BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM TP HỒ CHÍ MINH

BÁO CÁO TỔNG KẾT

BẢO MẬT VÀ AN NINH MẠNG

TÌM HIỂU THUẬT TOÁN LSB VÀ ỨNG DỤNG GIẤU TIN TRONG FILE ÂM THANH

Nhóm SV thực hiện:

Nhóm HKT

Lâm Phát Tài	44.01.104.188
Bùi Chí Tùng	44.01.104.200
Võ Tuấn Hào	44.01.104.081
Lâm Hoàng Khánh	44.01.104.112
Nguyễn Xuân Tính	44.01.104.196

Người hướng dẫn: ThS. Lương Trần Hy Hiến

TP Hồ Chí Minh, 5/2021

MỤC LỤC

LỜI CẢM ƠN

Đầu tiên, xin gửi lời cảm ơn chân thành đến Thầy Lương Trần Hy Hiến, người đã tận tình hướng dẫn, động viên, giúp đỡ chúng em trong suốt thời gian thực hiện đề tài. Trong thời gian làm việc với Thầy chúng em không những học hỏi được nhiều kiến thức bổ ích mà còn học được tinh thần và thái độ làm việc nghiêm túc cũng như những kiến thức về cuộc sống rất quý báu của Thầy.

Mặc dù nhóm đã cố gắng hoàn thiện đề tài này với tất cả sự nỗ lực nhưng không thể tránh khỏi những thiếu sót. Chúng em mong nhận được sự thông cảm và chỉ bảo của Thầy.

Tp. Hồ Chí Minh, ngày 16 tháng 05 năm 2021

Nhóm sinh viên

PHÂN CÔNG NHIỆM VỤ

STT	Họ và tên	Nhiệm vụ
1	Lâm Phát Tài	Tìm hiểu về thuật toán Hoàn thiện tài liệu báo cáo
2	Bùi Chí Tùng	Tìm hiểu về thuật toán Hoàn thiện tài liệu báo cáo
3	Võ Tuấn Hào	Tìm hiểu về thuật toán Hoàn thiện slide báo cáo
4	Lâm Hoàng Khánh	Tìm hiểu về thuật toán Hoàn thiện Demo
5	Nguyễn Xuân Tính	Tìm hiểu về thuật toán Hoàn thiện Demo

DANH MỤC HÌNH ẢNH

CHƯƠNG 1: TỔNG QUAN VỀ GIẤU TIN

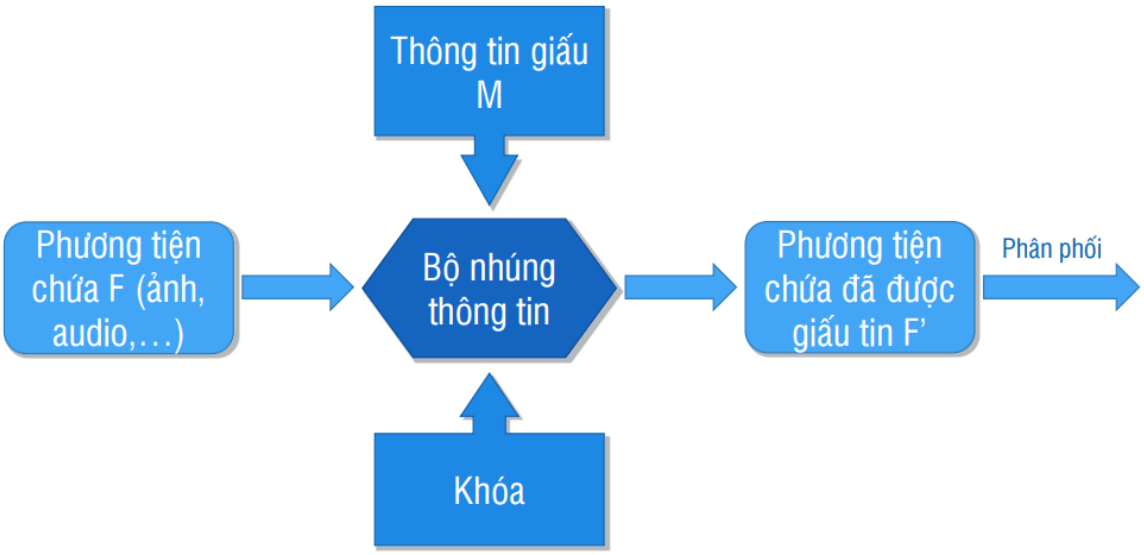
Giấu tin (Information hiding) là kỹ thuật nhúng (hay còn gọi là giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác.

Kỹ thuật giấu tin hay kỹ thuật giấu thư, kỹ thuật ẩn mã (steganography) là nghệ thuật và khoa học về việc viết và chuyển tải các thông điệp một cách bí mật, sao cho ngoại trừ người gửi và người nhận, không ai biết đến sự tồn tại của thông điệp, là một dạng của bảo mật bằng cách che giấu. Trong kỹ thuật giấu tin, thông thường thông điệp xuất hiện dưới một dạng khác trong quá trình truyền tải: hình ảnh, bài báo, danh sách mua hàng, bì thư, hoặc thông điệp ẩn có thể được viết bằng mực vô hình giữa các khoảng trống trong một lá thư bình thường.

