MỘT SỐ GIẢI PHÁP MỚI GIẤU VĂN BẢN THUẦN TÚY TRONG ÂM THANH SỐ
SOME NEW METHODS FOR HIDDING PLAINTEXT INTO DIGITAL AUDIO

HỒ THỊ HƯƠNG THƠM, NGUYỄN HẠNH PHÚC
Khoa Công nghệ thông tin, Trường Đại học Hàng hải Việt Nam

Tóm tắt

Trong bài báo này nhóm tác nghiên cứu phương pháp giấu tin trong tín hiệu âm thanh số (Audio) nói chung và đề xuất hai giải pháp giấu văn bản thuần túy trong tín hiệu âm thanh. Các phương pháp giấu đề xuất có thể mở rộng để giấu các dữ liệu khác khi dữ liệu đó có thể chuyển hóa sang dạng nhị phân. Kết quả thử nghiệm cho thấy phương pháp giấu tin đề xuất ảnh hưởng không nhiều đến chất lượng của âm thanh ban đầu và có thể giấu lượng thông tin (bit) với tỉ lệ lớn so với lượng tín hiệu của âm thanh.

Abstract

The aim of this paper is to present two new methods that can hide a secret text into an audio file, the proposed methods can be advanced to hide other secret data if these data can be converted into binary string. Experimental results show that these approaches has little effect on the quality of cover audio and can hide information with large ratio when compared to the amount of cover audio signals.

Key words: *Cover, stego, steganography, watermarking.*

1. Giới thiệu

Giấu thông tin (Hiding information) là kỹ thuật giấu thông tin quan trọng vào đối tượng dữ liệu số mà ảnh hưởng rất ít đến chất lượng ban đầu của dữ liệu số. Dữ liệu số dùng để che giấu tin có thể là ảnh số (image), âm thanh số (audio), phim hoặc đoạn clip (video)... Giấu tin có hai mục đích chính: thứ nhất, giấu tin nhằm mục đích bảo vệ cho chính tài liệu số dùng để bao che thông tin giấu, đây chính là hình thức dùng để bảo vệ bản quyền hoặc chống xuyên tạc nội dung ... hình thức giấu này gọi là thủy vân số (Watermarking); thứ hai, giấu tin nhằm mục đích trao đổi thông tin mật đến một đối tượng đồng minh mà không muốn đối tượng thứ ba (không mong muốn) có thể phát hiện ra hay nghi ngờ… hình thức giấu này là giấu tin mật (Steganography), các kỹ thuật giấu theo hình thức này thường cố gắng giấu được càng nhiều thông tin vào dữ liệu số càng tốt nhưng vẫn đảm bảo chất lượng nội dung ban đầu của dữ liệu số [1, 2].

Với hai mục đích chính trên, bài báo này đề xuất hai phương pháp giấu tin trên tín hiệu âm thanh đó là: giấu tin trên miền tín hiệu thời gian thực và giấu tin trên miền tần số (Fourier, Cosine hoặc wavelet) [5]. Trong nghiên cứu này, nhóm tác giả chỉ tập trung vào phương pháp giấu tin trên bit có trọng số thấp LSB (Least Significant Bit) của tín hiệu âm thanh, nội dung nghiên cứu được trình bày chi tiết trong mục 2, 3, 4 và 5 là phần thử nghiệm, đánh giá và kết luận.

2. Kỹ thuật giấu trong LSB

Phương pháp giấu tin trên bit có trọng số thấp hay còn gọi là phương pháp mã hóa LSB (Least Significant Bit) là phương pháp nhúng bit thông tin vào các bit có trọng số thấp của dữ liệu audio. Giả sử một tín hiệu A có giá trị bằng 218 ứng với 8 bit nhị phân 11011010, khi đó bit bên trái nhất (có giá trị 1) được gọi là bit có trọng số lớn nhất MSB (Most significant bit), và bit bên phải nhất (có giá trị là 0) được gọi là bit có trọng số thấp nhất LSB (Least significant bit). Với bit có trọng số thấp nhất khi thay đổi giá trị từ 0 sang 1 hoặc từ 1 sang 0 sẽ không làm thay đổi nhiều giá trị gốc ban đầu. Do vậy khi nhúng thông tin mật vào tín hiệu audio chúng ta có thể nhúng vào bit có trọng số thấp nhất này để không làm ảnh hưởng đến thính giác của người nghe.

