MỘT KỸ THUẬT GIẤU TIN TRONG ÂM THANH SỬ DỤNG PHÉP BIẾN ĐỔI WAVELET

A METHOD FOR HIDING DATA IN AUDIO USING WAVELET TRANSFORMATION

Nguyễn Xuân Huy[1], Huỳnh Bá Diệu[2]

[1]Viện Công nghệ Thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam; nxhuy64@gmail.com
[2]Trường Đại học Duy Tân; dieuhb@gmail.com

Tóm tắt - Bài báo này trình bày một thuật toán giấu tin mật trong âm thanh. Dữ liệu âm thanh được chuyển sang miền tần số bằng phép biến đổi wavelet. Chuỗi tin mật được giấu lần lượt vào các đoạn dữ liệu âm thanh, bằng cách điều chỉnh các hệ số trên miền tần số cao của mỗi đoạn, kết hợp với các giá trị chuỗi ngẫu nhiên. Thuật toán đề xuất có thể giấu tin và giải tin chính xác. Quá trình giải tin không cần sử dụng dữ liệu gốc ban đầu và chất lượng âm thanh được đảm bảo.Tin giấu được rút trích chính xác khi thực hiện tấn công giảm số bit biểu diễn mẫu dữ liệu từ 16 bit xuống 8 bit. Ngoài ra thuật toán còn bền vững trước tấn công thêm nhiễu trắng ở mức thấp. Kết quả thử nghiệm chứng tỏ thuật toán đề xuất có thể sử dụng để giấu tin mật trong tệp âm thanh.

Từ khóa - giấu tin; lượng tử hoá; tỉ lệ dữ liệu; tính bền vững; biến đổi wavelet.

Abstract - This paper presents a new algorithm for hiding data into digital audio signals. Audio data is transferred to the frequency domain using wavelet transformation. The secret message is hidden in the audio data segments, by adjusting the coefficients on high-frequency domain of each segment, combined with the random number value. The proposed algorithm can hide and extract secret message accurately when attacks reduce the bit number of data sample to 8 from 16. The extraction process does not need host signal and sound quality is ensured. Experimental results show that the stego audio has good imperceptibility and is robust against different kinds of attacks, such as noise adding, re-sampling. The proposed algorithm can be used to hide secret messages in an audio file.

Key words - data hiding; quantization; data rate; robustness; transform wavelet.

1. Đặt vấn đề

Sự phát triển mạnh mẽ của công nghệ số và nhu cầu trao đổi thông tin thông qua các hệ thống được kết nối mạng đòi hỏi chúng ta cần phải có các giải pháp để bảo vệ thông tin. Các vi phạm liên quan đến thông tin thường gặp là xâm nhập trái phép, lấy cắp, thay đổi nội dung hay vi phạm bản quyền. Ngoài việc thiết lập các cơ chế bảo vệ như phân quyền truy cập, mã hoá thông tin, chúng ta còn có một cách khác là thực hiện các giao dịch ngầm bên trong các giao dịch công khai, đó là giấu thông tin.

Giấu thông tin số là kỹ thuật nhúng một lượng dữ liệu vào trong đối tượng chứa số khác. Nhiều kiểu dữ liệu số có thể được chọn làm dữ liệu chứa cho bài toán giấu tin như ảnh, video, âm thanh. Các nghiên cứu về giấu tin trong ảnh, video đã có nhiều kết quả và ứng dụng quan trọng. So với giấu tin trong ảnh và video, giấu tin trong âm thanh được nghiên cứu sau và có ít kết quả hơn. Giấu tin trong âm thanh dựa vào hệ thống thính giác. So với hệ thống thị giác thì hệ thống thính giác của con người khá nhạy và phức tạp. Hai thuộc tính của hệ thống thính giác của con người được khai thác để giấu tin là dựa vào hiện tượng che khuất trong miền thời gian (temporal masking) và che khuất trong miền tần số (frequency masking). Các phương pháp giấu tin trong âm thanh thực hiện điều chỉnh các mẫu dữ liệu âm thanh để giấu tin, nhưng chúng ta không thể phân biệt được có sự sai khác giữa âm thanh ban đầu và âm thanh sau khi điều chỉnh khi nghe.

