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 đã tận tình giúp đỡ em rất nhiều trong suốt quá trình tìm hiểu nghiên cứu và hoàn thành báo cáo tốt nghiệp.

Em xin chân thành cảm ơn các thầy cô trong bộ môn tin còn 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 chân thành cảm ơn các bạn trong và ngoài lớp đã động viên và tạo điều kiện thuận lợi cho em trong quá trình làm báo cáo thực tập.

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 hết mực và động viên em.

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

Em xin chân thành cảm ơn!

Hải phòng ngày 10 tháng 7 năm 2010

Sinh viên

Vũ Văn Tập

LỜI MỞ ĐẦU

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. Tuy nhiên nó cũng làm tăng nguy cơ sử dụng trái phép, 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 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 phần nào giải quyết được các 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 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.

MỤC LỤC

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 (Steganoeraphy)

1.1.1 Định nghĩa kỹ thuật giấu tin

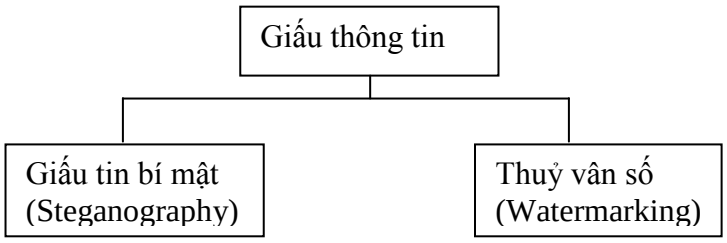
Giấu thông tin là một kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác (giấu thông tin chỉ mang tính quy ước không phải là một hành động cụ thể).

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.



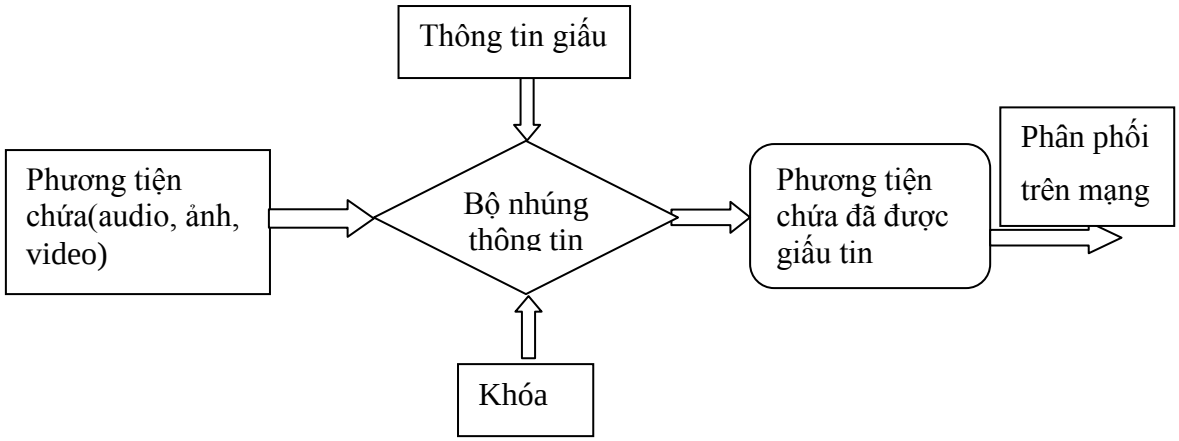
Hình 1.1. Hai lĩnh vực chính của kỹ thuật giấu thông tin

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 không phát hiện được.

Kỹ thuật giấu thông tin theo kiểu đánh giấu (watermarking) để bảo vệ bản quyền của đối tượng chứa thông tin thì lại 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.

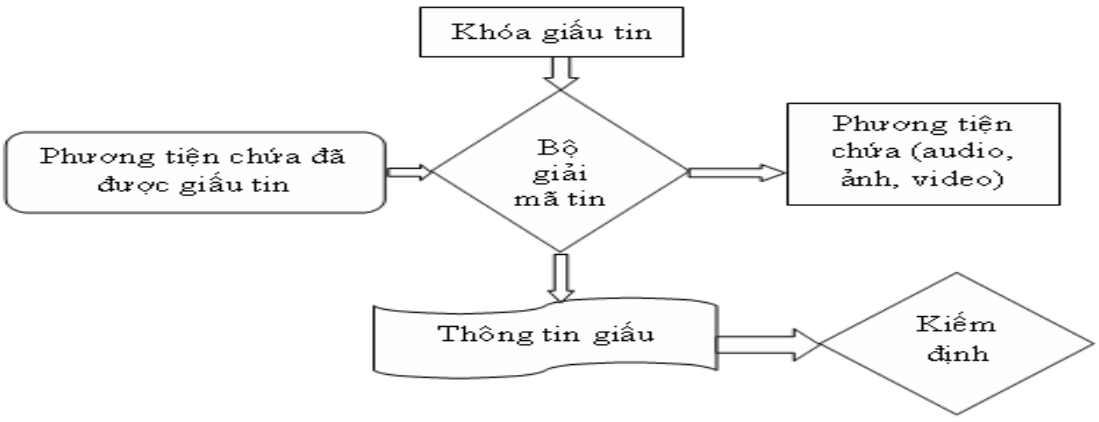
- Phương tiện chứa: các file ảnh, text, audio… là môi trường để nhúng tin.

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 Một số đặc diểm của việc giấu thông 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.

1.1.6.1 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 trước 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.

1.1.6.2 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.

1.1.6.3 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.*

1.1.6.4 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.

1.1.6.5 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.

1.2 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 multimedia. Giống như thám mã, mục đích của Steganalysis là phát hiện ra thông tin ẩn và phá vỡ tính bí mật của vật mang tin ẩn.

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 0A 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: NGHIÊN CỨU KỸ THUẬT GIẤU TIN DỰA VÀO LƯỢC ĐỒ THỦY VÂN RCM (REVERSIBLE CONTRAST MAPPING)

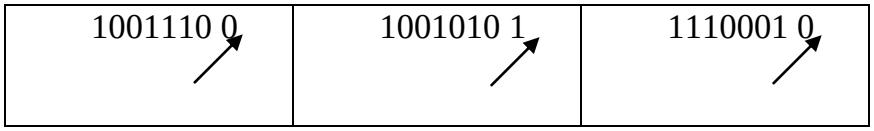
Kỹ thuật giấu tin sử dụng kỹ thuật giấu RCM [7] do Coltuc và các đồng nghiệp đưa ra vào tháng 4 năm 2007. Kỹ thuật giấu này nhanh và giấu được lượng thông tin lớn. Nó chỉ giấu thông tin trong những cặp điểm ảnh của ảnh thuộc miền RCM, do đó cung cấp khả năng khôi phục lại ảnh gốc một cách hoàn hảo.

3.1 Các khái niệm cơ bản

3.1.1 Khái niệm về bit có trọng số thấp (LSB - Least Significant Bit):

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. Ví dụ với ảnh 256 màu thì bit cuối cùng trong 8 bit biểu diễn một điểm ảnh được coi là bit ít quan trọng nhất, nghĩa là nếu thay đổi bit này thì ảnh hưởng ít nhất đến cảm nhận của mắt người về điểm ảnh. Hay 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 ta sẽ tách bit này ra ở mỗi điểm ảnh để giấu tin… Như vậy kỹ thuật tách bit trong xử lý ảnh được sử dụng rất nhiều trong qui trình giấu tin.