Trong trường hợp tín hiệu audio được lấy mẫu với tần số lấy mẫu là 44.1kHz thì tín hiệu audio có thể biểu diễn dưới dạng 16 bit, khi đó người ta có thể giấu thông tin từ 1 đến 8 bit có trọng số thấp thay vì 1 bit có trọng số thấp [7,8]. Với trường hợp giấu trong LSB này có thể giấu với tỉ lệ thông tin rất lớn so với lượng tín hiệu của audio mà không làm ảnh hưởng nhiều đến hệ thống thính giác của con người [5-7], do vậy người ta có thể lựa chọn giấu trên nhiều bit LSB

để có thể trao đổi nhiều thông tin mật trong một tệp audio nào đó trong quá trình truyền tin.

Để tăng độ an toàn cho quá trình giấu tin và tách tin chúng ta có thể chọn số lượng bit LSB dùng để giấu tin sao cho phù hợp nhất mà không ảnh hưởng đến chất lượng âm thanh ban đầu.

3. Phương pháp giấu văn bản đề xuất

3.1. Dữ liệu văn bản

Thông tin văn bản là dạng thông tin có nội dung toàn văn bản ký tự và số đơn thuần, trong nội dung không chứa các thông tin bảng biểu, biểu đồ, tranh ảnh hoặc hình vẽ… khi lưu trữ trong máy tính có thể lưu trong các tệp text của ứng dụng NotePad (*.txt) hoặc WordPad (*.rtf). Mỗi ký tự lưu trong tệp ứng với một mã ASCII có giá trị là 1 byte (giá trị từ 0 đến 255) nhưng chỉ có 128 ký tự đầu là hay dùng, còn lại là các ký tự mở rộng. Các ký tự có mã từ 0 đến 30 gọi là các ký tự điều khiển, không in ra được, được dùng để điều khiển các thiết bị ngoại vi, chẳng hạn ký tự có mã giá trị là 7 dùng để tạo một tiếng kêu bip, ký tự có mã là 13 dùng để chuyển con trỏ màn hình xuống đầu dòng dưới… do đó để truyền thông tin mật dưới dạng văn bản đặc biệt văn bản tiếng Anh ta chỉ cần sử dụng các ký tự từ 32 đến 127 là có thể biểu diễn đủ nội dung cơ bản cần trao đổi. Do đó, tác giả xin đề xuất hai phương pháp giấu văn bản trong tín hiệu audio bằng cách sử dụng 7 bit MSB của tín hiệu để ẩn dữ liệu mà không ảnh hưởng nhiều đến tín hiệu audio gốc.

3.2. Phương pháp giấu văn bản 1

Mỗi ký tự trong mẩu tin cần giấu được chuyển đổi 7 bit nhị phân, 7 bit này so sánh với 7 bit MSB của các tín hiệu âm thanh gốc, nếu gặp tín hiệu âm thanh nào trùng khớp, đánh dấu sự có mặt của tin giấu trong tín hiệu đó bằng cách sử dụng 4 bit LSB của tín hiệu âm thanh, theo nguyên tắc điều chỉnh số bit 1 trong 4 bit LSB là số lẻ. Trong trường hợp 7 bit cao MSB của tín hiệu gốc không trùng khớp với 7 bit của tin giấu ta sẽ điều chỉnh số bit 1 trong 4 bit LSB của tín hiệu là số chẵn để đánh dấu tín hiệu này không giấu tin. Quá trình giấu sẽ lặp lại cho đến khi giấu hết thông điệp.

Quá trình tách tin được thực hiện bằng cách kiểm tra 4 bit LSB của từng tín hiệu audio, nếu số bit 1 của 4 bit này là lẻ thì tách ra 7 bit MSB được ký tự của mẩu tin đã giấu, ngược lại nếu số bit 1 là chẵn thì bỏ qua và thực hiện kiểm tra tiếp các tín hiệu tiếp theo.

Với phương pháp giấu tin này chúng ta không làm thay đổi quá nhiều số bit LSB để giấu 7 bit thông tin. Khi cài đặt chúng ta có thể điều chỉnh sử dụng 2 hoặc 4 bit LSB để kiểm tra tính chẵn lẻ của bit 1 trong chuỗi.

