niektórzy autorzy implementują w swoich algorytmach 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 [6, 7, 13].

Aby uniknąć wprowadzania dodatkowych zniekształceń sygnału modyfikacje mogą zostać wykonane w istniejącym w utworze szumie. Niektórzy autorzy proponują wykorzystanie odpowiednio zmodyfikowanych algorytmów usuwania szumu, przez co możliwa jest poprawa jakości sygnału podczas steganograficznego ukrywania danych [17, 21].

Uzyskanie większej odporności ukrytych danych wymaga zastosowania przekształceń odpornych na modyfikację sygnału. Najczęściej jednak wprowadzają one znaczne zniekształcenia. Konieczne staje się więc wykorzystanie niedoskonałości HAS do zamaskowania wprowadzonych zmian.

Dużą popularność zyskały metody steganograficzne oparte na dołączaniu echa. Różne formy tego podejścia [15, 3, 14, 11, 18, 9, 10] pozwoliły na uzyskanie dobrej odporności na uszkodzenia ukrytych danych. Wysoki poziom odporności oferuje również metoda filtracji subpasmowej zaprezentowana w [9], lecz w pewnych przypadkach może ona generować słyszalne zakłócenia.

Wysoka odporność możliwa jest do uzyskania przy pomocy technik wykorzystujących kodowanie lub modulację fazy dźwięku [15, 3, 19]. Metody te charakteryzują się niewielką pojemnością steganograficzną. O wiele trudniej jest uzyskać odporność operując w dziedzinie czasu. Udało się tego dokonać poprzez ukrycie danych poprzez modyfikację histogramu [24, 25] oraz poprzez modyfikację odległości pomiędzy znaczącymi punktami sygnału.

W [22, 2] zaproponowano wykorzystanie technik ukrywania w obrazie. Sygnał audio jest tu przekształcany do postaci obrazu, który służy do ukrycia informacji. Uzyskany stegokontener przekształcany jest z powrotem na dźwięk. Podejście to pozwala na uzyskanie odporności na kompresję mp3.

Metody wykorzystujące przekształcenie Fouriera nie zyskały popularności w steganografii sygnałów dźwiękowych. Powodem tego było generowanie przez nie słyszalnych zakłóceń. Uzyskanie przezroczystego ukrywania możliwe było jedynie poprzez wykorzystanie pasma niesłyszalnego lub zastosowanie bardzo małej siły wprowadzanych zmian. Żadne z tych rozwiązań nie dawało jednak przewagi nad innymi metodami, bowiem przekształcenie Fouriera wykonywane jest na blokach (fragmentach) sygnału co ogranicza pojemność steganograficzną metod bazujących na nim. Zaletą jest natomiast duża trwałość wprowadzonych zmian a co za tym idzie odporność dołączonych danych na uszkodzenie. Wy-

maga to jednak zastosowania odpowiednio dużej mocy zmian. Ze względu na sprzeczność wymagań koniecznych do osiągnięcia odporności i niesłyszalności wprowadzanych zakłóceń nie udało się osiągnąć odporności w paśmie słyszalnym. Możliwe to było jedynie w paśmie niesłyszalnym. Jednak pasmo to jest najczęściej usuwane podczas kompresji stratnej. Ponadto energia występujących tam częstotliwości jest zazwyczaj bardzo mała. Wykonanie modyfikacji wprowadza znaczne zmiany, które są łatwo zauważalne podczas analizy widma co czyni to podejście nieprzydatnym do zastosowań steganograficznych [15].

W artykule zaprezentowane zostało rozwiązanie pozwalające na wykorzystanie transformaty Fouriera jako przekształcenia bazowego do konstrukcji metody steganograficznej wykorzystującej dźwięk jako nośnik ukrytej informacji. Proponowany algorytm ukrywa dane w paśmie słyszalnym dźwięku dzięki czemu możliwe jest uzyskanie dobrej odporności na uszkodzenia dołączonych danych. Aby możliwe było wykonanie modyfikacji bez generowania słyszalnych zakłóceń wykorzystywane jest zjawisko maskowania do ukrycia wprowadzanych zmian.