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



Hình 3.1 Mỗi điểm ảnh bểu 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, hay 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

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

3.1.2 Phép biến đổi RCM

Cho 1 ảnh có t-bit và (a, b) là 1 cặp điểm ảnh. Phép biến đổi RCM được định nghĩa như sau:

$$\begin{cases} a' = 2a - b \\ b' = 2b - a \end{cases} \quad \textbf{(3.1)}$$

Cặp điểm ảnh (a,b) thuộc miền RCM ((a, b) Є RCM) nếu:

$$\begin{cases} 0 \le a' \le 2^t - 1 \\ 0 \le b' \le 2^t - 1 \end{cases} \quad \textbf{(3.2)}$$

3.2 Thuật toán RCM

3.2.1 Ý tưởng thuật toán

- Cho thông điệp nhúng W. W có thể là:
  - Một chuỗi bit 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 = Viet Nam → phải đổi W sang hệ nhị phân).
  - Ảnh 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.
- Giấu thông_điệp vào tất cả các cặp điểm ảnh (a, b) thuộc miền RCM.

3.2.2 Thuật toán giấu tin gồm có 2 bước:

+ Bước 1: Chia dữ liệu ảnh thành các cặp theo chiều quét tùy ý (trên hàng, trên cột)

+ Bước 2: Đối với mỗi cặp (a, b):

  - Nếu (a, b) ∈ RCM, và LSB của chúng không phải là (1,1) (nghĩa là LSB của chúng thuộc {(0,1), (1,0),(0,0)}) biến đổi cặp này sử dụng công thức (3.1) ta được (a', b'), đặt LSB của a' là "1", và đặt bit thông điệp vào LSB của b'.
  - Nếu (a,b) ∈ RCM và LSB của chúng là (1,1) , đặt LSB của a là "0" và đặt bit thông điệp vào LSB của b.

- Nếu (a, b) không thuộc RCM, đặt LSB của a là "0", LSB ban đầu của a được coi như là bit thông điệp và nhúng vào trong ảnh (nghĩa là bit này sẽ được nối vào chuỗi thông điệp để nhúng tiếp vào ảnh).

3.2.3 Thuật toán tách thông điệp và khôi phục ảnh gốc

a. Ý tưởng thuật toán

- Chia dữ liệu ảnh thành các cặp theo chiều quét tùy ý (trên hàng, trên cột).
- Tách tất cả các bit LSB của các cặp điểm ảnh theo chiều quét.
- Từ chuỗi bit LSB tách được, tiến hành tách lấy độ dài của thông điệp (24 bit đầu tiên).
- Có được độ dài thông điệp, ta tiến hành tách lấy thông điệp gốc và khôi phục ảnh gốc.

b. Thuật toán tách và khôi phục ảnh gốc

+ Bước 1: Chia dữ liệu ảnh thành các cặp theo chiều quét tùy ý (trên hàng, trên cột).

+ Bước 2: Đối với mỗi cặp (a', b'):

- Nếu LSB(a') = 1, trích LSB của b' và lưu trữ. Thiết lập LSB(a') và LSB(b') = 0 sau đó khôi phục cặp điểm ảnh gốc (a, b) theo công thức:

$$\begin{cases} a = \left\lceil \frac{2}{3}a' + \frac{1}{3}b' \right\rceil \\ b = \left\lceil \frac{1}{3}a' + \frac{2}{3}b' \right\rceil \end{cases} \quad \textbf{(3.3)}$$

- Nếu LSB(a') = 0 và LSB của a', b' sau khi thiết lập bằng 1 mà thuộc miền RCM thì trích LSB(b'), lưu trữ và khôi phục cặp điểm ảnh gốc (a, b) chính là (a', b') sau khi LSB của chúng được thiết lập bằng 1.
- Nếu LSB(a') = 0 và LSB của a', b' sau khi thiết lập bằng 1 mà không thuộc miền RCM, cặp điểm ảnh gốc sẽ được khôi phục bằng cách thay thế LSB(a') với giá trị thực được trích từ thủy vân**.**

CHƯƠNG 4: KỸ THUẬT PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU RCM

Kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RCM [7] do Coltue và các đồng nghiệp đưa ra. Ý tưởng của kỹ thuật này dựa vào xác suất xuất hiện của các bit ít đặc trưng nhất (bit LSB).

4.1 Phân tích vấn đề an toàn của kỹ thuật RCM

Cho 1 ảnh O, chia dữ liệu ảnh thành các cặp điểm ảnh (x, y). Theo phép biến đổi RCM (Chương 3, phần 3.1.2), chúng ta chia cặp điểm ảnh của O thành hai bộ là:

- Bộ S_{RCM} gồm tất cả các cặp điểm ảnh thuộc miền RCM.
- Bộ $S_{\overline{RCM}}$ chứa các cặp điểm ảnh không thuộc miền RCM.

Chúng ta tiến hành kiểm tra sự thay đổi của biểu đồ LSB của lược đồ thủy vân RCM. Không làm mất tính tổng quát, cho (x, y) và $(\bar{x}, \bar{y})$ lần lượt tương ứng với cặp điểm ảnh trong ảnh gốc và ảnh sau khi giấu tin. Chúng ta phải chú ý đến ba quy tắc đánh dấu của lược đồ thủy vân RCM.

Trong cách chọn đánh dấu thứ nhất, (x, y) thuộc S_{RCM} và LSB của (x, y) là một trong các giá trị {(0, 0), (0, 1), (1, 0)}. Cho thấy dữ liệu LSB của ảnh gốc là được phân bổ một cách ngẫu nhiên, ba giá trị được đề cập ở trên sẽ xảy ra với xác suất giống nhau. Rất dễ để tính toán được xác suất của bit 0 và 1 lần lượt là 2/3 và 1/3. Trong trường hợp này, LSB của $(\bar{x}, \bar{y})$ là (1, 0) hoặc (1, 1) và xác suất xuất hiện của chúng là giống nhau. Hiển nhiên, xác suất của bit 0 và 1 lần lượt là 1/4 và 3/4.

Trong cách chọn thứ hai, (x, y) thuộc S_{RCM} và LSB của (x, y) là (1, 1). Xác xuất của bit 0 và 1 lần lượt là 0.0 và 1.0. Trong trường hợp này, LSB của $(\bar{x}, \bar{y})$ là (0, 0) hoặc (0, 1) và xác suất xuất hiện của chúng là giống nhau. Xác suất bit 0 và 1 của $(\bar{x}, \bar{y})$ lần lượt là 3/4 và 1/4.

Trong cách chọn thứ ba, (x, y) thuộc $S_{\overline{RCM}}$ và LSB của (x, y) là 1 trong các giá trị {(0, 0), (0, 1), (1, 0), (1, 1)}. Trong trường hợp này, xác suất bit 0 và 1 của (x, y)

lần lượt là 1/2 và 1/2. Giống với trường hợp hai, LSB của ($\bar{x}$, $\bar{y}$) là (0, 0) hoặc (0, 1). Xác suất bit 0 và 1 của ($\bar{x}$, $\bar{y}$) lần lượt là 3/4 và 1/4.