3.3. Phương pháp giấu văn bản 2

Trong trường hợp số lượng thông tin văn bản cần giấu quá nhiều so với số lượng trùng khớp của việc so sánh với tín hiệu âm thanh, khi đó chúng ta có thể tăng khả năng trùng khớp thay vì sử dụng so sánh 7 bit thông tin cần giấu với 7 bit MSB của tín hiệu âm thanh, chúng ta sử dụng phương pháp so sánh 4 bit như sau: ứng với 7 bit của mỗi ký tự đem giấu ta chỉ so khớp 4 bit của ký tự với 4 bit MSB của tín hiệu audio nếu trùng khớp ta thay thế 3 bit cuối của tín hiệu bằng 3 bit cuối của ký tự. Còn trong trường hợp không trùng khớp ta điều chỉnh 3 bit LSB của tín hiệu đều bằng 0 để đánh dấu tín hiệu này không giấu thông tin.

Trong trường hợp 3 bit cuối của thông tin giấu có thể đều bằng 0 khi đó giấu vào tín hiệu sẽ trùng với trường hợp đánh giấu không giấu tin, điều đó dẫn đến mất thông tin trong quá trình tách tin. Để tránh xảy ra trường hợp này chúng ta sử dụng thêm một bit LSB thứ 4 (nằm sau 3 bit LSB đầu) đánh giấu là 1 nếu giấu tin ngược lại đánh giấu 0.

Trong quá trình tách tin chúng ta chỉ việc kiểm tra 4 bit LSB nếu đều bằng 0 là không giấu tin, ngược lại ta tách tin giấu bằng cách lấy 4 bit MSB ghép với 3 bit LSB của tín hiệu âm thanh được ký tự đã giấu.

3.4. Phương pháp giấu chuỗi bit thông tin bất kỳ

Trong trường hợp thông tin cần giấu là ảnh nhị phân, ảnh cấp xám hay là một đoạn âm thanh nào đó có thể chuyển đổi sang chuỗi bit nhị phân chúng ta có thể hiệu chỉnh phương pháp 1 và phương pháp 2 để có thể giấu vào tín hiệu âm thanh như sau:

Giả sử chuỗi bit thông tin cần giấu có L bit biểu diễn dưới dạng M = $b_0b_1b_2...$ b_L thực hiện chia chuỗi M thành các chuỗi con gồm *k* bit khi đó thông tin biểu diễn dưới dạng M=

$||M_0||M_1||M_2||...||M_N||$. Nếu k = 7 bit thì chúng ta có thể áp dụng phương pháp 1 hoặc phương pháp 2 để giấu từng chuỗi con M_i (i = 0,1...N) vào các tín hiệu âm thanh.

Nếu thông tin cần giấu là ảnh cấp xám 8 bit thì mỗi điểm ảnh chuyển sang nhị phân là chuỗi 8 bit, khi đó chuỗi bit M = $b_0b_1b_2...$ b_L tương ứng nên chia thành chuỗi con với k=8 (M= $||M_0||M_1||M_2||...||M_N||$), ta có thể giấu vào tín hiệu âm thanh bằng cách sử dụng phương pháp 2 với hiệu chỉnh như sau: với mỗi chuỗi con M_i 8 bit ta thực hiện so khớp 4 bit MSB của M_i với 4 bit MSB của tín hiệu âm thanh, nếu trùng khớp ta thay thế 4 bit LSB của M_i vào 4 bit LSB của tín hiệu âm thanh nếu trùng khớp trong trường hợp ngược lại ta đánh dấu tín hiệu này không giấu tin bằng cách thay 3 (hoặc 4) bit LSB đều bằng bit 0. Khi đó trong trường hợp tách tin ta chỉ cần kiểm tra 3 bit (hoặc 4 bit) LSB của mỗi tín hiệu nếu đều bằng 0 thì bỏ qua không tách tin, ngược lại tách 4 bit MSB và 4 bit LSB của tín hiệu âm thanh ta được chuỗi bit đã giấu vào tín hiệu.