2. TRANSFORMATA FOURIERA

Metody transformacyjne opierają się na przekształceniu tradycyjnego zapisu sygnału w dziedzinę częstotliwości, które wykonywane jest przy pomocy dowolnej transformaty. Modyfikacja wybranych współczynników transformaty pozwala na dołączenie dodatkowych danych do istniejącego sygnału. Powrót do dziedziny czasu następuje poprzez wykonanie przekształcenia odwrotnego. Aby przekształcenie mogło być wykorzystane w steganografii, musi być w pełni odwracalne.

Do ukrywania informacji może być wykorzystana transformata Fouriera. Jest to przekształcenie polegające na aproksymacji sygnału przy pomocy złożenia wielu funkcji $\sin \omega x$ i $\cos \omega x$ [7]. Do przetwarzania sygnału cyfrowego stosowana jest dyskretna transformata Fouriera (DFT) sygnału liniowego, która przyjmuje postać:

$$F(u) = \frac{1}{N} \sum_{x=0}^{N-1} f(x) \exp(-\frac{\mathrm{j}2\pi v x}{N}) \tag{1}$$

gdzie:

v – częstotliwość sygnału,

N – ilość próbek sygnału.

Aby reprezentację częstotliwościową sygnału zamienić ponownie na przebieg czasowy należy wykonać odwrotną dyskretną transformatę Fouriera (IDFT), która przyjmuje postać:

$$a_n = \sum_{k=0}^{N-1} A_k \omega_N^{kn}, \ 0 \le n \le N-1 \tag{2}$$

gdzie:

k – numer harmonicznej,
n – numer próbki sygnału,
a_n – wartość próbki sygnału,
N – liczba próbek [7].

W dotychczas opracowanych metodach steganograficznych bazujących na transformacie Fouriera ukrywanie informacji odbywa się poprzez modyfikację wartości wybranych częstotliwości składowych. Może to być modyfikacja jednej częstotliwości. W takim przypadku obecność tej składowej odpowiada ukrytej wartości binarnej jeden a jej brak zeru. W przypadku wykorzystania dwóch częstotliwości analizie podlega stosunek ich wartości. Jeśli większy udział ma częstotliwość f_1 to jest to równoznaczne z zakodowaniem jedynki a jeśli f_2 to ukryte jest zero. W przedstawiony sposób można ukryć jeden bit dodatkowych danych w jednym fragmencie przetwarzanego sygnału.

3. MASKOWANIE

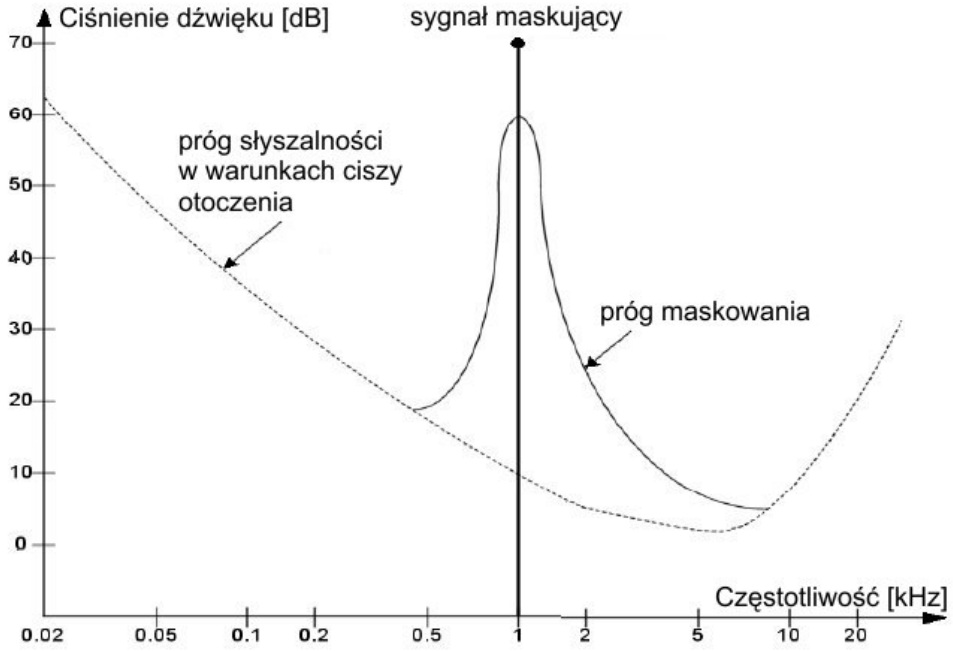
Maskowanie to zjawisko, które powoduje, że słuch nie jest w stanie zarejestrować pewnych dźwięków (maskowanych), ponieważ są one „zagłuszane" przez inne dźwięki (maskery). Możemy wyróżnić dwa rodzaje maskowania:

