LỜI CẢM ƠN

Trước hết em xin bày tỏ lòng biết ơn sâu sắc nhất tới cô giáo hướng dẫn Thạc sỹ Hồ Thị Hương Thơm – giảng viên khoa CNTT trường ĐHDL Hải Phòng là người đã tận tình giúp đỡ em rất nhiều trong suốt quá trình tìm hiểu nghiên cứu và hoàn thành đồ án tốt nghiệp này.

Em xin chân thành cảm ơn các thầy cô trong bộ môn công nghệ thông tin – trường DHDL hải phòng cũng như các thầy cô trong trường đã trang bị cho em những kiến thức cơ bản cần thiết để em có thể hoàn thành báo cáo.

Xin gửi lời cảm ơn đến bạn bè những người luôn bên em đã động viên và tạo điều kiện thuận lợi cho em, tận tình giúp đỡ chỉ bảo em những gì em còn thiếu sót trong quá trình làm báo cáo tốt nghiệp.

Cuối cùng em xin bày tỏ lòng biết ơn sâu sắc tới những người thân trong gia đình đã dành cho em sự quan tâm đặc biệt và luôn động viên em.

Vì thời gian có hạn, trình độ hiểu biết của bản thân còn nhiều hạn chế. Cho nên trong đồ án không tránh khỏi những thiếu sót, em rất mong nhận được sự đóng góp ý kiến của tất cả các thầy cô giáo cũng như các bạn bè để đồ án của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải phòng, ngày tháng năm 2010

Sinh viên thực hiện

Phạm Quang Tùng.

LỜI 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, ảnh tĩnh…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 về kỹ thuật giấu và phát hiện ảnh có giấu tin. Đồng thời trình bày một số kỹ thuật giấu và phát hiện thông tin trên ảnh số, từ đó đưa ra các thực nghiệm và đánh giá cho việc phát hiện thông tin ẩn giấu trong ảnh số.

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 (Steganography)

1.1.1 Định nghĩa kỹ thuật giấu tin

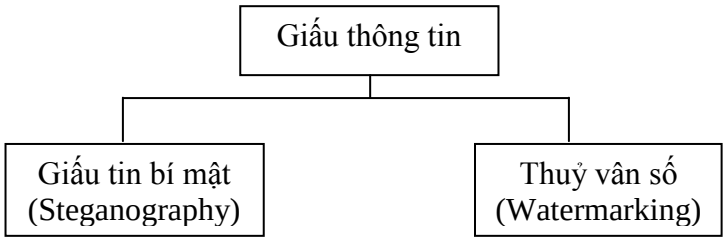
Giấu thông tin là một kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác (giấu thông tin chỉ mang tính quy ước không phải là một hành động cụ thể).

1.1.2 Mục đích của giấu tin

Có hai mục đích của giấu tin:

- Bảo mật cho những dữ liệu được giấu
- Bảo đảm an toàn (bảo vệ bản quyền) cho chính các đối tượng chứa dữ liệu giấu trong đó và phát hiện xuyên tạc thông tin.

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

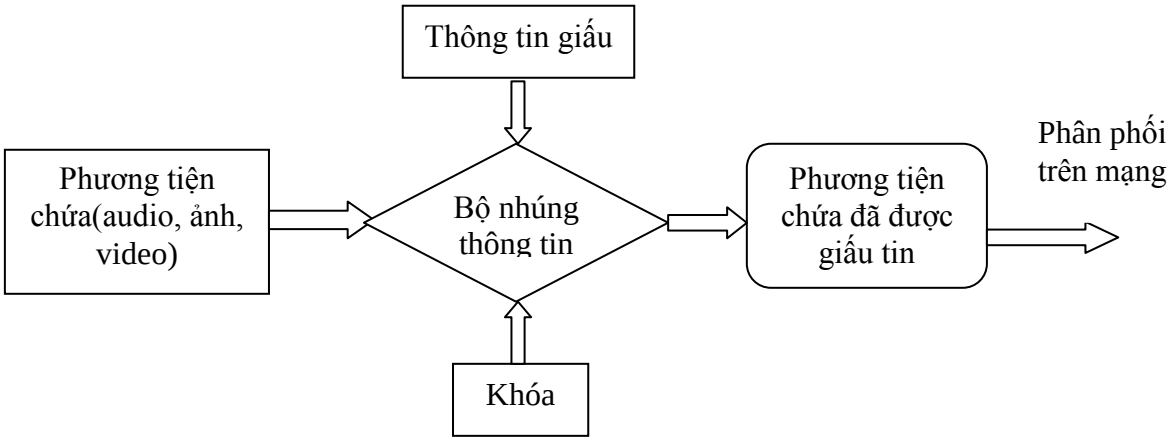
Kỹ thuật giấu thông tin bí mật (Steganography): với mục đích đảm bảo an toàn và bảo mật thông tin tập trung vào các kỹ thuật giấu tin để có thể giấu được nhiều thông tin nhất. Thông tin mật được giấu kỹ trong một đối tượng khác sao cho người khác khó phát hiện được.

Kỹ thuật giấu thông tin theo kiểu đánh giấu – 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 điệp (với các tin bí mật) hay các logo, hình ảnh bản quyền.

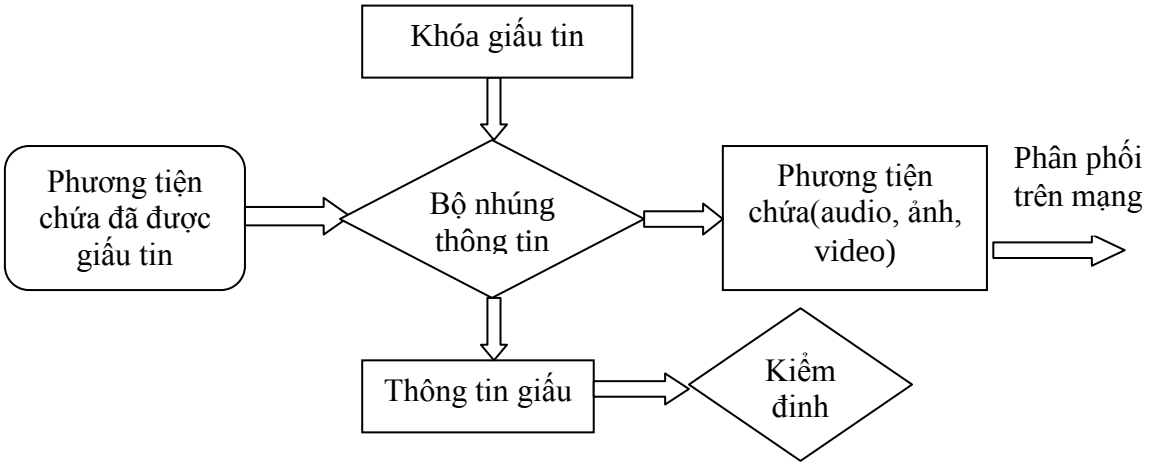
- Phương tiện chứa: các file ảnh, text, audio… là môi trường để nhúng tin.

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 giải mã 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 không nhìn thấy: là một trong 3 yêu cầu của bất kì 1 hệ giấu tin nào. Tính không nhìn thấy là tính chất vô hình của thông tin nhúng trong phương tiện nhúng.
- Tính mạnh mẽ: là yêu cầu thứ 2 của một hệ giấu tin. Tính mạnh mẽ 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, nhận thức 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 diểm của việc giấu tin trên ảnh

Một kỹ thuật giấu tin trên ảnh có một số đặc điểm sau:

- Tính vô hình của thông tin được giấu.
- Số lượng thông tin được giấu.
- Tính an toàn và bảo mật của thông tin.
- Ảnh môi trường đối với quá trình giải mã.

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 Tỷ lệ giấu 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 mãn (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 môi trường. 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 (Steganalysis)

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 (stego image) hay không, để từ đó có thể đưa ra bước xử lý tiếp theo.

1.2.2 Phân tích tin ẩn giấu thường dựa vào các yếu tố sau:

- 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 điệp 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 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 các ảnh dữ liệu lớn.

CHƯƠNG 2. CẤU TRÚC ẢNH BITMAP

2.1 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 2.1:

Bảng 2.1 Cấu trúc ảnh BitMap

Bitmap Header (54 byte)
Color Palette
Bitmap Data

2.1.1 Bitmap Header

Thành phần bitcount (Bảng 2.2 Thông tin về Bitmap Header) 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" thi 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 2.2 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)	

2.1.2 Palette màu

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

Bảng 2.3 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

2.1.3 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.

2.2 Cấu trúc ảnh PNG

2.2.1 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 trong nước 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 trên hình ảnh, nhất 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 vơi 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.

2.2.2 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.

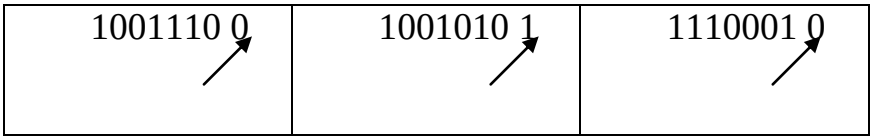
- IHDR phải là thành phần đầu tiên, nó chứa đựng header
- PLTE chứa đựng bảng màu (danh sách các màu)
- IDAT chứa đựng ảnh. Ảnh này có thể được chia nhỏ chứa trong nhiều phần IDAT. Điều này làm tăng kích cỡ của tệp lên một ít nhưng nó làm cho việc phát sinh ảnh PNG mượt hơn (streaming manner).
- IEND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

CHƯƠNG 3: KỸ THUẬT GIẤU TIN TRÊN LSB

3.1 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 sắc của mỗi điểm ảnh, vì vậy khi ta thay đổi bit ít quan trọng của một điểm ảnh thì màu sắc 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 3.1*:* 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

3.2 Thuật toán giấu thông điệp trên LSB

3.2.1 Ý tưởng thuật toán

+ Cho thông điệp nhúng W. W có thể là:
  - Một chuỗi bít thông điệp (vd: W = [0 0 1 1 0 1 0 1 1 1 1 0 0 1]).
  - Một chuỗi các kí tự (vd: W = HPU → phải đổi W sang hệ nhị phân).

+ Tính độ dài L_W của thông điệp W, đổi L_W ra hệ nhị phân sau đó nối vào trước W để có được thông điệp nhúng cuối cùng (thông_điệp) nhúng vào ảnh.
+ Thông_điệp thu được ở bước trên nhúng vào tất cả các bit LSB của điểm ảnh lần lượt từ trái qua phải, từ trên xuống dưới đến hết.

3.2.2 Thuật toán giấu

Input

Ma trận dữ liệu ảnh cấp xám I.

Mảng nhị phân l_w (gồm 24 bit chứa độ dài thông điệp và thông điệp).

Output

Ảnh có giấu tin.

Các bước thực hiện như sau:

Duyệt ma trận I và chuyển tất cả các LSB của các điểm ảnh theo chiều quét từ trái qua phải từ trên xuống dưới về 0.

Thay thế các bit LSB của điểm ảnh bằng bit thông điệp.

3.2.3 Thuật toán giấu LSB cải tiến

Input: Ảnh cấp xám I kích cỡ m*n

Chuỗi thông điệp cần giấu M

Output: Ảnh có chứa thông điệp giấu.

Các bước thực hiên như sau:

B1: Sử dụng bộ khởi tạo bước đi giả ngẫu nhiên để chọn pixel sẽ giấu thông điệp. Lưu chỉ số của điểm ảnh được chọn vào một mảng (key).