Giấu tin có thể dùng để bảo vệ tin giấu (steganography) hoặc bảo vệ cho đối tượng chứa tin giấu (watermarking). Các phương pháp giấu tin có thể thực hiện trên miền thời gian hoặc trên miền biến đổi. Đối với các phương pháp trên miền thời gian, các bit tin mật sẽ được giấu trực tiếp vào các mẫu dữ liệu. Các phương pháp trên miền biến đổi sẽ thực hiện biến đổi dữ liệu âm thanh từ miền thời gian sang miền biến đổi, thực hiện điều chỉnh các giá trị trên miền biến đổi để giấu tin, sau đó các giá trị trên miền biến đổi sẽ được biến đổi ngược lại miền thời gian. Các phương pháp giấu trên miền thời gian có ưu điểm là dễ cài đặt và tỉ lệ dữ liệu giấu cao, nhưng có hạn chế là không bền vững trước các tấn công dạng xử lý số thông thường. Các phương pháp điều chỉnh LSB (Least Significant Bit), lượng tử hoá, mã hoá tiếng vọng là thuộc loại này. Các phương pháp giấu tin trên miền biến đổi làm cho tin giấu bền vững hơn trước các tấn công, nhưng lại làm tăng chi phí tính toán, do phải thực hiện các lần biến đổi. Các phép biến đổi hay được dùng là biến đổi Fourier, biến đổi wavelet.

Trong [4], [12] sử dụng kỹ thuật điều chỉnh tiếng vọng để giấu tin. Thuật toán trong [4] dùng cách thêm tiếng vọng sau và sao chép dữ liệu để giấu tin, trong khi đó thuật toán trong [12] thêm hai tiếng vọng (trước và sau) để giấu tin. Công thức thêm tiếng vọng để giấu tin trong [12] như sau:

$$d(n) = d(n) \mp \alpha d(n - d_0) \mp \alpha d(n + d_0) \pm \\ \pm \alpha d(n - d_1) \pm \alpha d(n + d_1) \qquad (1)$$

Một số thuật toán liên quan đến kỹ thuật giấu tin trong âm thanh bằng cách điều chỉnh LSB được trình bày trong [1], [3], [5], [8]. Các thuật toán giấu có thể thực hiện trên các mẫu dữ liệu âm thanh đơn lẻ hoặc dựa vào nhóm các mẫu dữ liệu của đoạn âm thanh. Các thuật toán giấu dùng phương pháp điều chỉnh LSB có thể giấu với tỉ lệ dữ liệu cao. Trong [2] đề xuất một thuật toán giấu sử dụng phổ (spectrum) của hai đoạn âm thanh kề nhau. Trong [6], [11] trình bày hai thuật toán trên miền biến đổi Fourier. Thuật toán đề xuất trong [6] có thể bền vững trước các tấn công như thêm nhiễu trắng, lấy lại mẫu. Thuật toán trong [11] thực hiện điều chỉnh pha của tín hiệu gốc để giấu tin. Đây là kỹ thuật không gây nhiễu cho tín hiệu chứa, nhưng có tỉ lệ dữ liệu thấp. Trong [7], [9], [10] đề xuất các thuật toán giấu trên miền biến đổi wavelet. Thuật toán đề xuất trong

[9] có thể tự đồng bộ dữ liệu bằng cách thêm mã đồng bộ vào tin giấu. Phương pháp này có thể chống các tấn công dạng cắt xén, dịch chuyển tệp chứa. Thuật toán trong [10] là thuật toán bền vững trước tấn công chuyển định dạng.

Trong bài báo này chúng tôi đề xuất một thuật toán giấu tin trong âm thanh trên miền biến đổi, sử dụng phương pháp điều chỉnh giá trị trung bình của hai đoạn con trong một đoạn dữ liệu để giấu tin. Phép biến đổi được sử dụng là phép biến đổi wavelet.

2. Thuật toán đề xuất

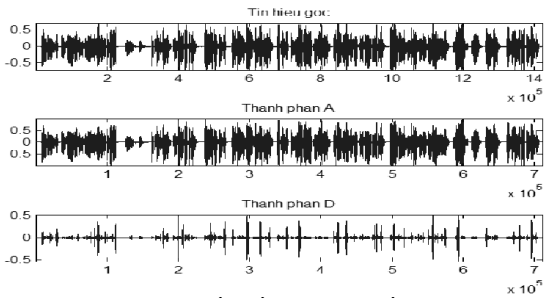
Trong thuật toán đề xuất, chúng tôi sử dụng phương pháp lượng tử hoá giá trị trung bình các hệ số của phép biến đổi wavelet để giấu tin. Dữ liệu âm thanh sẽ được đọc vào từ tệp âm thanh, dùng phép biến đổi wavelet để chuyển sang miền tần số, thực hiện giấu tin trên miền tần số, sau đó chuyển ngược lại từ miền tần số sang miền thời gian.

