VỀ MỘT PHƯƠNG PHÁP NÂNG CAO HIỆU NĂNG CHE GIẤU THÔNG TIN TRONG ÂM THANH

Lê Mạnh Hùng*

Tóm tắt: *Bài viết trình bày ứng dụng biến đổi Fourier để ẩn mã trong âm thanh và phương pháp nâng cao hiệu năng che giấu thông tin trong âm thanh bằng biến đổi Fourier cải biến và phương pháp kết hợp giữa mật mã và ẩn mã.*

Từ khóa: Ẩn mã, Biến đổi Fourier, Bảo vệ thông tin, Mã hóa.

1. GIỚI THIỆU

Ẩn mã (steganography) là một ngành khoa học liên quan đến bảo vệ thông tin. Được thực hiện bằng cách che giấu thông tin có giá trị trong một vật mang tin không có giá trị. Các phương tiện mang tin có chứa dữ liệu được che giấu gọi là stegocontainer. Ẩn mã không phải là một khoa học mới, từ xa xưa thường được thực hiện nhờ sử dụng mực vô hình hoặc kỹ thuật in *microdots*. Sự phát triển của ẩn mã số cùng với sự phát triển của kỹ thuật số đã thay đổi cách thức ẩn mã vì dữ liệu cần che dấu không phụ thuộc vào vật mang tin. Bài viết sau chỉ trình bày về ẩn mã số hoạt động vẫn như ẩn mã tương tự (analog), nhưng kỹ thuật che giấu đã thay đổi. Ẩn mã số che giấu dữ liệu bằng cách đưa vào những thay đổi nhỏ không thể nhận thấy ở dữ liệu số khác và có thể được thực hiện bằng nhiều phương pháp. Cách đơn giản nhất là dựa vào kỹ thuật các bit có trọng số thấp nhất (LSB), trong đó bao gồm việc thay thế các bit có trọng số thấp nhất (LSB) tín hiệu ban đầu bằng các bit thông tin cần che giấu. Phương pháp này cho phép thực hiện ẩn mã dung lượng cao. Đáng tiếc, phương pháp LSB có khả năng đề kháng thấp khi thay đổi vật mang tin. Hơn nữa, khi thay đổi một số lượng quá nhiều bit có trọng số thấp nhất trong tín hiệu xuất hiện nhiễu có thể nghe được.

Phương pháp LSB thường gặp hoạt động trong cả miền thời gian và tần số [3, 4, 5]. Quan trọng là biến đổi sử dụng để biến đổi các tín hiệu sang các miền lựa chọn có tính biến đổi ngược. Phương pháp ẩn mã xử lý trong miền thời gian không đạt được mức độ đề kháng cao so với các phương pháp xử lý trong miền tần số. Thực tế, đã có nhiều phương pháp sử dụng biến đổi tín hiệu trong miền thời gian, tuy nhiên thường tạo thêm nhiễu tạp âm thanh. Vì vậy, nghiên cứu nâng cao hiệu năng che giấu thông tin trong âm thanh bằng biến đổi Fourier cải biến và phương pháp kết hợp giữa mật mã và ẩn mã là bài toán có tính thời sự cao.

2. PHƯƠNG PHÁP SỬ DỤNG BIẾN ĐỔI FOURIER (TF) VÀ BIẾN ĐỔI FOURIER CẢI TIẾN (MF)

2.1. Phương pháp sử dụng biến đổi Fourier (TF)

Nhờ sử dụng biến đổi Fourier chúng ta có được dạng của tín hiệu trong miền tần số. Thay đổi giá trị cụ thể của phổ vạch hoặc phổ pha tín hiệu cho phép đưa vào những thay đổi ổn định trong tín hiệu để che dấu các thông tin nhúng kèm. Hiện có kỹ thuật ẩn mã dựa trên thay đổi các giá trị cụ thể của phổ vạch mô-đun phổ hoặc pha tín hiệu. Trong số đó, chúng ta có thể phân ra một vài nhóm:

- Kỹ thuật bit có trọng số thấp hay còn gọi là phương pháp LSB (*Least Significant Bit*) - phương pháp dựa trên thay đổi các các bit có trọng số thấp nhất của mô-đun phổ tín hiệu bằng các bit của thông tin cần che giấu, hoạt động tương tự như phương pháp các bit có trọng số thấp nhất truyền thống. Khác biệt duy nhất là biểu diễn tín hiệu trong miền tần số thay vì thời gian và có thể đạt được khả năng đề kháng lớn hơn trước đe dọa làm hỏng dữ liệu cần che giấu.