B2: LSB của pixel được chọn sẽ được thay thế bằng một bit thông điệp nhị phân thuộc M

B3: Lặp lại bước 1 và bước 2 cho đến khi giấu hết các bit thông điệp trong M

3.3 Thuật toán tách thông điệp.

3.3.1 Ý tưởng thuật toán tách.

+ Duyệt ảnh theo chiều quét từ trái qua phải, từ trên xuống.
+ Tách lấy tất cả các LSB của các điểm ảnh theo chiều quét sử dụng trong quá trình giấu tin lưu vào một mảng M.
+ Từ mảng M tách được tách 24 bit đầu để lấy ra độ dài thông điệp.
+ Sau khi đã có độ dài chuỗi thông điệp nhúng, tiến hành tách lấy thông điệp gốc.

3.3.2 Thuật toán tách.

Input :

Ma trận dữ liệu ảnh cấp xám I, ảnh có giấu tin.

Output :

Thông điệp giấu.

Các bước thực hiện như sau:

B1: Duyệt ma trận I lần lượt từ trên xuống, trái qua phải tách lấy tất cả các LSB các điểm ảnh của ma trận dữ liệu I bằng cách lấy dư cho 2, được mảng nhị phân M

B2: Tách 24 bít đầu của mảng M, đổi sang cơ số 10 ta được độ dài của chuỗi thông điệp nhúng.

B3: Trích bit thông điệp sau khi thu được độ dài ở bước trên

3.3.3 Thuật toán tách cho trường hợp giấu LSB cải tiến.

Input :

Ma trận dữ liệu ảnh cấp xám I, ảnh có giấu tin.

Ma trận bước đi chứa chỉ số của các điểm ảnh được giấu(key).

Output :

Thông điệp giấu.

Các bước thực hiện như sau:

B1: Duyệt ma trận I và so sánh chỉ số của các điểm ảnh với key xem nó có được giấu không. Nếu chỉ số điểm ảnh đang xét có trong key thì tách lấy LSB của điểm đó và lưu vào một màng w. Duyệt cho đền khi hết ma trận dữ liệu ảnh.

B2: Mảng w có chứa bit nhị phân của thông điệp cần tách. Ta tiến hành đổi giá trị của mảng w sang kiểu chuỗi thì thu được thông điệp cần tách.

CHƯƠNG 4: KỸ THUẬT PHÁT HIỆN ẢNH CÓ GIẤU TIN TRÊN LSB

4.1 Trình bày kỹ thuật

Kỹ thuật phát hiện ảnh có giấu tin dựa trên tương quan biểu đồ tần số sai khác của ảnh được Tao Zhang và Xijian Ping giới thiệu, trong đó sử dụng biện pháp tương quan giữa các miền bit liên tiếp để phân loại và đánh giá giữa hình ảnh cover-images và stego images. Theo tính chất của kỹ thuật giấu LSB steganography, biểu đồ tần số sai khác (diference image histogram) của ảnh được sử dụng như là một công cụ phân tích thống kê. Giá trị sai khác của ảnh được định nghĩa như sau:

$$D(i,j) = I(i+1,j) - I(i,j) \qquad (4.1)$$

Hình 4.1 Diference image histogram của ảnh lena.bmp

Trong đó ***I(i,j)*** là giá trị của một điểm ảnh có tọa độ (i,j) của ảnh I. T.Zhang và X.Ping cho rằng, tồn tại sự khác biệt giữa biểu đồ tần số sai khác của ảnh bình thường và ảnh thu được sau khi đảo các bit trên miền LSB của ảnh. Thực tế nó được sử dụng để phát hiện cho kỹ thuật steganalysis. Để giải thích chi tiết phương thức của biểu đồ tần số sai khác(DIH) của ảnh, chúng ta cần định nghĩa một số khái niệm sau. Đặt I là một ảnh thử, I có kích cỡ M*N pixel. Tỉ lệ nhúng ***p*** là tỉ lệ phần trăm giữa độ dài của thông điệp nhúng với khả năng giấu tin tối đa của ảnh.

Nếu ký hiệu biểu đồ tần số sai khác của ảnh ban đầu là h_i, biểu đồ tấn số sai khác của ảnh sau khi đảo các bit LSB trong miền LSB là f_i, và g_i là ký hiệu

biểu đồ tần số sai khác của ảnh sau khi đặt tất cả các bit trong miền LSB bằng 0. Khi đó ta có mối quan hệ giữa h_i, f_i và g_i như sau :

$$h_i = f_{2i} = a_{2i,2i}g_{2i} \quad (4.2)$$

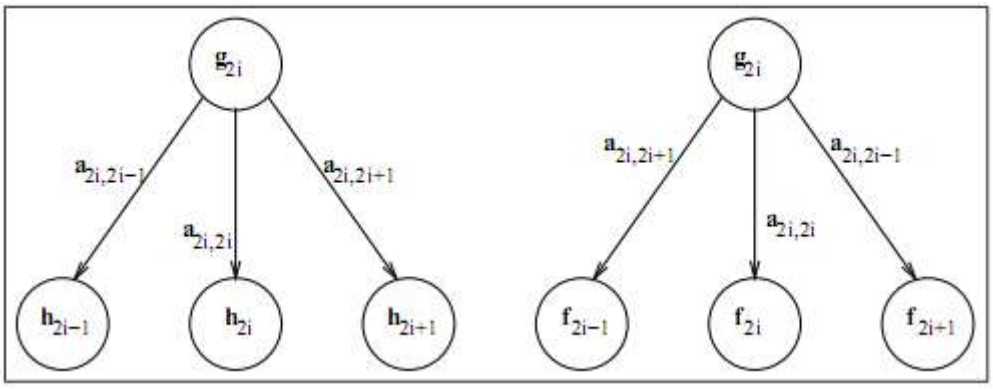
$$h_{2i+1} = a_{2i,2i+1}g_{2i} + a_{2i+2,2i+1}g_{2i+2} \quad (4.3)$$

$$f_{2i+1} = a_{2i,2i-1}g_{2i} + a_{2i+2,2i+3}g_{2i+2} \quad (4.4)$$

Trong đó $a_{2i,2i+j}$ được định nghĩa là hệ số biến đổi từ biểu đồ g_i sang h_i. Với $j = 0,1,-1$ ta có $0 < a_{2i,2i+j} < 1$ nếu không $a_{2i,2i+j} = 0$, và chúng thỏa mãn

$$a_{2i,2i-1} + a_{2i,2i} + a_{2i,2i+1} = 1 \quad (4.5)$$

Hình 4.2 thể hiện mối quan hệ giữa g_i, h_i, f_i và $a_{2i,2i+j}$



Hình 4.2 sơ đồ biến đổi từ g_i sang h_i, f_i

Bắt đầu từ sự đối xứng của biểu đồ tần số sai khác về i=0, nhận được $a_{0,1} \sim= a_{0,-1}$ lúc đầu. Kết hợp với phương trình (**4.2-4.5**), chúng ta có được công thức tính hệ số biến đổi cho các số nguyên dương i

$$\begin{cases} a_{0,1} = a_{0,-1} = \dfrac{g_0 - h_0}{2g_0} \\ a_{2i,2i} = \dfrac{h_{2i}}{g_{2i}} \\ a_{2i,2i-1} = \dfrac{h_{2i-1} - a_{2i-2,2i-1}g_{2i-2}}{g_{2i}}, i \geq 1 \\ a_{2i,2i+1} = 1 - a_{2i,2i} - a_{2i,2i-1}, i \geq 1 \end{cases} \quad (4.6)$$

Khi nhúng một thông điệp mật ngẫu nhiên vào các bit LSB của ảnh stego-image với miền LSB được nhúng hoàn toàn (p=100%), đối với những ảnh stego như vậy chúng ta có $\mathbf{a_{2i,2i-1}}$~=0.25, $\mathbf{a_{2i,2i}}$~=0.5, $\mathbf{a_{2i,2i+1}}$~=0.25. Dưới đây là một vài hệ số biến đổi với ảnh chuẩn "Lena" và 2 ảnh stego-images với tỉ lệ nhúng p=50% và p=100% được liệt kê trong bảng 4.1.

Bảng 4.1. Một số hệ số biến đổi

		$a_{2i,2i-1}$	$a_{2i,2i}$	$a_{2i,2i+1}$
Original	i=0	0.2316	0.5368	0.2316
	i=1	0.3115	0.5025	0.1860
	i=2	0.3527	0.4841	0.1632
p=50%	i=0	0.2451	0.5098	0.2451
	i=1	0.2805	0.5009	0.2186
	i=2	0.3025	0.4934	0.2041
p=100%	i=0	0.2503	0.4993	0.2503
	i=1	0.2502	0.5004	0.2494
	i=2	0.2508	0.5005	0.2487

Từ phương trình (**4.3**) chúng ta biết rằng $\boldsymbol{h_{2i+1}}$ bao gồm 2 thành phần: $\mathbf{a_{2i,2i+1}}\,\mathbf{g_{2i}}$ và $\mathbf{a_{2i+2,2i+1}}\mathbf{g_{2i+2}}$, và phép thống kê kiểm tra cho thấy đối với một ảnh gốc thì bao gồm 2 khoảng bằng nhau tạo thành $\mathbf{h_{2i+1}}$, nghĩa là ta có:

$$\mathbf{a_{2i,2i+1}g_{2i}} \approx \mathbf{a_{2i+2,2i+1}g_{2i+2}} \qquad \textbf{(4.7)}$$

Chúng ta hãy đặt:

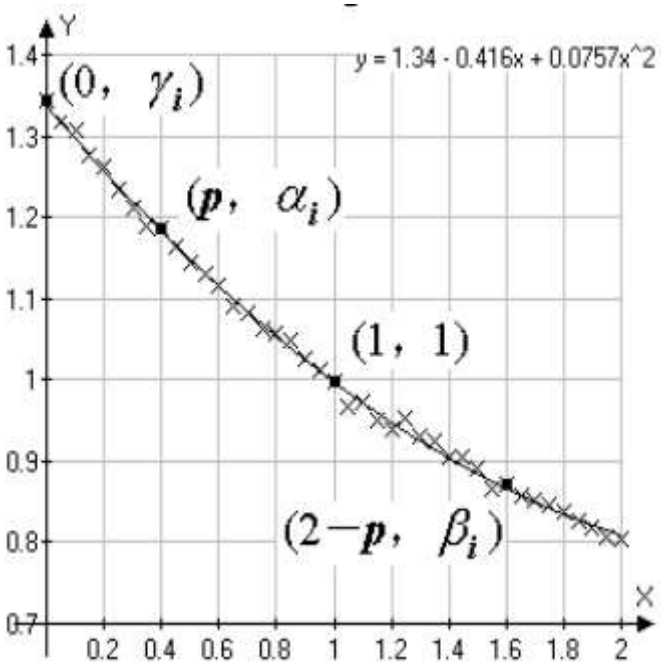
$$\alpha_i = \frac{a_{2i+2,2i+1}}{a_{2i,2i+1}} \quad , \quad \beta_i = \frac{a_{2i+2,2i+3}}{a_{2i,2i-1}} \quad \gamma_i = \frac{g_{2i}}{g_{2i+2}}$$

Và giả thuyết thống kê đối với phương pháp phát hiện steganalytic cho một ảnh gốc thì nó phải thỏa mãn:

$$\boldsymbol{\alpha_i \approx \gamma_i} \qquad \textbf{(4.8)}$$

Trong khi với ảnh stego-images với miền LSB được nhúng hoàn toàn ta có:

$$\boldsymbol{\alpha_i \approx 1} \qquad \textbf{(4.9)}$$



Hình 4.3. Mối quan hệ chức năng giữa α_i và tỉ lệ nhúng p khi i=0 cho ảnh "Lena"

Chúng ta mô hình hóa mối quan hệ giữa α_i và tỉ lệ nhúng p sử dụng đa thức bậc hai: $y=ax^2+bx+c$, bằng cách tìm mối quan hệ ràng buộc của bốn điểm quan trọng $P_1(0,\gamma_i)$, $P_2(p, \alpha_i)$, $P_3(1,1)$, $P_4(2-p,\beta_i)$ để ước lượng p. Khi đó ta thiết lập được hệ phương trình sau:

$$\begin{cases} c = \gamma_i \\ ap^2 + bp + c = \alpha_i \\ a(2-p)^2 + b(2-p) + c = \beta_i \\ a + b + c = 1 \end{cases} \qquad \textbf{(4.10)}$$

Đặt $d_1 = 1 - \gamma_i$, $d_2 = \alpha_i - \gamma_i$, $d_3 = \beta_i - \gamma_i$ thay vào biểu thức **(4.10)**, giản lượng hóa ta được phương trình sau:

$$2d_1p^2 + (d_3 - 4d_1 - d_2)p + 2d_2 = 0 \qquad \textbf{(4.11)}$$

Từ phương trình **(4.11)** ta có thể tính được tỉ lệ nhúng p, nếu hệ số của phương trình là nhỏ hơn không thì giá trị của tỉ lệ nhúng p tính được là $\mathbf{p \approx 1}$.