Dữ liệu âm thanh ở miền tần số sẽ được chia thành các đoạn bằng nhau và mỗi một bit mật sẽ được giấu vào trong mỗi đoạn, do đó dữ liệu âm thanh được chọn phải đủ dài để có thể chứa hết tin giấu. Cụ thể, để giấu n bit thì số đoạn ít nhất cần phải có là n. Ngoài ra, để tránh tin giấu không bị phát hiện thì dữ liệu âm thanh được chọn phải bao gồm các mẫu có khác nhau (tương tự như ta không chọn ảnh chỉ có một màu để giấu tin).

Để tăng tính mật, thuật toán đề xuất sử dụng khóa mật. Khóa mật K là bộ gồm 3 giá trị (seed, a, m), là các tham số để sinh chuỗi ngẫu nhiên. Chuỗi ngẫu nhiên được sinh theo phương pháp đồng dư tuyến tính [13] với giá trị c= 2*a.

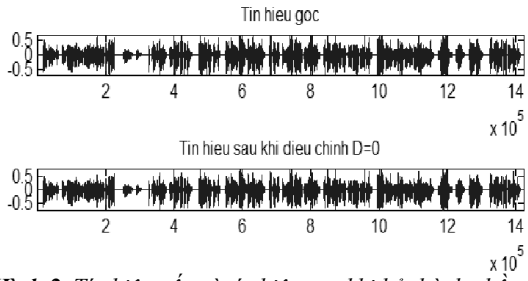
2.1. Phép biến đổi wavelet

Phép biến đổi wavelet được đưa ra đầu tiên bởi Alfréd Haar. Phép biến đổi này sẽ phân tích tín hiệu thành hai thành phần là thành phần xấp xỉ A (Approximation) và thành phần chi tiết D (Detail). Thành phần xấp xỉ A tương ứng với thành phần tần số thấp và thành phần chi tiết D tương ứng với thành phần tần số cao. Hình 1 minh hoạ cho việc phân giải tín hiệu thành hai thành phần.



Hình 1. *Thành phần xấp xỉ và chi tiết của tín hiệu*

Trong hai thành phần A và D, thành phần D là không quan trọng và những thay đổi trên thành phần này ít ảnh hưởng đến tín hiệu gốc khi ta biến đổi ngược lại. Ví dụ, nếu thay đổi thành phần D=0 và thực hiện biến đổi ngược lại, ta sẽ có dãy tín hiệu như Hình 2. Đây là đặc điểm của phép biến đổi wavelet. Nếu chỉ có những điều chỉnh nhỏ trên thành phần D thì nó gần như không ảnh hưởng đến dữ liệu gốc khi khôi phục lại và chúng ta không thể phân biệt được có sự điều chỉnh khi nghe bằng tai thường. Dựa vào đặc tính này, chúng tôi đề xuất cách điều chỉnh trên các giá trị trên thành phần này để giấu tin.



Hình 2. *Tín hiệu gốc và tín hiệu sau khi bỏ thành phần D*

2.2. Sự lượng tử hoá (quantization)

Để giấu một bit dữ liệu mật vào trong dữ liệu chứa, chúng ta cần điều chỉnh dữ liệu chứa. Các cách thay đổi giá trị một mẫu dữ liệu gốc x thành mẫu y để giấu tin được gọi là lượng tử hoá. Có nhiều phương pháp để thay đổi, như phương pháp dựa vào bước lượng tử, phương pháp dùng phép chia lấy dư (mod).

Trong bài báo này chúng tôi dùng phương pháp điều chỉnh dựa vào phép chia lấy dư. Để giấu bit mật vào trong mẫu x, trước tiên tính giá trị k= x mod d, trong đó d là một số thực dương. Ta qui ước sẽ điều chỉnh để giá trị k>d/2 khi muốn giấu bit 1 và k<=d/2 khi muốn giấu bit 0.

Trong thuật toán đề xuất, thay vì lượng tử cho các mẫu riêng lẻ, chúng tôi thực hiện lượng tử cho giá trị trung bình các mẫu. Mỗi một bit sẽ được giấu vào đoạn gồm *fw* mẫu được đánh số từ 1 đến *fw*. Chi tiết về phép điều chỉnh sẽ được trình bày ở phần sau.