- Kỹ thuật sửa đổi giá trị các phổ vạch mô-đun phổ tín hiệu, đạt được khả năng đề kháng cao chống gây lỗi. Một lượng nhỏ các phổ vạch được cải biến làm cho sự thay đổi trong toàn bộ tín hiệu nhỏ và khó phát hiện. Phương pháp này có sức đề kháng cao trước tấn công gây hại và phá hủy các thông tin kèm theo. Tuy nhiên, phương pháp này làm giảm đáng kể dung lượng ẩn mã và gây nên nhiễu tạp âm thanh. Để nhúng thông tin che giấu có thể sử dụng chỉ một phổ vạch. Để trích xuất thông tin có thể thực hiện bằng cách so sánh phổ của vật mang tin (stegocontainer) với phổ gốc. Phương pháp này ít được sử dụng do cần có một kênh an toàn để trao đổi dữ liệu gốc. Những nhược điểm của phương pháp này có thể khắc phục nếu sử dụng một số lớn các phổ vạch để nhúng thông tin mật. Thông thường sử dụng hai phổ vạch. Trong trường hợp sử dụng hai tần số, việc thay đổi dựa trên sự tương quan giá trị của chúng. Nếu số lớn phổ vạch có tần số f1, sẽ được mã hóa "1" và ngược lại f2 nhiều hơn được mã hóa "0" (phương pháp này được ký hiệu TF - Transformation Fourier). Trong một số phương pháp, sử dụng ba phổ vạch. Nếu như xuất hiện tỷ số giá trị f1 <f2 <f3 được nhúng kèm thêm "0", Nếu f1> f2> f3 được nhúng kèm thêm "1". Nếu không thỏa mãn bất kỳ bất đẳng thức nêu trên có nghĩa là đoạn này không đính kèm thêm thông tin nào cả. Cách tiếp cận này cho phép tăng thêm độ tin cậy khi trích xuất thông tin và giảm sự méo mó có thể bằng cách loại bỏ được những sửa đổi trong các đoạn có thể gây nên sự méo mó.

- Kỹ thuật thay đổi pha tín hiệu để giấu thông tin bằng cách thay đổi quá trình biến đổi pha của tín hiệu. Phương pháp này có tính đề kháng cao chống lại sự phá hủy nhưng lại có dung lượng ẩn mã thấp, do cần phải sửa đổi pha trong cả quá trình xử lý.

Phương pháp sử dụng toàn bộ tín hiệu để che giấu các bit thông tin, tín hiệu được chia thành các khối. Mỗi khối mang một bit thông tin. Đầu tiên, khối tín hiệu được biến đổi nhờ sử dụng biến đổi fourier rời rạc (discrete Fourier transform - DFT) để biểu diễn về miền tần số, xác định ra các giá trị phổ vạch lựa chọn. Sau đó, sửa đổi các giá trị đó theo thuật toán đã chọn. Khi phổ đã sẵn sàng được chuyển trở lại về miền thời gian nhờ sử dụng IDFT. Các khối sau xử lý được kết hợp thành một tín hiệu duy nhất.

Phương pháp dựa trên biến đổi Fourier thường được sử dụng trong ẩn mã ảnh. Trường hợp các tín hiệu audio thì việc sử dụng biến đổi Fourier thường gây nhiễu âm thanh do tích hợp thêm một lượng lớn thông tin. Các tín hiệu gắn thêm thông tin bằng các phương pháp trên thường có công suất bé nên khả năng kháng nhiễu thấp. Các dải tần của âm thanh thường là trong khoảng từ 20 Hz đến 10 kHz. Vì vậy, sự xuất hiện các tín hiệu có tần số cao hơn trong quá trình phân tích tần số tín hiệu dễ gây nên sự chú ý và các thông tin nhúng kèm dễ bị phát hiện.

2.2. Phương pháp biến đổi Fourier cải tiến (MF)

Trên cơ sở của phương pháp biến đổi Fourier (TF) người ta phát triển phương pháp biến đổi Fourier cải tiến (Modified Fourier transform - MF), giống như phương pháp trước đây, là người ta dùng hai vạch phổ để che giấu thông tin đính kèm. Những thay đổi đó bao gồm:

- Sử dụng hiện tượng mặt nạ để xác định tần số mặt nạ,
- Lựa chọn tần số thích hợp để cải biến, sao cho các thay đổi đưa vào nằm ở vùng lân cận các phổ vạch tần số tín hiệu có giá trị lớn nhất,
- Các giá trị của các thay đổi đưa vào phải thích ứng với các tham số tín hiệu ở đoạn tín hiệu xử lý,
- Sửa đổi cách mã hóa các giá trị nhị phân thông tin che giấu: Giấu bằng số không nhị phân "0" trong trường hợp khi giá trị của cả hai phổ vạch được chọn bằng nhau và bằng số một nhị phân "1" khi hiệu các giá trị của cả hai phổ vạch được chọn (R) đạt được một giá trị xác định.