Dựa vào sự bàn luận ở trên, xác suất của bit 0 và 1 trong LSB của lược đồ thủy vân RCM của ảnh sau khi giấu tin có thể được tính toán. Giả sử xác suất của cặp điểm ảnh thuộc RCM và xác suất của cặp điểm ảnh không thuộc RCM lần lượt là P_{RCM} và $P_{\overline{RCM}}$, P_E là tỉ lệ nhúng. Xác suất LSB của bit b={0, 1} của ảnh sau khi giấu tin có thể được tính toán nhờ sử dụng công thức E_q sau:

$$P_{LSB}(b) = \begin{cases} P_E \times (0.375 \times P_{RCM} + 0.75 \times P_{\overline{RCM}}) + P_{\overline{E}} \times 0.5, \\ \qquad if \quad b = 0, \\ P_E \times (0.625 \times P_{RCM} + 0.25 \times P_{\overline{RCM}}) + P_{\overline{E}} \times 0.5, \\ \qquad if \quad b = 1. \end{cases} \tag{4.1}$$

Cho 1 ảnh môi trường, giả sử LSB được phân bổ một cách ngẫu nhiên, sau đó coi P(0) = P(1), ví dụ $P_{LSB}(0) = P_{LSB}(1) = 0.5$. Để ý ví dụ nhúng sau của thủy vân RCM. Giả sử xác suất nhúng của 1 ảnh là $P_{RCM} = 0.9$ và một nửa của tổng số cặp điểm ảnh có thể giấu tin được sử dụng để nhúng thông điệp, cho tỉ lệ nhúng $P_E = 0.9x0.5 = 0.45$. Từ E_q (3) chúng ta có:

$P_{LSB}(0) = 0.45x(0.375x0.9+0.75x0.1)+0.55x0.5 = 0.460625$

$P_{LSB}(1) = 1- 0.460625 = 0.539375.$

Chúng ta có thể nhìn thấy sự xuất hiện khác nhau của bit 0 và 1 trong LSB của lược đồ thủy vân RCM của ảnh sau khi giấu tin đối với ảnh gốc. Dựa trên nhận xét này, quy tắc sau được đưa ra để phân biệt một ảnh sau khi giấu tin từ một ảnh môi trường.

$$W(\bar{x}) = \begin{cases} true, if \left| P_{LSB}(0) - P_{LSB}(1) \right| > \delta, \\ \qquad false, otherwise. \end{cases} \tag{4.2}$$

Trong công thức (4.2), một ảnh được phát hiện là được đánh dấu bằng phương pháp thủy vân RCM nếu giá trị tuyệt đối $\left| P_{LSB}(0) - P_{LSB}(1) \right| > \delta$ ($0 \le \delta \le 1$), δ là một ngưỡng được sử dụng để kiểm soát biên giới quyết định của ảnh môi trường và ảnh thủy vân. Giá trị của δ có thể được đánh giá thông qua việc phân tích ảnh sau khi giấu tin và có thể được chọn để phù hợp yêu cầu cho từng ứng dụng cụ thể.

Để thấy được tính khả thi của phương pháp đã đề xuất, tác giả bài báo lấy 500 ảnh từ CSDL ảnh CBIR [8] và biến đổi chúng trong định dạng 8-bit cấp xám. Các ảnh được chia làm hai nhóm, nhóm một gồm 250 ảnh được sử dụng trong thí nghiệm một và nhóm hai gồm 250 ảnh còn lại được sử dụng trong thí nghiệm hai. Thông điệp nhúng sử dụng trong các thí nghiệm được tạo ra bằng cách sinh số giả ngẫu nhiên.

Trong thí nghiệm một, tác giả nhúng lượng thông tin khác nhau sử dụng kỹ thuật RCM và quan sát sự biến đổi của lược đồ LSB trong ảnh sau khi giấu tin. Các tỷ lệ nhúng 0%, 25%, 50%, 75% và 100% được sử dụng trong thí nghiệm và thu được giá trị $\left| PLSB(0) - PLSB(1) \right|$ của ảnh sau khi giấu tin.

Trong thí nghiệm hai, tác giả đánh giá chính xác phương pháp đề ra trong việc phát hiện thủy vân RCM trong các tỉ lệ nhúng khác nhau và ngưỡng δ. Từ dữ liệu trong bảng 4.1, chúng ta thấy rằng khi ngưỡng $\delta = 0.03$, chúng ta thu được kết quả khả quan nhất trong việc phát hiện thủy vân RCM.

Bảng 4.1 Sự phát hiện chính xác của phương pháp được đề ra dưới những tỷ lệ nhúng khác nhau và các giá trị giới hạn δ.

δ Embedding ratio (%)	0.01	0.02	0.03	0.04	0.05
0	60.4%	66.8%	71.2%	74.8%	77.2%
25	93.2%	84.8%	75.2%	58.4%	37.2%
50	99.6%	98.8%	95.2%	91.6%	88.8%
75	100%	100%	99.6%	99.6%	99.6%
100	100%	100%	100%	100%	100%

4.2 Kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RCM

+ Đầu vào: cho một ảnh bất kỳ có kích cỡ (H x W).

+ Xử lý:

- Tính tong_pixel_cua_anh = (H * W)/2
- B1: Tách toàn bộ LSB của ảnh.
- B2: Đếm trên toàn bộ LSB của ảnh xem có bao nhiêu LSB= =0 gán vào biến Sum_LSB_0.
- B3: Đếm trên toàn bộ LSB của ảnh xem có bao nhiêu LSB= = 1 gán vào biến Sum_LSB_1.
- B4: Tính xác suất xuất hiện của bit 0 là:

  P_0=Sum_LSB_0/tong_pixel_cua_anh.

- B5: Tính xác suất xuất hiện của bit 1 là:

  P_1= Sum_LSB_1/tong_pixel_cua_anh.

- B6: Tính abs(P_0 – P_1) và so sánh với $\delta = 0.03$ (sử dụng công thức 4.2):

  Nếu abs(P_0 – P_1) ≤ 0.03: ảnh không giấu tin.

  Ngược lại, abs(P_0 – P_1) > 0.03: ảnh có giấu tin.

+ Đầu ra: Kết luận ảnh có giấu tin hay không?

CHƯƠNG 5: CÀI ĐẶT VÀ THỰC NGHIỆM

5.1 Môi trường cài đặt

- Ngôn ngữ cài đặt: là ngôn ngữ lập trình Matlab 2007b.
- Môi trường soạn thảo: Matlab 2007b.
- Môi trường chạy chương trình: môi trường giao diện Matlab 2007b.

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 thông điệp:

- Giấu một chuỗi bit ngẫu nhiên: thực hiện giấu một chuỗi bit được sinh ngẫu nhiên có độ dài do người dùng nhập vào.

Tên hàm: Loi=giau_ngau_nhien(image_name,L_message,name_output)

+ Các tham số đầu vào:
    - image_name: tên ảnh cần giấu tin.
    - L_message: độ dài chuỗi bit ngẫu nhiên
    - name_output: tên ảnh sau khi giấu tin
+ Các tham số đầu ra:
    - Loi: các lỗi có thể xảy ra khi chạy chương trình.

- Giấu tin theo tỷ lệ nhúng: thực hiện giấu với chuỗi bit ngẫu nhiên với kích thước được tính toán theo tỷ lệ % của ảnh(tỷ lệ do người dùng nhập).

Tên hàm: [Thong_bao_co_loi] = giau_tylenhung (cover_image_name,tln, name_output)

+ Các tham số đầu vào:
    - cover_image_name: tên ảnh cần giấu tin.
    - tln: tỷ lệ nhúng tin.
    - name_output: tên ảnh sau khi giấu tin**.**
+ Các tham số đầu ra:
    - Thong_bao_co_loi: các lỗi có thể xảy ra khi chạy chương trình.

- Giấu một chuỗi bất kì: thực hiện giấu một chuỗi thông điệp do người dùng nhập vào.

Tên hàm: Thong_bao_loi = giau_1chuoi (cover_image_name, str_message, name_output)

+ Các tham số đầu vào:
    - cover_image_name: tên ảnh cần giấu tin.
    - str_message: thông điệp nhúng.
    - name_output: tên ảnh sau khi giấu tin
+ Các tham số đầu ra:
    - Thong_bao_co_loi: các lỗi có thể xảy ra khi chạy chương trình.

- Giấu một tệp bất kì: thực hiện giấu một tệp văn bản do người dùng chọn.

Thong_bao _loi=giau_thongdiep(cover_image_name, str_message,name_output)

+ Các tham số đầu vào:
    - cover_image_name: tên ảnh cần giấu tin.
    - str_message: nội dung của tệp văn bản nhúng.
    - name_output: tên ảnh sau khi giấu tin.
+ Các tham số đầu ra:
    - Thong_bao _loi: các lỗi có thể xảy ra khi chạy chương trình.