Chuỗi ngẫu nhiên được sinh ra từ khóa mật được dùng để xáo trộn chuỗi bit mật trước khi giấu. Mục đích của việc xáo trộn này là làm cho người thám tin khó khôi lại chuỗi tin mật nếu như biết cách giấu. Trong trường hợp người thám tin biết cách điều chỉnh mỗi đoạn, các tham số để điều chỉnh mỗi đoạn, họ có thể rút trích chuỗi bit giấu trong dữ liệu âm thanh. Tuy nhiên, nếu không có khóa thì khả năng khôi phục lại chuỗi bit mật từ chuỗi bit nhận được cũng là bài toán khó. Cách biến đổi bit mật dựa vào chuỗi ngẫu nhiên sẽ được trình bày ở mục sau.

2.3. Thuật toán giấu tin và giải tin

2.3.1. Thuật toán giấu 1 bit

Đầu vào: - Dãy D gồm *fw* phần tử D[1..fw], bit cần giấu b, số thực d.

Đầu ra: - Dãy D đã được điều chỉnh để chứa bit mật b.

Phương pháp

Bước 1: Tính giá trị trung bình của nửa đoạn trước và nửa đoạn sau của D theo công thức (2).

$$h_1 = (\sum_1^{\frac{fw}{2}} D[i])/(fw/2) \qquad (2)$$

$$h_2 = (\sum_{\frac{fw}{2}+1}^{fw} D[i])/(\frac{fw}{2})$$

Bước 2: Tính giá trị lệch giá trị trung bình giữa hai đoạn, theo modulo d:

$$k = abs(h1 - h2)\ mod\ d$$

Bước 3: Điều chỉnh giá trị để giấu bit b:

Nếu b=1 và k> d/2 hoặc b=0 và k<= d/2 thì return;

Ngược lại: Nếu b=1 thì cộng d/2 cho nửa đoạn trước:

D[i]= D[i] + d/2, với i= 1 đến fw/2.

Ngược lại thì cộng d/2 cho nửa đoạn sau:

D[i]= D[i] + d/2, với i= fw +1 đến fw.

2.3.2. Thuật toán trích 1 bit

Đầu vào: - Dãy D gồm *fw* phần tử D[1..fw], số thực d.

Đầu ra: - Bit mật b.

Phương pháp

Bước 1: Tính giá trị trung bình của nửa đoạn trước h_1 và nửa đoạn sau h_2 của D theo công thức (2)

Bước 2: Tính giá trị lệch giá trị trung bình giữa hai đoạn, theo modulo d:

$$k = abs(h1 - h2)\ mod\ d$$

Bước 3: Trích bit b: Nếu k> d/2 thì b=1, ngược lại b=0.

2.3.3. Thuật toán giấu tin

Dưới đây là thuật toán giấu chuỗi bit mật M gồm n phần tử và tệp âm thanh H.

Đầu vào: - Khoá K, tệp gốc H, chuỗi bit mật M.

Đầu ra: - Tệp chứa tin mật S.

Phương pháp

Bước 1: Dùng khoá K để sinh ra chuỗi ngẫu nhiên R.

Bước 2: Biến đổi chuỗi bit mật M thành M' dựa vào R, trong đó:

$$M'(i) = \begin{cases} M(i) nếu R(i) lẻ \\ \overline{M(i)} nếu R(i) chẵn \end{cases} \quad (3)$$

Bước 3: Đọc dữ liệu các mẫu từ tệp âm thanh H vào mảng y. Thực hiện biến đổi wavelet cho dãy y.

$$[A, D] = DWT(y)$$

Bước 4: Chia dãy D thành các đoạn D_i có cùng kích thước fw, điều chỉnh các đoạn để giấu lần lượt từng phần tử $M'(i)$ vào các đoạn D_i, ta được D_i'.

Bước 5: Biến đổi wavelet ngược [A, D'] để có được y' và ghi y' ra tệp kết quả S.

2.3.4. Thuật toán giải tin

Đầu vào: - Khoá K, tệp chứa tin S.

Đầu ra: - Chuỗi bit mật M.