4. Thử nghiệm

4.1. Phương pháp đánh giá chất lượng âm thanh sau khi giấu tin

Để đánh giá chất lượng của tín hiệu âm thanh ở đầu ra của bộ mã hoá, người ta thường sử dụng hai tham số: sai số bình phương trung bình – MSE (Mean Square Error) và phương pháp hệ số tỷ lệ tín hiệu / tín hiệu nhiễu PSNR (Peak Signal to Noise Ratio).

$$PSNR = 10*\log10\left(\frac{\max(x_i)^2}{MSE}\right)$$

Thông thường, nếu PSNR > 35dB [7] thì hệ thống thính giác của con người gần như không phân biệt được sự khác biệt giữa tín hiệu gốc và tín hiệu bị biến đổi để giấu tin. PSNR càng cao thì chất lượng của tín hiệu càng ít bị thay đổi so với gốc. Khi hai tín hiệu giống hệt nhau, MSE sẽ bằng 0 và PSNR đi đến vô hạn.

4.2. Thử nghiệm

Trong bài báo này, cài đặt và thử nghiệm các phương pháp giấu tin trong tín hiệu âm thanh được thực hiện trên môi trường Matlab 2008a. Tập âm thanh dùng để giấu thông tin gồm 20 tệp âm thanh (10 tệp có lời và 10 tệp không lời) định dạng WAV chuẩn PCM (Pulse-code modulation) với tần số lấy mẫu 44.1kHz. Các tệp âm thanh này đều có kích cỡ xấp xỉ nhau khoảng 5.5Mb (ứng với 1463616 tín hiệu âm thanh).

Đoạn văn bản cần giấu là một đoạn văn bản đơn thuần (chỉ bao gồm các ký tự chữ cái và chữ số) là chuỗi văn bản bao gồm 4064 ký tự (một trang giấy A4), chuyển sang chuỗi nhị phân với mỗi ký tự ứng với 7 bit ta được một chuỗi mới gồm 28448 bit.

Thực hiện giấu tin trong tập tín hiệu âm thanh với bốn trường hợp sau:

+ *Trường hợp 1*: Giấu trên LSB sử dụng phương pháp giấu trên 1 bit LSB (thay thế 1 bit LSB của tín hiệu bằng 1 bit cần giấu)

+ *Trường hợp 2*: Giấu trên LSB sử dụng phương pháp giấu trên 7 bit LSB (thay thế 7 bit LSB của tín hiệu bằng 7 bit LSB cần giấu [7])

+ *Trường hợp 3*: Giấu trên LSB sử dụng phương pháp giấu văn bản 1

+ *Trường hợp 4*: Giấu trên LSB sử dụng phương pháp giấu văn bản 2

Sử dụng phương pháp đánh giá bằng PSNR cho bốn trường hợp này chúng ta có kết quả thể hiện trên biểu đồ trong Hình 1.

Dựa vào kết quả trong hình 1 chúng ta có thể dễ dàng quan sát thấy thay đổi 1 bit LSB (sử dụng Phương pháp 1 đề xuất) và 3 bit LSB (sử dụng phương pháp 2 đề xuất) có giá trị PSNR cao hơn so với trường hợp thay đổi 1 bit LSB và 7 bit LSB đơn giản. Điều này có thể giải thích đơn giản như sau phương pháp giấu sử dụng thay thế 7 bit LSB sẽ làm thay đổi giá trị rất nhiều tín hiệu âm thanh ban đầu, còn đối với phương pháp 1 và 2 đề xuất sẽ chỉ làm thay đổi ½ số bit LSB của tín hiệu âm thanh cần thiết để giấu tin vì nếu coi chuỗi bit cần giấu là đại lượng ngẫu nhiên thì $P(0)\approx P(1)\approx 0.5$ (do đó ½ số bit LSB của tín hiệu âm thanh còn lại sẽ vẫn giữ nguyên như ban đầu). Vì vậy muốn giấu 28448 bit với trường hợp 1 sẽ thay đổi 14224 bit LSB của dữ liệu âm thanh gốc, trường hợp 3 sẽ thay đổi 2032 bit của tín hiệu âm thanh gốc, trường hợp 4 sẽ thay đổi 6096 bit LSB của tin hiệu âm thanh gốc. trường hợp 6 thay đổi 7112 bit tín hiệu gốc.

