LỜI CẢM ƠN!

Trước hết, Em xin được bày tỏ lòng biết ơn sâu sắc tới TS.Hồ Thị Hương Thơm, người đã trực tiếp hướng dẫn, tận tình chỉ bảo em trong suốt quá trình làm đồ án tốt nghiệp.

Em cũng xin chân thành cảm ơn tất cả các thầy cô giáo trong khoa Công nghệ thông tin nói riêng và các thầy cô trong Trường ĐHDL Hải Phòng nói chung, những người đã nhiệt tình giảng dạy và trang bị đầy đủ kiến thức cho em trong thời gian em theo học tại trường.

Cuối cùng em xin cảm ơn gia đình, người thân và bạn bè đã động viên và tạo điều kiện giúp đỡ em trong suốt quá trình học tập và làm đồ án tốt nghiệp vừa qua.

Em xin chân thành cảm ơn!

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

DANH MỤC CHỮ VIẾT TẮT

LSB	Least Significant Bit	Bit ít quan trọng nhất
DCT	Discrete Consine Transform	Phép biến đổi cosin rời rạc
IMG	Image	Ảnh đen trắng img
PCX	Personal Computer Exchange	Ảnh xám PCX
GIF	Graphics Interchange Format	Định dạng ảnh đồ họa GIF
BMP	Bitmap	Ảnh không nén Bitmap
PNG	Portable Network Graphics	Ảnh PNG
JPEG	Joint Photographic Expert Group	Ảnh nén JPEG
GLCM	Gray level co-occurrence matrix	Ma trận mức xám

MỞ ĐẦU

Ngày nay, khi Internet ngày càng phát triển mạnh mẽ và dần trở thành môi trường thế giới ảo được sử dụng trên toàn cầu. Cùng với cuộc cách mạng thông tin kỹ thuật số đã đem lại những thay đổi sâu sắc trong xã hội và trong cuộc sống của chúng ta. Những thuận lợi mà thông tin kỹ thuật số mang lại cũng sinh ra những thách thức và cơ hội mới cho quá trình phát triển. Internet và mạng không dây đã trợ giúp cho việc chuyển phát một khối lượng thông tin rất lớn qua mạng giúp cho việc truyền thông và giao tiếp trở nên thuận lợi hơn. Tuy nhiên nó cũng làm tăng nguy cơ sử dụng trái phép, ăn cắp thông tin, xuyên tạc bất hợp pháp các thông tin được lưu chuyển trên mạng, đồng thời việc sử dụng một cách bình đẳng và an toàn các dữ liệu đa phương tiện cũng như cung cấp một cách kịp thời thông tin tới rất nhiều người dùng cuối và các thiết bị cuối cũng là một vấn đề quan trọng và còn nhiều thách thức. Hơn nữa sự phát triển của các phương tiện kỹ thuật số đã làm cho việc lưu trữ, sửa đổi và sao chép dữ liệu ngày càng đơn giản, từ đó việc bảo vệ bản quyền và chống xâm phạm trái phép các dữ liệu đa phương tiện (âm thanh, hình ảnh, tài liệu) cũng gặp nhiều khó khăn.

Một công nghệ mới được ra đời đã giải quyết phần nào một số khó khăn trên là giấu thông tin trong các nguồn đa phương tiện như các nguồn âm thanh, hình ảnh… Xét theo khía cạnh tổng quát thì giấu thông tin cũng là một hệ mật mã nhằm đảm bảo tính an toàn thông tin, những phương pháp này ưu điểm ở chỗ giảm được khả năng phát hiện ra sự tồn tại của thông tin trong các nguồn mạng. Không giống như mã hoá thông tin là để chống sự truy cập và sửa chữa một cách trái phép thông tin. Giấu và phát hiện thông tin là kỹ thuật còn tương đối mới và đang phát triển rất nhanh thu hút được sự quan tâm của cả giới khoa học và giới công nghiệp nhưng cũng còn rất nhiều thách thức.

Bản báo cáo này trình bày tổng quan về kỹ thuật giấu và phát hiện ảnh có giấu tin. Đồng thời trình bày một số kỹ thuật phát hiện thông tin giấu trên LSB của ảnh số, từ đó đưa ra các thực nghiệm và đánh giá cho việc phát hiện ảnh số có giấu tin được áp dụng.

Cấu trúc trình bày của đồ án bao gồm :

- Chương I: Tổng quan kỹ thuật giấu tin và phát hiện ảnh có giấu tin.
- Chương II: Kỹ thuật phát hiện ảnh có giấu tin trên LSB
- Chương III: Cài đặt và thực nghiệm.

CHƯƠNG 1. TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN VÀ PHÁT HIỆN ẢNH CÓ GIẤU TIN

1.1 TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN

1.1.1 Định nghĩa kỹ thuật giấu tin

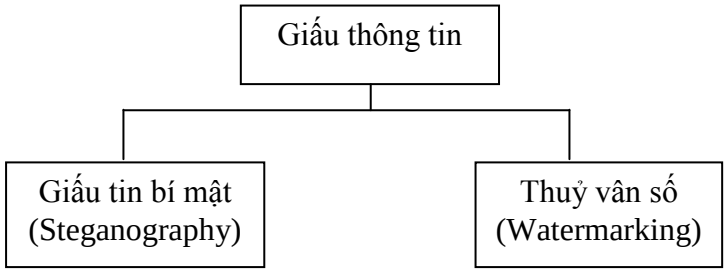
Giấu thông tin là một kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác (giấu thông tin chỉ mang tính quy ước không phải là một hành động cụ thể).

1.1.2 Mục đích của giấu tin

Có hai mục đích của giấu tin:

- Trao đổi thông tin mật.
- Bảo đảm an toàn và phát hiện xuyên tạc thông tin cho chính các đối tượng chứa dữ liệu giấu trong đó.

Có thể thấy 2 mục đích này hoàn toàn trái ngược nhau và dần phát triển thành 2 lĩnh vực với những yêu cầu và tính chất khác nhau.



Hình 1.1. *Hai lĩnh vực chính của kỹ thuật giấu thông tin*

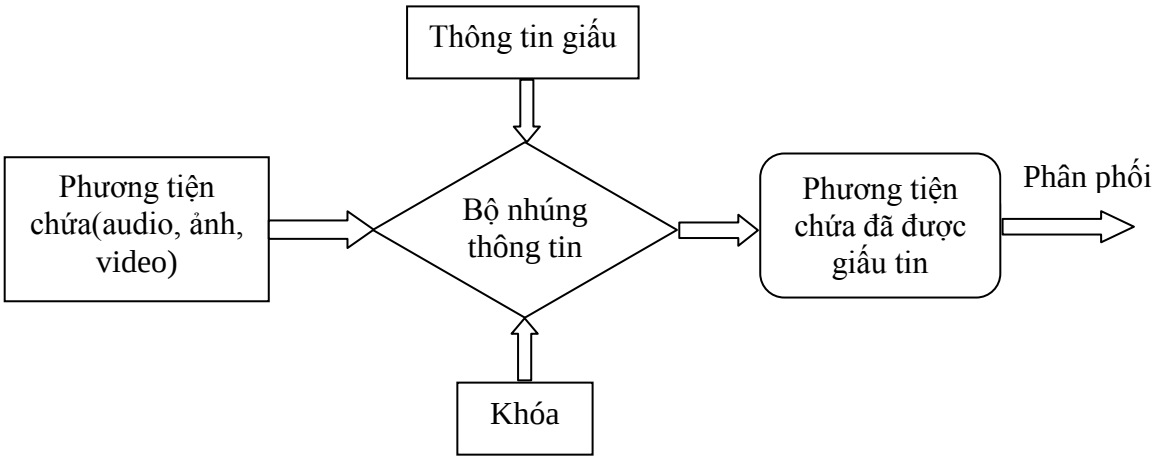
Kỹ thuật giấu thông tin bí mật (Steganography): với mục đích đảm bảo an toàn và bảo mật thông tin tập trung vào các kỹ thuật giấu tin để có thể giấu được nhiều thông tin nhất. Thông tin mật được giấu một cách vô hình trong một đối tượng khác sao cho người khác khó phát hiện được.

Kỹ thuật giấu thông tin theo kiểu đánh dấu – thủy vân (watermarking) với mục đích để bảo vệ bản quyền chính đối tượng dùng để chứa thông tin, thường tập

trung đảm bảo một số các yêu cầu như đảm bảo tính bền vững… Đây là ứng dụng cơ bản nhất của kỹ thuật thuỷ vân số.