1.1. Mô hình giấu tin

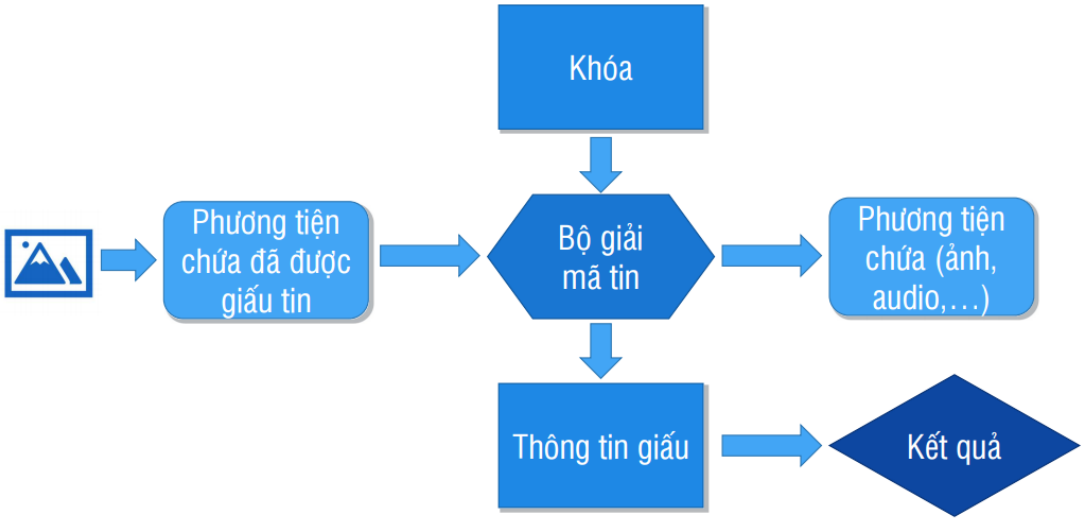
Để thực hiện giấu tin cần xây dựng được các thủ tục giấu tin. Các thủ tục này sẽ thực hiện nhúng thông tin cần giấu vào môi trường giấu tin. Các thủ tục giấu tin thường được thực hiện với một khóa giống như trong các hệ mật mã để tăng tính bảo mật.Thành phần cơ bản của kỹ thuật giấu thông tin gồm: Thuật toán giấu tin và bộ giải mã thông tin(tính đến cả khóa mật).

Thuật toán giấu tin được dùng để giấu thông tin vào một phương tiện chứa bằng cách sử dụng một khóa bí mật được dùng chung bởi người mã và người giải mã, việc giải mã thông tin chỉ có thể thực hiện được khi có khoá. Bộ giải mã thực hiện quá trình giải mã trên phương tiện chứa đã chứa dữ liệu và trả lại thông điệp ẩn trong đó. Phương tiện để giấu tin bao gồm các đối tượng môi trường như text, audio, video... thông tin giấu là một lượng thông tin mang một ý nghĩa nào đó như ảnh, logo, đoạn văn bản... tuỳ thuộc vào mục đích của người sử dụng. Thông tin sẽ được giấu vào trong phương tiện chứa nhờ một bộ nhúng. Bộ nhúng là những chương trình, triển khai các thuật toán để giấu tin và được thực hiện với một khoá bí mật giống như các hệ mật mã cổ điển. Sau khi giấu tin, ta thu được phương tiện chứa bản tin đã giấu và có thể phân phối sử dụng trên mạng.



Hình 1 Mô hình giấu tin

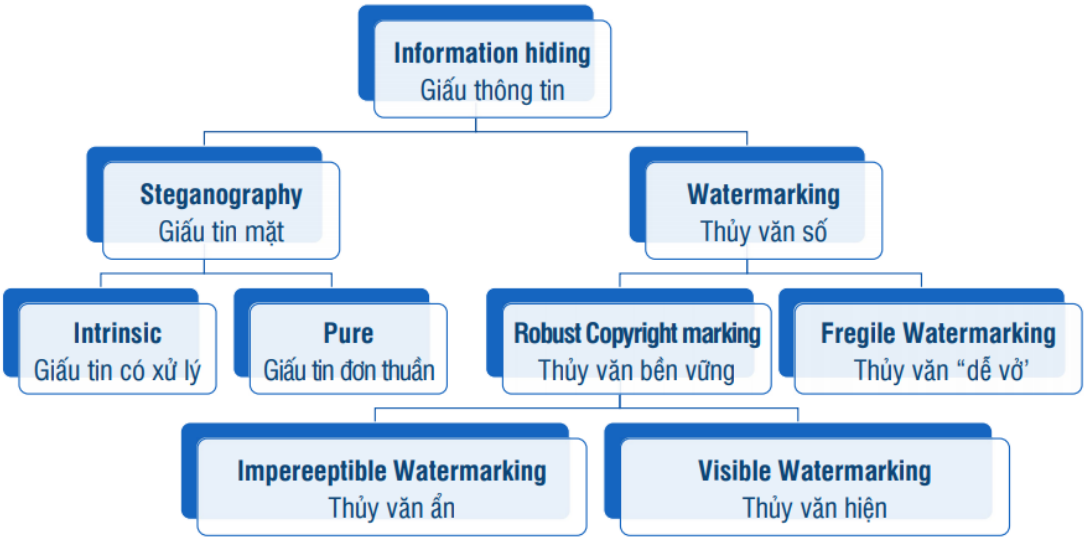
Quá trình giải mã được thực hiện thông qua một bộ giải mã tương ứng với bộ nhúng thông tin cùng với khoá của quá trình nhúng. Kết quả thu được gồm phương tiện chứa gốc và thông tin đã giấu. Bước tiếp theo thông tin giấu sẽ được xử lý kiểm định so sánh với thông tin giấu ban đầu.



Hình 2 Mô hình giải mã

1.2. Các kĩ thuật giấu tin

Các kĩ thuật giấu tin mới được chú ý phát triển mạnh trong khoảng 10 năm trở lại đây,nên việc phân loại còn chưa được thống nhất. Sơ đồ phân loại sau được đưa ra năm 1999 và được nhiều người chấp nhận:



Hình 3 Phân loại các mô hình giấu tin

Theo sơ đồ này, giấu tin được chia thành hai hướng chính là giấu tin mật (Steganography) và thủy vân số (Watermarking). Giấu tin mật quan tâm chủ yếu đến lượng tin có thể giấu,còn thủy vân số quan tâm đến tính bền vững của thông tin giấu. Trong từng hướng chính lại được chia ra các hướng nhỏ hơn,chẳng hạn với thủy vân số thì có thủy vân bền vững và thủy vân dễ vỡ. Thủy vân bền vững cần được bảo toàn được các thông tin thủy vân trước các tấn công như dịch chuyển ,cắt xén,xoay đối với ảnh. Ngược lại thủy vân dễ vỡ cần phải dễ bị phá hủy khi gặp các tấn công nói trên. Bảng bên dưới giúp chúng ta phân biệt giữa Steganography và Watermarking.