- nierównoczesne,
- równoczesne.

Maskowanie nierównoczesne polega na blokowaniu percepcji sygnału przez inny głośniejszy sygnał następujący w odstępnie czasu nie większym niż 40 ms po lub do 200 ms przed maskowanym[16].

Maskowanie częstotliwościowe (równoczesne) polega na maskowaniu dźwięku cichszego przez równocześnie występujący dźwięk głośniejszy o zbliżonej częstotliwości. Warunkiem maskowania jest to, aby dźwięk maskowany znajdował się poniżej progu maskowania. Wartość progu maskowania zależy od częs-

totliwości oraz charakteru tonu maskowanego i maskera (czy będzie to czysty dźwięk czy też wąskopasmowy szum). Zależność tą przedstawia rysunek 1.



Rys. 1. Próg maskowania równoczesnego dla 1 kHz sinusoidalnego sygnału maskera, przy maskowaniu „czystego" dźwięku [20]

Dzięki maskowaniu równoczesnemu można wycinać oraz dodawać dźwięki spełniające powyższe warunki bez zmiany jakości sygnału audio. Wykorzystywane jest to w algorytmach kompresji pozwalając zmniejszyć ilość danych w ścieżce dźwiękowej jak również w steganografii do ukrywania dodatkowych danych, które mogą być kodowane przy pomocy dodawanych dźwięków. Należy jednak zauważyć, że dane te mogą być usuwane przez algorytmy kompresujące korzystające z tych samych zależności [21, 19].

4. BUDOWA ALGORYTMU

Aby uniknąć wprowadzania słyszalnych zakłóceń można do celów steganografii sygnałów dźwiękowych wykorzystać częstotliwości maskowane. Jako że niezbędne jest dopasowanie się do istniejącego nośnika jak również niemożliwe jest wprowadzanie dodatkowych dźwięków w celu zamaskowania

wprowadzonych zmian, konieczne jest zaprojektowanie algorytmu ukrywania w taki sposób by wykorzystywał istniejące w przetwarzanym dźwięku maskery. Na podstawie przedstawionych w poprzednich rozdziałach informacji oraz przeprowadzonych badań opracowany został algorytm dołączania informacji do dźwięku. Pierwszym etapem jest wykonanie DFT na przetwarzanym fragmencie. Z uzyskanych wyników wyliczane jest widmo częstotliwościowe dźwięku, w którym wyszukiwany jest prążek o największej wartości oznaczany jako $p_{\max}$. Jego wartość oznaczmy symbolem $W_{\max.}$ Prążek ten odpowiada częstotliwości $f_{\max}$ mającej największy udział w sygnale. Możemy go więc traktować jako sygnał maskera. Z zakresu maskowanego przez tą częstotliwość wybierane są dwa prążki widma, które posłużą do ukrycia bitu informacji. Oznaczmy je jako f_1 i f_2 a ich wartości odpowiednio jako w_1 i w_2. Wybór prążków zależny jest od klucza steganograficznego. Aby prążek mógł przenosić informację musi spełniać określone warunki:

- znajdować się w przedziale odległości (F_{dif1}, F_{dif2}) od $f_{\max}$,
- mieć wartość nie większą niż określona zależnością.

$$W_n \le (a - (f_{\max} - f_n)^2 / b) \cdot W_{\max} \tag{3}$$

Wartości F_{dif1}, F_{dif2}, a, b pochodzą z klucza steganograficznego, f_{n} jest częstotliwością odpowiadającą n-temu prążkowi.

Prążki spełniające powyższe warunki umieszczane są w tablicy według kolejności określonej przez klucz. Następnie kolejno są sprawdzane tak by dobrać parę pozwalającą na ukrycie określonej wartości binarnej. Wybrana para wykorzystywana jest do dołączenia bitu informacji. W przypadku jeśli w tablicy przed wybranymi prążkami występują inne pominięte, wówczas ich wartość jest modyfikowana tak by nie spełniała nierówności (3).

Następnie wyliczana jest różnica wartości pomiędzy prążkami f_1 i f_2 w celu określenia czy wymaga modyfikacji czy też jest zgodna z oczekiwaną. Oczekiwana różnica wartości (R) jest wyliczana na podstawie klucza steganograficznego, który zawiera wartość R_{p} określającą stosunek R do wartości maksymalnej $W_{\max}$. Wartość R obliczana jest zgodnie ze wzorem:

$$R = W_{\max} \cdot R_p \tag{4}$$

Takie rozwiązanie pozwala na dostosowywanie siły modyfikacji do siły sygnału oraz umożliwia wykorzystanie wszystkich fragmentów sygnału. Ukrycie bitu b w sygnale polega na przetworzeniu sygnału w taki sposób by spełnić zależność:

$$\begin{cases} |w_1 - w_2| \geq R, \text{ dla } b = 1 \\ |w_1 - w_2| \leq \beta, \text{ dla } b = 0 \end{cases} \tag{5}$$

gdzie β jest wartością umieszczoną w kluczu oznaczającą maksymalny zakres wartości losowej dodawanej do obliczonej wartości prążka.

Po spełnieniu powyższej nierówności, fragment transformowany jest z powrotem do dziedziny czasu przy pomocy odwrotnej transformaty Fouriera (IDFT) i umieszczany w sygnale w miejsce oryginalnego.

Gdy istnieje konieczność wprowadzenia zmian wartości prążków to najpierw modyfikacji poddawany jest prążek o mniejszej wartości. Pozwala to na ograniczenie wzmocnienia drugiego prążka. W ten sposób redukujemy siłę drugiej wzmacnianej częstotliwości a co za tym idzie uzyskujemy zniekształcenie, które o wiele łatwiej będzie maskowane. Ze względu na to, że w widmie sygnału praktycznie nie występują wartości zerowe autor zdecydował, że zmniejszenie wartości mniejszego prążka będzie następowało przez podzielenie go przez wartość z przedziału (1, $\theta_{max}>$. θ_{max} jest wartością zdefiniowaną w kluczu steganograficznym. Pozwoli to na uniknięcie wprowadzania zerowych wartości prążków.

Wprowadzenie zmian powoduje powstawanie nieciągłości na łączeniach bloków, które mogą powodować słyszalne zakłócenia w postaci trzasków. Niezbędne jest więc przywrócenie ciągłości sygnału. Najkorzystniejszym rozwiązaniem jest umieszczenie pomiędzy blokami przenoszącymi informację bloków łączących. Kształt sygnału wewnątrz tych bloków jest modyfikowany tak by wartości sąsiadujących próbek dwóch bloków były jednakowe.