Phương pháp

Bước 1: Đọc dữ liệu các mẫu từ tệp âm thanh S vào mảng y. Thực hiện biến đổi wavelet cho dãy y.

$$[A, D] = DWT(y)$$

Bước 2: Chia dãy D thành các đoạn D_i có cùng kích thước fw và trích lấy lần lượt từng phần tử $M'(i)$ từ các đoạn D_i theo thuật toán trích bit.

Bước 3: Dùng khoá K để sinh ra chuỗi ngẫu nhiên R.

Bước 4: Biến đổi chuỗi M' thành M dựa vào R theo công thức (4):

$$M(i) = \begin{cases} M'(i)\ nếu\ R(i)\ lẻ \\ \overline{M'(i)}\ nếu\ R(i)\ chẵn \end{cases} \quad (4)$$

3. Kết quả thử nghiệm và đánh giá

Để đánh giá kỹ thuật đề xuất, chúng tôi dựa vào 3 độ đo là SRN (Signal – to – Noise Ratio), BER (Bit Error Rate) và NCC (Normalized Cross Correlation). Giá trị của SNR chỉ số lượng thay đổi trên dữ liệu gốc do chèn chuỗi tin mật vào, giá trị BER dùng để đo sự khác nhau giữa chuỗi tin khi giấu và chuỗi tin nhận được và giá trị NCC chỉ độ tương quan giữa hai chuỗi số, có thể dùng để đo độ tương quan giữa âm thanh gốc và âm thanh có chứa tin, hoặc chuỗi bit giấu đem giấu và chuỗi bit nhận được khi bị các tấn công.

Độ đo SNR được tính như sau:

$$SRN = 10\ \log_{10} \frac{\sum_{i=0}^{N} x(i)^2}{\sum_{i=0}^{N} [x(i) - y(i)]^2} \quad (5)$$

trong đó x (n) thể hiện âm thanh gốc và y(n) thể hiện âm thanh chứa tin giấu.

Các kỹ thuật giấu tin trong âm thanh phải đảm bảo giá trị SRN>=20 vì giá trị SRN dưới 20 dB được xem là nhiễu.

Công thức để tính BER như sau:

$$BER = {}^{1}/_{n} \sum_{1}^{n} abs(m(i) - m'(i)) \quad (6)$$

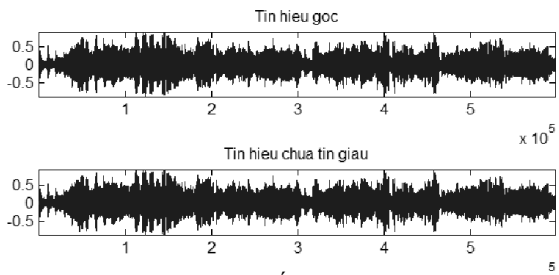
trong đó $m(i)$ là chuỗi tin giấu và $m'^{(i)}$ là chuỗi tin nhận được.

Công thức để tính NCC như sau:

$$NCC = \frac{1}{n} * \sum_{i=1}^{n} \frac{[x(i) * y(i)]}{[x(i)]^2} \quad (7)$$

trong đó $x(i)$ là chuỗi số gốc và $y(i)$ là chuỗi nhận được khi thực hiện biến đổi.

Giá trị của NCC nằm trong khoảng từ 0 đến 1. Nếu giá trị này càng gần 1 chứng tỏ hai chuỗi càng giống nhau.



Hình 3. *Tín hiệu âm thanh gốc và âm thanh có chứa tin mật*

Trong phần thử nghiệm, chúng tôi chọn các tệp âm thanh mono lượng tử 16 bit, để giấu các chuỗi bit. Các tệp âm thanh được chọn ở nhiều thể loại khác nhau, như bản hòa tấu, thông báo, hay âm thanh hỗn hợp. Độ dài các chuỗi bit được giấu được thử nghiệm tuỳ thuộc vào tệp âm thanh chứa. Giá trị d được chọn là 0.1 và kích thước mỗi đoạn để giấu 1 bit là 200. Hình 3 minh họa cho giấu 2000 bit vào trong tệp âm thanh, là bản hòa tấu nhiều nhạc cụ.