1.1.3 Mô hình kỹ thuật giấu thông tin cơ bản

Giấu thông tin vào phương tiện chứa và tách lấy thông tin là 2 quá trình trái ngược nhau và có thể mô tả qua sơ đồ khối của hệ thống như hình 1.2:



Hình 1.2 *Lược đồ chung cho quá trình giấu tin*

- Thông tin cần giấu tuỳ theo mục đích của người sử dụng, nó có thể là thông tin mật (với các tin bí mật) hay các logo, hình ảnh bản quyền.

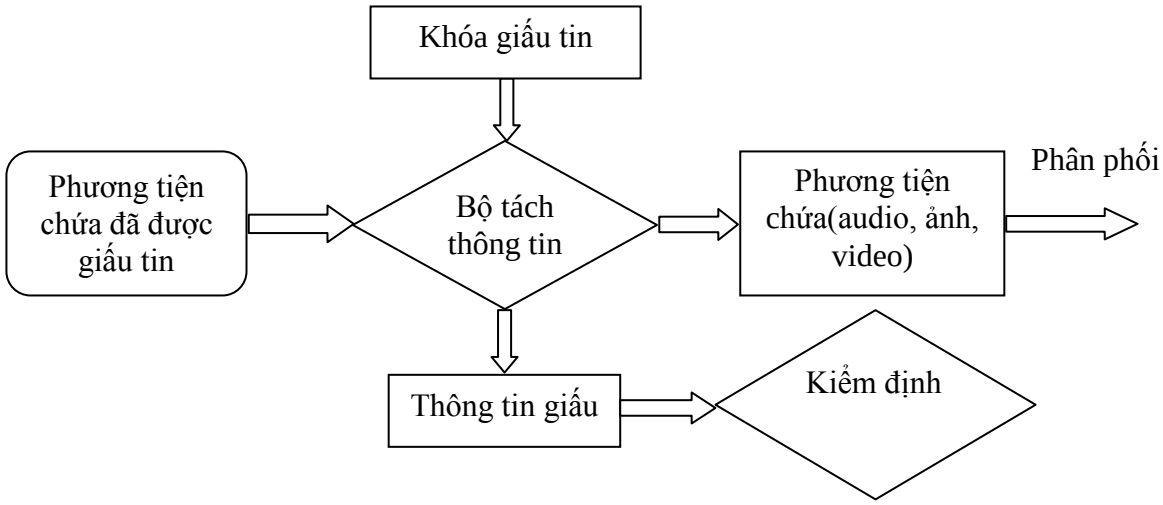
- Phương tiện chứa: các file ảnh, text, audio… là môi trường để nhúng tin.

Bộ nhúng thông tin: là những chương trình thực hiện việc giấu tin

Đầu ra: là các phương tiện chứa đã có tin giấu trong đó

Tách thông tin từ các phương tiện chứa diễn ra theo quy trình ngược lại với đầu ra là các thông tin đã được giấu vào phương tiện chứa. Phương tiện chứa sau khi tách lấy thông tin có thể được sử dụng, quản lý theo những yêu cầu khác nhau.

1.1.4 Mô hình kỹ thuật tách thông tin cơ bản



Hình 1.3 *Lược đồ chung cho quá trình tách thông tin*

Hình 1.3 chỉ ra các công việc giải mã thông tin đã giấu. Sau khi nhận được đối tượng phương tiện chứa có giấu thông 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 đã giấu sẽ được xử lý kiểm định so sánh với thông tin ban đầu.

1.1.5 Yêu cầu thiết yếu đối với một hệ thống giấu tin

Có 3 yêu cầu thiết yếu đối với một hệ thống giấu tin:

- Tính vô hình: là một trong 3 yêu cầu của bất kì 1 hệ giấu tin nào.
- Tính bền vững: là yêu cầu thứ 2 của một hệ giấu tin. Tính bền vững là nói đến khả năng chịu được các thao tác biến đổi nào đó trên phương tiện nhúng và các cuộc tấn công có chủ đích.
- Khả năng nhúng: là yêu cầu thứ 3 của một hệ giấu tin. Khả năng nhúng chính là số lượng thông tin nhúng được nhúng trong phương tiện chứa.

1.1.6 Môi trường giấu tin

a. Giấu tin trong ảnh

- Giấu tin trong ảnh hiện đang rất được quan tâm. Nó đóng vai trò hết sức quan trọng trong hầu hết các ứng dụng bảo vệ an toàn thông tin như: nhận thực thông tin, xác định xuyên tạc thông tin, bảo vệ bản quyền tác giả…
- Một đặc điểm của giấu thông tin trong ảnh nữa đó là thông tin được giấu một cách vô hình, nó như là cách truyền thông tin mật cho nhau mà người khác không thể biết được bởi sau khi giấu thông tin chất lượng ảnh gần như không thay đổi đặc biệt đối với ảnh màu hay ảnh xám.

b. Giấu tin trong audio

- Khác với kỹ thuật giấu thông tin trong ảnh: phụ thuộc vào hệ thống thị giác của con người – HSV (Human Vision System), kỹ thuật giấu thông tin trong audio lại phụ thuộc vào hệ thống thính giác HAS (Human Auditory System). Bởi vì tai con người rất kém trong việc phát hiện sự khác biệt giữa các giải tần và công suất, có nghĩa là các âm thanh to, cao tần có thể che giấu đi được các âm thanh nhỏ, thấp một cách dễ dàng.
- Yêu cầu cơ bản và quan trọng nhất của giấu tin trong audio là đảm bảo tính chất ẩn của thông tin được giấu đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu.

c. Giấu tin trong video

- Cũng giống như giấu thông tin trong ảnh hay trong audio, giấu tin trong video cũng được quan tâm và được phát triển mạnh mẽ cho nhiều ứng dụng như điều khiển truy cập thông tin, xác thực thông tin, bản quyền tác giả…
- Một phương pháp giấu tin trong video được đưa ra bởi Cox là phương pháp phân bố đều. Ý tưởng cơ bản của phương pháp là phân phối thông tin giấu dàn trải theo tần số của dữ liệu gốc.

d. Giấu thông tin trong văn bản dạng text

- Giấu tin trong văn bản dạng text khó thực hiện hơn do có ít các thông tin dư thừa, để làm được điều này người ta phải khéo léo khai thác các dư thừa tự nhiên của ngôn ngữ. Một cách khác là tận dụng các định dạng văn bản (mã hoá thông tin vào khoảng cách giữa các từ hay các dòng văn bản) => Kỹ thuật giấu tin đang được áp dụng cho nhiều loại đối tượng chứ không riêng dữ liệu đa phương tiện như ảnh, audio, video.

1.1.7 Một số đặc điểm của việc giấu tin trên ảnh

1.1.7.1 Tính vô hình của thông tin

Khái niệm này dựa trên đặc điểm của hệ thống thị giác của con người. Thông tin nhúng là không tri giác được nếu một người với thị giác bình thường không phân biệt được ảnh môi trường và ảnh kết quả (tức là không phân biệt được ảnh trược và sau khi giấu thông tin). Trong khi *image hiding (Steganography)*yêu cầu tính vô hình của thông tin ở mức độ cao thì *watermarking* lại chỉ yêu cầu ở một cấp độ nhất định. Chẳng hạn như người ta áp dụng watermarking cho việc gắn một biểu tượng mờ vào một chương trình truyền hình để bảo vệ bản quyền.

1.1.7.2 Khả năng nhúng tin

Lượng thông tin giấu so với kích thước ảnh môi trường cũng là một vấn đề cần quan tâm trong một thuật toán giấu tin. Rõ ràng là có thể chỉ giấu 1 bit thông tin vào mỗi ảnh mà không cần lo lắng về độ nhiễu của ảnh nhưng như vậy sẽ rất kém hiệu quả khi mà thông tin giấu có kích thước bằng Kb. Các thuật toán đều cố gắng đạt được mục đích làm thế nào giấu được nhiều thông tin nhất mà không gây ra nhiễu đáng kể.

1.1.7.3 Tính bảo mật

Thuật toán nhúng tin được coi là có tính bảo mật nếu thông tin được nhúng không bị tìm ra khi bị tấn công một cách có chủ đích trên cơ sở có hiểu biết đầy đủ về thuật toán nhúng tin và có bộ giải mã (trừ khóa bí mật), hơn nữa còn có được ảnh có mang thông tin (ảnh kết quả). Đây là một yêu cầu rất quan trọng đối với ảnh *image hiding.*

1.1.7.4 Ảnh môi trường đối với quá trình giải mã

Yêu cầu cuối cùng là thuật toán phải cho phép lấy lại được những thông tin đã giấu trong ảnh mà không có ảnh gốc. Điều này là một thuận lợi khi ảnh môi trường là duy nhất nhưng lại làm giới hạn khả năng ứng dụng của kỹ thuật giấu tin.