Tách thông điệp:

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

Tên hàm: thong_diep=tach_ngau_nhien(image_name,L_message,name_output)

+ Các tham số đầu vào:
    - image_name: tên ảnh cần tách thông điệp.
    - L_message: độ dài chuỗi bit thông điệp.
    - name_output: tên ảnh sau khi tách thông điệp.
+ Các tham số đầu ra:
    - thong_diep: lưu thông điệp tách được từ ảnh đầu vào.

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

Tên hàm: bin_message=tach_tylenhung(image_name,name_output)

+ Các tham số đầu vào:
    - image_name: tên ảnh cần tách thông điệp.
    - name_output: tên ảnh sau khi tách thông điệp.
+ Các tham số đầu ra:
    - bin_message: lưu thông điệp tách được từ ảnh đầu vào.

- Tách một chuỗi bất kì: thực hiện tách một chuỗi thông điệp từ ảnh đã được nhúng bởi chức năng “giấu một chuỗi bất bì”.

function str_message=tach_1chuoi(image_name,name_output)

+ Các tham số đầu vào:
    - image_name: tên ảnh cần tách thông điệp.
    - name_output: tên ảnh sau khi tách thông điệp**.**
+ Các tham số đầu ra:
    - str_message: thông điệp tách được.

- Tách một tệp bất kì: thực hiện tách một tệp văn bản từ ảnh đã được nhúng bởi chức năng “giấu một tệp bất kì”.

Tên hàm: str_message=tach_thongdiep(image_name,name_output)

+ Các tham số đầu vào:
    - image_name: tên ảnh cần tách thông điệp.
    - name_output: tên ảnh sau khi tách thông điệp.
+ Các tham số đầu ra:
    - str_message: lưu thông điệp tách được từ ảnh đầu vào.

Phát hiện: kiểm tra một ảnh xem ảnh đó có giấu tin hay không.

Tten hàm: [ketqua,trangthai]=phathien(image_name)

+ Các tham số đầu vào:
    - image_name: tên ảnh cần kiểm tra giấu tin.
+ Các tham số đầu ra:
    - ketqua: kết luận ảnh có giấu tin hoặc không có giấu tin.
    - trangthai: các trạng thái trong quá trình phát hiện (sẵn sàng; đang kiểm tra; đã kiểm tra xong).

5.2.2 Giao diện có chi tiết các module giấu tin

Hình 5.2 Giao diện có chi tiết các module giấu tin.

5.2.3 Giao diện có chi tiết các module tách tin

Hình 5.3 Giao diện có chi tiết các module tách tin.

5.2.4 Màn hình giao diện một trường hợp giấu tin

Từ giao diện chính chương trình ta chọn menu “Giau thong diep” và chọn chức năng “Giau mot tep bat ki”.

Hình 5.4 Chọn chức năng giấu một tệp bất kì.

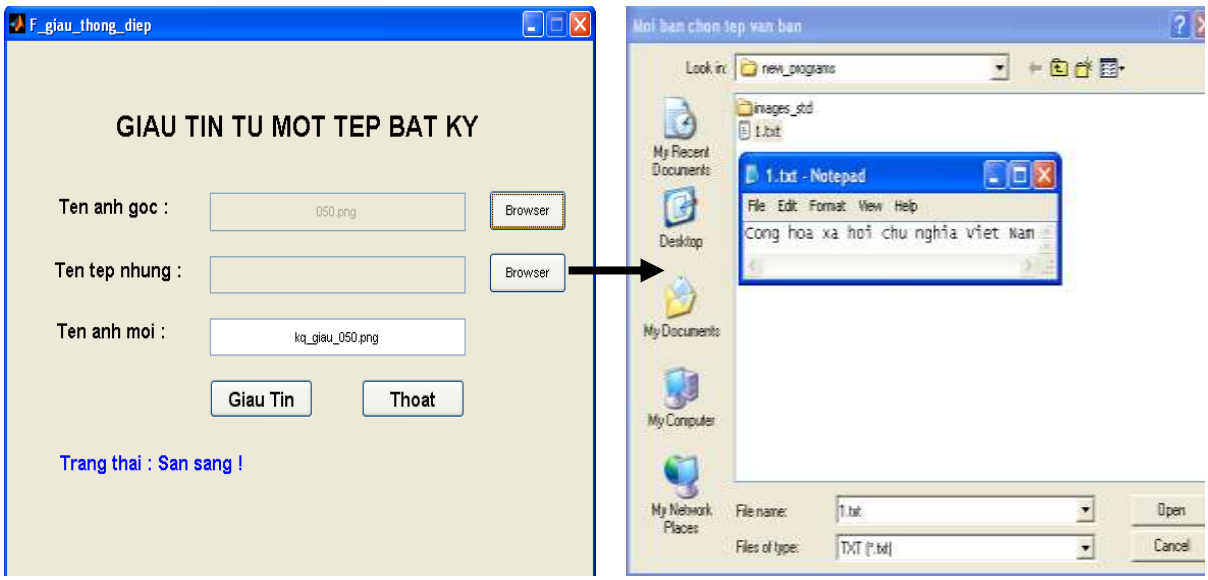
Giao diện của chức năng “Giấu một tệp bất kì”.

Hình 5.4 Giao diện chức năng giấu một tệp bất kì.

Để nhập tên ảnh cần giấu tin (Ten anh goc) ta chọn nút Browser và tiến hành chọn ảnh. Tên ảnh sau khi giấu tin (Ten anh moi) sẽ được sinh tự động sau khi chọn ảnh và người dùng có thể thay đổi trường này.

Hình 5.5 Giai đoạn chọn ảnh nhúng.

Để nhập tên tệp chứa thông điệp nhúng (Ten tep nhung) ta chọn nút Browser và tiến hành chọn tệp nhúng.



Hình 5.6 Giai đoạn chọn thông điệp nhúng.

Sau khi làm các bước trên, ta tiến hành chọn nút “Giau tin” để thực hiện chức năng giấu tin (Figure 1: ảnh trước khi giấu tin – Figure 2: ảnh sau khi giấu tin).

Hình 5.7 Giai đoạn thực hiện giấu tin

Để thoát khỏi giao diện giấu tin ta chọn nút “Thoat”.