Thuật toán ẩn mã đề xuất trên được thực hiện trong 5 bước:

1. Phân chia tín hiệu ra các khối - là chia tín hiệu thành các đoạn để che giấu thông tin. Kích thước và vị trí của các đoạn phụ thuộc vào khóa ẩn mã.

2. Xử lý các khối bằng biến đổi Fourier rời rạc (DFT) - cho phép chuyển về miền tần số.

3. Đính kèm bit thông tin cần che giấu - thực hiện bằng cách chọn một cặp phổ vạch và sửa đổi thích hợp giá trị của chúng.

4. Sử dụng phép biến đổi Fourier ngược (IDFT) để biến đổi các khối trên đưa tín hiệu trở về miền thời gian.

5. Phối ghép các khối đã xử lý nhằm liên kết tất cả các đoạn của tín hiệu.

2.3. Đánh giá chất lượng âm thanh sau khi giấu tin

Để đánh giá chất lượng âm thanh của phương pháp đề xuất thường so sánh các bộ chứa thông tin che giấu (stegocontainer) được tạo ra bằng cách sử dụng phương pháp biến đổi fourier (TF). Do các đặc tính khác nhau thu được khi giấu thông tin bằng phương pháp TF trong dải tần nghe được và không nghe được, nên thường chia ra hai bộ chứa tin che giấu: Bộ dùng cho phương pháp TF thông thường sử dụng băng tần 330-360 Hz, ký hiệu là TF_{aud} và bộ thứ hai được ký hiệu là TF_{inaud}, khi sử dụng băng thông lớn hơn 20 kHz .

Để đánh giá chất lượng âm thanh sau khi giấu tin ta thực hiện các số đo sau:

1) Sai số toàn phương trung bình MSE (Mean squared error)

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

2) Tỷ lệ tín hiệu so với tạp âm (decibel)

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

3) Tỉ số tín hiệu cực đại trên tạp âm (peak signal-to-noise ratio)

$$PSNR = 10\log(R^2 / MSE)$$

4) Trung bình sai số tuyệt đối giữa các tín hiệu:

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

Một số kết quả thực nghiệm đánh giá chất lượng của các phương pháp trên được [6] trình bày trong bảng 1.

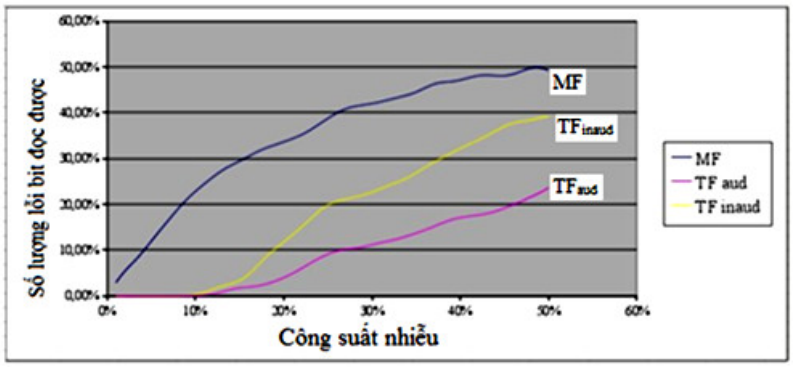
Bảng 1. *So sánh độ biến dạng qua các phương pháp thực hiện.*

Phương pháp	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

Phân tích các kết quả cho phép kết luận phương pháp MF đạt được tốt hơn phương pháp TF (Điều này thể hiện rõ trong các số đo được AF).

2.4. Tính đề kháng của dữ liệu che giấu đính kèm trước nguy cơ phá hủy

Khi thực hiện ẩn mã trên kênh truyền thông nếu cần thay đổi vật mang tin thì phải chọn phương pháp đảm bảo tính đề kháng cao trước nguy cơ thông tin che giấu bị phá hủy. Vật mang tin ẩn mã (Stegocontainer) với các phương pháp trên được thực hiện bằng các phép biến đổi khác nhau. Sau khi lọc các thông tin được che dấu cần đánh giá số lượng các lỗi bit (BER). Một số kết quả được trình bày ở hình 1 [6].