Trong bài báo cáo này em chỉ chọn $i= 0,1,2$ và lấy giá trị trung bình của ba trường hợp cho dự đoán cuối cùng cho tỉ lệ nhúng **p**.

4.2 Thuật toán phát hiện ảnh có giấu tin

Input: cho một ảnh bất kỳ có kích cỡ (m*n).

Output: Tỉ lệ nhúng *p* của ảnh

Các bước thực hiện

B1: Chọn một ảnh trong tập ảnh thử nghiệm I

B2: Tính tần số sai khác của ảnh I(i,j): ***D(i,j)=I(i,j) – I(i,j+1)***

B3: Tính biểu đồ tần số sai khác của ảnh trước (h_i) và sau khi đảo miền LSB bit về "zero" (g_i);

Biểu đồ tần số sai khác của ảnh được chia làm 2 phần h_1gồm những giá trị lớn hơn hoặc bằng không được tính bằng $h_1(D(i,j)+1)=h_1(D(i,j)+1)+1$. Và h_2 gồm những giá trị nhỏ hơn không và được tính bằng $h_2(abs(D(i,j))+1) = h_2(abs(D(i,j))+1)+1$. Vì $h_1$và h_2 gồm những giá trị đối xứng nhau qua gốc tọa độ **(0,0)** nên ở đây $h(D(i,j))=h(D(i,j)+1)$.

Gán tất cả các LSB của ảnh **I** bằng "0" ta được ảnh

I_0 = floor(I/2)*2

Tính biểu đồ tần số sai khác g_1, g_2 của I_0 tương tự như biện pháp tính h_1 và h_2.

B4: Tính $a_{2i,2i-1}$, $a_{2i,2i}$, $a_{2i,2i+1}$ sử dụng công thức **(4.6)**:

$$a_{0,1} = a_{0,-1} = \frac{g_0 - h_0}{2g_0},$$

$$a_{2i,2i} = \frac{h_{2i}}{g_{2i}},$$

$$a_{2i,2i-1} = \frac{h_{2i-1} - a_{2i-2,2i-1} g_{2i-2}}{g_{2i}},$$

$$a_{2i,2i+1} = 1 - a_{2i,2i} - a_{2i,2i-1}.$$

B5: Tính $\alpha_i, \beta_i, \gamma_i$ sử dụng các công thức tính:

$$\alpha_i = \frac{a_{2i+2,2i+1}}{a_{2i,2i+1}}$$

$$\beta_i = \frac{a_{2i+2,2i+3}}{a_{2i,2i-1}}$$

$$\gamma_i = \frac{g_{2i}}{g_{2i+2}}$$

B6. Gán giá trị cho $\mathbf{d_1}$, **d2**, $\mathbf{d_3}$:

$$d_1 = 1 - \gamma_i$$

$$d_2 = \alpha_i - \gamma_i$$

$$d_3 = \beta_i - \gamma_i$$

B7: Giải phương trình bậc hai:

$$2d_1p^2 + (d_3 - 4d_1 - d_2)p + 2d_2 = 0$$

B8: Lặp lai các bước từ B4 – B7 cho mỗi giá trị của i= 0,1,2

B9: Lấy giá trị trung bình của ***p*** cho ***i= 0,1,2*** để đưa ra kết luận cuối cùng cho tỉ lệ nhúng ***p*** của ảnh.

CHƯƠNG 5: CÀI ĐẶT VÀ THỰC NGHIỆM

5.1 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 2007b.
- Hệ điều hành Window XP và môi trường NetFarme Work 2.0
- Yêu cầu cấu hình:

5.2 Giao diện chương trình

5.2.1 Giao diện chính chương trình

Hình 5.1 Giao diện chính của chương trình

Các chức năng chính của chương trình:

Giấu tin LSB:

Giấu theo tỷ lệ ảnh: Người dùng chọn một ảnh cần nhúng và nhập vào tỉ lệ nhúng, chương trình sẽ sinh ra một chuỗi bit ngẫu nhiên có độ dài tính bằng tỉ lệ nhúng của ảnh mà bạn vừa nhập.

Tên hàm: LSB_embed(image_name,stego_name,tile)

Các tham số đầu vào:

image_name: tên ảnh cần giấu tin.

stego_name: tên ảnh sau khi giấu tin**.**

tile: tỷ lệ nhúng tin.

Đầu ra: Ảnh đã giấu tin.

Giấu chuỗi ký tự: Giấu một chuỗi thông điệp bất kỳ do người dung nhập vào từ bàn phím.

Tên hàm: [Trang_thai stego_image] = embed_chuoi(image_name,name_output,message)

Các tham số đầu vào**:**

image_name: tên ảnh cần giấu tin.

name_output: tên ảnh sau khi giấu tin.

message: Chuỗi thông điệp được người dung nhập vào.

Các tham số đầu ra:

Trang_thai: Trạng thái ảnh sau khi thực hiện giấu tin.

Stego_image: Ảnh đã giấu tin.

Giấu tệp văn bản: cho phép người dùng chọn một tệp văn bản dạng file *.txt để giấu vào ảnh.

Tên hàm: [Trang_thai stego_image] = giau_thong_diep(image_name,str_message,name_output)

Các tham số đầu vào:

Image_name: tên ảnh cần giấu tin.

Str_message: Nội dung của tệp văn bản cần nhúng.

Name_output: Tên ảnh sau khi giấu tin.

Các tham số đầu ra:

Trang_thai: Trạng thái ảnh sau khi thực hiện giấu tin.

Stego_image: Ảnh đã giấu tin.

Tách thông điệp:

Tách một chuỗi bit ngẫu nhiên: thực hiện tách một chuỗi bit từ ảnh đã được nhúng bởi chức năng "giấu theo tỷ lệ".

Tên hàm: [str_message]=LSB_extract(image_name,tile,name_output)

Các tham số đầu vào:

image_name: tên ảnh cần tách tin.

tile: tỷ lệ nhúng tin.

name_output: tên ảnh sau khi tách tin**.**

Các tham số đầu ra:

M: Mảng bit tách được

Tách chuỗi thông điệp nhúng: thực hiện tách một chuỗi thông điệp từ ảnh đã được nhúng bởi chức năng "giấu chuỗi ký tự".

Tên hàm: thongdiep=tach_chuoi(image_name,name_output)

Các tham số đầu vào:

image_name: tên ảnh cần tách tin.

name_output: tên ảnh sau khi tách tin**.**

Các tham số đầu ra:

thongdiep: thông điệp tách được.

Tách file văn bản *.txt: Tách chuỗi thông điệp và lưu vào file *.txt

Tên hàm: [str_message]=tach_thongdiep(image_name,name_output)

Các tham số đầu vào:

image_name: tên ảnh cần tách tin.

name_output: tên ảnh sau khi tách tin**.**

Các tham số đầu ra:

Str_message: mảng bit chứa chuỗi thông điệp sau khi tách

Phát hiện ảnh có giấu tin: chức năng kiểm tra tỉ lệ nhúng tin của một ảnh đua vào

Tên hàm: tile=phathien_DH(image_name)

Các tham số đầu vào:

Image_name: tên ảnh cần kiểm tra.

Các tham số đầu ra:

Tile: tỉ lệ nhúng tin của ảnh.

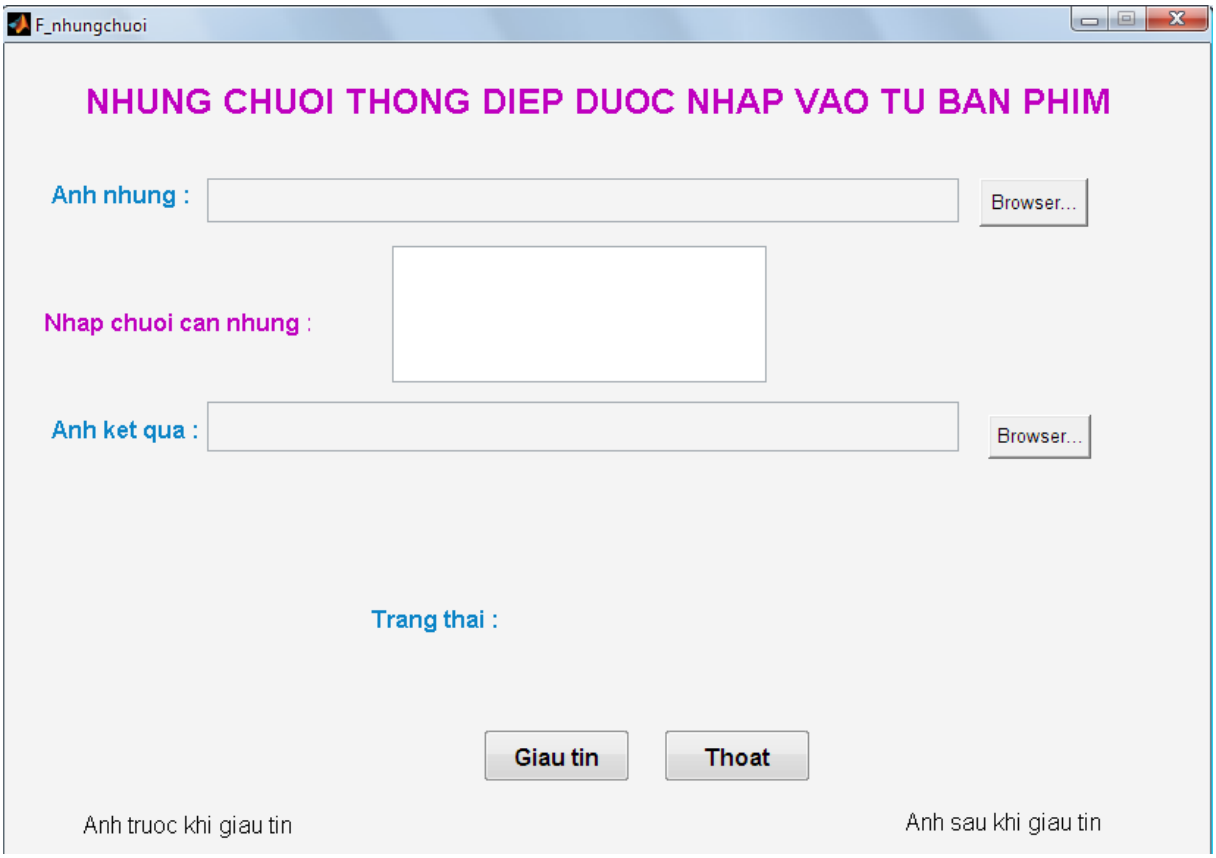
Hình 5.2 Giao diện các chức năng giấu tin LSB chương trình chính.