5.2.5 Màn hình giao diện một trường hợp tách tin và khôi phục ảnh gốc

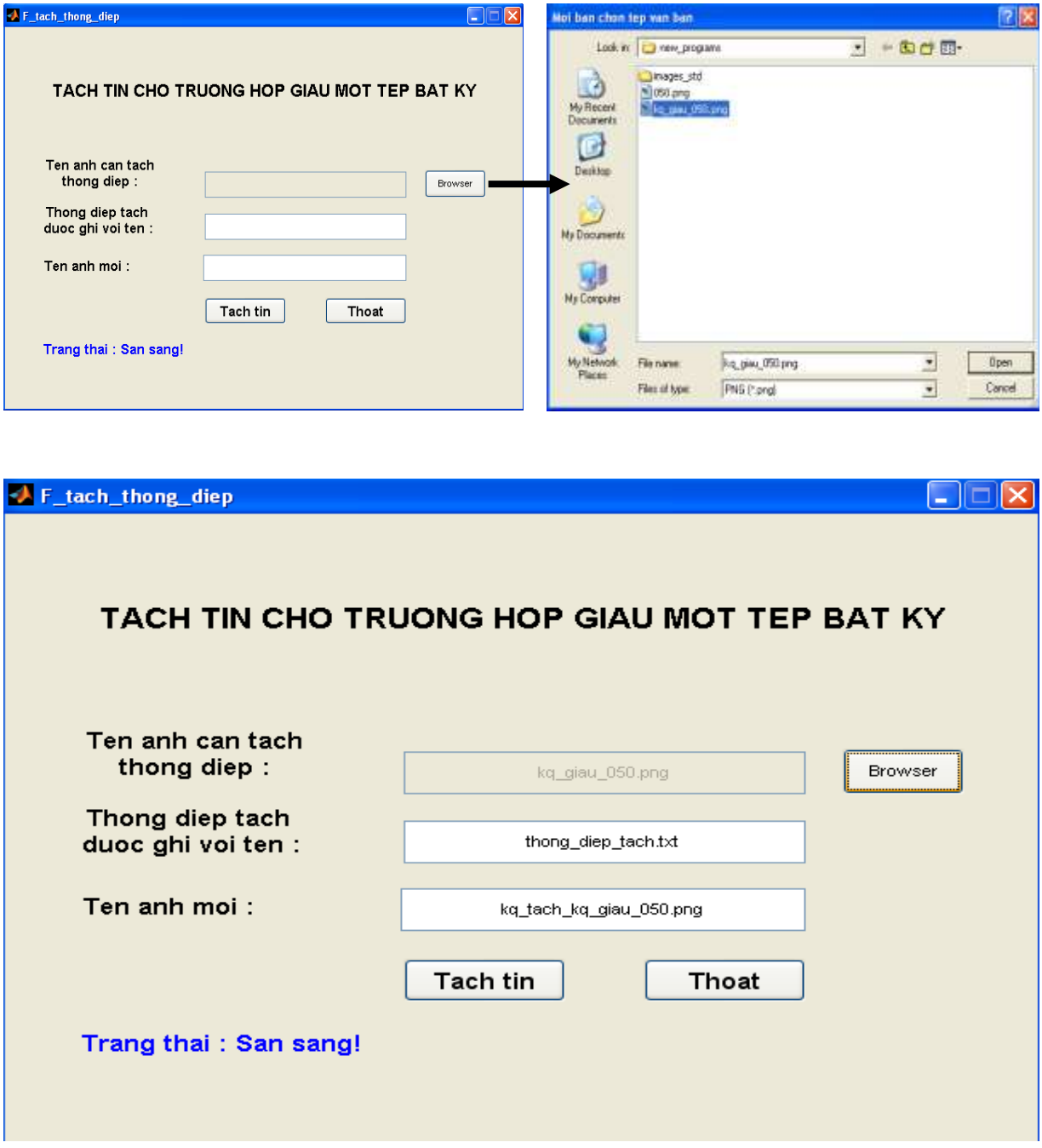
Từ giao diện chính chương trình ta chọn menu "Tach thong diep" và chọn chức năng "Tach mot tep bat ki".

Hình 5.7 Giao diện chọn chức năng tách một tệp bất kì.

Giao diện của chức năng "Tách một tệp bất kì".

Hình 5.8 Giao diện của chức năng tách một tệp bất kì.

Để nhập tên ảnh cần tách tin (Ten anh can tach thong diep) ta chọn nút Browser và tiến hành chọn ảnh. Tên ảnh sau khi tách tin (Ten anh moi) và tên tệp chứa nội dung thông điệp sau khi tách (Thong diep tach duoc ghi voi ten) sẽ được sinh tự động sau khi chọn ảnh và người dùng có thể thay đổi trường hai này.



Hình 5.9 Giai đoạn chọn ảnh cần tách tin.

Sau khi làm các bước trên, ta tiến hành chọn nút "Tach tin" để thực hiện chức năng tách thông điệp và khôi phục ảnh gốc (Figure 1: ảnh trước khi tách thông điệp – Figure 2: ảnh sau khi được khôi phục).

Hình 5.10 Giai đoạn thực hiện tách tin.

Để thoát khỏi giao diện tách thông điệp ta chọn nút "Thoat".

5.2.6 Màn hình một trường hợp kiểm tra một ảnh bất kỳ có giấu tin hay không (giao diện phát hiện ảnh có giấu tin hay không)

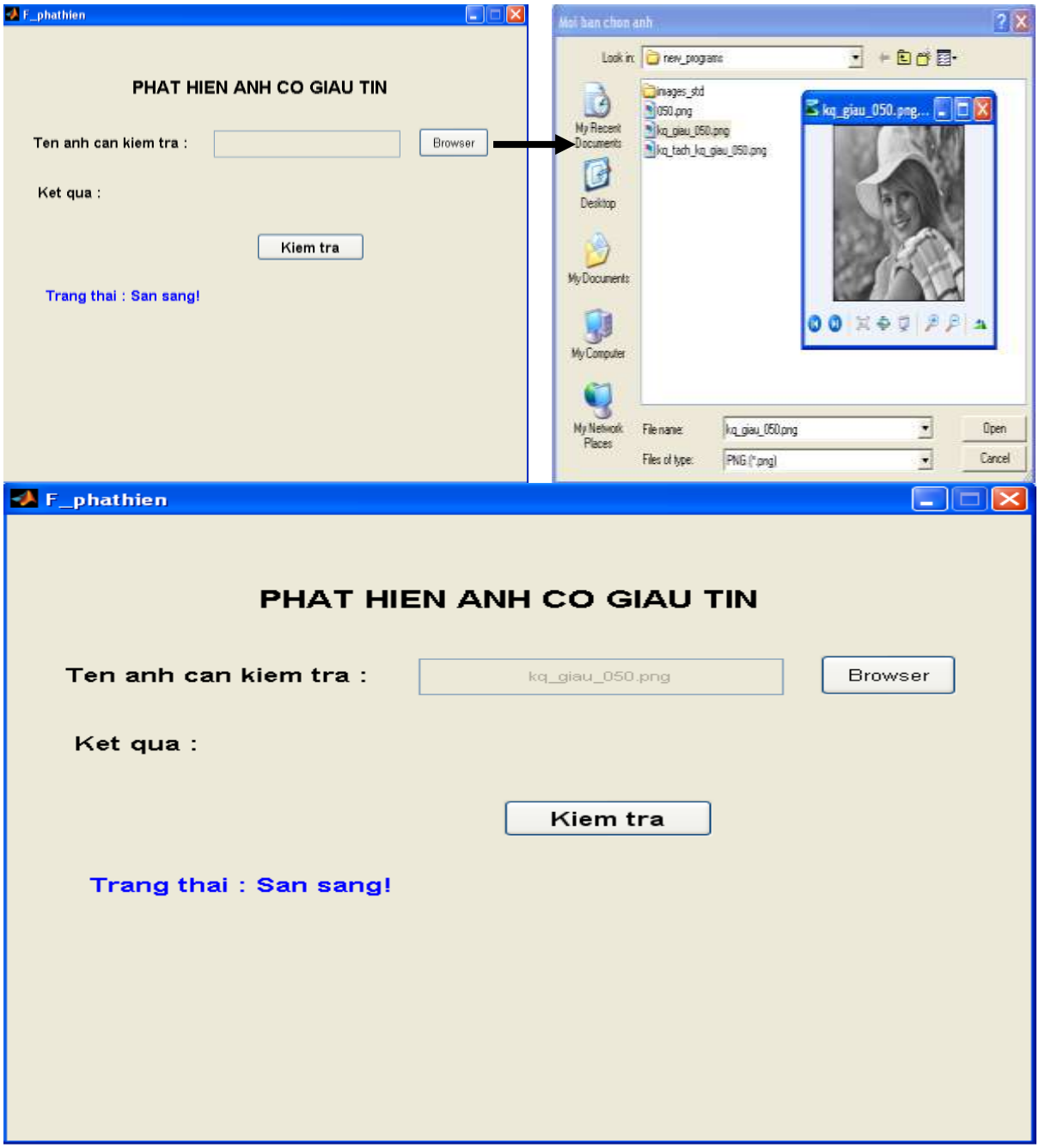
Từ giao diện chính của chương trình ta chọn menu "Phat hien" để thực hiện chức năng phát hiện ảnh giấu tin.

Hình 5.11 Giao diện chọn chức năng phát hiện ảnh giấu tin

Giao diện của chức năng "Phat hien".

Hình 5.12 Giao diện của chức năng phát hiện ảnh có giấu tin.