Steganography	Watermarking
- Tập trung vào việc giấu được càng nhiều thông tin càng tốt, ứng dụng trong truyền dữ liệu thông tin mật. - Cố gắng làm nhỏ nhất những ảnh hưởng đến chất lượng của đối tượng vỏ để không bị chú ý đến dữ liệu đã được giấu trong đó. - Thay đổi stego-object cũng làm cho dữ liệu dấu bị sai lệch (nhất là ứng dụng trong nhận thực thông tin)	- Không cần giấu nhiều thông tin, chỉ cần lượng thông tin nhỏ đặc trưng cho bản quyền của người sở hữu. - Trong trường hợp thuỷ vân nhìn thấy thì thuỷ vân sẽ hiện ra. - Thuỷ vân phải bền vững với mọi tấn công có chủ đích hoặc không có chủ đích vào sản phẩm.

1.2.1. Một số thuật toán giấu thông tin trong khối bit

1.2.1.1. Kỹ thuật giấu tin ngây thơ

Kỹ thuật giấu tin này khá đơn giản, bí mật của phương pháp chỉ là kích thước của khối ảnh. Bản chất của giấu tin được thực hiện trong kỹ thuật này là cách thức giấu thông tin theo quy ước chẵn lẻ.

Quá trình giấu tin:

Một số bước tiền xử lý sau đây được thực hiện trước khi thực hiện thuật toán:

- Chuyển file thông tin cần giấu sang dạng nhị phân bởi thuật toán sẽ giấu từng bit thông tin vào trong ảnh. Quá trình giải tin là biến đổi ngược, thu được file thông tin đã giấu.
- Đọc header của ảnh để lấy thông tin ảnh. Sau đó đọc toàn bộ dữ liệu ảnh vào một mảng hai chiều để sử dụng cho việc giấu tin.

Quá trình giải tin:

Khi nhận được ảnh có giấu tin, quá trình giải tin sẽ được thực hiện theo các bước sau đây:

- Gỡ header của ảnh để biết các thông tin về ảnh.
- Lấy phần dữ liệu ảnh vào mảng hai chiều.

1.2.1.2. Kỹ thuật giấu tin Chen – Pan – Tseng

- Ý tưởng

Thuật toán giấu thông tin trong ảnh đen trắng được Yu Yuan Chen, Hsiang Kuang Pan và Yu Chee Tseng, khoa Công Nghệ thông tin và Khoa học máy tính thuộc trường Đại học quốc gia Đài Loan đề nghị [18]. Trong phương pháp này, ngoài ma trận khoá (K) còn sử dụng thêm một ma trận trọng số (W) khi giấu thông tin. Thuật toán đảm bảo tốt an toàn và giấu được nhiều thông tin trong ảnh, bằng cách thay đổi nhiều nhất 2 bit mỗi khối ảnh. Nhược điểm của phương pháp này là chất lượng ảnh chưa cao, dễ bị phát hiện, chỉ nên áp dụng cho ảnh màu. Thuật toán cải tiến sẽ cải thiện rất nhiều chất lượng ảnh bằng kỹ thuật chọn hệ số phân bố bit đen trắng và số bit giấu tương đương.

- Thuật toán

- Dữ liệu vào:

F : là một ma trận ảnh gốc mà ta dùng để nhúng thông tin. F được chia thành các khối nhỏ Fi , mỗi ma trận điểm ảnh Fi có kích thước là (m x n), để đơn giản ta giả sử rằng F là bội của các Fi .

K : là một ma trận khoá ngẫu nhiên có kích thước (m x n).

W: là một ma trận trọng số ngẫu nhiên, cùng kích thước của K

r : Số lượng bit có thể giấu trong mỗi một khối ảnh (m x n).

B : Là lượng thông tin cần giấu , B = b1b2...bz (mỗi bi có r bit)

d : độ chênh lệch trọng số.

- Dữ liệu ra:

Các ma trận điểm ảnh Fi' được thay đổi từ Fi . Các Fi' cho ra ảnh F' đã có thông tin giấu.

Thuật toán sẽ thực hiện việc biến đổi mỗi Fi thành Fi' sao cho luôn thoả mãn điều kiện sau:

SUM((Fi ' K) W) b1b2...br (mod 2r).

Mỗi Fi bị biến đổi nhiều nhất là 2 bit. Quá trình biến đổi gồm 4 bước sau đây:

+ B1: Tính ma trận T=Fi K
+ B2: Tính tổng SUM(T W)
+ B3: Với ma trận T và với mọi w = 1,2,...,2r -1 ta xác định tập hợp Sw như sau:

Sw = {(x,y) | (W[x,y]=w T[x,y]=0) (W[x,y]=2r -w T[x,y]=1)}

Dễ nhận thấy Sw là tập hợp các toạ độ (x,y) của ma trận Fi[x,y]sao cho khi đảo bit Fi[x,y] thì Sum ở bước 2 tăng lên w. Thực vậy, ta có :

Trường hợp 1: Nếu W[x,y] = w và T[x,y] = 0

Khi đó đảo bit Fi[x,y] sẽ làm cho T[x,y] = 1, do đó Sum tăng lên w

Trường hợp 2: Nếu W[x,y] = 2r - w và T[x,y] = 1

Khi đó đảo bit Fi[x,y] sẽ làm T[x,y] = 0, do đó Sum sẽ giảm đi 2 r - w, tức là tăng lên w theo mod 2r .

Qui ước rằng với mọi w' w (mod 2r) trong đó w = 1, 2, ... , 2r -1, ta có: Sw' = Sw

+ B4: Kí hiệu d = (b1b2...bz) - SUM((Fi K) W) mod 2r .

Ta cần thực hiện việc đảo bit trên Fi để được Fi ' sao cho tổng Sum tính được ở B2 khi thay Fi bởi Fi ' sẽ tăng lên d.