Prezentowany algorytm pozwala na osiągnięcie pojemności steganograficznej rzędu 40 bitów na sekundę sygnału próbkowanego z częstotliwością 44100 Hz.

Aby odczytać ukrytą informację należy określić położenie bloków będących stegokontenerami, dla każdego z nich wykonać DFT. W uzyskanym widmie określamy położenie zmodyfikowanych prążków i badamy różnicę ich wartości R'. Określamy również wartość największego prążka $W_{\max}$. Następnie odczytujemy wartość ukrytego bitu b zgodnie z zależnością:

$$\begin{cases} b = 1, \text{ gdy } R' \geq (R_p - M) \cdot W_{\max} \\ b = 0, \text{ gdy } R' \leq M \cdot W_{\max} \\ b = -1, \text{ gdy } M \cdot W_{\max} < R' < (R_p - M) \cdot W_{\max} \end{cases} \tag{6}$$

gdzie M jest wartością zdefiniowaną w kluczu. b = -1 oznacza, że odczytana wartość jest traktowana jako nieokreślona.

5. REZULTATY BADAŃ

Najistotniejszym zadaniem steganograficznego dołączania danych jest ich dobre ukrycie. Oznacza to konieczność stosowania algorytmów, które nie wprowadzają zmian, które mogły by być wykryte przy pomocy analizy numerycznej lub były by słyszalne. Dlatego aby ocenić zaprojektowaną metodę niezbędne jest zbadania poziomu wprowadzanych zniekształceń oraz sprawdzenie czy w wyniku wykonywanych przekształceń nie powstają słyszalne zakłócenia.

Do określenia poziomu zniekształceń wprowadzanych podczas procesu dołączania użyto miar obiektywnych według [15]:

- błędu średniokwadratowego (MSE),
- znormalizowanego błędu średniokwadratowego (NMSE),
- odległości sygnału od szumu (SNR),
- szczytowej wartości odległości sygnału od szumu (PSNR),
- normy LP (LP),
- maksymalnej różnicy pomiędzy sygnałem oryginalnym i zmodyfikowanym (MD),
- średniej bezwzględnej różnicy pomiędzy sygnałami (AD),
- znormalizowanej średniej bezwzględnej różnicy pomiędzy sygnałami (NAD),
- przezroczystości ukrytych danych (AF).

Uzyskane wyniki zaprezentowane zostały w tabeli 1.

TABELA 1
Poziom zniekształceń wprowadzanych podczas ukrywania informacji w dźwięku

Rp	MSE	NMSE	SNR [dB]	PSNR [dB]	LP	MD	AD	NAD	AF
1%	7E-6	13E-4	29	100	7 E-6	0,06	10E-4	0,02	1
10%	9E-6	17E-4	27	99	9 E-6	0,06	16E-4	0,03	1
15%	14E-6	27E-4	25	96	14E-6	0,06	20E-E	0,04	1
20%	23E-6	43E-4	23	94	23E-6	0,06	28E-4	0,06	1
30%	56E-6	1E-3	19	91	56E-6	0,06	43E-4	0,09	0,99
40%	1E-7	2E-3	17	88	1E-4	0,08	58E-4	0,12	0,98