1.2 TỔNG QUAN VỀ KỸ THUẬT PHÁT HIỆN ẢNH CÓ GIẤU TIN

1.2.1 Khái niệm

Steganalysis là kỹ thuật phát hiện sự tồn tại của thông tin ẩn giấu trong nguồn đa phương tiện(multimedia). Giống như thám mã, mục đích của Steganalysis là phát hiện ra ảnh có mang thông tin mật và phá vỡ tính bí mật của vật mang tin ẩn.

Mục đích của kỹ thuật phát hiện là để phân loại một ảnh số bất kỳ có phải là ảnh gốc (cover image) hay ảnh có giấu tin (đã giấu tin image) hay không, để từ đó có thể đưa ra bước xử lý tiếp theo.

1.2.2 Phân tích ảnh giấu tin thường dựa vào các yếu tố

- Phân tích dựa vào các đối tượng đã mang tin.

- Phân tích bằng so sánh đặc trưng: So sánh vật mang tin chưa được giấu tin với vật mang tin đã được giấu tin, đưa ra sự khác biệt giữa chúng.

- Phân tích dựa vào thông tin mật cần giấu để dò tìm.

- Phân tích dựa vào các thuật toán giấu tin và các đối tượng giấu đã biết: Kiểu phân tích này phải quyết định các đặc trưng của đối tượng giấu tin, chỉ ra công cụ giấu tin (thuật toán) đã sử dụng.

- Phân tích dựa vào thuật toán giấu tin, đối tượng gốc và đối tượng sau khi giấu tin.

1.2.3 Các phương pháp phân tích ảnh có giấu tin

- Phân tích trực quan: Thường dựa vào quan sát hoặc dùng biểu đồ tần suất (histogram) giữa ảnh gốc và ảnh chưa giấu tin để phát hiện ra sự khác biệt giữa hai ảnh căn cứ đưa ra vấn đề nghi vấn. Với phương pháp phân tích này thường khó phát hiện với ảnh có độ nhiễu cao và kích cỡ lớn.

- Phân tích theo dạng ảnh: Phương pháp này thường dựa vào các dạng ảnh bitmap hay là ảnh nén để đoán nhận kỹ thuật giấu hay sử dụng như các ảnh bitmap thường hay sử dụng giấu trên miền LSB, ảnh nén thường sử dụng kỹ thuật giấu trên các hệ số biến đổi như DCT, DWT, DFT.

- Phân tích theo thống kê: Đây là phương pháp sử dụng các lý thuyết thống kê và thống kê toán sau khi đã xác định được nghi vấn đặc trưng. Phương pháp này thường đưa ra độ tin cậy cao hơn và đặc biệt là cho tập ảnh lớn.

1.3 MỘT SỐ ẢNH ĐỊNH DẠNG BITMAP PHỔ BIẾN

1.3.1 Cấu trúc ảnh Bitmap

Ảnh BMP (Bitmap) được phát triển bởi Microsoft Corporation, được lưu trữ dưới dạng độc lập thiết bị cho phép Windows hiển thị dữ liệu không phụ thuộc vào khung chỉ định màu trên bất kì phần cứng nào. Tên file mở rộng mặc định của một file ảnh Bitmap là ".BMP". Ảnh BMP được sử dụng trên Microsoft Windows và các ứng dụng chạy trên Windows từ version 3.0 trở lên.

Mỗi file ảnh Bitmap gồm 3 phần như bảng 1.1:

Bảng 1.1 *Cấu trúc ảnh BitMap*

Bitmap Header (54 byte)
Color Palette
Bitmap Data

1.3.1.1 Bitmap Header

Thành phần bitcount (Bảng 1.2) của cấu trúc Bitmap Header cho biết số bit dành cho mỗi điểm ảnh và số lượng màu lớn nhất của ảnh. Bitcount có thể nhận các giá trị sau:

- 1: Bitmap là ảnh đen trắng, mỗi bit biểu diễn 1 điểm ảnh. Nếu bit mang giá tri "0" thì điểm ảnh là điểm đen, nếu bit mang giá trị "1" thì điểm ảnh là điểm trắng.

- 4: Bitmap là ảnh 16 màu, mỗi điểm ảnh được biểu diễn bằng 4 bit.
- 8: Bitmap là ảnh 256 màu, mỗi điểm ảnh được biểu diễn bằng 8 bit.
- 16: Bitmap là ảnh High Color, mỗi dãy 2 byte liên tiếp trong Bitmap biểu diễn cường độ tương đối của màu đỏ, xanh lá cây và xanh lơ (RGB) của điểm ảnh.
- 24: Bitmap là ảnh True Color, mỗi dãy 3 byte liên tiếp trong Bitmap biểu diễn cường độ tương đối của màu đỏ, xanh lá cây và xanh lơ (RGB) của điểm ảnh.

Thành phần Color Used của cấu trúc Bitmap Header xác định số lượng màu của Palete thực sự được sử dụng để hiển thị Bitmap. Nếu thành phần này được đặt là 0, Bitmap sử dụng số màu lớn nhất tương ứng với giá trị của bitcount.

Bảng 1.2 *Thông tin về Bitmap Header*

Byte thứ	**Ý nghĩa**	**Giá trị**
1-2	Nhận dạng file	'BM' hay 19778
3-6	Kích thước file	Kiểu long trong Turbo C
7-10	Dự trữ	Thường mang giá trị 0
11-14	Byte bắt đầu vùng dữ liệu	Offset của byte bắt đầu vùng dữ liệu
15-18	Số byte cho vùng thông tin	4 byte
19-22	Chiều rộng ảnh BMP	Tính bằng pixel
23-26	Chiều cao ảnh BMP	Tính bằng pixel
27-28	Số Planes màu	Cố định là 1
29-30	Số bit cho 1 pixel (bitcount)	Có thể là: 1,4,8,16,24 tùy theo loại ảnh
31-34	Kiểu nén dữ liệu	0: Không nén

		1: Nén runlength 8bits/pixel 2: Nén runlength 4bits/pixel
35-38	Kích thước ảnh	Tính bằng byte
39-42	Độ phân giải ngang	Tính bằng pixel / metter
43-46	Độ phân giải dọc	Tính bằng pixel / metter
47-50	Số màu sử dụng trong ảnh	
51-54	Số màu được sử dụng khi hiển thị ảnh (Color Used)	

1.3.1.2 Palette màu

Bảng màu của ảnh. Chỉ những ảnh nhỏ hơn hoặc bằng 8 bit mới có bảng màu.

Bảng 1.3 *Bảng màu của ảnh BITMAP*

Địa chỉ (Offset)	**Tên**	**Ý nghĩa**
0	RgbBlue	Giá trị cho màu xanh blue
1	RgbGreen	Giá trị cho màu xanh Green
2	RgbRed	Giá trị cho màu đỏ
3	RgbReserved	Dự trữ

1.3.1.3 Bitmap data

Phần này nằm ngay sau phần Palete màu của ảnh BMP. Đây là phần chứa giá trị màu của điểm ảnh trong ảnh BMP. Các dòng ảnh được lưu từ dưới lên trên, các điểm ảnh được lưu trữ từ trái sang phải. Giá trị của mỗi điểm ảnh là một chỉ số trỏ tới phần tử màu tương ứng trong Palete màu.

1.3.2 Cấu trúc ảnh PNG

1.3.2.1 Lịch sử và phát triển

Động cơ thúc đẩy cho việc tạo ra định dạng PNG bắt đầu vào khoảng đầu năm 1995, sau khi Unisys công bố họ sẽ áp dụng bằng sáng chế vào thuật toán nén dữ liệu LZW- được sử dụng trong định dạng GIF. Thuật toán được bảo vệ bởi bằng công nhận độc quyền sáng tạo ở Mỹ và tất cả các nước trên thế giới. Tuy nhiên, cũng đã có một số vấn đề với định dạng GIF khi cần có một số thay đổi nhất định trên hình ảnh, giới hạn của nó là 256 màu trong thời điểm máy tính có khả năng hiển thị nhiều hơn 256 màu đang trở nên phổ biến. Mặc dù định dạng GIF có thể thể hiện các hình ảnh động, song PNG vẫn được quyết định là định dạng hình ảnh đơn (chỉ có một hình duy nhất). Một người "anh em" của nó là MNG đã được tạo ra để giải quyết vấn đề ảnh động. PNG lại tăng thêm sự phổ biến của nó vào tháng 8 năm 1999, sau khi hãng Unisys huỷ bỏ giấy phép của họ đối với các lập trình viên phần mềm miễn phí, và phi thương mại.