Hình 5.3 Giao diện các chức năng tách tin của chương trình chính

Hình 5.4 Giao diện chức năng phát hiện ảnh có giấu tin

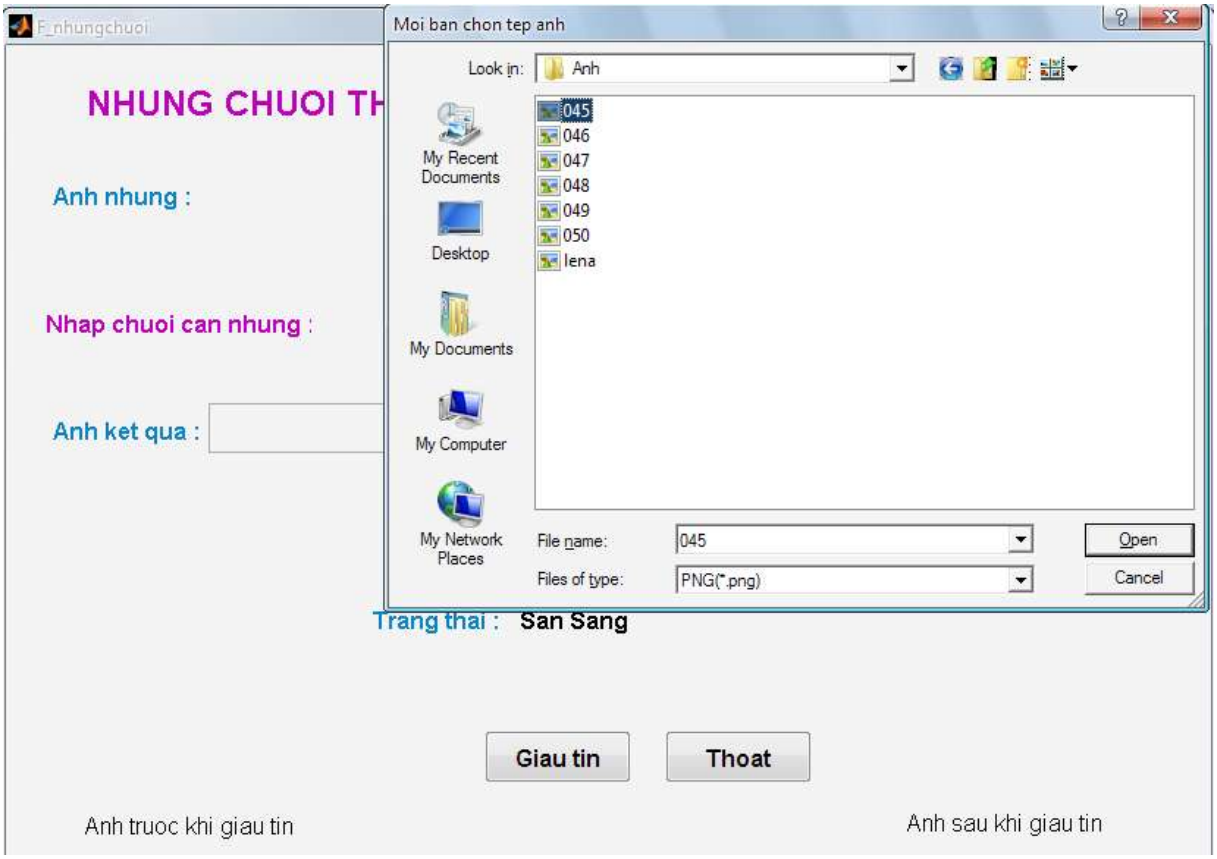
5.2.2 Giao diện chi tiết các modul của chương trình

5.2.2.1 Giao diện chi tiết chức năng một modul giấu tin.



Hình 5.5 Giao diện giấu một chuỗi kỳ do người dùng nhập vào từ bàn phím

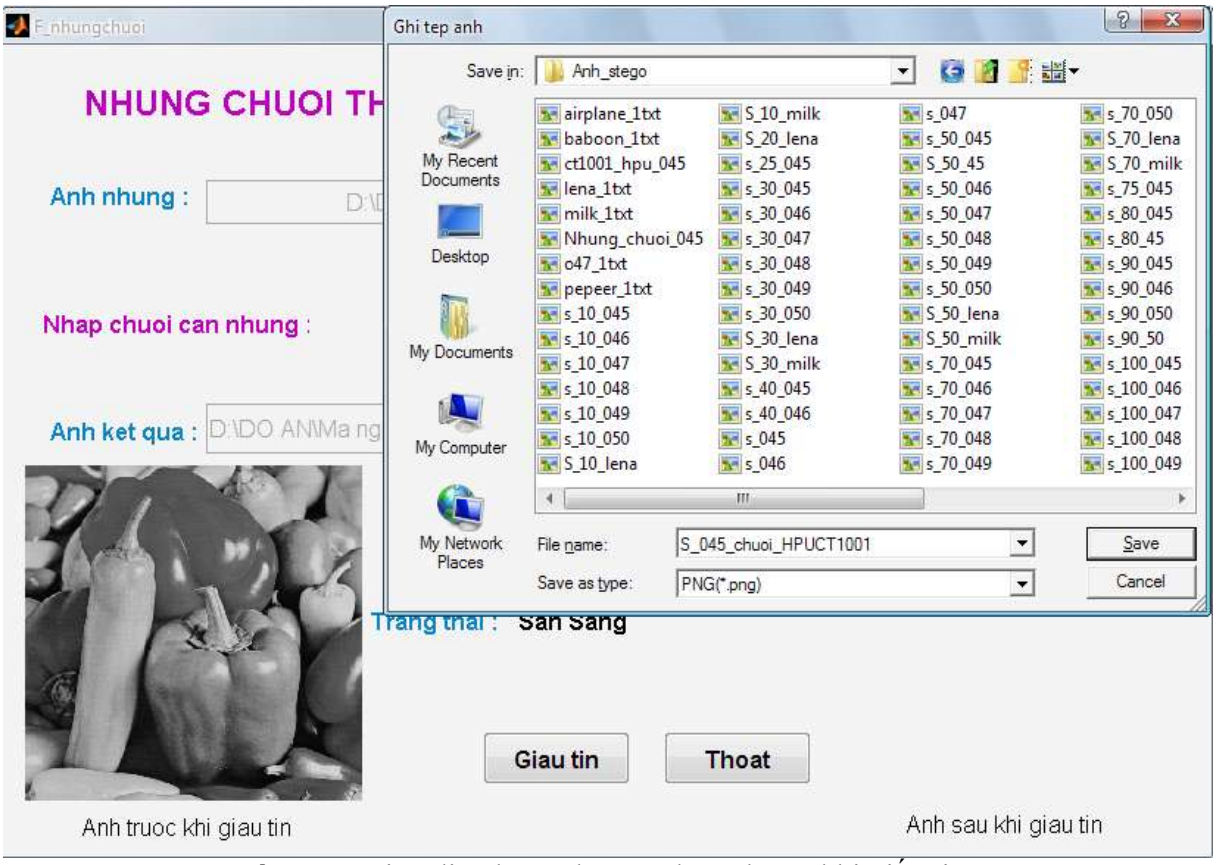
Từ giao diện modul nhúng chuỗi thong điệp được nhậ vào từ bàn phím ta chọn vào "Browser" để tìm ảnh cần giấu, và nhập vào chuỗi thong điệp cần giấu.



Hình 5.6 Giao diện bước chọn ảnh cần giấu tin.

Hình 5.7 Giao diện bước nhập thong điệp cần giấu.

Chọn nơi lưu ảnh kết quả và đặt tên cho ảnh sau khi giấu



Hình 5.8 Giao diện bước đặt tên cho ảnh sau khi giấu tin.

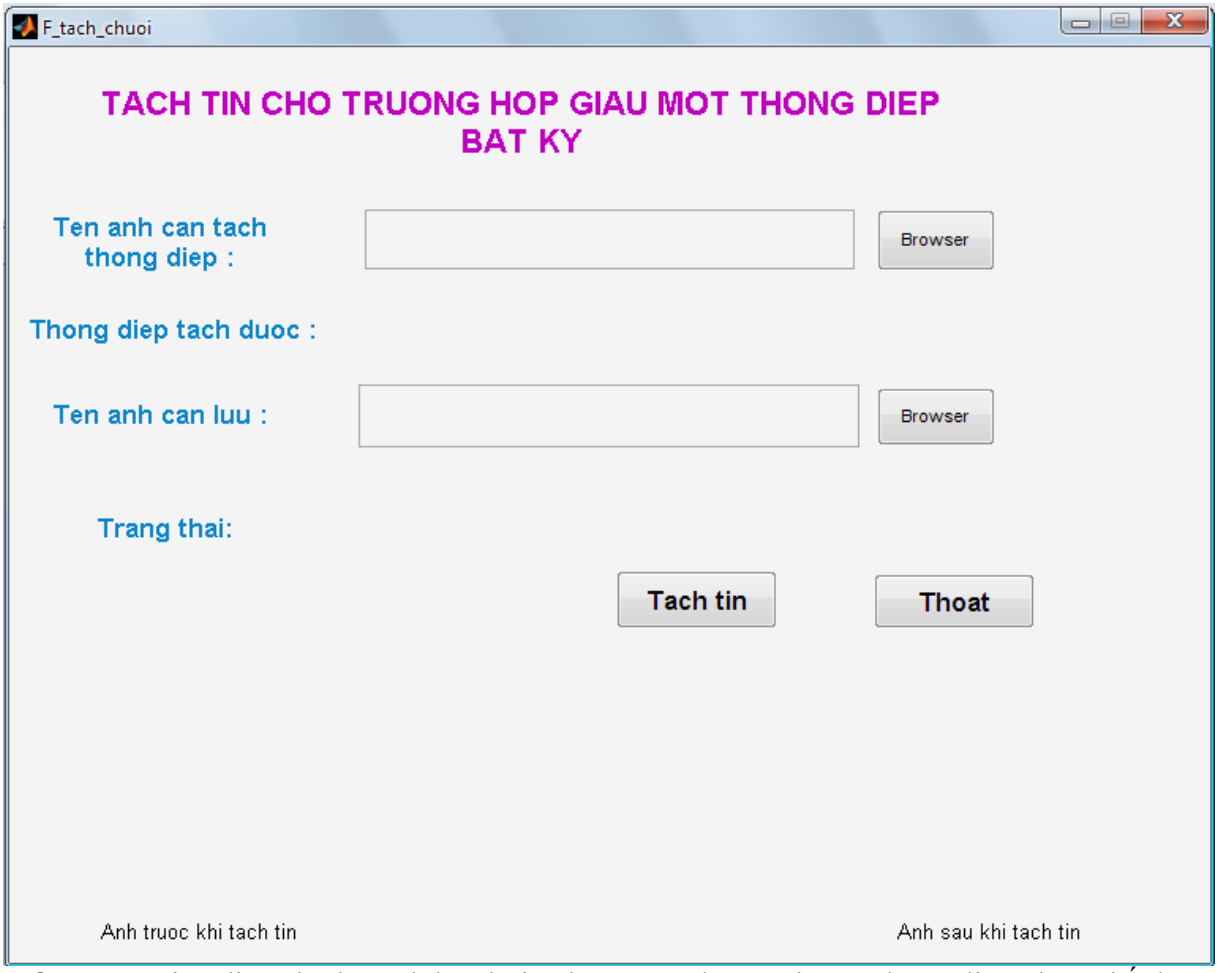
Hình 5.9 Giao diện quá trình nhúng tin

Click vào nút “giau tin” để bắt đầu quá trình giấu tin như trong hình 5.9.