Bảng 1. *Giá trị SRN và NCC sau khi giấu tin*

Tên tệp	Dạng âm thanh	Kích thước tệp	Số bit giấu	SRN	NCC
S.wav	Bài nói	6.5 Mb	2000	22.18	0.9989
B.wav	Đoạn nhạc	1.14 Mb	1400	21.67	0.9965
C.wav	Tiếng cười	104 Kb	100	25.74	0.9987
E.wav	Thông báo	2.71 Mb	2000	20.55	0.9955

Bảng 1 thể hiện độ đo SRN và độ đo NCC khi tiến hành giấu các chuỗi bit vào các tệp âm thanh. Các giá trị của hệ số SRN trong Bảng 1 chứng tỏ kỹ thuật đề xuất đạt được tiêu chuẩn về tỉ lệ nhiễu khi giấu tin. Các giá trị của hệ số NCC khi giấu vào các tệp đều đạt lớn hơn 99%, thể hiện sự tương đối giống nhau giữa tệp âm thanh gốc và

tệp âm thanh có chứa tin mật.

Các thử nghiệm cho thấy thuật toán đề xuất rút trích tin giấu chính xác, nếu như tệp âm thanh chứa tin mật không bị các tấn công. Chúng tôi cũng thử nghiệm giảm số bit lượng tử các mẫu dữ liệu âm thanh từ 16 bit xuống 8 bit, kết quả cho thấy tấn công này không làm sai chuỗi bit trong quá trình giải tin.

Để kiểm tra tính bền vững của kỹ thuật đề xuất, chúng tôi cũng thực hiện tấn công thêm nhiễu vào tệp chứa tin giấu bằng các hàm thêm nhiễu trong Matlab. Kết quả thực nghiệm cho thấy kỹ thuật đề xuất bền vững với tấn công thêm nhiễu trắng (White Gaussian Noise) khi hệ số gây nhiễu (SRN) lớn hơn 15. Đối với hệ số gây nhiễu nhỏ hơn 10, làm thay đổi rõ rệt dữ liệu chứa, có làm ảnh hưởng đến tin giấu. Kết quả thử nghiệm thể hiện trong Bảng 2.

Bảng 2. *Giá trị BER và NCC khi thêm nhiễu trắng*

Tên tệp	Tỉ lệ bit sai / Độ tương quan		
	SRN= 7	SRN= 10	SRN>=15
S1.wav	0.005/ 0.9989	0/1	0/ 1
B1.wav	0.044/ 0.9148	0.057/ 0.9987	0/1
C1.wav	0.12/ 0.7648	0.04/ 0.9202	0/1
E1.wav	0.002/ 0.9950	0/1	0/1

Đối với tấn công thêm nhiễu hạt tiêu (pepper) và nhiễu đốm (speckle), tin giấu trong dữ liệu chứa không bền vững. Chúng tôi thực hiện giấu 1444 bit, là dữ liệu ảnh của ảnh đen trắng như Hình 4(a) vào tệp S1.wav. Hình 4.b và 4.c là quả ảnh rút trích từ tệp âm thanh sau khi thực hiện thêm nhiễu hạt tiêu với hệ số d= 0.001 (*imnoise(y1,'salt & pepper', 0.001)*) và nhiễu đốm với hệ số v=0.001 (*imnoise(y1,'speckle', 0.001)*). Các thông số cụ thể khác được thể hiện trong Bảng 3.

Hình 4. *Ảnh gốc (a) và ảnh nhận được khi tệp âm thanh chứa tin bị thêm nhiễu hạt tiêu (b) và nhiễu đốm (c)*

Bảng 3. *Giá trị BER và NCC khi thêm nhiễu hạt tiêu và nhiễu đốm*

	Thêm nhiễu hạt tiêu	**Thêm nhiễu đốm**
Số bit sai khác	383	389
BER	0.26523	0.26939
NCC	0.56568	0.55967

Độ tương quan trong Bảng 2 và Bảng 3 là so sánh giữa chuỗi tin giấu và chuỗi tin nhận được khi chịu các tấn công.

Kỹ thuật đề xuất hướng đến mục tiêu dùng để giấu tin mật, nên chọn miền điều chỉnh ít ảnh hưởng đến nội dung tệp dữ liệu chứa, là vùng tần số cao. Các nghiên cứu [7], [9], [10] thực hiện giấu trên miền tần số thấp, được thực hiện cho mục đích thủy vân số.

Độ an toàn của sơ đồ giấu phụ thuộc vào khóa K, dùng để sinh chuỗi ngẫu nhiên. Từ chuỗi ngẫu nhiên này ta sẽ xác định được các bit cần lấy là 0 hay 1. Nếu không có chuỗi ngẫu nhiên này, người thám tin sẽ không biết được là lấy bit nào, dù biết cách trích tin ra từ tệp âm thanh. Ngoài ra ta có thể điều chỉnh chiều dài của mỗi đoạn *fw* và giá trị của ngưỡng d để tăng độ mật cho kỹ thuật giấu.