- Phiên bản 1.0 của đặc tả PNG được phát hành vào ngày 1 tháng 7 năm 1996, và sau đó xuất hiện với tư cách RFC 2083. Nó được tổ chức W3C khuyến nghị vào ngày 1 tháng 10 năm 1996.
- Phiên bản 1.1, với một số thay đổi nhỏ và thêm vào 3 thành phần mới, được phát hành vào ngày 31 tháng 12 năm 1998.
- Phiên bản 1.2, thêm vào một thành phần mở rộng, được phát hành vào ngày 11 tháng 8 năm 1999.
- PNG giờ đây là một chuẩn quốc tế (ISO/IEC 15948:2003), và cũng được công bố như một khuyến nghị của W3C vào ngày 10 tháng 11 năm 2003. Phiên bản hiện tại của PNG chỉ khác chút ít so với phiên bản 1.2 và không có thêm thành phần mới nào.

1.3.2.2 Thông tin kỹ thuật

a. Phần đầu của tập tin

Một tập tin PNG bao gồm 8-byte kí hiệu (89 50 4E 47 0D 0A 1A) được viết trong hệ thống có cơ số 16, chứa các chữ "PNG" và hai dấu xuống dòng, ở giữa là

sắp xếp theo số lượng của các thành phần, mỗi thành phần đều chứa thông tin về hình ảnh. Cấu trúc dựa trên các thành phần được thiết kế cho phép định dạng PNG có thể tương thích với các phiên bản cũ khi sử dụng.

b. Các "thành phần" trong tập tin

PNG là cấu trúc như một chuỗi các thành phần, mỗi thành phần chứa kích thước, kiểu, dữ liệu, và mã sửa lỗi CRC ngay trong nó.

Chuỗi được gán tên bằng 4 chữ cái phân biệt chữ hoa chữ thường. Sự phân biệt này giúp bộ giải mã phát hiện bản chất của chuỗi khi nó không nhận dạng được.

Với chữ cái đầu, viết hoa thể hiện chuỗi này là thiết yếu, nếu không thì ít cần thiết hơn (ancillary). Chuỗi thiết yếu chứa thông tin cần thiết để đọc được tệp và nếu bộ giải mã không nhận dạng được chuỗi thiết yếu, việc đọc tệp phải được hủy.

c. Thành phần cơ bản

Một bộ giải mã (decoder) phải có thể thông dịch để đọc và hiển thị một tệp PNG.

- IHDR phải là thành phần đầu tiên, nó chứa đựng header
- PLTE chứa đựng bảng màu (danh sách các màu)
- IDAT chứa đựng ảnh. Ảnh này có thể được chia nhỏ chứa trong nhiều phần IDAT.Điều này làm tăng kích cỡ của tệp lên một ít nhưng nó làm cho việc phát sinh ảnh PNG mượt hơn (streaming manner).
- IEND đánh dấu điểm kết thúc của ảnh.

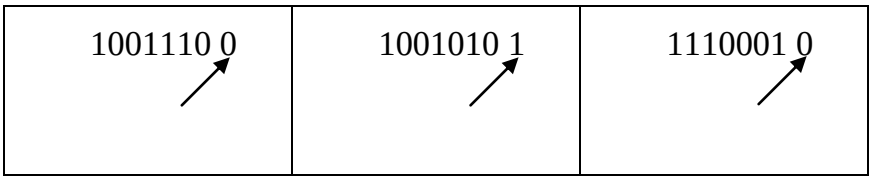
CHƯƠNG 2: KỸ THUẬT PHÁT HIỆN ẢNH CÓ GIẤU TIN TRÊN LSB

2.1 KỸ THUẬT GIẤU TIN TRÊN LSB

2.1.1 Khái niệm bit có trọng số thấp (LSB – least significant bit)

Bit có trọng số thấp là bit có ảnh hưởng ít nhất tới việc quyết định tới màu của mỗi điểm ảnh, vì vậy khi ta thay đổi bit ít quan trọng của một điểm ảnh thì màu của mỗi điểm ảnh mới sẽ tương đối gần với điểm ảnh cũ. Như vậy kỹ thuật tách bit trong xử lý ảnh được sử dụng rất nhiều trong quy trình giấu tin. Việc xác định LSB của mỗi điểm ảnh trong một bức ảnh phụ thuộc vào định dạng của ảnh và số bit màu dành cho mỗi điểm của ảnh đó. Ví dụ đối với ảnh 16 bit thì 15 bit là biểu diễn 3 màu RGB của điểm ảnh còn bit cuối cùng không dùng đến thì ra sẽ tách bit này ra ở mỗi điểm ảnh để giấu tin, hoặc với ảnh 256 màu thì bit cuối cùng trong 8 bit biểu diễn một điểm ảnh được coi là bit ít quan trọng nhất…

Ví dụ: Tách bit cuối cùng trong 8 bit biểu diễn mỗi điểm ảnh của ảnh 256 màu



Hình 2.1*: Mỗi điểm ảnh biểu diễn bởi 8 bit, bit cuối cùng được coi là bit ít quan trọng nhất tức là bit bên phải nhất*

Trong phép tách này ta coi bit cuối cùng là bit ít quan trọng nhất, thay đổi giá trị của bit này thì sẽ thay đổi giá trị của điểm ảnh lên hoặc xuống đúng một đơn vị, ví dụ như giá trị điểm ảnh là 234 thì khi thay đổi bit cuối cùng nó có thể mang giá trị mới là 235 nếu đổi bit cuối cùng từ 0 thành 1. Với sự thay đổi nhỏ đó ta hi vọng là cấp độ màu của điểm ảnh sẽ không bị thay đổi nhiều

2.1.2 Thuật toán giấu thông tin mật trên LSB theo tỷ lệ

2.1.2.1 Ý tưởng thuật toán

+ Cho tỷ lệ p% (so với kích cỡ của ảnh) thông tin mật cần giấu, tạo một ma trận ngẫu nhiên các bit nhị phân có kích thước bằng p% ảnh cần giấu.

+ Thực hiện thay thế các bit thông tin mật trong ma trận ngẫu nhiên vào các bit có giá trị thấp (LSB) của ảnh cho đến khi bit thông tin mật trong ma trận không còn nữa thì ngừng.
+ Ảnh thu được là ảnh có giấu p% thông tin của ảnh vào tất cả các bit LSB của ảnh lần lượt từ trái qua phải, từ trên xuống dưới.

2.1.2.2 Thuật toán giấu

Đầu vào: Ảnh cover và tỷ lệ p% thông tin mật cần nhúng.

Đầu ra: Ảnh có giấu tin.

Các bước thực hiện :

- Bước 1: Chuyển dữ liệu ảnh sang mảng 2 chiều M*N
- Bước 2: Tính kích thước ma trận ngẫu nhiên cần tạo ra:

$$L=p*M*N/100$$

- Bước 3: Tạo một ma trận các bit nhị phân ngẫu nhiên có số hàng M và số cột

$$R=L/M$$

- Bước 4: Thay thế lần lượt các bit thông tin mật trong ma trận ngẫu nhiên vào các bit có giá trị thấp (LSB) của ảnh theo quy tắc từ trái sang phải từ trên xuống cho đến khi các bit thông tin mật trong ma trận ngẫu nhiên được giấu hết thì dừng.

2.2 KỸ THUẬT PHÁT HIỆN ẢNH GIẤU TIN TRÊN LSB

Đây là kỹ thuật phát hiện ảnh có giấu tin trên LSB sử dụng ma trận mức xám để đánh giá đặc trưng ảnh trước và sau khi giấu tin. Phương pháp này được đưa ra bởi nhóm tác giả: Fangjun Huang, Bin Li, Jiwu Huang thuộc phòng bảo mật thông tin, khoa điện tử viễn thông, trường đại học Sun Yat-Sen, Quảng Châu, Quảng Đông, Trung Quốc.

2.2.1 Tổng quan về thuật toán

Theo ý kiến của một số chuyên gia giấu tin, ảnh xám không nén là ảnh gốc an toàn nhất cho việc giấu tin. Trong phương pháp này, chúng ta chỉ xem xét ảnh xám không nén. Giả sử một ảnh xám kích cỡ M x N, I(x,y) là một mảng gồm 8 bit từ $I_0 \sim I_7$, khác nhau từ tầng bit 0 trọng số thấp nhất cho đến tầng bit 7

trọng số cao nhất. Phương pháp giấu trên LSB chủ yếu ảnh hưởng đến các bit trọng số thấp.