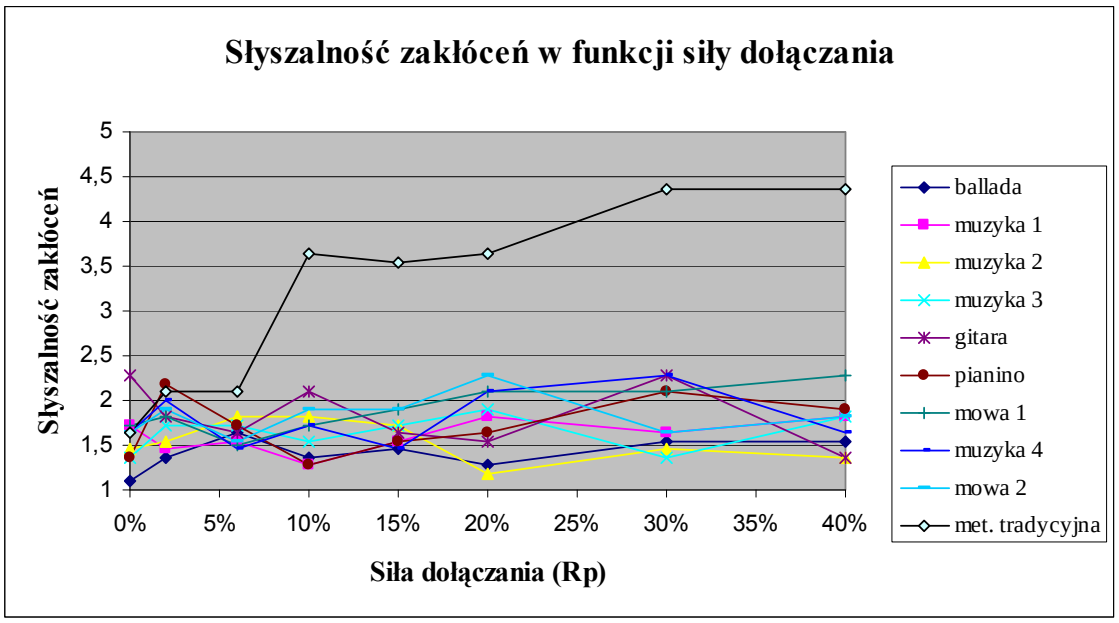
Wyniki przedstawione w tabeli 1 wykazują, że proponowana metoda wprowadza bardzo małe zniekształcenia sygnału. Świadczy o tym wartość SNR, która w szerokim przedziale spełnia rygorystyczne warunki stawiane znakom

wodnym, dla których SNR musi być większe od 22 dB. Dodatkowo miara przezroczystości dołączonych danych (AF) przyjmuje najwyższe z możliwych wartości.

Weryfikacja rzeczywistej słyszalności wprowadzanych zakłóceń przeprowadzona została poprzez wykonanie podwójnie ślepego testu odsłuchowego na grupie 20 osób. Ocena porównywanego materiału dokonywana była przez każdego z testerów niezależnie, przy użyciu pięciostopniowej skali:

1 – brak zakłóceń,
2 – brak pewności czy zakłócenia występują czy nie,
3 – bardzo słabe,
4 – słabe,
5 – wyraźne.

Na osi odciętych rysunku 2 umieszczona została moc dołączania (R_p). Wartość R_p = 0% oznacza, że ocena dotyczyła kopii oryginalnego nagrania umieszczonych w teście w celu porównania z wynikami uzyskanymi dla nośników zmodyfikowanych. Łatwo można zauważyć, że średnia ocena słyszalności zakłóceń w nośnikach zmodyfikowanych jest zbliżona do oceny jaka została uzyskana dla nośników nie zmodyfikowanych. Większość uzyskanych wyników nie przekracza wartości 2, która oznacza że osoby testujące nie były pewne czy w ocenianym fragmencie były wprowadzone jakiekolwiek zmiany czy nie. Pozwala to na stwierdzenie, że zniekształcenia generowane przez prezentowany algorytm są niesłyszalne dla przeciętnego odbiorcy.



Rys. 2. Poziom zakłóceń wprowadzanych przez badaną metodę określony w wyniku testu odsłuchowego

Dodatkowo przeprowadzono testy odporności dołączonych danych na zniszczenie podczas popularnych operacji wykonywanych na dźwięku. Badaniu poddawano nagranie stereo utworu muzycznego, dźwięku pianina oraz mowy zapisane w formacie *.wav o częstotliwości próbkowania 44100 Hz z rozdzielczością 16 bitów na próbkę, w którym zastosowano siłę dołączania R_{p} = 15%. Sygnał z dołączonymi danymi poddawany był badanym operacjom a następnie konwertowany z powrotem do postaci wyjściowej. Wyniki zaprezentowane zostały w tabeli 2.