Hình 5.10 Trạng thái sau khi nhúng tin xong.

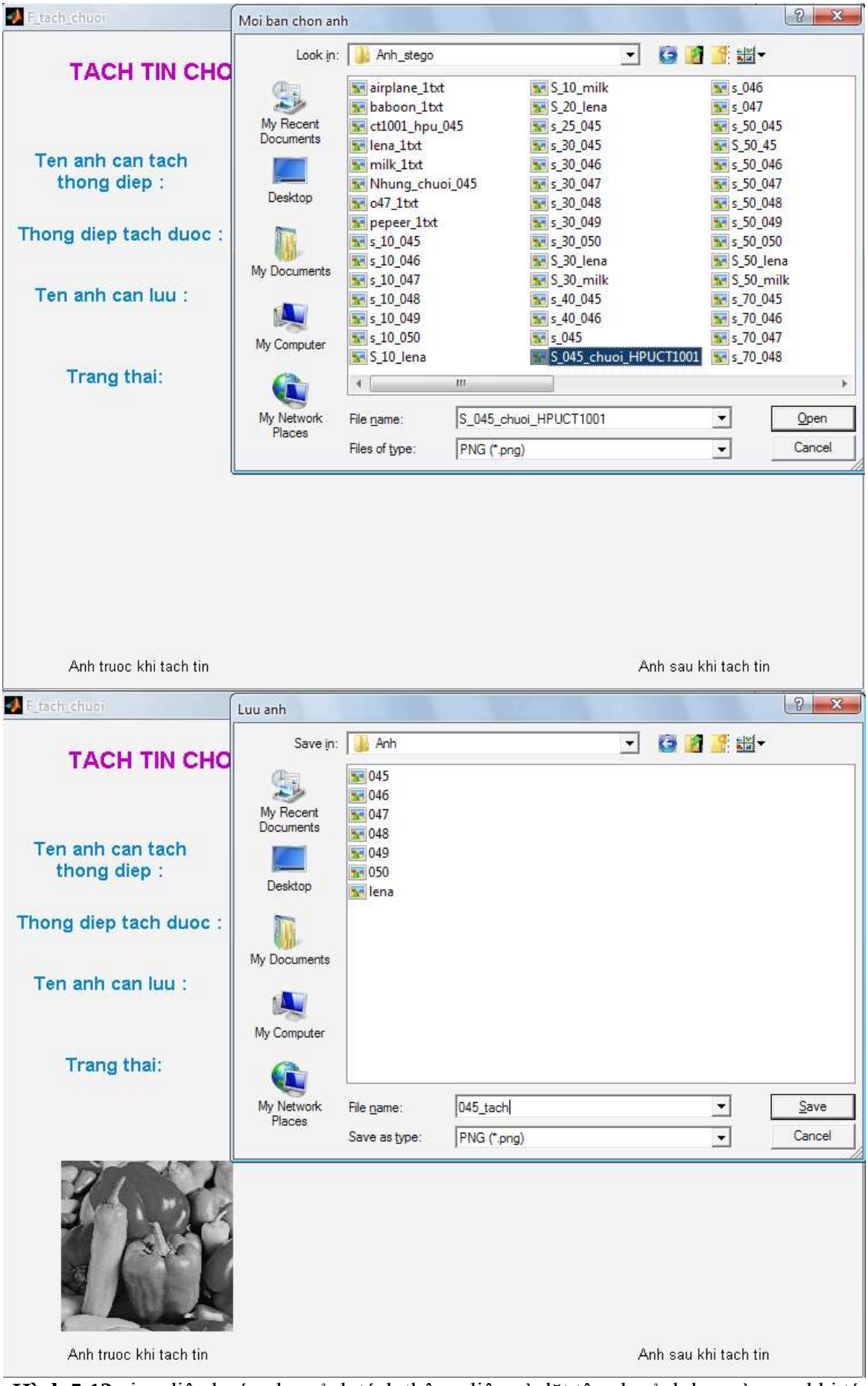
Để thoát khỏi giao diện nhúng tin ta click vào nút “thoat”.

5.2.2.2 giao diện một chi tiết một chức năng của modul tách tin.



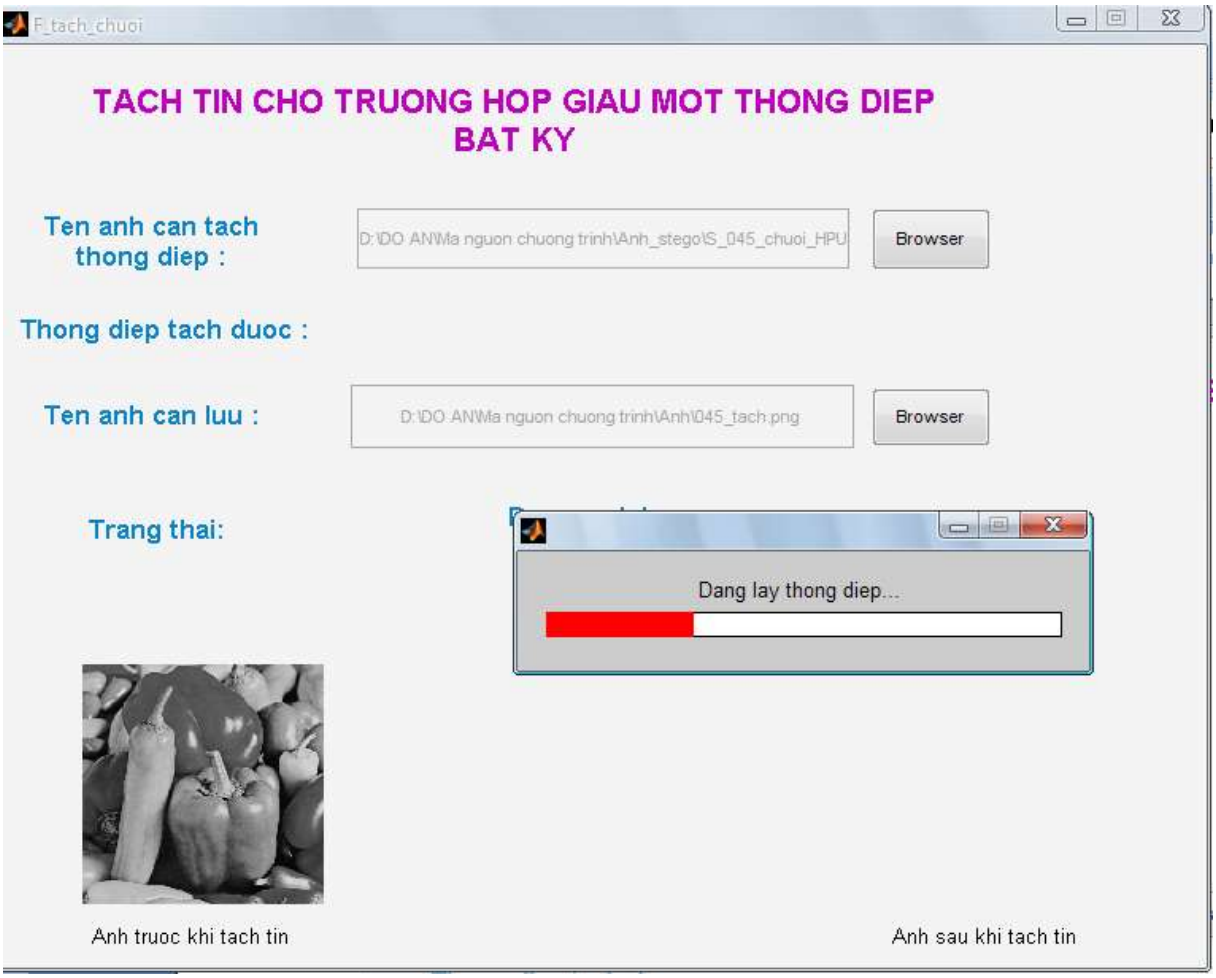
Hình 5.11 giao diện chính modul tách tin cho trường hợp tách một thông điệp nhúng bất kỳ.

Từ giao diện chính của modul, chon "Browser" để chọn ảnh càn tách thông điệp, chọn nơi lưu ảnh và đặt tên cho ảnh sau khi tách tin.

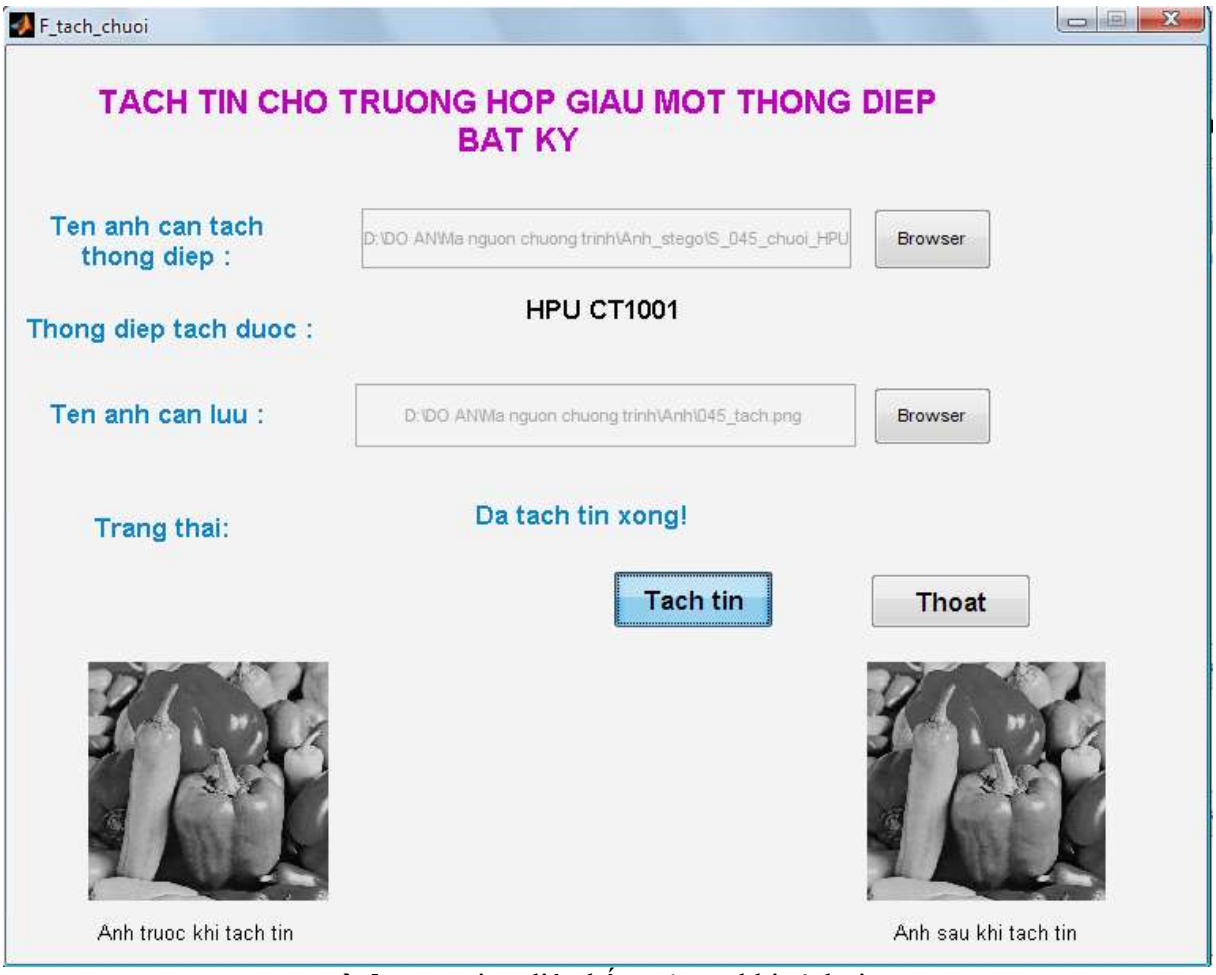


Hình 5.12 giao diện bước chọn ảnh tách thông điệp và đặt tên cho ảnh lưu vào sau khi tách.