Sau đây chúng ta xét hai tầng bit có trọng số thấp nhất (I_0, I_1):

$$A(x,y)= I_0(x,y) + I_1 (x,y)*2 \ (1\leq x\leq M, 1\leq y \leq N)$$

Khi đó miền giá trị của A chỉ có 4 mức xám đó là 0, 1, 2 và 3.

Chia A thành các ma trận con (ảnh con) kích cỡ 3x3 có nạp chồng. Mỗi ma trận con này đếm số lượng các mức xám trong ảnh nhỏ 3 × 3, từ đó có thể phân các ma trận con vào bốn tập sau:

- T_1: Chỉ gồm 1 mức xám. Nghĩa là, tất cả các điểm ảnh trong ma trận con này có cùng một giá trị.
- T_2: Bao gồm hai mức độ màu xám. Nghĩa là, tất cả ma trận con này có hai cấp độ màu xám.
- T_3: Bao gồm ba mức xám. Nghĩa là, tất cả các ma trận con này có ba mức độ màu xám.
- T_4: Bao gồm bốn mức độ màu xám. Nghĩa là, tất cả các ma trận con này có bốn cấp độ màu xám.

Để phân ảnh gốc và ảnh giấu tin dựa trên ý tưởng sau đây. Trong quá trình nhúng thông tin, xác suất những ma trận con thay đổi từ T_1 đến T_i ($2\leq i\leq 4$) là nhiều hơn so với xác suất mà những ảnh nhỏ thay đổi từ T_i ($2\leq i\leq 4$) đến T_1.

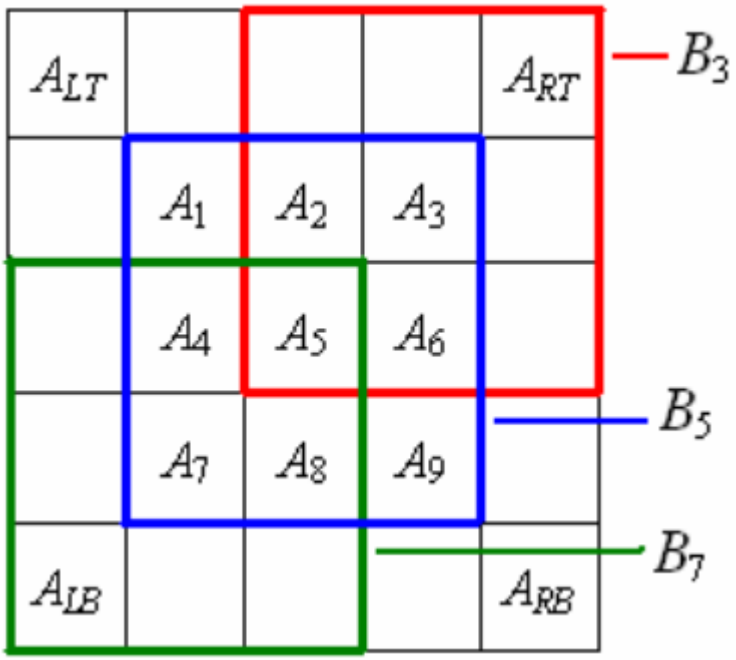
Ví dụ, cho một ma trận con thuộc T_1, thì bất kỳ một điểm ảnh nào bị thay đổi (khi giấu tin), xác suất mà nó thuộc T_i ($2\leq i\leq 4$) là 100%. Ngược lại, đối với các ảnh nhỏ thuộc T_i ($2\leq i\leq 4$) sau khi giấu tin, xác suất mà ảnh nhỏ thuộc T_1 sẽ ít hơn nhiều so với 100%. Vì vậy, chúng ta có thể kết luận rằng $|T_1|$ sẽ giảm sau khi nhúng ($|T_1|$ biểu thị số lượng của các thành phần thuộc T_1).

Tuy nhiên, để xác định một ngưỡng cho $|T_1|$ khi phân loại ảnh gốc và ảnh có giấu tin là rất khó khăn. Do có nhiều loại ảnh khác nhau, giá trị của $|T_1|$ phân tán trong một phạm vi rất rộng.

Trong bài báo [3] nhóm tác giả đã có phát hiện một phương pháp cho phép phân loại hình ảnh gốc và ảnh đã giấu tin một cách tin cậy. Giả sử $|T_1^C|$ là số của các ảnh nhỏ thuộc T_1 của ảnh gốc $I_C(x,y)$ và $|T_1^S|$ là số của các ảnh nhỏ thuộc T_1 của ảnh đã giấu tin tương ứng $I_S(x,y)$. Nhúng một chuỗi ngẫu nhiên thông tin vào ảnh gốc và ảnh đã giấu tin bằng kỹ thuật giấu trên LSB, chúng ta được $|T_1^{C*}|$ và $|T_1^{S*}|$. Tỷ lệ thay đổi được biểu thức sau:

$$k_c = \frac{\left|T_1^C\right| - \left|T_1^{C*}\right|}{\left|T_1^C\right|} \quad \text{và} \quad k_s = \frac{\left|T_1^S\right| - \left|T_1^{S*}\right|}{\left|T_1^S\right|}$$

Lưu ý: $k_C > k_S$ thường đúng nếu hình ảnh đã giấu tin chứa một số lượng lớn các dữ liệu ẩn.



Hình 2.2 Thể hiện sự nạp chồng của các ảnh con

Giả sử ta có một ảnh kích cỡ 5 x 5, tách ra miền bit có trọng số thấp nhất thứ 0 và thứ 1 ta được A, chia A thành các ảnh con (ma trận điểm ảnh) nạp chồng ta được 9 ảnh nhỏ kích cỡ 3x3 (*hình 2.2*), A_1 ~ A9 là các điểm ảnh trung tâm thuộc 9 ma trận con này. Để đơn giản, ta chỉ xét ba ma trận con B_3, B_5, B_7 được đánh nhãn tương ứng. Theo các thí nghiệm khác nhau, các ảnh con thuộc

T_1 tập trung ở những khu vực có kết cấu ít phức tạp. Trước hết ta giả sử tất cả các ma trận con đều thuộc T_1. Sau khi nạp chồng, hai hay nhiều hơn những ma trận con sẽ bị thay đổi từ T_1 sang T_i ($2 \leq i \leq 4$) nếu chúng ta nhúng một lượng bit bất kỳ vào trong các điểm ảnh ngoại trừ bốn điểm ảnh: A_{LT}, A_{LB}, A_{RT} và A_{RB}. Đặc biệt, khi chúng ta nhúng một lượng bit bất kỳ vào điểm ảnh A_5, tất cả 9 ma trận con sẽ bị thay đổi từ T_1 sang T_i ($2 \leq i \leq 4$). Tuy nhiên, nếu *hình 2.2* là một vùng ma trận thu được từ một ảnh đã giấu tin và một số bit của tin đã được nhúng thì những ma trận con thuộc T_1 sẽ không nạp chồng được giống như trước và một số những ma trận đó sẽ thuộc T_i ($2 \leq i \leq 4$). Khi một lượng tin bất kỳ được nhúng, số những ma trận con thay đổi từ T_1 sang T_i ($2 \leq i \leq 4$) sẽ giảm đáng kể.

Từ những phân tích trên, chúng ta có thể thấy công thức trên vẫn đúng. Tuy nhiên, nếu ảnh giấu tin chỉ chứa một lượng nhỏ dữ liệu ẩn so với kích thước ảnh gốc thì gần như không có một bit nào của thông tin được nhúng vào vùng ma trận 5x5 như đã miêu tả trên *hình 2.2*, như vậy rất khó để chúng ta có thể phân biệt giữa ảnh gốc và ảnh giấu tin dựa vào công thức trên.

Dựa trên những phân tích trên, nhóm tác giả (*Fangjun Huang, Bin Li, Jiwu Huang*) đưa ra các bước thực hiện của thuật toán phát hiện như sau:

1. Đối với một ảnh bất kỳ được chọn, tính toán $|T_1|$.
2. Nhúng một chuỗi ngẫu nhiên với chiều dài L vào hình ảnh được đưa ra trên LSB. Ví dụ, L = 0.5 nghĩa là cứ mỗi hai điểm ảnh của hình ảnh được chọn sẽ có một bit tin nhắn được nhúng.
3. Tính toán $|T_1^*|$ của ảnh mới thu được.
4. Chúng ta có được tỷ lệ thay đổi *k* bằng công thức sau:

$$k = \frac{|T_1| - |T_1^*|}{|T_1|}$$

So sánh *k* giá trị với một ngưỡng định trước, chúng ta có thể xác định xem đó là ảnh gốc hay ảnh đã giấu tin.

2.2.2 Thuật toán và các bước thực hiện

Thuật toán:

Đầu vào: Môt ảnh cấp xám C bất kỳ.