Nếu d = 0, không cần thay đổi Fi

Nếu d 0 ta thực hiện các công việc sau:

1. Chọn h bất kỳ thuộc tập {0, 1, 2, ... , 2r -1 } sao cho Shd và S-(h-1)d

2. Chọn (x,y) bất kỳ thuộc Shd và đảo bit Fi[x,y] (nếu là 0 thì đổi thành 1 và ngược lại, 1 đổi thành 0).

3. Chọn (x,y) bất kỳ thuộc S-(h-1)d và đảo bit Fi[x,y] .

Rõ ràng, để tăng Sum lên d, ta có thể chọn 2 tập khác rỗng Shd và S-(h-1)d. Thật vậy, hai tập này chứa các vị trí bit trong khối Fi mà ta có thể đảo để tăng Sum lên hd và -(h-1)d một cách tương ứng, kết quả cuối cùng là Sum sẽ tăng lên hd + (-(h-1)d) = d.

Tương tự như các tập Sw khác ta cũng có thể coi tập So là tập chứa các vị trí mà khi đảo những bit có vị trí này trên Fi thì sẽ tăng Sum lên 0. Kết quả này cũng đạt được nếu ta không đảo bất kỳ bit nào trên Fi . Vì vậy ta có thể coi So là tập rỗng và khi nói "đảo 1 bit có vị trí thuộc tập So" có nghĩa là không cần làm gì cả.

1.3. Ứng dụng chính của giấu tin

- Bảo vệ bản quyền tác giả

Mục đích của thuỷ vân với bảo vệ bản quyền là gắn một "dấu hiệu" vào dữ liệu ảnh mà có thể xác định được người nắm giữ bản quyền. Và ta cũng có thể gắn thêm một dấu hiệu khác gọi là vân tay để xác định người dùng của sản phẩm. Dấu hiệu có 11 thể là một dãy số như mã hàng hoá quốc tế, một message hoặc một logo… Thuật ngữ thuỷ vân xuất phát từ phương thức đánh dấu giấy tờ với một logo từ thời xa xưa với mục đích tương tự. Do các Watermark có thể vừa không thể nhận thấy vừa không thể tách rời tác phẩm chứa nó nên chúng là giải pháp tốt hơn dòng chữ đối với việc nhận ra người sở hữu nếu người dùng tác phẩm được cung cấp bộ dò Watermark. Như vậy, nhúng thông tin của người giữ tác quyền của một tác phẩm như là một Watermark. Watermark không chỉ được dùng để chỉ ra thông tin tác quyền mà còn được dùng để chứng minh tác quyền.

- Điều khiển và ngăn chặn sao chép

Ngăn chặn những hành vi bất hợp pháp như sao chép dữ liệu mà không được phép, như vậy nếu có một ứng dụng kiểm soát sao chép ngăn chặn sẽ không cho tạo ra các

bản sao bất hợp pháp từ nội dung đã có bản quyền. Mã hóa cũng có thể dùng để cài đặt cho ứng dụng dạng này. Tài liệu được mã hóa với một khóa duy nhất, nếu không có khóa thì không dùng được.

- Chống giả mạo và gian lận

Một ứng dụng khác của thuỷ vân là xác thực ảnh và phát hiện giả mạo. Ảnh số ngày càng được sử dụng như các bằng chứng quan trọng trong điều tra của cảnh sát, bằng chứng trước pháp luật ngày nay, sự giả mạo có thể gây ra nhiều vấn đề nghiêm trọng. Các tác phẩm kỹ thuật số ngày nay đứng trước nguy cơ bị làm giả nhiều hơn, dễ dàng hơn và tinh vi hơn. Vấn đề là cần xác thực được tính hợp pháp của ảnh này. Thuỷ vân được sử dụng ở đây để xác định xem ảnh là nguyên bản hay đã chịu tác động của con người, bằng các ứng dụng xử lý ảnh. Thuỷ vân được dấu lúc đầu phải mang tính chất không bền vững, để bất kỳ sự thay đổi nhỏ nào tới ảnh cũng có thể làm hỏng thuỷ vân hoặc phát hiện được thay đổi đối với thuỷ vân này. Tuy vậy, thuỷ vân vẫn phải tồn tại với các phép biến đổi ảnh thông thường như chuyển đổi định dạng, lấy mẫu, nén…

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1. Sơ lược về file audio wave

Tệp WAV là định dạng âm thanh thô được tạo bởi Microsoft và IBM. Định dạng sử dụng các vùng chứa để lưu trữ dữ liệu âm thanh, số lượng theo dõi, tốc độ mẫu và tốc độ bit. Các tệp WAV là âm thanh lossless không nén và như vậy có thể chiếm khá nhiều dung lượng, đạt khoảng 10 MB mỗi phút với kích thước tệp tối đa là 4 GB.

Các định dạng tệp WAV sử dụng các vùng chứa để chứa âm thanh trong các đoạn dữ liệu thô và không nén được nén bằng cách sử dụng định dạng tệp trao đổi tài nguyên (RIFF). Đây là phương pháp phổ biến mà Windows sử dụng để lưu trữ các tệp âm thanh và video - như AVI- nhưng cũng có thể được sử dụng cho dữ liệu tùy ý.

Các tệp WAV thường sẽ lớn hơn nhiều so với các loại tệp âm thanh phổ biến khác, như MP3, do thực tế chúng thường không được nén (tuy nhiên, hỗ trợ nén). Do đó, chúng chủ yếu được sử dụng trong ngành công nghiệp ghi âm nhạc chuyên nghiệp để duy trì chất lượng âm thanh tối đa.