Để nhập tên ảnh cần kiểm tra ta chọn nút "Browser" và tiến hành chọn ảnh.



Hình 5.13 Giao diện chọn ảnh cần phát hiện.

Để thực hiện chức năng phát hiện ảnh giấu tin ta chọn nút “Kiem tra”.

Hình 5.14 Thực hiện chức năng phát hiện ảnh có giấu tin.

Để thoát khỏi giao diện “PHAT HIEN ANH CO GIAU TIN” ta chọn nút “Thoat”.

5.3. Kết quả thử nghiệm

Sử dụng 2 tập thử nghiệm:

+ Tập thử nghiệm 1 gồm 6 ảnh chuẩn (lena, baboon, airplane, tiffany, beer, peppers).

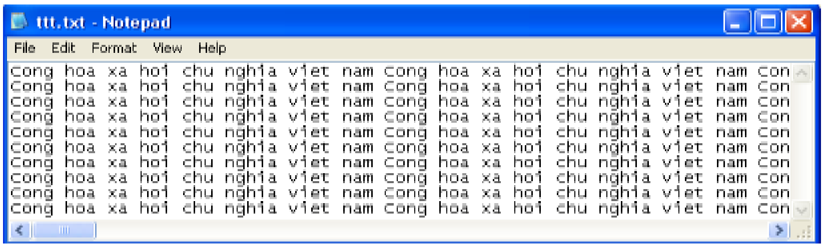
Hình 5.15 Tập ảnh thử nghiệm 1

+ Tập ảnh thử nghiệm 2 gồm 50 ảnh với nhiều kích cỡ khác nhau:

Hình 5.16 Tập ảnh thử nghiệm 2

Tiếp tục sử dụng 2 tập ảnh thử nghiệm trên để giấu thông điệp bằng kỹ thuật giấu RCM (reversible contrast mapping) với 2 trường hợp:

+ Giấu theo tỷ lệ nhúng: 0%, 30%, 70% và 100% .
+ Giấu cho trước một tệp.



Hình 5.17 Tệp thông điệp nhúng.

Sau đó sử dụng chương trình phát hiện được cài đặt theo kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RCM (kỹ thuật phát hiện giấu tin của bản đồ thủy vân tương phản thuận nghịch). Kết quả phát hiện được thể hiện trong **Bảng 5.1** và **Bảng 5.2**:

Bảng 5.1 Kết quả phát hiện của tập ảnh thử nghiệm 1

Độ dài	Giấu cho trước một tệp	0%	30%	70%	100%
Có giấu	100%	0%	100%	100%	100%
Không giấu	0%	100%	0%	0%	0%

Bảng 5.2 Kết quả phát hiện của tập ảnh thử nghiệm 2

Độ dài	Giấu cho trước một tệp	0%	30%	70%	100%
Có giấu	38%	44%	34%	34%	34%

Không giấu	62%	56%	76%	76%	76%

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:

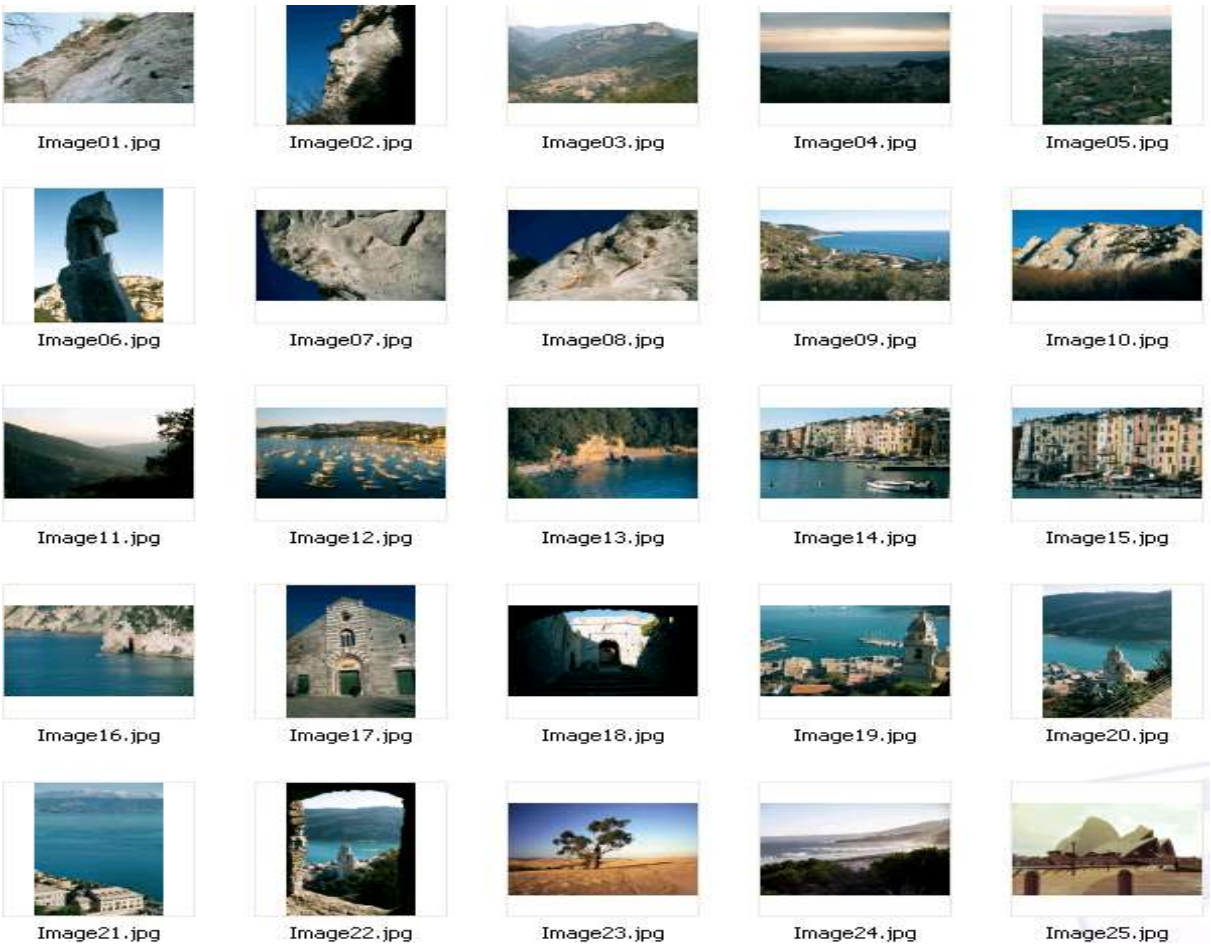
$$F_\beta = (1+\beta^2).\frac{precision.recall}{\beta^2.precision+recall}$$