Tác giả cũng đã tiến hành thử nghiệm cho trường hợp số lượng thông tin văn bản lớn có số bit bằng ½ (50%) số tín hiệu của âm thanh gốc, sau đó thử nghiệm đánh giá với PSNR cho thấy giá trị trung bình của PSNR vẫn rất cao lớn hơn 43 dB (trong phạm vi cho phép), vì giới hạn

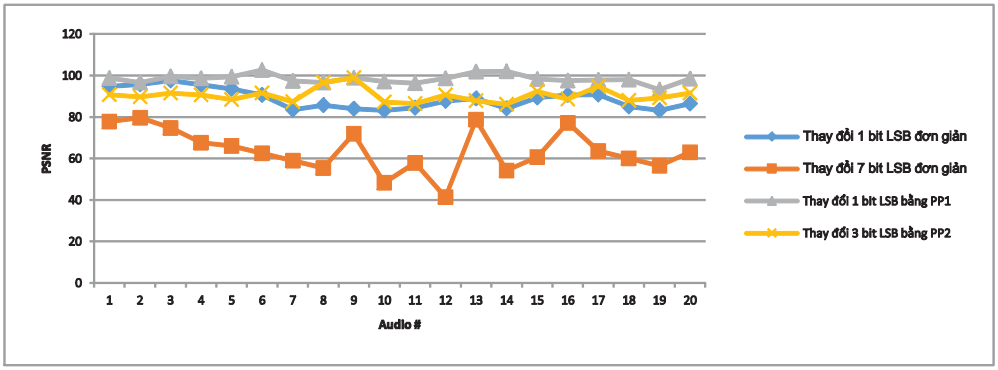
không gian trình bày hạn chế nên không trình bày thử nghiệm ở đây cho trường hợp này.

5. Kết luận

Trong nghiên cứu này nhóm tác giả đã đề xuất phương pháp giấu thông tin vào dữ liệu âm thanh với thông tin giấu là văn bản thuần túy. Dựa vào kết quả thử nghiệm cho thấy tín hiệu âm thanh sau khi giấu biến đổi ở mức rất thấp (theo đánh giá PSNR), không ảnh hưởng nhiều đến chất lượng âm thanh khi đánh giá bằng thính giác của con người. Phương pháp này có thể mở rộng để giấu thông tin bất kỳ khi thông tin đó có thể chuyển hóa sang chuỗi bit nhị phân. Đây là phương pháp có thể ứng dụng trong an toàn thông tin nhằm mục đích trao đổi thông tin mật.

Tuy nhiên đây không phải là phương pháp giấu bền vững, có thể mất thông tin dưới bất kỳ sự tác động nhỏ nào đến tín hiệu âm thanh. Phương pháp này mới chỉ áp dụng được cho các tệp âm thanh với các tín hiệu được mã hóa 16 bit, nhạc chưa nén wave chuẩn PCM, tác giả chưa thử nghiệm và đánh giá được cho tệp âm thanh định dạng khác hoặc nhạc nén mp3, mp4, mpeg...

Do đó, hướng nghiên cứu tiếp theo của tác giả sẽ nghiên cứu kỹ thuật giấu tin bền vững trên các loại âm thanh để có thể ứng dụng cho bản quyền số và toàn vẹn thông tin.



Hình 1. PSNR của 20 tệp âm thanh sau khi giấu tin văn bản sử dụng 4 phương pháp thay đổi LSB

TÀI LIỆU THAM KHẢO

[1]. Ingemar Cox, Jeffrey Bloom, Matthew Miller, Ton Kalker, Jessica Fridrich (2008), *Digital Watermarking and Steganography*, Second Edition, Morgan Kaufmann Press, USA.

[2]. Jessica Fridrich (2009), *Steganography in digital media: principles, algorithms, and applications*, Cambridge University Press

[3]. http://www.infotech.oulu.fi/Annual/2003/MTEAM.html

[4]. Min Wu, *Multimedia Data Hiding*, Princeton University, USA, 2001.

[5]. Michael Arnold, Dr. Christoph Busch, *Watermarking of Audio, Music Scores and 3D Models*, INI-GraphicsNet - Press & Media, 2003.

[6]. Chun-Shien Lu, *Multimedia Security: Steganography and Digital Watermarking techniques for Protection of Intellectual Property*, IDEA Group Publishing, 2005.

[7]. https://www.clear.rice.edu/elec301/Projects01/smokey_steg

[8]. Pradeep Kumar Singh, R.K.Aggrawal: "*Enhancement of LSB based Steganography for Hiding Image in Audio*", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1652-1658.

Ngày nhận bài: 03/3/2016
Ngày phản biện: 11/3/2016
Ngày chỉnh sửa: 14/3/2016
Ngày duyệt đăng: 15/3/2016