2.2. Giấu tin trong audio

Phương pháp mã hóa LSB là cách đơn giản nhất để nhúng thông tin vào trong dữ liệu audio. Phương pháp này sẽ thay thế bit ít quan trọng nhất, các bit được gọi là bit ít quan trọng khi ta thay đổi giá trị của bit đó từ 0 sang 1 hay từ 1 sang 0 thì sự thay đổi giá trị của mẫu dữ liệu không lớn và nó không gây ra sự khác biệt nào đối với hệ thống tri giác của con người (thường là bit cuối) của mỗi mẫu dữ liệu bằng bit thông tin giấu. Ví dụ mẫu 8 bit như sau:

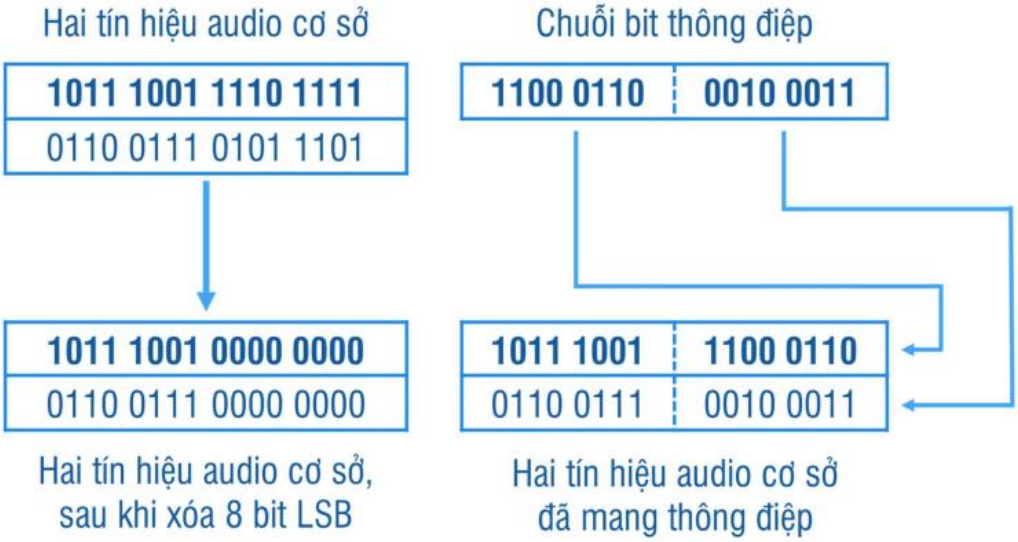
0	1	0	1	1	1	1	0

Sau khi giấu bit 1 sẽ như sau:

0	1	0	1	1	1	1	1

Ưu điểm của phương pháp này là dễ cài đặt và cho phép giấu dữ liệu nhiều. Để tăng độ bền vững của kỹ thuật giấu tin này chúng ta có thể tăng thêm dữ liệu giấu bằng cách tăng số lượng bit LSB dùng để giấu tin sao cho phù hợp nhất mà không

ảnh hưởng đến chất lượng âm thanh ban đầu. Tuy nhiên cách làm này cũng làm tăng nhiễu trên đối tượng chứa dẫn đến đối phương dễ phát hiện và thực hiện các tấn công.



Hình 4 Sơ đồ giấu tin trên 8 bit LSB của tín hiệu audio cơ sở

- **Thuật toán giấu tin:**

Đầu vào: Audio gốc A có độ dài tín hiệu L, chuỗi tin cần giấu M.

Đầu ra: Audio đã giấu tin.

Các bước thực hiện:

Bước 1: đọc audio vào A, dựa vào tần số lấy mẫu và các thông số liên quan đến cấu trúc lưu trữ của tệp audio ta được vector giá trị của tín hiệu mẫu lưu vào mảng một chiều để thực hiện giấu tin.(ví dụ, tần số lấy mẫu là 44100Hz thì tín hiệu audio có thể biểu diễn dưới dạng 16 bit, khi đó ta có thể giấu thông tin đến 8 bit có trọng số thấp).

Bước 2: thực hiện chuyển đổi chuỗi tin cần giấu M sang chuỗi bit nhị phân để có thể giấu vào audio, tính độ dài số bit thông điệp lưu vào L.

Bước 3: chọn giá trị k phù hợp nhất (tức là chọn số bit LSB của tín hiệu audio sẽ giấu tin).

Bước 4: dựa vào k được chọn ở bước 3, thực hiện giấu L (độ dài bit thông điệp) vào LSB của ba tín hiệu đầu tiên hoặc cuối cùng của tín hiệu audio để phục vụ tách tin.

Bước 5: dựa vào k đã chọn và độ dài L của thông điệp ta thực hiện chia chuỗi bit thông điệp thành các chuỗi con có độ dài k bit. Mỗi chuỗi con này sẽ được thay thế vào k bit LSB của L/k tín hiệu audio để có thể giấu đủ L bit thông điệp.

Bước 6: Lưu lại các tín hiệu audio vào tệp audio kết quả ta được audio đã giấu tin S.

- **Thuật toán tách tin:**

Đầu vào: Audio đã giấu tin S.

Đầu ra: Thông điệp đã giấu M.

Các bước thực hiện:

Bước 1: đọc audio vào S, dựa vào tần số lấy mẫu và các thông số liên quan đến cấu trúc lưu trữ của tệp audio ta được vector giá trị của tín hiệu mẫu lưu vào mảng một chiều để thực hiện tách tin.

Bước 2: cho biết giá trị k (số bit LSB đã giấu tin).

Bước 3: tách ra độ dài bit L đã giấu trên ba tín hiệu đầu tiên hoặc cuối cùng của tín hiệu audio.

Bước 4: thực hiện tách k bit LSB của L/k tín hiệu đã giấu tin ghép lại thành chuỗi bit, ta được chuỗi bit đã giấu.

Bước 5: Chuyển đổi chuỗi bit đã tách về dạng ban đầu ta được thông điệp cần tách.