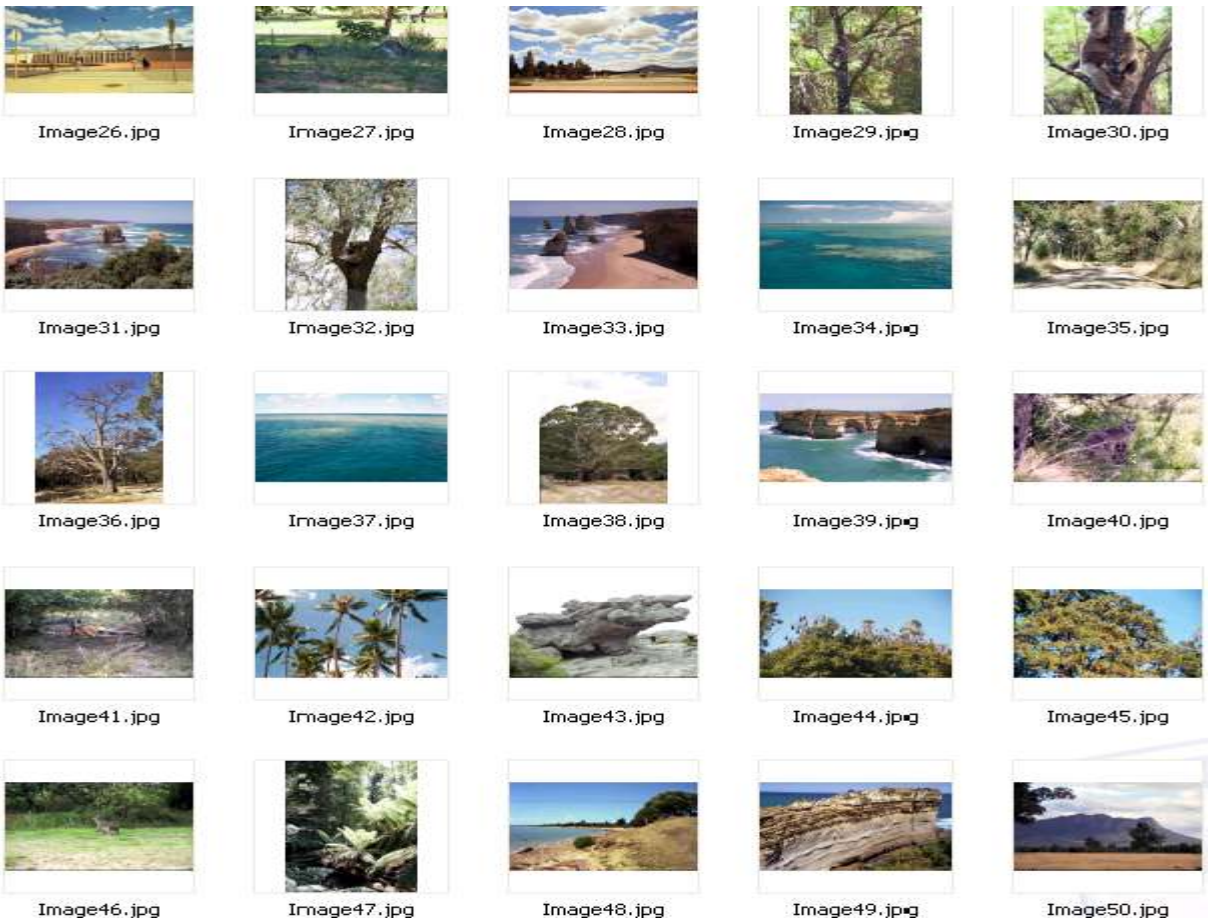
trong đó β là một tham số có giá trị nằm giữa 0 và 1. Nếu β = 1, *F-measure* bằng với precision và nếu β = 0, *F-measure* bằng với *recall*. Giữa đoạn đó, giá trị β càng cao, độ quan trọng của *precision* càng cao so với *recall*. Ta sử dụng giá trị thường được dùng là β = 0.5, nghĩa là:

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

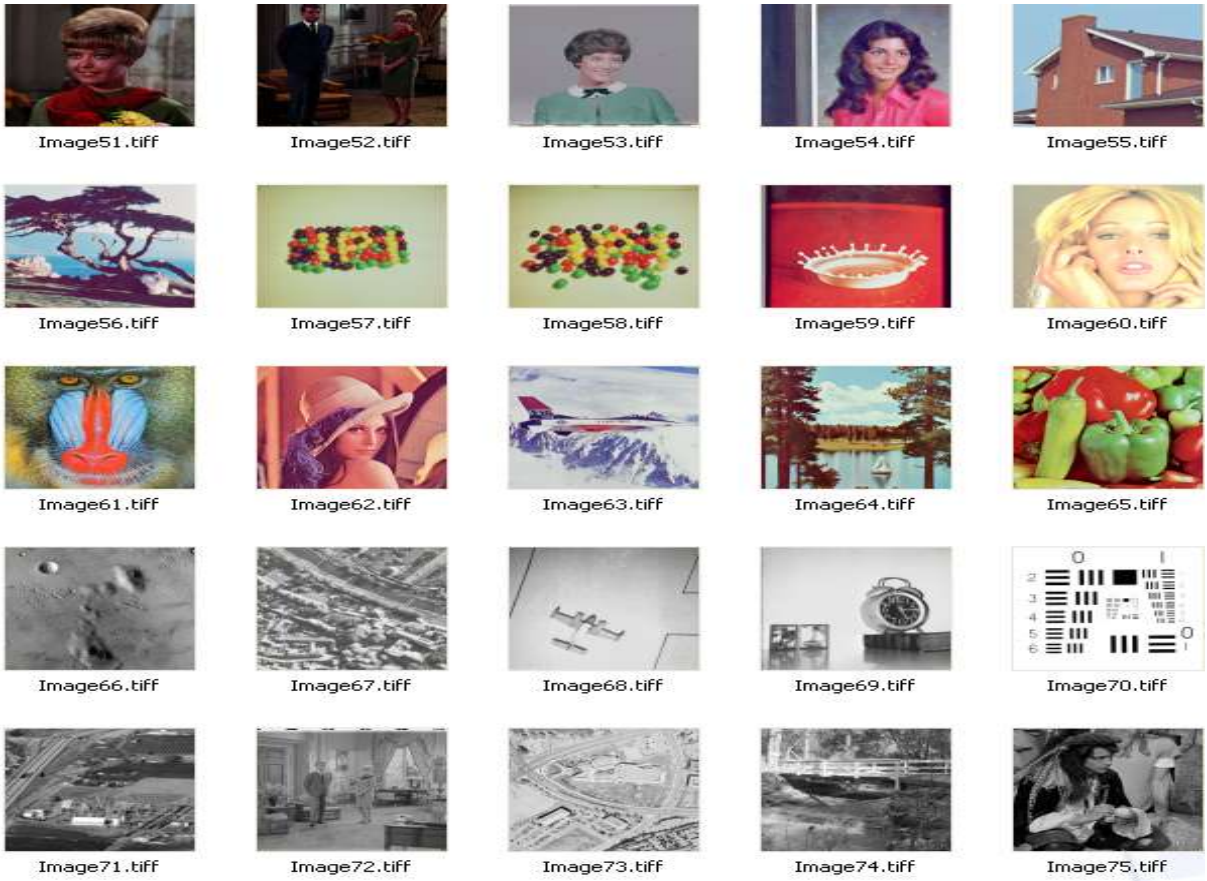
5.4.2 Kết quả thử nghiệm

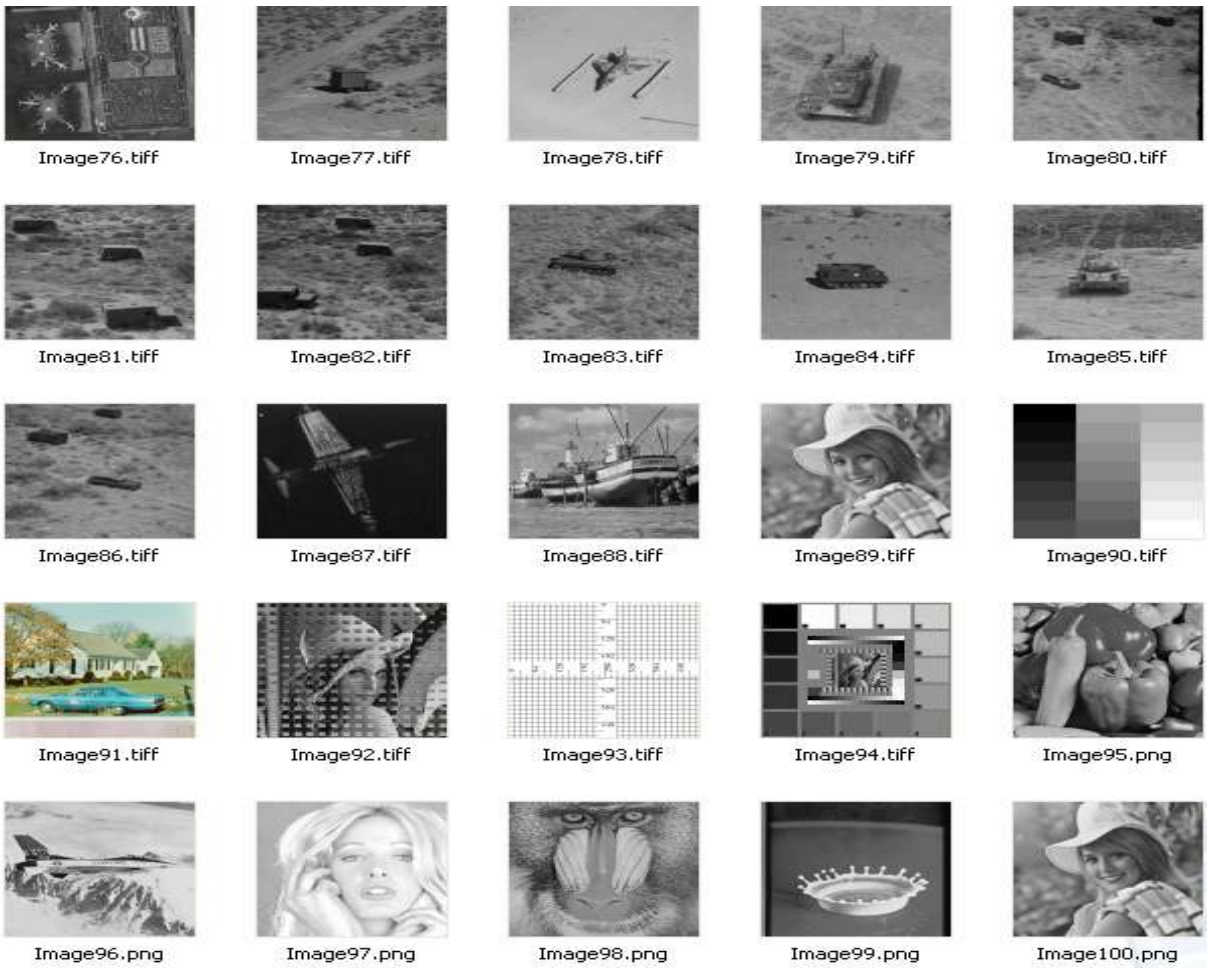
Tập ảnh thử nghiệm D1 gồm 50 ảnh chưa giấu tin (từ Image01.jpg đến Image50.jpg), kích thước 768x512 và 512x768 và D2 gồm 50 ảnh kích thước 756x504 dùng để giấu tin với lượng giấu 50%, 100% (Image51.tiff đến Image94.tiff và Image95.png đến Image100.png).





Hình 5.18 Tập 50 ảnh chưa giấu tin bất kì





Hình 5.19 Tập 50 ảnh dùng để giấu tin với lượng giấu 50% hoặc 100%

Chọn tập ảnh D50_percent gồm 100 ảnh trong đó 50 ảnh có giấu tin với lượng giấu 50% (D2) và 50 ảnh không giấu tin (D1). 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	T (True)	T
Image02.jpg	F (False)	F

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image03.jpg	T	T
Image04.jpg	T	T
Image05.jpg	T	T
Image06.jpg	T	T
Image07.jpg	T	T
Image08.jpg	T	T
Image09.jpg	T	T
Image10.jpg	T	T
Image11.jpg	F	F
Image12.jpg	T	T
Image13.jpg	T	T
Image14.jpg	T	T
Image15.jpg	T	T
Image16.jpg	T	T
Image17.jpg	T	T
Image18.jpg	F	F
Image19.jpg	T	T
Image20.jpg	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image21.jpg	T	T
Image22.jpg	T	T
Image23.jpg	T	T
Image24.jpg	T	T
Image25.jpg	T	T
Image26.jpg	T	T
Image27.jpg	T	T
Image28.jpg	T	T
Image29.jpg	T	T
Image30.jpg	T	T
Image31.jpg	T	T
Image32.jpg	T	T
Image33.jpg	T	T
Image34.jpg	T	T
Image35.jpg	T	T
Image36.jpg	T	T
Image37.jpg	T	T
Image38.jpg	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image39.jpg	T	T
Image40.jpg	T	T
Image41.jpg	T	T
Image42.jpg	T	T
Image43.jpg	F	F
Image44.jpg	T	T
Image45.jpg	T	T
Image46.jpg	T	T
Image47.jpg	T	T
Image48.jpg	T	T
Image49.jpg	T	T
Image50.jpg	T	T
Image51.tiff	T	T
Image52.tiff	T	T
Image53.tiff	T	T
Image54.tiff	T	T
Image55.tiff	T	T
Image56.tiff	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
Image57.tiff	T	T
Image58.tiff	T	T
Image59.tiff	T	T
Image60.tiff	T	T
Image61.tiff	T	T
Image62.tiff	T	T
Image63.tiff	T	T
Image64.tiff	T	T
Image65.tiff	T	T
Image66.tiff	T	T
Image67.tiff	T	T
Image68.tiff	T	T
Image69.tiff	T	T
Image70.tiff	T	T
Image71.tiff	T	T
Image72.tiff	T	T
Image73.tiff	T	T
Image74.tiff	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
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	T	T
Image83.tiff	T	T
Image84.tiff	T	T
Image85.tiff	T	T
Image86.tiff	T	T
Image87.tiff	T	T
Image88.tiff	T	T
Image89.tiff	T	T
Image90.tiff	T	T
Image91.tiff	T	T
Image92.tiff	T	T

Tập thử nghiệm / Tên ảnh	D50_percent	D100_percent
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	46	4
	D2	3	47

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

$$\text{Precision} = \frac{46}{46+4} = 0.92$$

$$\text{Recall} = \frac{46}{46+3} = 0.94$$

$$\text{F - measure} = 2\frac{0.92*0.94}{0.92+0.94} = 0.93$$

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	46	4
	D2	0	50

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

$$\text{Precision} = \frac{46}{46+4} = 0.92$$

$$\text{Recall} = \frac{46}{46+0} = 1$$

$$\text{F - measure} = 2\frac{0.92*1}{0.92+1} = 0.96$$

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%	0.92	0.94	0.93
Kỹ thuật phát hiện cho lượng giấu 100%	0.92	1	0.96

5.4.3 Nhận xét

Nhìn vào kết quả của bảng 5.5 ta thấy độ đo đánh giá F-measure là rất cao, cho thấy thuật toán phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RCM được trình bày ở chương 4 là có độ chính xác và hiệu quả, phát hiện ảnh có giấu tin là rất lớn.

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 RCM và phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RCM.

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 RCM trên miền dữ liệu ảnh.
- Nghiên cứu kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RCM.
- Cài đặt và thử nghiệm bằng matlab 2007b.

Trong quá trình làm đồ án, do 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] Nguyễn Xuân Huy, Trần Quốc Dũng, Giáo trình giấu tin và thuỷ vân ảnh, Trung tâm thông tin tư liệu, TTKHTN - CN 2003

[2] Trần Thị Thu Hà, Luận văn tốt nghiệp, ngành Công nghệ thông tin, năm 2009

[3] Mặc Như Hiển, Luận văn tốt nghiệp ngành CNTT, năm 2009

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

[5] Yeh-Shun Chen, Ran-Zan Wang, Yeuan-Kuen Lee, Shih-Yu Huang, Steganalysis

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

[7] D.Cotuc and J. M. Chassery, "Very fast watermarking by reversible contrast mapping", IEEE Signal Processing Lett., vol. 14, no. 4, pp.255-258, Apr. 2007.

[8] CBIR Image Database, University of Washington, http://www.cs.washington.edu/reseach/imagedatabase/groundtruth/.