TABELA 2
Ilość błędnie odczytanych bitów (BER) po spowodowana przekształceniem nośnika

Przekształcenie lub format zapisu	muzyka	pianino	mowa
Ogg	2,5%	0%	2,5%
Mp3 64 kbit/s	9%	4,3%	10,7%
Mp3 128 kbit/s	19,6%	1,4%	12%
Aac 64 kbit/s	12,4%	6,4%	10,5%
Aac 128 kbit/s	4%	1,4%	7,5%
ape	0%	0,0%	0,0%
Wma quality = 98%	0,0%	0,0%	1,1%
Wma quality = 50%	3,1%	2,1%	8,0%
Redukcja częstotliwości próbkowania do 22 kHz	1%	2,9%	3,7%
Redukcja rozdzielczości próbki do 8 bitów	2%	0,7%	5%
Filtrowanie pasmowoprzepustowe 1 Hz-10 kHz	0,5%	0,7%	3,7%

Jak można zauważyć podczas analizy tabeli 2, metoda wykazuje wysoką odporność na różnego rodzaju przekształcenia dźwięku. Możliwe jest uzyskanie większej odporności od przedstawionej w tabeli poprzez zastosowanie większej siły dołączania (R_{p}).

6. PODSUMOWANIE

Przeprowadzone badania pozwoliły na udowodnienie, że możliwe jest opracowanie efektywnej metody steganograficznej wykorzystującej dźwięk jako nośnik ukrytej informacji przy wykorzystaniu transformaty Fouriera jako prze-

kształcenia bazowego. Zaproponowana metoda osiąga wysoką odporność na różne przekształcenia nośnika, przy jednoczesnym zachowaniu dobrej jakości nośnika. Możliwe jest to dzięki dostosowywaniu wprowadzanych zmian do parametrów nośnika w przetwarzanym fragmencie sygnału. Częstotliwość wykorzystywana do ukrycia informacji nie jest determinowana przez klucz lecz wyszukiwane są prążki położone w sąsiedztwie silniejszego maskera. Pozwala to zarówno uniknąć wprowadzania słyszalnych zmian jak również rozproszyć wprowadzane zmiany w szerokim paśmie częstotliwości co znacznie zwiększa bezpieczeństwo steganograficzne oraz utrudnia usunięcie dołączonych danych. Zaprojektowana metoda z powodzeniem może być wykorzystywana do realizacji ukrytych kanałów komunikacyjnych. Spełnia ona wymagania pojemności steganograficznej, która powinna osiągać poziom kilkudziesięciu bitów na sekundę sygnału w przypadku ukrytej komunikacji a dodatkowo charakteryzuje się dużą odpornością co ma bardzo duże znaczenie w przypadku wykorzystywania kanałów o dużym poziomie błędów przesyłu lub w sytuacjach gdy nośnik może podlegać modyfikacjom pomiędzy nadawcą a odbiorcą.