Đầu ra: Kết luận ảnh cấp xám C là ảnh đã giấu tin hay ảnh gốc.

Các bước thược hiện:

- Bước 1: Từ ảnh C ta tính được ma trận ảnh A (tách ra miền bit có trọng số thấp nhất thứ 0 và thứ 1).
- Bước 2: Chia A thành các ma trận nhỏ cỡ 3x3 có nạp chồng.
- Bước 3: Trong tất cả những ma trận ảnh nhỏ có được, ta lọc ra các ma trận thuộc loại T_1.
- Bước 4: Nhúng một lượng tin L=30% bằng thuật toán giấu ngẫu nhiên trên LSB vào ảnh gốc C để được ảnh giấu tin S.
- Bước 5: Lặp lại bước 2, 3 và 4 đối với ảnh S được số ma trận con thuộc T_1^*.
- Bước 6: Sau khi có được số ma trận con thuộc T_1và T_1^*, ta tính tỷ lệ *k* sau công thức sau:

$$k = \frac{|T_1| - |T_1^*|}{|T_1|}$$

Công thức 2.1 Công thức tính ngưỡng *k*

- Bước 7: Từ giá trị *k* thu được, dựa nếu k<T (ngưỡng phân loại) là ảnh có giấu tin ngược lại là ảnh không giấu tin (ảnh gốc).

CHƯƠNG 3: CÀI ĐẶT VÀ THỰC NGHIỆM

3.1 MÔI TRƯỜNG CÀI ĐẶT VÀ ĐỀ MÔ

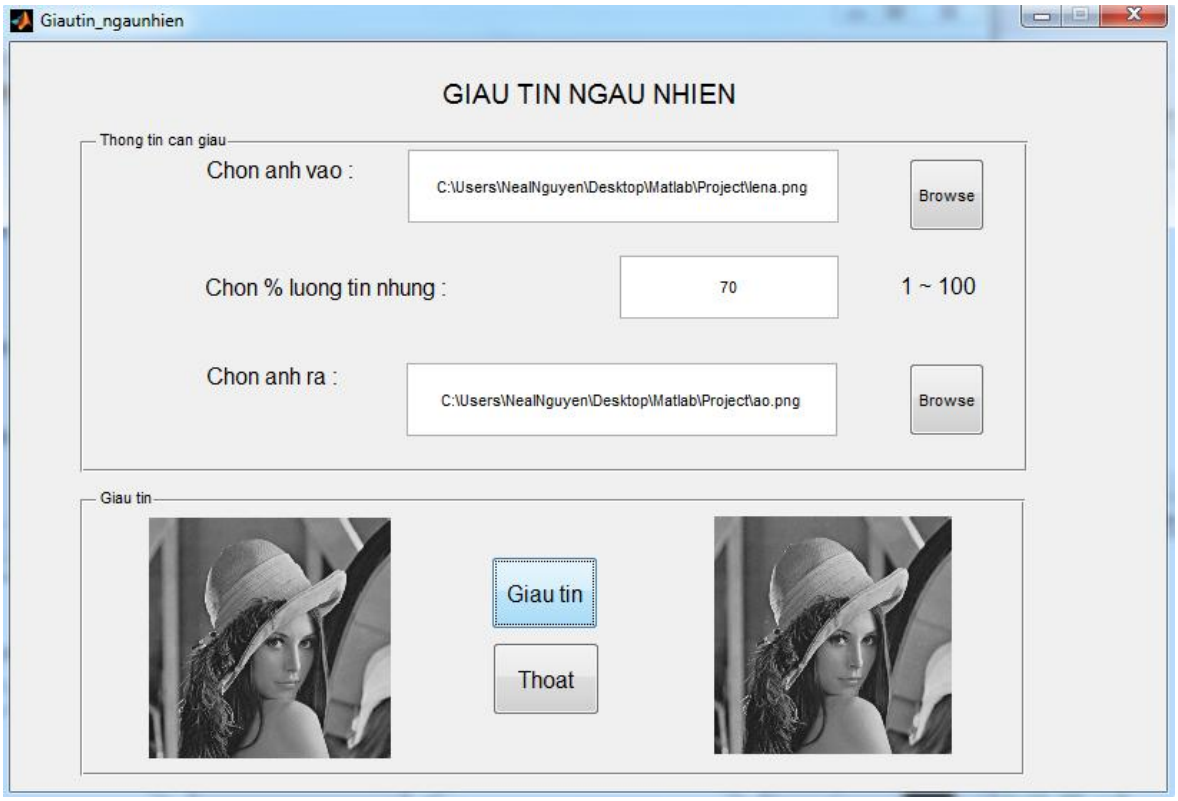
3.1.1 Môi trường cài đặt

- ✓ Ngôn ngữ cài đặt, môi trường soạn thảo và chạy chương trình được thực hiện trên ngôn ngữ lập trình Matlab 7.14.0 (R2012a).
- ✓ Hệ điều hành Window7 và môi trường NetFarme Work 4.0
- ✓ Yêu cầu cấu hình:

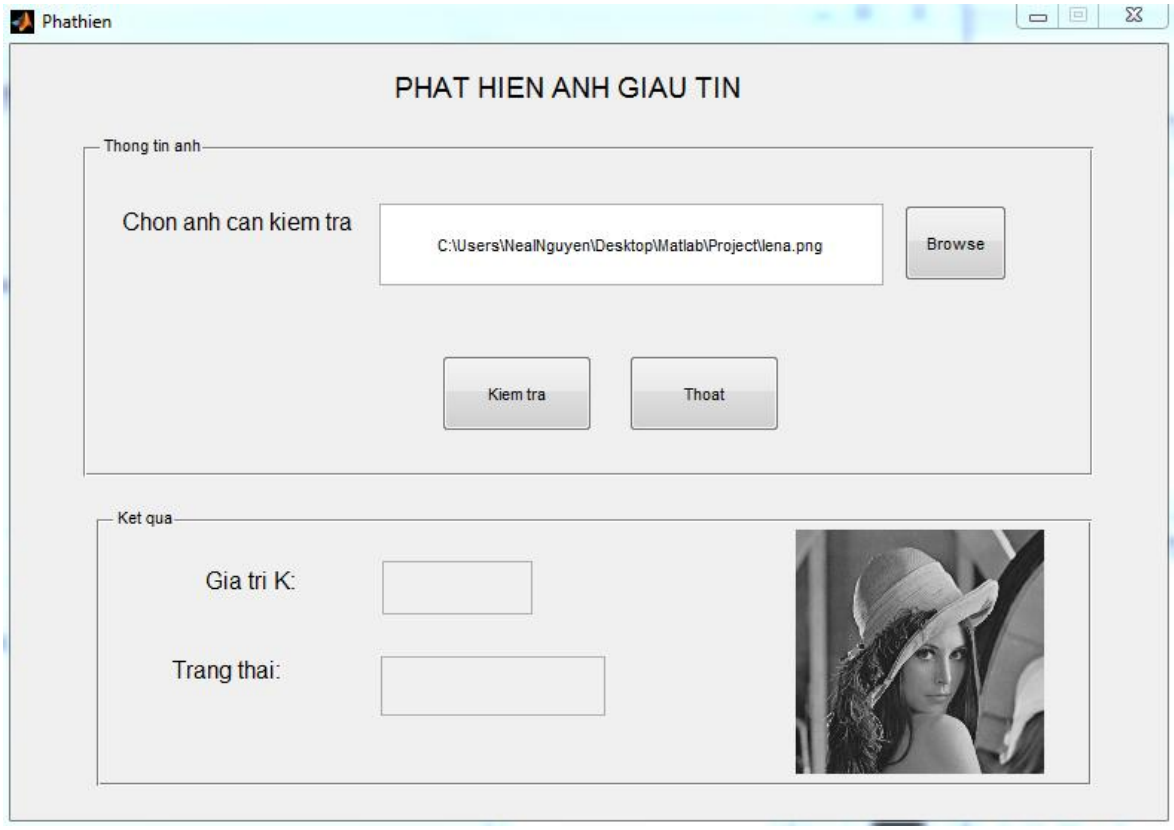
3.1.2 Đề mô chương trình

Một số hình ảnh giao diện chương trình

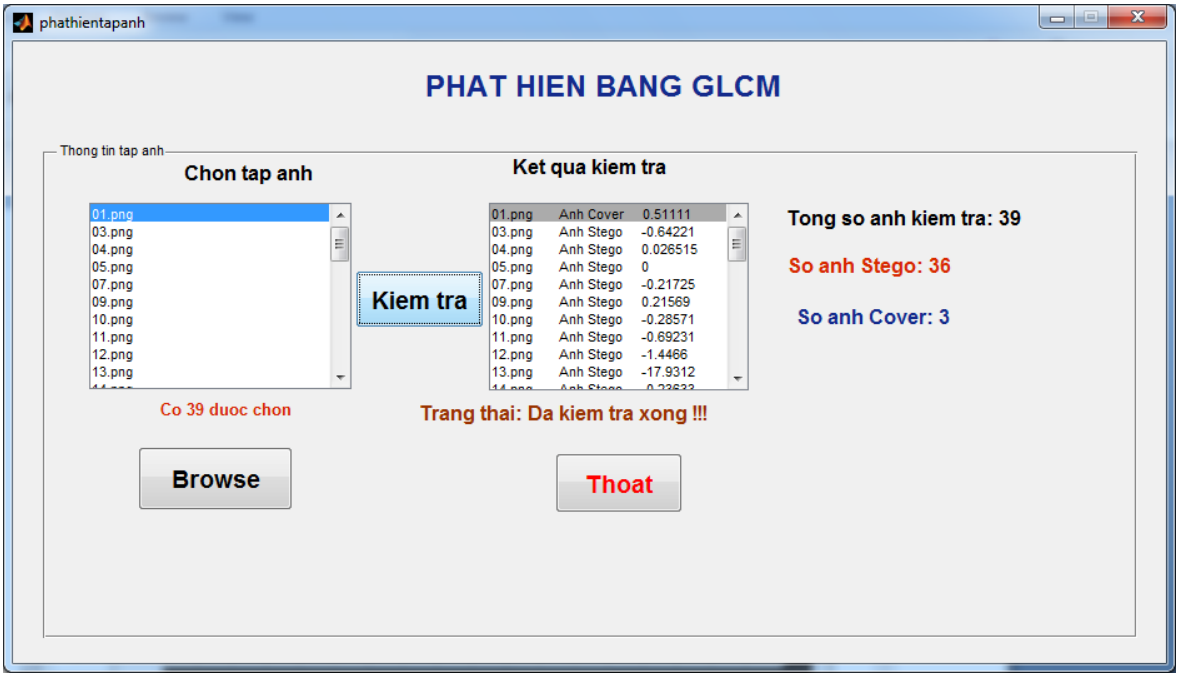
Hình 3.1 Giao diện chương trình chính



Hình 3.2 Giao diện chương trình giấu tin ngẫu nhiên



Hình 3.3 Giao diện chương trình phát hiện ảnh giấu tin



Hình 3.4 Giao diện chương trình phát hiện tập ảnh giấu tin

3.2 THỬ NGHIỆM VÀ NHẬN XÉT

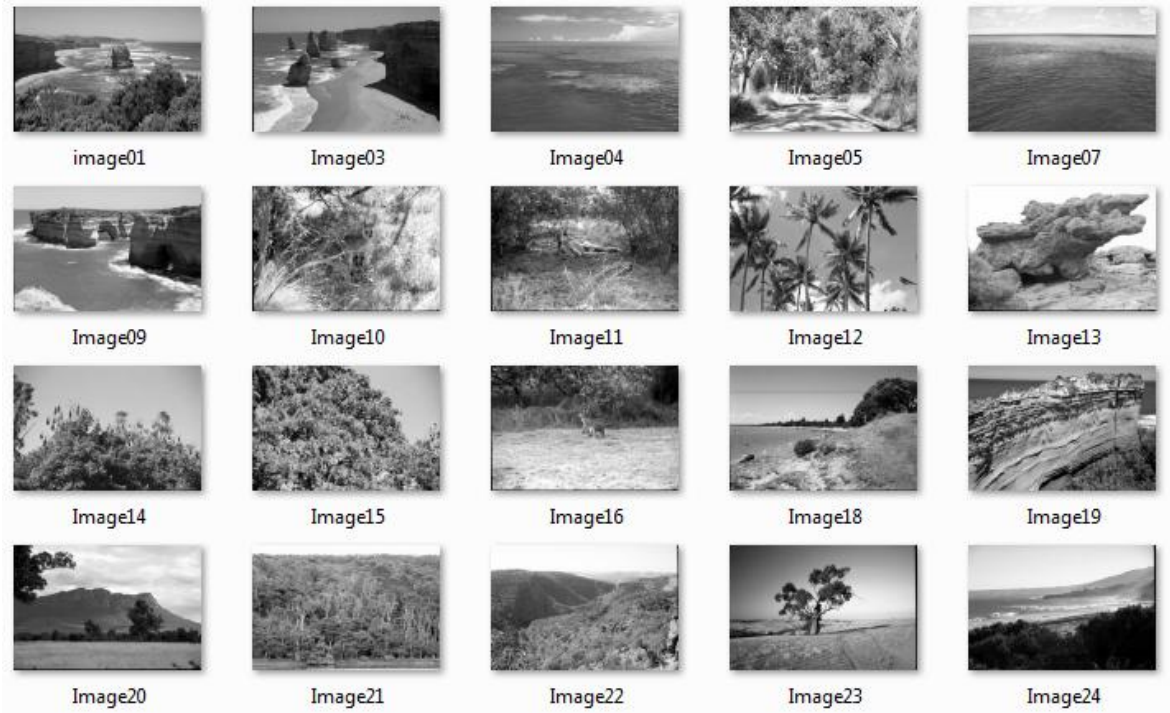
3.2.1 Thử Nghiệm

- Tập ảnh thử nghiệm gồm hai tập ảnh:

+ Tập C1 gồm 9 ảnh chuẩn được tải về từ [4] (hình 3.4) có cùng kích cỡ 512 x 512.

+ Tập C2 gồm 40 ảnh màu được tạo ra từ máy ảnh kỹ thuật số sau đó được chuyển sang ảnh cấp xám 8 bit (hình 3.5) kích cỡ khác nhau.

Hình 3.5 Tập ảnh C1



Hình 3.6 Tập ảnh C2

Sử dụng kỹ thuật giấu tin ngẫu nhiên trên LSB như sau:

+ Trên tập C1: Giấu một lượng thông điệp (sinh ngẫu nhiên) với các tỉ lệ giấu: 30%, 60% ta được tập ảnh tương ứng S1_30, S1_60.

+ Trên tập C2: Giấu một lượng thông điệp (sinh ngẫu nhiên) với các tỉ lệ giấu: 30%, 60% ta được tập ảnh tương ứng S2_30, S2_60.

- Thực hiện phát hiện

Sử dụng kỹ thuật phát hiện ảnh có giấu tin với ngưỡng T=0.25 cho tập ảnh C1, S1_30, S1_60, ta được kết quả theo bảng 3.1.

Tập ảnh	C1		S1_30		S1_60	
	Cover	Stego	Cover	Stego	Cover	Stego
Tỉ lệ phát hiện	5/9	4/9	1/9	8/9	0/9	9/9

Bảng 3.1. Kết quả phát hiện trên 3 tập ảnh C1, S1_30, S1_60

Sử dụng kỹ thuật phát hiện ảnh có giấu tin với ngưỡng T=0.25 cho tập ảnh C2, S2_30, S2_60, ta được kết quả theo bảng 3.2.

Tập ảnh	C2		S2_30		S2_60	
	Cover	Stego	Cover	Stego	Cover	Stego
Tỉ lệ phát hiện	25/40	15/40	1/40	39/40	3/40	36/40

Bảng 3.2. Kết quả phát hiện trên 3 tập ảnh C2, S2_30, S2_60

3.2.2 Nhận xét

Qua quá trình thực nghiệm và thông qua kết quả thu được từ *bảng 3.1* và *bảng 3.2*, Em có thể đưa ra mốt số nhận xét về khả năng phát hiện ảnh giấu tin sử dụng ma trận cấp xám (GLCM) như sau:

- Lượng tin nhúng ít: Khi ảnh chỉ được nhúng với một lượng tin nhỏ (dưới 20% kích cỡ của ảnh) thì khả năng phân biệt giữa ảnh gốc và ảnh đã giấu tin không cao vì giá trị tìm được của $|T_1|$ và $|T_1^*|$ không chênh lệch nhau nhiều, do đó hệ số *k* sẽ thay đổi trong phạm vi nhỏ.
- Lượng tin nhúng lớn: Khi ảnh được nhúng với lượng tin trên 20% kích cỡ của ảnh thì khả năng phát hiện của thuật toán này là tương đối cao (khoảng 85%).
- Trong trường hợp nhúng lượng tin lớn (từ 80% đến 100%) so với kích cỡ của ảnh. Thì khả năng phát hiện ảnh giấu tin của kỹ thuật này là không cao bằng trường hợp nhúng dưới 60%. Vì với lượng tin nhúng này, giá trị của $|T_1|$ và $|T_1^*|$ sẽ dần chạy về giá trị $|T_1|$ và $|T_1^*|$ của ảnh gốc ban đầu.