Chọn “Tach tin” để bắt đầu thực hiện quá trình tách tin.



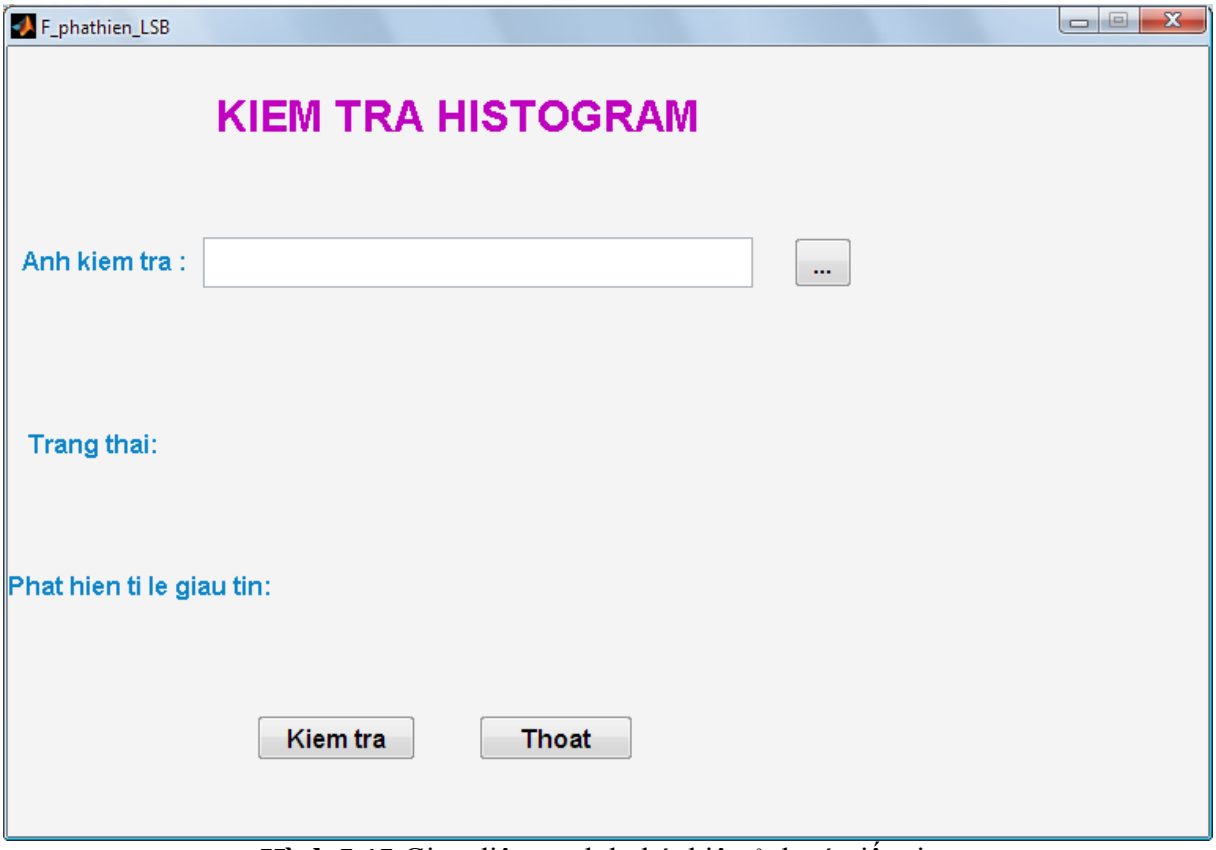
Hình 5.13 Quá trình tách tin.



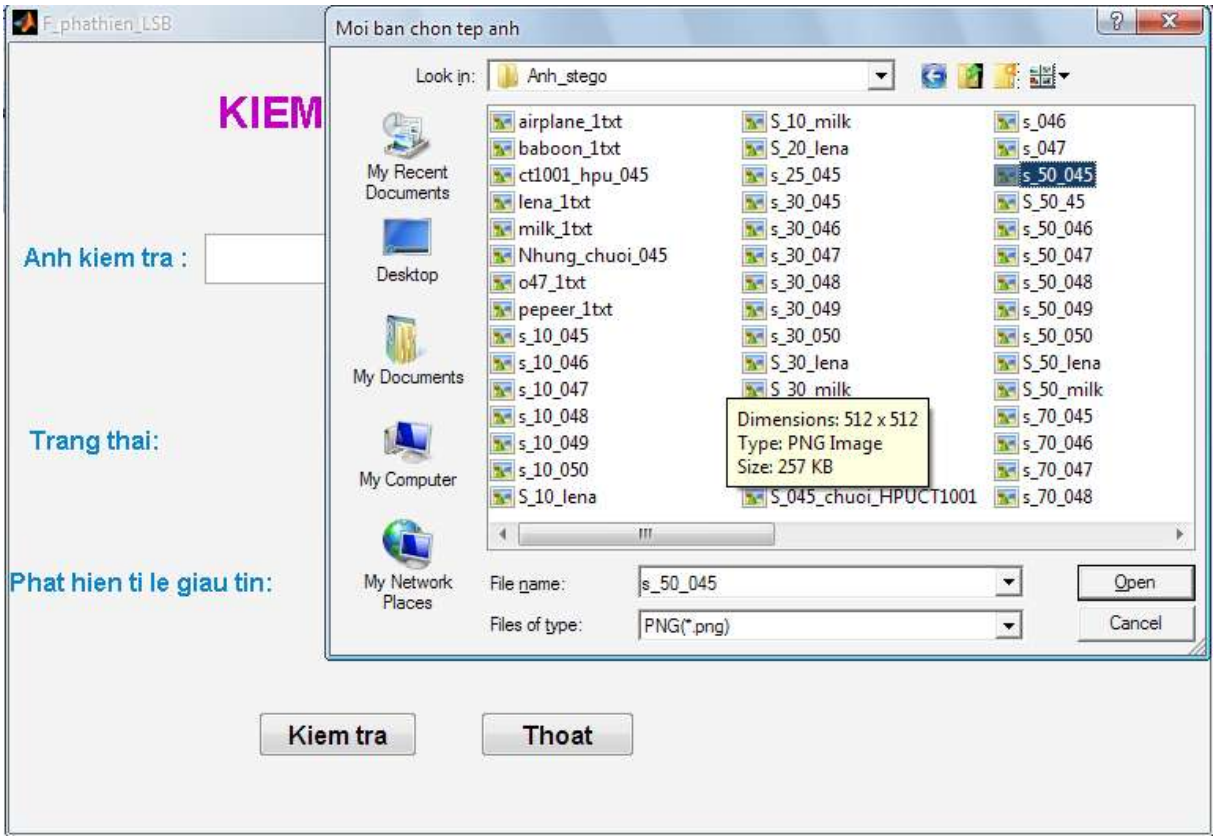
Hình 5.14 giao diện kết quả sau khi tách tin.

Để thoát khỏi giao diện chương trình tách tin chọn nút "Thoat".

5.2.2.3 Giao diện chi tiết modul kiểm tra ảnh có giấu tin



Hình 5.15 Giao diện modul phát hiện ảnh có giấu tin.



Hình 5.16 Giao diện bước chọn ảnh để kiểm tra.

Chọn ảnh cần kiểm tra.

Sau khi chọn ảnh cần kiểm tra, chọn nút "Kiem tra" để bắt đầu thực hiện kiểm tra tỉ lệ giấu tin trong ảnh.

Hình 5.17 Kết quả kiểm tra.

5.3 Kết quả thử nghiệm.

Tập ảnh thử nghiệm gồm có 6 ảnh chuẩn (airplane, baboon, beer, lena, peppers, tiffany)

Hình 5.18 tập ảnh thử nghiệm

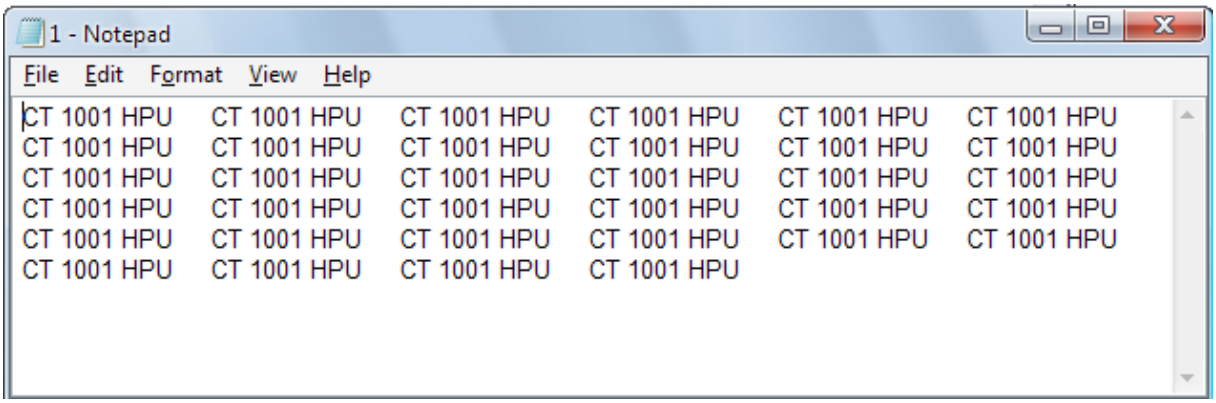
Hình 5.19 Một số ảnh tải về từ Internet

Và một số ảnh có kích cỡ tùy ý tải về từ mạng Internet

Sử dụng chương trình thực hiện giấu thông điệp cho 2 trường hợp:

Giấu theo tỷ lệ nhúng : 0%, 10%, 30%, 50%, 70%, 100%

Giấu thông điệp từ một tệp văn bản.



Hình 5.19 Tệp văn bản 1.txt được dùng làm thử nghiệm

Sau đó sử dụng chương trình phát hiện tỉ lệ nhúng ***p*** cho mỗi ảnh với mỗi trường hợp.

Bảng 5.1 Kết quả kiểm tra tỉ lệ nhúng.

	peppers	milk	lena	tiffany	baboon	airplane
0%	6	26	12	9	-22	6
10%	18	37	27	17	-29	15
30%	34	41	44	34	-36	40
50%	48	56	51	47	38	52
70%	64	67	81	75	60	68
100%	97	93	91	86.7	83	85

Bảng 5.2 Kết quả kiểm tra ảnh được nhúng tệp văn bản

	peppers	milk	lena	tiffany	baboon	airplane
1.txt	9	28	14	10	-27	8

5.4 Đánh giá kỹ thuật phát hiện theo F-measure

5.4.1 Độ đo đánh giá

Trong những thử nghiệm này, em sử dụng các độ đo đánh giá là: *precision, recall và f-measure* thường được áp dụng trong phân loại dữ liệu. *Precision* là độ đo tính chính xác và đúng đắn của việc phân loại. *Recall* là độ đo tính toàn vẹn của việc phân lớp.