Hình 1. *Khả năng đề kháng của các phương pháp trên trước nhiễu đính kèm [6].*

Có thể thấy phương pháp biến đổi Fourier - TF (trong cả hai trường hợp) khả năng chống nhiễu tốt hơn trước tạp âm đính kèm. Phương pháp biến đổi Fourier cải tiến - MF có tính đề kháng thấp nhưng đối với nhiễu tạp không lớn thì tỷ lệ lỗi rất thấp có thể sửa chữa lỗi bằng cách sử dụng thuật toán sửa sai. Kết quả về tính đề kháng khá khác nhau trước biến đổi động được thể hiện trong Bảng 2 [6].

Bảng 2. *Số lượng lỗi tạo ra do biến đổi động [6].*

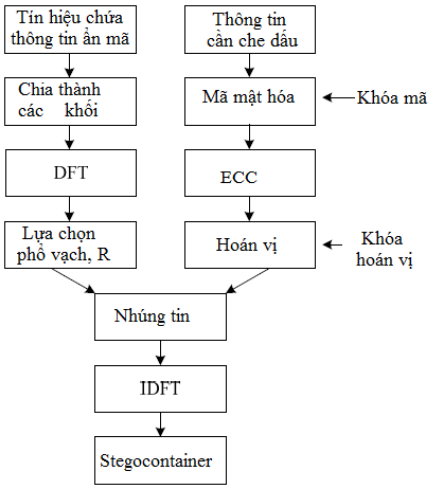
Phương pháp	Êm dịu				Chuẩn hóa			
	Âm nhạc	Tiếng nói	Dương cầm	Kèn	Âm nhạc	Tiếng nói	Dương cầm	Kèn
MF	**4,4%**	**4,6%**	**2,1%**	**1,3%**	**4,4%**	**5,3%**	**2,1%**	**0%**
TF_{aud}	56,6%	50%	58,3%	48,9%	47,7%	49,4%	60,8%	49,7%
TF_{inaud}	0%	0%	0%	0%	0%	0%	0%	0%

Phân tích các kết quả trình bày trong bảng 2 [6] cho thấy phương pháp MF có khả năng đề kháng cao trước biến đổi động. Tính đề kháng của phương pháp này phụ thuộc vào băng tần sử dụng - trong dải âm tần thì phương pháp TF có tính đề kháng không bền vững. Phương pháp TF hoạt động trong dải tần cao có lợi thế hơn các phương pháp còn lại. Phương pháp MF cho phép đạt được một mức độ đề kháng tốt trước khả năng phá hủy thông tin che giấu, số lượng các lỗi này là quá nhỏ nên có thể hiệu chỉnh bằng các thuật toán sửa sai.

3. NÂNG CAO HIỆU NĂNG CHE GIẤU THÔNG TIN TRONG ÂM THANH BẰNG PHƯƠNG PHÁP KẾT HỢP GIỮA MẬT MÃ VÀ ẨN MÃ

Hình 2 trình bày mô hình hệ thống che giấu thông tin trong âm thanh bằng biến đổi Fourier cải biến và phương pháp kết hợp giữa mật mã và ẩn mã. Trong giai đoạn đầu quá trình xử lý diễn ra trong hai kênh độc lập. Một trong số đó xử lý thông tin cần che dấu, trong khi kênh thứ hai là xử lý số vật phủ mang tin che giấu (container). Mục đích của xử lý thông tin cần che giấu là chuẩn bị thông tin để giấu và tạo cho chúng có đặc tính càng gần các chuỗi ngẫu nhiên càng tốt. Quá trình đó gồm ba giai đoạn:

1. Mã mật nhằm tăng cường hiệu năng



Hình 2. *Sơ đồ giấu tin mật trong mô hình khi kết hợp mật mã và ẩn mã.*

bảo mật thông tin trước khi nhúng vào vật phủ, làm thay đổi đặc tính chuỗi ký tự đính kèm, nhờ vậy cho dù đối phương phát hiện và trích xuất cũng không thể xác định được liệu đó là dữ liệu thật, hay chỉ là một chuỗi ngẫu nhiên các bit. Bằng cách này chúng ta tăng độ an toàn của dữ liệu đính kèm, kết hợp được hai kỹ thuật: mật mã và ẩn mã bảo vệ thông tin một cách hiệu quả nhất. Để mã hóa cần biết phân phối và quản lý khóa mã khi sử dụng. Giai đoạn này không ảnh hưởng đến độ an toàn của phương pháp ẩn mã.