KẾT LUẬN

Đây là một trong những phương pháp pháp hiện ảnh có giấu tin tương đối phổ biến hiện nay. Với sự phát triển một cách bùng nổ của ngành công nghệ thông tin hiện nay, chúng ta cũng phải bắt kịp sự phát triển của thế giới để có thể tự bảo vệ quyền lợi của bản thân, của quốc gia.

Đồ án của em đã thực hiện những nhiệm vụ sau:

1. Trình bày một số khái niệm cơ bản về: Giấu tin trong ảnh, phát hiện giấu tin trong ảnh, tổng quan về ảnh Bitmap, kĩ thuật giấu tin ngẫu trên LSB,
2. Kỹ thuật phát hiện ảnh giấu tin trên GLCM.

Do còn nhiều hạn chế về thời gian nghiên cứu nên đề tài này không tránh khỏi những thiếu sót, vì vậy em rất mong nhận được sự đóng góp ý kiến của các thầy cô cùng các bạn để báo cáo của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Xuân Huy, Trần Quốc Dũng, ***Giáo trình giấu tin và thuỷ vân ảnh***, Trung tâm thông tin tư liệu, TTKHTN - CN 2003

[2]. Ingemar Cox, Jeffrey Bloom, Matthew Miller, Ton Kalker, Jessica Fridrich, ***Digital Watermarking and Steganography***, Morgan Kaufmann, 2008.

[3]. **Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels**, Fangjun Huang, Bin Li, Jiwu Huang.

[4]. http://sipi.usc.edu/database/database.php

Một số đồ án tốt nghiệp ngành CNTT *từ khóa 7 đến khóa 11 liên quan đến kỹ thuật giấu tin và phát hiện ảnh có giấu tin:*

[5]. Dương Uông Hiên_lớp CT701, **"Nghiên cứu kỹ thuật giấu tin mật trên vùng biến đổi DWT"**, tiểu án tốt nghiệp ngành CNTT – 2008.

[6]. Ngô Minh Long – Lớp CT701, **"Phát hiện ảnh có giấu tin trên Bit ít ý nghĩa nhất LSB"**, tiểu án tốt nghiệp ngành CNTT – 2008.

[7]. Đỗ Trọng Phú – CT702, **"Nghiên cứu kỹ thuật giấu tin trên miềm biến đổi DFT"**, tiểu án tốt nghiệp ngành CNTT – 2008.

[8]. Hoàng Thị Huyền Trang – CT802,**"Nghiên cứu kỹ thuật phát hiện ảnh giấu tin trên miền biến đổi của ảnh"**, đồ án tốt nghiệp ngành CNTT – 2008.

[9]. - Nguyễn Thị Kim Cúc – CT801, **"Nghiên cứu một số phương pháp bảo mật thông tin trước khi giấu tin trong ảnh"**, đồ án tốt nghiệp ngành CNTT – 2008.

[10]. *Vũ Tuấn Hoàng* – CT801, "***Nghiên cứu kỹ thuật phát hiện ảnh có giấu tin dựa trên LSB của ảnh cấp xám***", đồ án tốt nghiệp ngành CNTT – 2008.

[11]. Vũ Thị Hồng Phương – CT801, **"Nghiên cứu kỹ thuật giấu tin trong ảnh gif"**, đồ án tốt nghiệp ngành CNTT – 2008.

[12]. Đỗ Thị Nguyệt – CT901, "***Nghiên cứu một số kỹ thuật ước lượng độ dài thông điệp giấu trên bit có trọng số thấp***", đồ án tốt nghiệp ngành CNTT – 2009.

[13]. Mạc như Hiển – CT901, "**Nghiên cứu kỹ thuật giấu thông tin trong ảnh GIF**", đồ án tốt nghiệp ngành CNTT – 2009.

[14]. Phạm Thị Quỳnh – CT901, "***NGHIÊN CỨU KỸ THUẬT PHÁT HIỆN THÔNG TIN ẨN GIẤU TRONG ẢNH JPEG2000***", đồ án tốt nghiệp ngành CNTT – 2009.

[15]. Phạm Thị Thu Trang – CT901, "**Nghiên cứu kỹ thuật giấu thông tin trong ảnh JPEG2000",** đồ án tốt nghiệp ngành CNTT – 2009.

[16]. Trịnh Thị Thu Hà – CT901, "**NGHIÊN CỨU KỸ THUẬT PHÁT HIỆN THÔNG TIN ẨN GIẤU TRONG ẢNH GIF** ",đồ án tốt nghiệp ngành CNTT – 2009.

[17]. Vũ Trọng Hùng – CT801, "**Kỹ thuật giấu tin thuận nghịch dựa trên miền dữ liệu ảnh"**, tiểu án tốt nghiệp ngành CNTT – 2009.

[18]. Đỗ Lâm Hoàng – CT1001, **"Nghiên cứu kỹ thuật giấu tin thuận nghịch trên miền dữ liệu ảnh cấp xám"**, đồ án tốt nghiệp ngành CNTT – 2010.

[19]. Nguyễn trường Huy- CT1001, "**Nghiên cứu kỹ thuật giấu tin trên ảnh nhị phân**", đồ án tốt nghiệp ngành CNTT – 2010.

[20]. Vũ Văn Thành- CT1001, " **Tìm hiểu giải pháp và công nghệ xác thực điện tử sử dụng thủy vân số**", đồ án tốt nghiệp ngành CNTT – 2010.

[21]. Vũ Văn Tập – CT1001, "**Nghiên cứu kỹ thuật phát hiện ảnh có giấu tin trên miền dữ liệu của ảnh**", đồ án tốt nghiệp ngành CNTT – 2010.

[22]. Vũ Khắc Quyết – ct1001, **"Nghiên cứu kỹ thuật giấu tin với dung lượng thông điệp lớn",** đồ án tốt nghiệp ngành CNTT – 2010.

[23]. Phạm Quang Tùng – CT1001, **"Tìm hiểu kỹ thuật phát hiện ảnh có giấu tin dựa trên phân tích tương quan giữa các bit LSB của ảnh",** đồ án tốt nghiệp ngành CNTT – 2010.

[24]. Vũ Thị Ngọc – CT1101, **"Nghiên cứu một giải pháp giấu văn bản trong ảnh",**

[25]. Cao Thị Nhung – CT1101, **"Tìm hiểu kỹ thuật thủy vân số thuận nghịch cho ảnh nhị phân",** đồ án tốt nghiệp ngành CNTT – 2011.

[26]. Hoàng Thị Thuy Dung – CT1101, **"Kỹ thuật giấu tin trong ảnh dựa trên MBNS (Multiple Base Notational System)",** đồ án tốt nghiệp ngành CNTT – 2011.

[27]. **Vũ Thùy Dung – CT1101, "Kỹ thuật giấu tin trong ảnh SES (Steganography Evading Statistical analyses)",** đồ án tốt nghiệp ngành CNTT – 2011.

[28]. Trịnh Văn Thành – CT1101, "**Phát hiện ảnh có giấu tin trên LSB bằng phương pháp phân tích cặp mẫu",** đồ án tốt nghiệp ngành CNTT – 2011

[29]. Phạm Văn Đại – CT1101, **"Kỹ thuật giấu tin dựa trên biến đổi Contourlet"**,đồ án tốt nghiệp ngành CNTT – 2011

[30]. Nguyễn Mai Hương – CT1101, **"Kỹ thuật giấu tin PVD"**,đồ án tốt nghiệp ngành CNTT – 2011

[31]. Phạm Văn Minh, "**Kỹ thuật phát hiện mù cho ảnh có giấu tin bằng LLRT (Logarithm likelihood Ratio Test)",** đồ án tốt nghiệp ngành CNTT – 2011.

[32]. Nguyễn Thị Diễm Hương, "**Kỹ thuật giấu tin trên k bit LSB của ảnh**", đồ án tốt nghiệp ngành CNTT – 2012.

[33]. Bùi Văn Nhất, **"Kỹ thuật giấu tin thuận nghịch trong ảnh MMPOUA",** đồ án tốt nghiệp ngành CNTT – 2012.

[34]. Nguyễn Văn Cường – CT1201, **"Lược đồ giấu tin dựa trên hàm Modulus"**, đồ án tốt nghiệp ngành CNTT – 2012.

[35]. Trần Đại Dương, **"Kỹ thuật giấu tin thuận nghịch trong ảnh bằng hiệu chỉnh hệ số wavelet"**, đồ án tốt nghiệp ngành CNTT.