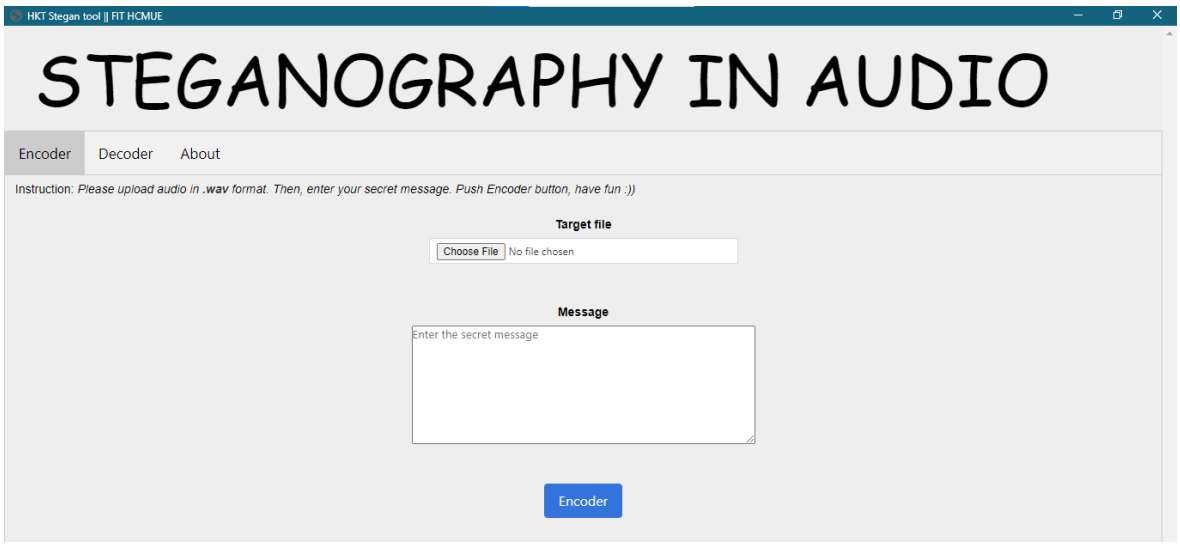
CHƯƠNG 3: ỨNG DỤNG GIẤU TIN TRONG FILE ÂM THANH

3.1. Môi trường cài đặt

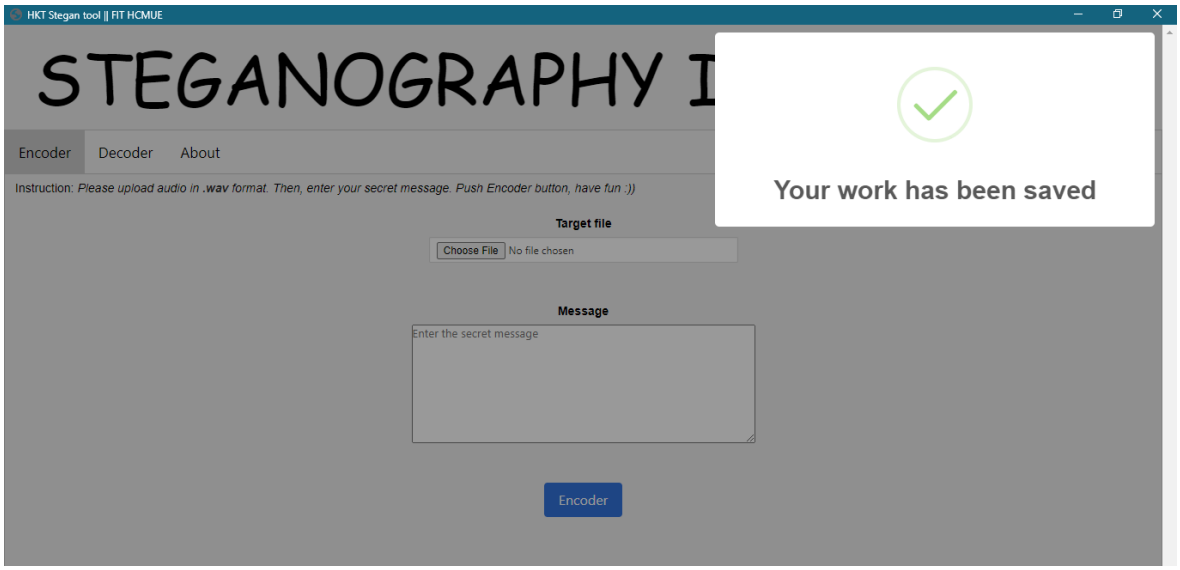
"ỨNG DỤNG GIẤU TIN TRONG FILE ÂM THANH" được xây dựng từ ngôn ngữ Python phiên bản 3.6. Bên cạnh đó, chúng em đã chọn thư viện **eel** để dễ dàng tạo giao diện cho website và **wave** chuyên xử lí file ".wav". Sau khi có đầy đủ thư viện nêu trên, người dùng chỉ cần gõ lệnh ở khung terminal để chạy file main.py. Một cửa sổ giao diện ứng dụng sẽ hiện lên và mọi thao tác với người dùng đều hiển thị trên giao diện này.