2. Mã hóa ECC - Sử dụng mã sửa sai (Error Correcting Code) để sửa chữa một số lỗi có thể phát sinh trong quá trình xử lý của stegocontainer.

3. Bước hoán vị, có nhiệm vụ xáo trộn dữ liệu theo ma trận hoán vị - một phần của khóa ẩn mã. Mục đích của giai đoạn này là để xáo trộn các bit thông tin cần che giấu để có được chuỗi gần như ngẫu nhiên. Bằng cách này, ngay cả sau khi trích xuất các thông tin ẩn từ stegocontainer thu được tập các bit ngẫu nhiên không gây sự nghi ngờ của đối phương.

Xử lý tín hiệu sẽ chứa thông tin ẩn mã (vật phủ - container) bao gồm ba giai đoạn:

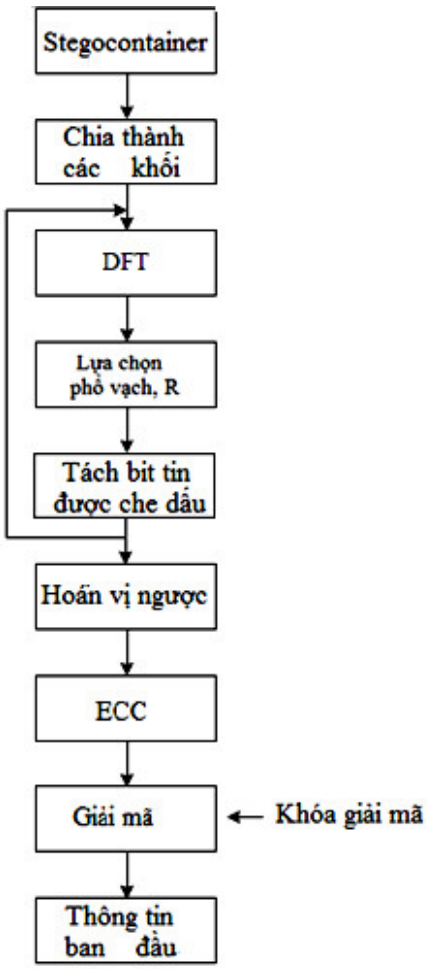
1. Phân chia tín hiệu thành thành từng đoạn, một số trong số đó được sử dụng để đính kèm thông tin cần che dấu. Phần còn lại được sử dụng để kết nối các khối mang thông tin. Kích thước và vị trí của các đoạn do khóa ẩn mã xác định.

2. Biến đổi Fourier rời rạc (DFT) có nhiệm vụ biến đổi dạng tín hiệu từ miền thời gian sang miền tần số, tính toán phổ tín hiệu.

3. Lựa chọn phổ vạch và tính R. Trong bước này sẽ lựa chọn các phổ vạch mang thông tin. Việc lựa chọn được thực hiện một cách độc lập trong mỗi đoạn tín hiệu. Để nhúng một bit thông tin sử dụng hai phổ vạch. Giá trị của những thay đổi được xác định tỷ lệ với kích thước của phổ vạch lớn nhất, do đó phương pháp này có thể thích ứng với các giá trị của các thay đổi năng lượng tín hiệu trong từng đoạn tín hiệu cụ thể. Cách chọn phổ vạch và giá trị thay đổi phụ thuộc vào khóa ẩn mã.

Sau khi chuẩn bị thông tin và thực hiện DFT, xác định các phổ vạch và giá trị thay đổi, tiến hành nhúng các bit thông tin trong từng đoạn theo thuật toán bằng cách thay đổi các giá trị của các phổ vạch được chọn để đạt được sự khác biệt giá trị giữa chúng theo giá trị đã xác định bởi thuật toán.

Thực hiện biến đổi Fourier ngược (IDFT), chuyển đoạn tín hiệu trở lại miền thời gian và khi đó đoạn tín hiệu này là vật phủ chứa thông tin che giấu - stegocontainer. Đoạn tín hiệu đã xử lý được xếp vào tín hiệu ở vị trí ban đầu.