LITERATURA

1. Agaian S.S., Akopian D., Caglayan O., D'Souza S.A.: Lossless adaptive digital audio steganographyy, Proc. IEEE Int. Conf. Signals, Systems and Computers, pp. 903–906, 2005.
2. Bao P., Ma X.: MP3-resistant music steganography based on dynamic range transform, IEEE Int. Sym. Intelligent Signal Processing and Communication Systems, pp. 266–271, 2004.
3. Bender W., Gruhl D., Morimoto N., Lu A.: Techniques for data hiding. IBM Systems Journal, Vol.35, Nos 3&4 (1996) 313–336.
4. Cvejic N., Seppanen T.: A wavelet domain LSB insertion algorithm for high capacity audio steganography, Proc. IEEE Digital Signal Processing Workshop, pp. 53–55, 2002.
5. Cvejic N., Seppanen T.: Increasing the capacity of LSB-based audio steganography, IEEE Workshop on Multimedia Signal Processing, pp. 336–338, 2002.
6. 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, pp. 533–537, 2004.
7. Czyżewski A.: Dźwięk cyfrowy, Exit, 2001.
8. Delforouzi A., Pooyan M.: Adaptive Digital Audio Steganography Based on Integer Wavelet Transform, Circuits Syst Signal Process Vol. 27 pp. 247–259, 2008.
9. Dymarski P.: Filtracja sygnałów dźwiękowych jako metoda znakowania wodnego i steganografii, Bydgoszcz 2006.
10. Dymarski P., A. Poblocki, C. Baras, N. Moreau: Algorytmy znakowania wodnego sygnałów dźwiękowych, Krajowe Sympozjum Telekomunikacji, Bydgoszcz 2003.
11. Garay A.: Measuring and evaluating digital watermarks in audio files, Washington 2002.
12. Gopalan K.: Audio steganography by cepstrum modification, Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 5, pp. 481–484, 2005.

13. Gopalan K.: Audio steganography using bit modification, Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Vol. 2, pp. 421–424, 2003.
14. Gruhl, D., Lu, A.: Echo Hiding. Information Hiding Workshop, Cambridge University, 295-315, U.K. 1996.
15. Mahbubur S. R., Syed M. R.: Multimedia Technologies, London 2008.
16. Jorasz U.: Selektywność ludzkiego słuchu, Poznań 1999.
17. Katzenbeisser S., Petricolas A. P.: Information Hiding, Artech House, 2000.
18. 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 No2, Seoul , Coree, Republique De (22/10/2003) 2004 , vol. 2939, pp. 456-466.
19. Matsuka H.: Spread spectrum audio steganography using sub-band phase shifting, IEEE Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), pp. 3–6, 2006.
20. Nedeljko C.: Algorithms for audio watermarking and steganography, Oulu University Press, 2004.
21. RLE, Massachusetts 1999, http://rleweb.mit.edu/Publications/currents/cur111/111watermark.htm
22. Santosa R.A., Bao P.: Audio-to-image wavelet transform based audio steganography, IEEE Int. Symp., pp. 209–212, 2005.
23. Wayner P.: Disappearing cryptography, Morgan Kaufmann, 2002.
24. 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, pp. 93-108.
25. Xiang S., Kim H., Huang J.: Audio watermarking robust against timescale modification and MP3 compression, http://ieeexplore.ieee.org.

Rękopis dostarczono dnia 11.05.2010 r.
Opiniował: prof. dr hab. inż. Zygmunt Piątek

FOURIER TRANSFORM USING POSSIBILLITIES IN SOUND STEGANOGRAPHY

Grzegorz KOZIEŁ

ABSTRACT *This article presents a new sound steganography method based on Fourier transform. Proposed method assure the steganographic capacity up to 40 bits per second. Hiding data is realised in frequency domain. Masking is used to avoid audible interference introducing. Idea of the algorithm relies on finding the biggest value strip in the spectrum. It is treeted as masking strip. Next*

we look for the strips which are masked by the biggest strip in it's proximity. Two of them are choosen to hide data. Their values are change to achieve the value difference meeting conditions for hiding bit value. In this way it is possibile to obtain signal withought audible interferencje thanks to the masking effect. Hidden data Has a big robustness to common sound processing operations and compression.

Mgr inż. Grzegorz KOZIEŁ – absolwent Politechniki Lubelskiej (2003) obecnie pracownik Zakładu Ochrony Informacji w Instytucie Informatyki na wydziale Elektrotechniki i Informatyki Politechniki Lubelskiej. W pracy badawczej zajmuje się problematyką steganografii wykorzystującej dźwięk jako nośnik ukrytej informacji.