Cụ thể cho bài toán phân loại ảnh có giấu tin và ảnh chưa giấu tin, giả sử ta có một tập ảnh đầu vào E (gồm cả ảnh giấu tin và ảnh chưa giấu tin) cần phân thành 2 tập con E_1 (ảnh có giấu tin) và E_2 (ảnh không giấu tin). Sau khi thực hiện phân lớp chúng ta được bảng sau:

		Kết quả phân lớp đúng	
		E_1	E_2
Kết quả phân lớp đạt được	E_1	tp (true positive)	fp (false positive)
	E_2	fn (false negative)	tn (true negative)

Khi đó precision và recall được tính toán theo công thức sau:

$$\text{Precision} = \frac{tp}{tp + fp} \qquad \textbf{(5.1)}$$

$$\text{Recall} = \frac{tp}{tp + fn} \qquad \textbf{(5.2)}$$

Mặc dù *precsion* và *recall* là những độ đo được dùng rộng rãi và phổ biến nhất, nhưng chúng lại gây khó khăn khi phải đánh giá các bài toán phân loại vì hai độ đo trên lại không tăng/giảm tương ứng với nhau. Bài toán đánh giá có *recall* cao có thể có *precision* thấp và ngược lại. Hơn nữa, việc so sánh mà chỉ dựa trên một mình precision và *recall* không phải là một ý hay. Với mục tiêu này, độ đo *F-measure* được sử dụng để đánh giá tổng quát các bài toán phân loại. *F-measure* là trung bình điều hoà có trọng số của *precision* và *recall* và có công thức:

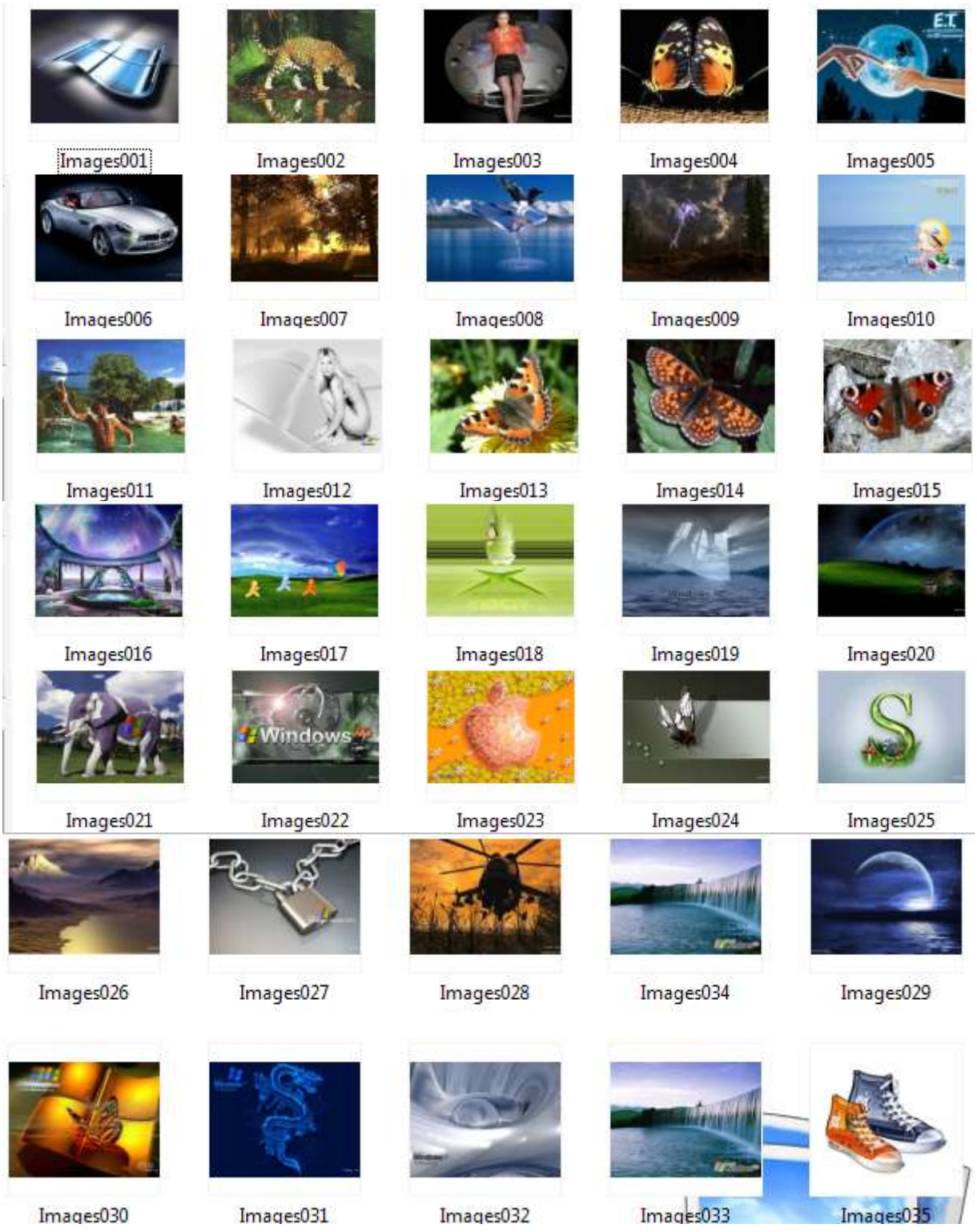
$$F_\beta = (1 + \beta^2) \cdot \frac{precision.recall}{\beta^2.precision + recall}$$

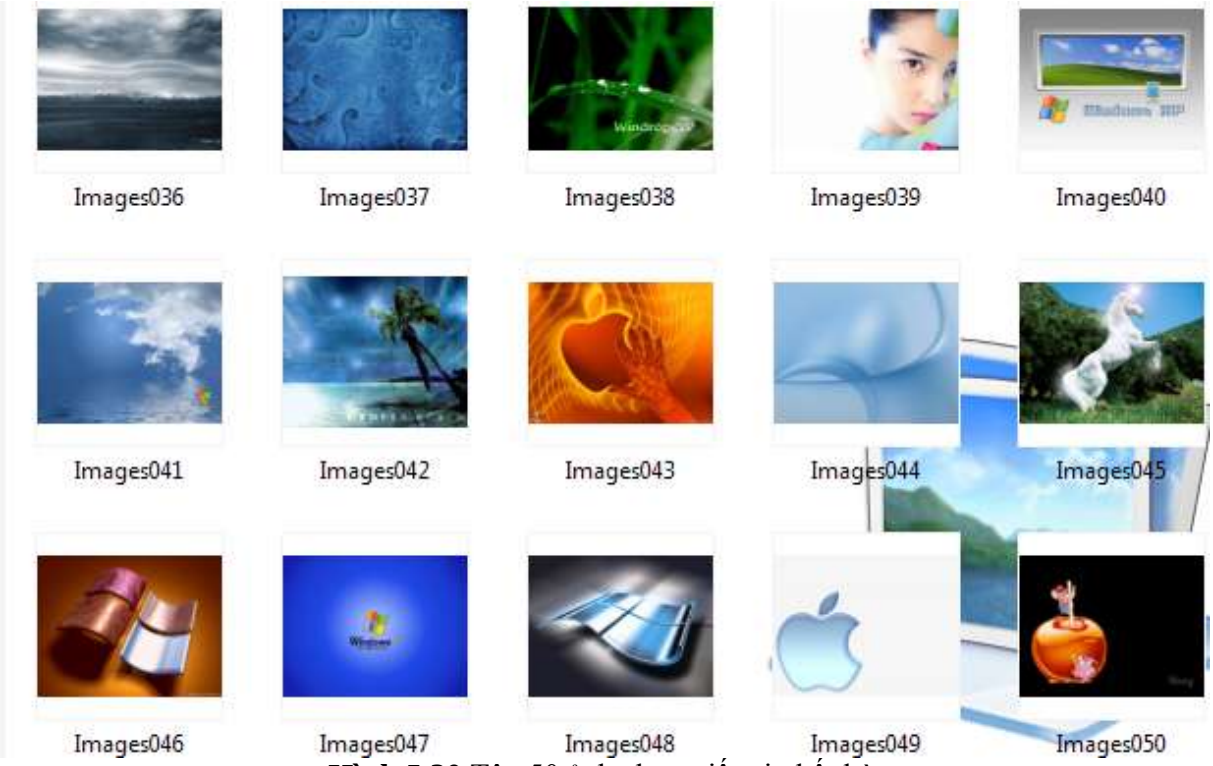
trong đó β là một tham số có giá trị nằm giữa 0 và 1. Nếu β = 1, *F-measure* bằng với precision và nếu β = 0, *F-measure* bằng với *recall*. Giữa đoạn đó, giá trị β càng cao, độ quan trọng của *precision* càng cao so với *recall*. Ta sử dụng giá trị thường được dùng là β = 0.5, nghĩa là:

$$F = 2.\frac{precision.recall}{precision + recall} \qquad \textbf{(5.3)}$$

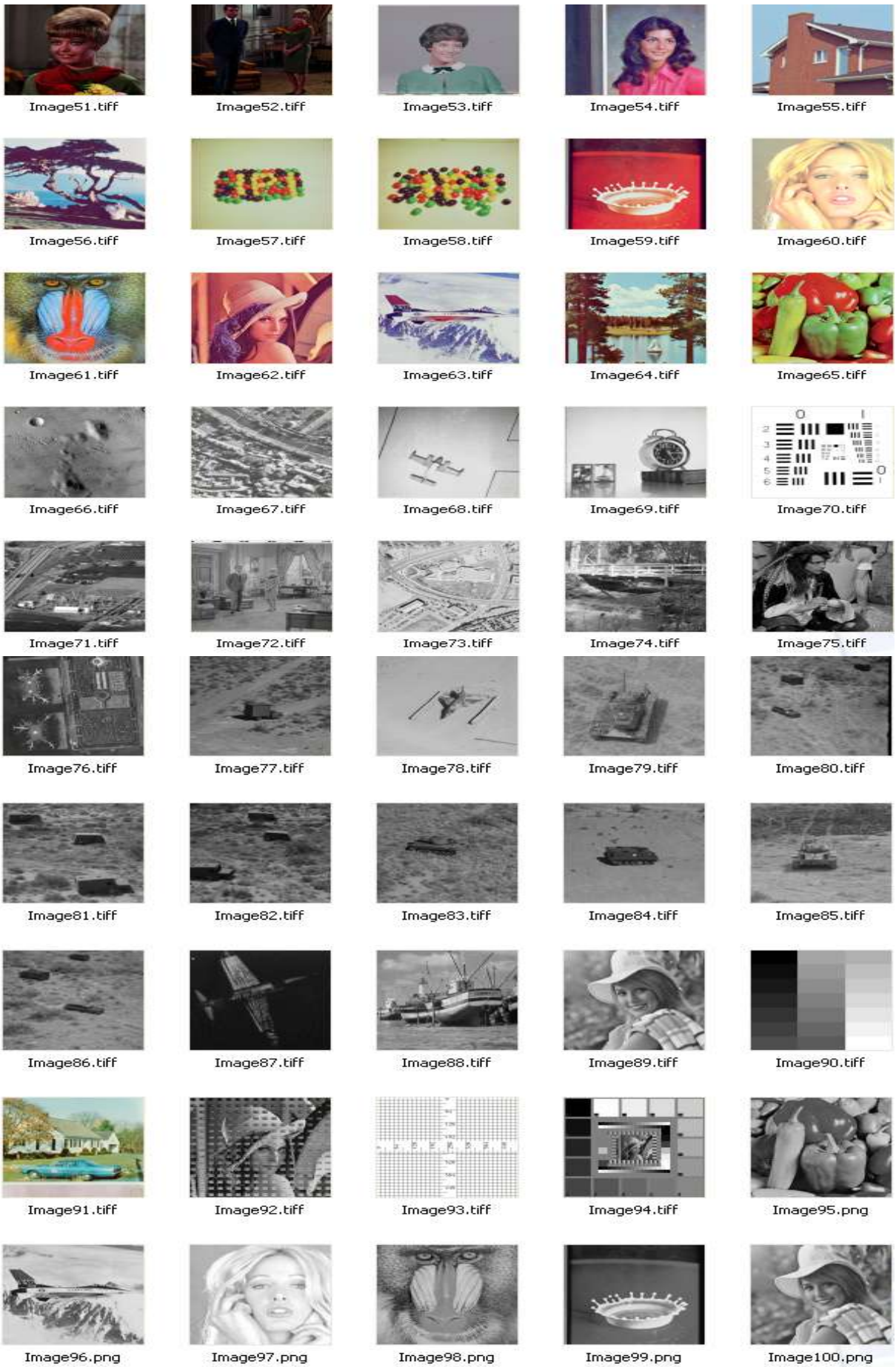
5.4.2 Kết quả thử nghiệm

Tập ảnh thử nghiệm D1 gồm 50 ảnh chưa giấu tin kích cỡ 800x600 (từ Image01.jpg đến Image50.jpg), kích thước tùy ý và D2 gồm 50 ảnh dùng để giấu tin với lượng giấu 50%, 100% .





Hình 5.20 Tập 50 ảnh chưa giấu tin bất kỳ



Hình 5.21 Tập 50 ảnh có giấu tin ngẫu nhiên 50% hoặc 100%.

Chọn tập ảnh D50_percent gồm 100 ảnh trong đó có 50 ảnh không giấu tin (D1) và 50 ảnh có giấu tin với lượng giấu 50% (D2). Một tập ảnh khác D100_percent gồm 100 ảnh với 50 ảnh chưa giấu (D1) và 50 ảnh có giấu với lượng giấu 100% (D2).

Sau đó dùng kỹ thuật phát hiện trên tập thử nghiệm này ta thu được kết quả như bảng 5.3:

Bảng 5.3 Bảng kết quả thử nghiệm trên hai tập ảnh D50_percent và D100_percent

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image01.jpg	F (False)	F
Image02.jpg	F	F
Image03.jpg	T (True)	T
Image04.jpg	T	T
Image05.jpg	F	F
Image06.jpg	T	T
Image07.jpg	F	F
Image08.jpg	F	F
Image09.jpg	T	T
Image10.jpg	F	F
Image11.jpg	F	F
Image12.jpg	T	T
Image13.jpg	T	T
Image14.jpg	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image15.jpg	F	F
Image16.jpg	T	T
Image17.jpg	T	T
Image18.jpg	F	F
Image19.jpg	T	T
Image20.jpg	F	F
Image21.jpg	T	T
Image22.jpg	T	T
Image23.jpg	T	T
Image24.jpg	F	F
Image25.jpg	T	T
Image26.jpg	T	T
Image27.jpg	F	F
Image28.jpg	T	T
Image29.jpg	F	F
Image30.jpg	F	F
Image31.jpg	F	F
Image32.jpg	F	F

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image33.jpg	T	T
Image34.jpg	T	T
Image35.jpg	F	F
Image36.jpg	T	T
Image37.jpg	T	T
Image38.jpg	F	F
Image39.jpg	T	T
Image40.jpg	T	T
Image41.jpg	F	F
Image42.jpg	T	T
Image43.jpg	T	T
Image44.jpg	F	F
Image45.jpg	T	T
Image46.jpg	T	T
Image47.jpg	T	T
Image48.jpg	F	F
Image49.jpg	T	T
Image50.jpg	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image51.tiff	T	T
Image52.tiff	T	T
Image53.tiff	T	T
Image54.tiff	T	T
Image55.tiff	F	T
Image56.tiff	T	T
Image57.tiff	T	T
Image58.tiff	T	T
Image59.tiff	F	T
Image60.tiff	T	T
Image61.tiff	F	T
Image62.tiff	T	T
Image63.tiff	T	T
Image64.tiff	T	T
Image65.tiff	F	T
Image66.tiff	T	T
Image67.tiff	T	T
Image68.tiff	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image69.tiff	T	T
Image70.tiff	F	T
Image71.tiff	T	T
Image72.tiff	T	T
Image73.tiff	T	T
Image74.tiff	T	T
Image75.tiff	T	T
Image76.tiff	T	T
Image77.tiff	F	T
Image78.tiff	T	T
Image79.tiff	T	T
Image80.tiff	T	T
Image81.tiff	T	T
Image82.tiff	F	T
Image83.tiff	T	T
Image84.tiff	T	T
Image85.tiff	T	T
Image86.tiff	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image87.tiff	T	T
Image88.tiff	T	T
Image89.tiff	T	T
Image90.tiff	T	T
Image91.tiff	F	T
Image92.tiff	T	T
Image93.tiff	F	T
Image94.tiff	F	T
Image95.tiff	T	T
Image96.png	T	T
Image97.png	T	T
Image98.png	T	T
Image99.png	T	T
Image100.png	T	T

Sau đó ta dùng các độ đo đánh giá là: *Precision, Recall và F-measure* để phân loại ảnh có giấu tin và ảnh chưa giấu tin. Sau khi thực hiện phân lớp trên hai tập thử nghiệm D50_percent và D100_percent ta được kết quả như bảng 5.4 và bảng 5.5.

Bảng 5.4 Tổng hợp kết quả từ bảng 5.3 của tập thử nghiệm D50_percent

		Kết quả phân lớp đúng	
		D1	D2
Kết quả phân lớp đạt được	D1	29	21
	D2	10	40

Áp dụng công thức (5.1) và (5.2) và (5.3) ta có:

$$\text{Precision} = \frac{29}{29+21} = 0.58$$

$$\text{Recall} = \frac{29}{29+10} = 0.74$$

$$\text{F - measure} = 2 * \frac{0.58 * 0.74}{0.58 + 0.74} = 0.65$$

Bảng 5.5 Tổng hợp kết quả từ bảng 5.3 của tập thử nghiệm D100_percent

		Kết quả phân lớp đúng	
		D1	D2
Kết quả phân lớp đạt được	D1	29	21
	D2	0	50

Áp dụng công thức (5.1), (5.2) và (5.3) ta có:

$$\text{Precision} = \frac{29}{29+21} = 0.58$$

$$\text{Recall} = \frac{29}{29+0} = 1$$

$$\text{F - measure} = 2 * \frac{0.58 * 1}{0.58 + 1} = 0.73$$

Bảng 5.5 Bảng thử nghiệm trên hai tập ảnh D50_percent và D100_percent

Độ đo / Kỹ thuật	Precision	Recall	F-measure
Kỹ thuật phát hiện cho lượng giấu 50%	0.58	0.74	0.65
Kỹ thuật phát hiện cho lượng giấu 100%	0.58	1	0.73

5.4.3 Nhận xét

Nếu dùng tỉ lệ nhúng ***p=0%*** làm mốc để kiểm tra ảnh có mang tin hay không thì với phương pháp phát hiện trong nghiên cứu này không được chính xác. Bởi vì ý tưởng của thuật toán phát hiện được sử dụng ở đây là so sánh tương quan sai khác giữa các biểu đồ tần số sai khác của ảnh. Đối với những ảnh chuẩn trong thực nghiệm thì biểu đồ tần số sai khác của ảnh là đối xứng nhau qua gốc tọa độ, nhưng trong thực tế thì tùy vào ảnh thường thì nó không cân bằng giữa số điểm ảnh tối và điểm ảnh sang nên biểu đồ tần số sai khác của ảnh là không đối xứng nhau. Vì thế cho nên kết quả độ đo đánh giá đạt được ở đây là không cao.

Qua nhiều lần thử nghiệm em thấy có những ảnh môi trường (cover images) khi kiểm tra đã có tỉ lệ nhúng tin rất cao p>20%, thông thường thì là p≈10%. Vì vậy chỉ nhìn vào kết quả tỉ lệ giấu tin p>0% đưa ra mà kết luận ảnh giấu tin thì kết quả không được như ta mong đợi. Giải pháp đưa ra ở đây là so sánh giữa tỉ lệ kiểm tra được với tỉ lệ giấu thu được của ảnh môi trường (cover image).

KẾT LUẬN

Phát hiện thông tin ẩn giấu trong dữ liệu đa phương tiện, đặc biệt là trong ảnh số là một vấn đề đang được quan tâm hiện nay trong nhiều lĩnh vực. Để phát hiện và phân biệt một ảnh số nào đó có mang tin mật hay không đòi hỏi rất nhiều yếu tố và kỹ thuật phức tạp.

Trong đồ án này đã đưa ra một cái nhìn tổng quan về giấu tin trên miền LSB và phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu LSB.

Trong thời gian làm đồ án em đã nghiên cứu được những vấn đề sau:

- Nghiên cứu tổng quan kỹ thuật giấu tin trong ảnh.
- Nghiên cứu cấu trúc ảnh BITMAP và PNG.
- Tìm hiểu chi tiết kỹ thuật giấu tin trên miền LSB của ảnh.
- Nghiên cứu kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu LSB.
- Cài đặt và thử nghiệm bằng matlab 2007b.

Trong quá trình làm đồ án, do kiến thức còn thiếu sót, hạn chế về thời gian nên việc nghiên cứu đề tài không thể tránh khỏi những thiếu sót. Rất mong nhận được sự đóng góp ý kiến của các thầy, cô và toàn thể các bạn đồng môn để báo cáo của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

[1] T.Zhangand X.Ping, "Reliable detection of LSB steganography based on the difference image histogram", IEEE International Conferenceon Acoustics, Speech, and Signal Processing, Volume3, April2003, pp.545-548.

[2] Đỗ Thị Nguyệt, Đồ án tốt nghiệp, ngành Công nghệ thông tin, năm 2009

[3] Vũ Văn Tập, Đồ án tốt nghiệp ngành Công nghệ thông tin, năm 2010

[4] Fridrich, M.Goljan, R.Du, "Detecting LSB Steganography in Color and Gray-Scale Images", IEEE Multimedia, October-November issue, 2001, pp.

[5] J.Fridrich, M.Goljanand R.Du, "Detecting LSB Steganography in Color and Grayscale Images", IEEE, vol.8(4) Multimedia, October – December 2001, pp. 22-28.

[6] of Reversible Contrast Mapping Watermarking, proceedings of the world congress on engineering 2008 Vol I WCE 2008, London, UK.

[7] J.Fridrich, M.Goljan, R.Du, "Reliable detection of LSB Steganography in grayscale and color images", Proceeding of ACM, Special Sessionon Multimedia Securityand Watermarking, Ottawa, Canada, 2001, pp. 27-30.

[8] CBIR Image Database, University of Washington,
http://www.cs.washing