3.2. Giao diện ứng dụng

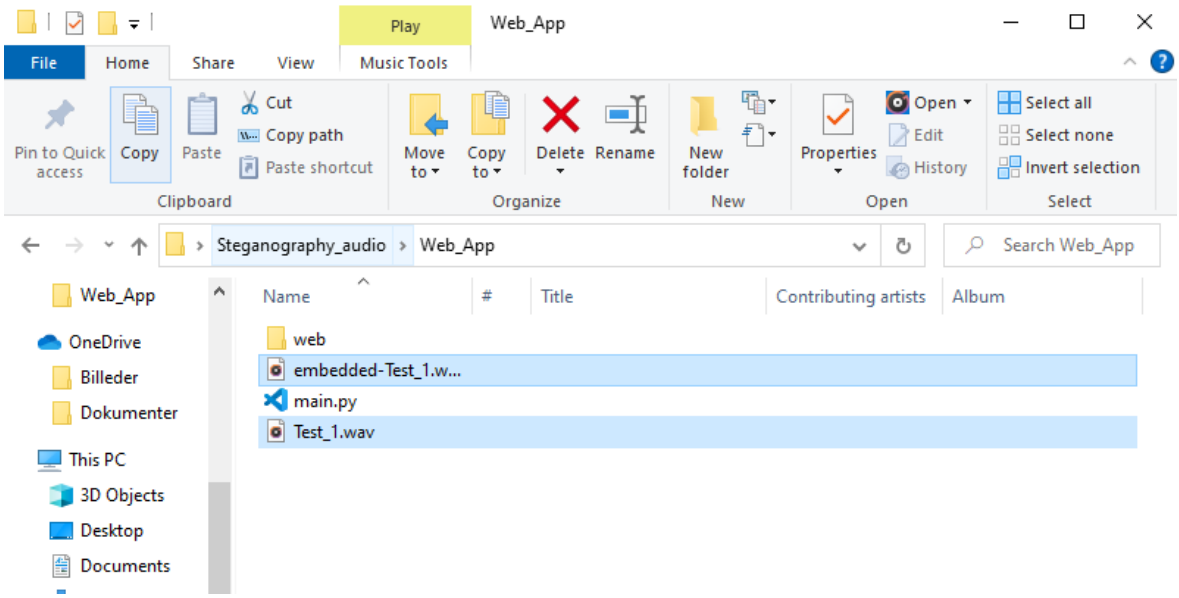
Sau đây là những ảnh giao diện chính của ứng dụng demo. Website gồm có 3 tabs: Encoder, Decoder và About. Màn hình Encoder có tác dụng giấu tin văn bản trong audio. Bắt đầu sử dụng, chương trình yêu cầu cần có file audio có định dạng **".wav"** và một đoạn văn bản chứa thông tin cần giữ bí mật (Hình 5). Bấm nút **Encoder** sau khi có thông tin đầy đủ theo yêu cầu và đồng thời chương trình sẽ hiện lên thông báo "Your work has been saved" (Hình 6). Khi đó một file mang tin mật đã được lưu lại với định dạng **"embedded-**Tên tệp âm thanh gốc**.wav"** ở thư mục cùng cấp với tệp âm thanh gốc (Hình 7).