4. Kết luận

Trong bài báo này, chúng tôi trình bày một kỹ thuật giấu tin mật trong âm thanh sử dụng phép biến đổi wavelet. Dữ liệu âm thanh gốc và âm thanh chứa tin mật tương tự với nhau, thỏa mãn yêu cầu về tỉ lệ nhiễu và độ tương quan. Thuật toán đề xuất cũng bền vững trước các tấn công như giảm số bit lượng tử, thêm nhiễu trắng, nhưng chưa bền vững trước tấn công thêm nhiễu hạt tiêu và nhiễu đốm. Để tăng tỉ lệ dữ liệu giấu và tính bền vững của tin giấu, trong tương lai chúng tôi dự kiến cải tiến cách giấu bằng cách kết hợp giấu trên cả hai thành phần xấp xỉ và thành phần chi tiết của phép biến đổi wavelet.

TÀI LIỆU THAM KHẢO

[1] Cvejic, N.; Seppanen, T., "Increasing robustness of LSB audio steganography using a novel embedding method", *Proceeding of the International Conference on Information Technology: Coding and Computing*, 2004, vol.2, pp. 533-537.

[2] Dymarski, P.; Markiewicz, R., "Time and sampling frequency offset correction in audio watermarking", *Proceeding of the 18th International Conference on Systems, Signals and Image Processing* , 2011, pp.1-4.

[3] Ghobadi, A.; Boroujerdizadeh, A.; Yaribakht, A.H.; Karimi, R., "Blind audio watermarking for tamper detection based on LSB", *Proceeding of the 15th International Conference on Advanced Communication Technology (ICACT)*, 2013, pp.1077-1082.

[4] H. Dieu, "An Improvement for Hiding Data in Audio Using Echo Modulation", *Proceeding of the Second International Conference on Informatics and Engineering and Information Science*, 2013, pp. 127-132.

[5] Huynh Ba Dieu; Nguyen Xuan Huy, "Hiding data in audio using modified CPT scheme", *Proceeding of the International Conference of Soft Computing and Pattern Recognition (SoCPaR)*, 2013, pp. 396-400.

[6] Liting Gao; Wei Zhao; Xiumei Wen; Lixia Wang, "An audio zero-watermarking algorithm based on FFT", *Proceeding of the 2nd International Conference on Networking and Digital Society (ICNDS)*, 2010, vol.1, pp.274-277.

[7] Liu Tianchi; Yang Guangming; Wang Qi, "A multiple audio watermarking algorithm based on shear resisting DWT and LSB", *Proceeding of the 7th International Conference on Networked Computing (INC)*, 2011, pp.78-83.

[8] Nguyen Xuan Huy; Huynh Ba Dieu, "An efficient method for hiding data in audio", *Proceeding of the International Conference Advanced Technologies for Communications (ATC)*, 2014, pp.167-171.

[9] Shaoquan Wu; Jiwu Huang; Daren Huang; Shi, Y.Q., "Self-synchronized audio watermark in DWT domain", *Proceeding of the 2004 International Symposium on Circuits and Systems*, 2004, vol.5, pp.712-715.

[10] Vongpraphip, S.; Ketcham, M., "An Intelligence Audio Watermarking Based on DWT- SVD Using ATS", *Global Congress on Intelligent Systems*, 2009, vol.3, pp.150-154.

[11] Xiumei Wen; Xuejun Ding; Jianhua Li; Liting Gao; Haoyue Sun, "An Audio Watermarking Algorithm Based on Fast Fourier Transform", *Proceeding of the 2009 International Conference on Information Management, Innovation Management and Industrial Engineering*,2009, vol.1, pp.363-366.

[12] Xulai Cao; Linghua Zhang, "Researches on echo kernels of audio digital watermarking technology based on echo hiding", *Proceeding of the International Conference on Wireless Communications and Signal Processing*, 2011pp.1-5, 2011.

[13] http://www.eternallyconfuzzled.com/tuts/algorithms/jsw_tut_rand.aspx (truy cập ngày 15 tháng 8 năm 2015).

(BBT nhận bài: 06/11/2015, phản biện xong: 19/12/2015)