Hình 3. *Sơ đồ trích xuất tin mật trong mô hình kết hợp mật mã và ẩn mã.*

Hình 3 trình bày phần tiếp theo của sơ đồ mô hình ẩn mã (stegosystem) nhằm trích xuất thông tin được che giấu từ vật phủ (stegocontainer). Để trích xuất các thông tin được che giấu ra cần có các khối chức năng trên và khóa mã tương ứng. Toàn bộ quá trình tách thông tinh được che giấu diễn ra theo trình tự ngược lại quá trình nhúng tin khi che giấu.

Để đánh giá ảnh hưởng của quá trình mã hóa và giải mã đối với phương pháp che giấu thông tin trong âm thanh bằng biến đổi Fourier cải biến kết hợp với mật mã chúng tôi đã xây dựng bộ phần mềm mã hóa dựa trên chuẩn mã hóa dữ liệu AES-256 với các kết quả thực hiện như sau:

Bảng 3. *Thời gian mã hóa và giải mã các tệp thông tin cần che dấu.*

Loại File	Độ dài File	Thời gian mã hóa [s]	Thời gian giải mã [s]
Ảnh	100 Kb	0.015	0.016
	500 Kb	0.031	0.031
	1 Mb	0.047	0.046
TEXT	100 Kb	0.008	0.007
	500 Kb	0.036	0.037
	1 Mb	0.048	0.053

Từ các kết quả trên ta dễ dàng nhận thấy thời gian mã hóa và giải mã các tệp thông tin cần che giấu hoàn toàn không ảnh hưởng gì đến quá trình ẩn mã mà chỉ làm tăng độ an toàn cho thông tin được che giấu và nâng cao hiệu năng hệ thống mà thôi.

4. KẾT LUẬN

Bài viết trình bày cách tiếp cận vấn đề ẩn mã máy tính, với sự kết hợp của hiện tượng mặt nạ tần số tín hiệu âm thanh với biến đổi Fourier rời rạc, mang lại một phương pháp hiệu quả và hiệu năng che giấu thông tin trong các vật chứa thông tin ẩn mã bằng tín hiệu âm thanh. Cách tiếp cận này dựa trên cách tìm trong dải phổ các phổ vạch có khả năng che giấu những thay đổi đưa vào trong phổ vạch tần số. Giải pháp này là cho phép lựa chọn độc lập các phổ vạch trong từng đoạn tín hiệu cho phép phân tán thông tin che giấu đính kèm trên một phổ tần số rộng, làm tăng độ khó khăn cho kẻ muốn gây thiệt hại có mục đích đối với dữ liệu được che giấu - đặc biệt, tần số cải biến hầu như luôn luôn nằm trong dải âm tần.

Bài viết cũng trình bày giải pháp nâng cao hiệu năng che giấu thông tin trong âm thanh bằng phương pháp kết hợp giữa mật mã và ẩn mã và thực hành mã hóa một số tệp dữ liệu cần che giấu khác nhau: text, hình ảnh…

TÀI LIỆU THAM KHẢO

[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]. 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.

[4]. Delforouzi A., Pooyan M.: "*Adaptive Digital Audio Steganography Based on Integer Wavelet Transform*". Circuits Syst Signal Process Vol. 27, 2008, s. 247÷259.

[5]. Gopalan K.: "*Audio steganography by cepstrum modification. Proc. IEEE Int. Conf. Acous-tics*", Speech, and Signal Processing, Vol. 5, 2005, s. 481÷484.

[6]. G Kozieł.: "*Zastosowanie transformaty Fouriera w steganografii sygnałów dźwiękowych*". Studia Informatica 32 (2A), 2011, p541-552.
[7]. D. Stinson, "*Cryptography: Theory and Practice*". CRC Press, LLC, 1995.
[8]. Mansour M., Tewfik A.: "*Audio Watermarking by Time-Scale Modification*". IEEE Interna-tional Conference on Acoustics, Speech and Signal Processing - Proceedings 3, 2001, s. 1353÷1356.

ABSTRACT

A METHOD OF ENHANCING THE PERFORMANCE FOR INFORMATION MASKING IN AUDIO

In the article, the Fourier transformation application for hiding the information in audio and methods for enhancing the performance of information masking in audio by modified Fourier transform and the method of combining cryptography and steganography are presented.

Keywords: Steganography, Fourier transformation, Information protect, Cryptography.

Nhận bài ngày 10 tháng 7 năm 2017
Hoàn thiện ngày 28 tháng 7 năm 2017
Chấp nhận đăng ngày 18 tháng 8 năm 2017

Địa chỉ: Học viện Kỹ thuật Mật mã.
* Email : lehung1412@yahoo.com.