Hình 5 Màn hình Encoder

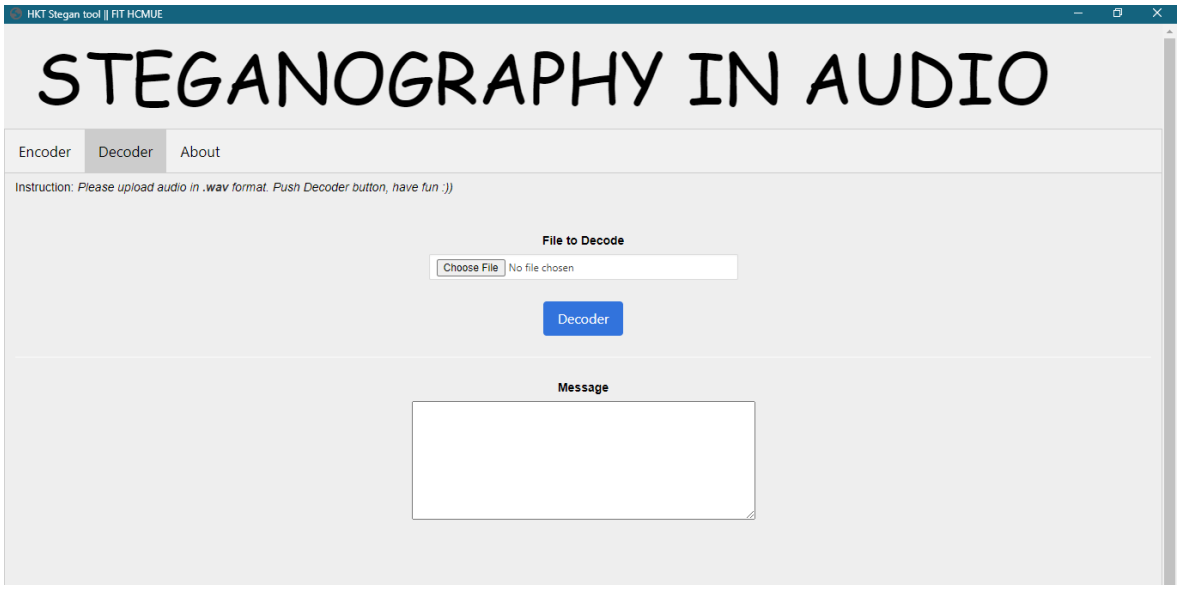


Hình 6 Thông báo khi đã giấu tin thành công

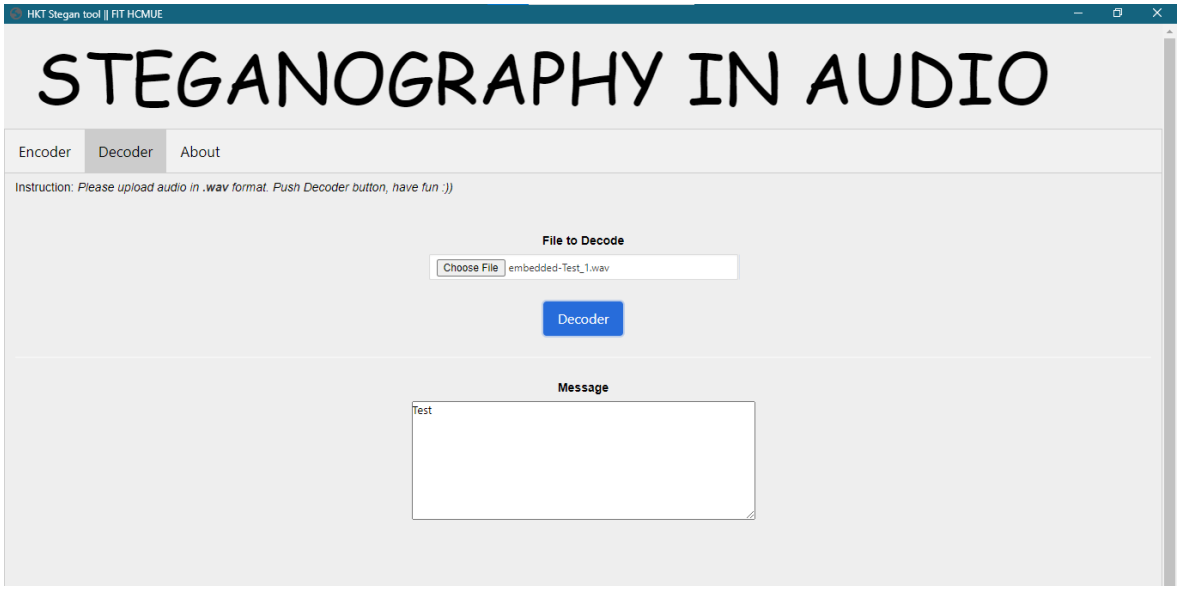


Hình 7 Vị trí lưu của tệp âm thanh đã được giấu tin

Màn hình Decoder có nhiệm vụ lấy thông tin từ file audio được tạo ra từ quá trình Encoder. Ta cần chuyển sang tab Decoder để thực hiện lấy tin.Với chức năng này, người cần lấy tin chỉ cần upload một tệp âm thanh có đuôi định dạng **".wav"**. Sau đó bấm nút Decoder (Hình 8). Mặc định khu vực Message ở màn hình Decoder sẽ không được chỉnh sửa để bảo toàn thông tin được tốt hơn. Kết quả thông tin được hiển thị như Hình 9.

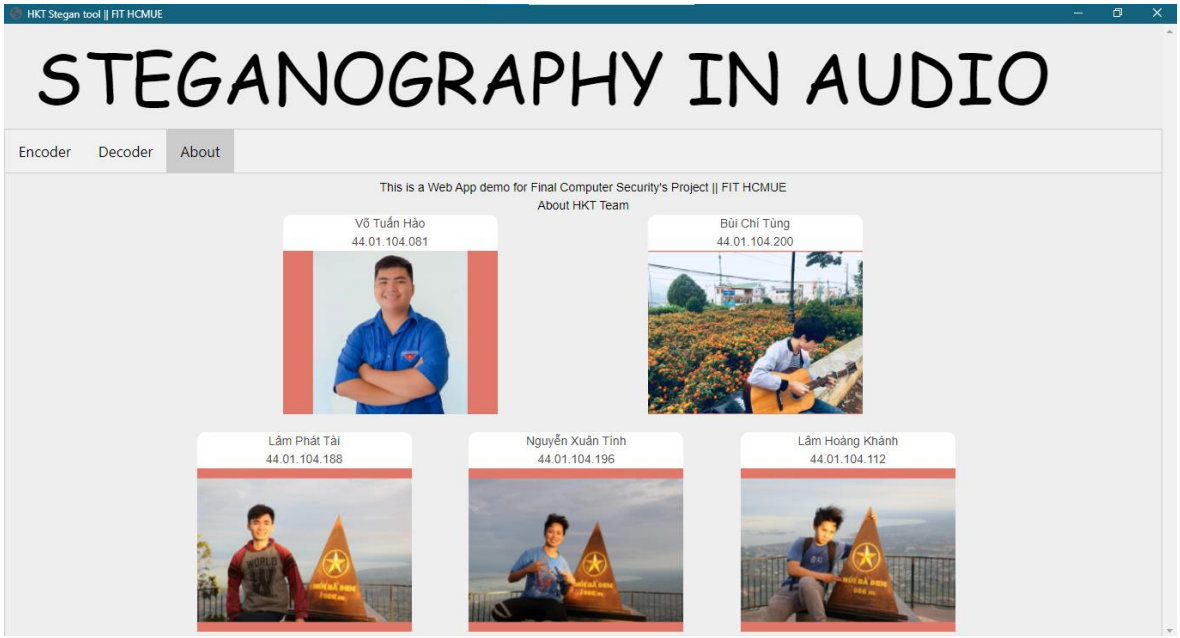


Hình 8 Màn hình Decoder



Hình 9 Kết quả lấy tin từ tệp âm thanh

Và cuối cùng là Tab hiển thị thông tin họ tên và mã số sinh viên của từng thành viên trong nhóm tác giả



Hình 10 Màn hình hiển thị thông tin thành viên nhóm HKT

CHƯƠNG 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Kỹ thuật giấu tin trong âm thanh số là một trong những hướng nghiên cứu chính của phương pháp giấu thông tin hiện nay và đã đạt được những kết quả khả quan.

Với đề tài "Giấu tin trong Audio bằng LSB" nhóm đã thành công trong việc xây dựng được một chương trình thực hiện tác vụ giấu tin. Tuy chương trình hoạt động khá đơn giản nhưng đã có thể đáp ứng được mục tiêu của nhóm đề ra là giấu một đoạn văn bản vào trong audio và từ đoạn audio đã được giấu tin có thể tách được thông tin đã giấu từ đoạn audio đó.

Hoàn thành đề tài lần này là một bước tiến cho nhóm trong việc hiểu rõ bản chất và tầm quan trọng của tác vụ giấu tin, qua đó nhóm nhận thấy "Bảo mật và An ninh mạng" đóng một vai trò to lớn trong ngành Công nghệ Thông tin, việc bảo vệ được thông tin của mình sẽ giúp chúng ta tránh được những việc không mong muốn trong quá trình học tập và làm việc như: bị rò rỉ thông tin hay bị người khác đánh cắp thông tin để phục vụ cho mục đích xấu ảnh hưởng đến cá nhân hay tổ chức của chúng ta.

TÀI LIỆU THAM KHẢO

[1] Roy, Sangita & Parida, Jyotirmayee & Singh, Avinash & Sairam, Ashok. (2012). Audio steganography using LSB encoding technique with increased capacity and bit error rate optimization. 372-376. 10.1145/2393216.2393279.

[2] Jayaram, & Ranganatha, & Anupama,. (2011). Information Hiding Using Audio Steganography - A Survey. The International journal of Multimedia & Its Applications. 3. 86-96. 10.5121/ijma.2011.3308.

[3] A. Binny and M. Koilakuntla, "Hiding Secret Information Using LSB Based Audio Steganography," 2014 International Conference on Soft Computing and Machine Intelligence, 2014, pp. 56-59, doi: 10.1109/ISCMI.2014.24.

[4] Darsana, R. & Vijayan, Asha. (2011). Audio Steganography Using Modified LSB and PVD. 10.1007/978-3-642-22543-7_2.