

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

Em xin chân thành cảm ơn các thầy cô trong bộ môn tin 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 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.

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.

Hải phòng, ngày ...tháng ...năm 2009

Sinh viên

Đỗ Thị Nguyệt

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 đổi mới. Sự ra đời những phần mềm có tính năng rất mạnh, các thiết bị mới như máy ảnh kỹ thuật số, máy quét chất lượng cao, máy in, máy ghi âm kỹ thuật số, v.v..., đã với tới thế giới tiêu dùng rộng lớn để sáng tạo, xử lý và thưởng thức các dữ liệu đa phương tiện (multimedia data). Mạng Internet toàn cầu đã biến thành một xã hội ảo nơi diễn ra quá trình trao đổi thông tin trong mọi lĩnh vực chính trị, quân sự, quốc phòng, kinh tế, thương mại... Và chính trong môi trường mở và tiện nghi như thế xuất hiện những vấn nạn, tiêu cực đang rất cần đến các giải pháp hữu hiệu cho vấn đề an toàn thông tin như nạn ăn cắp bản quyền, nạn xuyên tạc thông tin, truy nhập thông tin trái phép v.v.. Đi tìm giải pháp cho những vấn đề này không chỉ giúp ta hiểu thêm về công nghệ phức tạp đang phát triển rất nhanh này mà còn đưa ra những cơ hội kinh tế mới cần khám phá.

Trong một quá trình phát triển lâu dài, nhiều phương pháp bảo vệ thông tin đã được đưa ra trong đó giải pháp dùng mật mã học là giải pháp được ứng dụng rộng rãi nhất. Các hệ mã mật đã được phát triển nhanh chóng và được ứng dụng rất phổ biến cho đến tận ngày nay. Thông tin ban đầu sẽ được mã hoá thành các ký hiệu vô nghĩa, sau đó sẽ được lấy lại thông qua việc giải mã nhờ khoá của hệ mã. Đã có rất nhiều những hệ mã phức tạp được sử dụng như DES, RSA, NAPSACK...và phương pháp này đã được chứng minh thực tế là rất hiệu quả và được ứng dụng phổ biến.

Nhưng ở đây ta không định nói về các hệ mã mật mà ta tìm hiểu về một phương pháp đã và đang được nghiên cứu và ứng dụng rất mạnh mẽ ở nhiều nước trên thế giới đó là phương pháp giấu tin (data hiding). Đây là phương pháp mới và phức tạp, nó đang được xem như một công nghệ chìa khoá cho

vấn đề bảo vệ bản quyền, nhận thực thông tin và điều khiển truy cập... ứng dụng trong an toàn và bảo mật thông tin.

Nhưng cũng chính vì kỹ thuật đó ngày càng tinh xảo đã trở thành công cụ hỗ trợ đắc lực cho các đối tượng phản động truyền bá thông tin cho đồng minh làm cho vấn đề kiểm soát thông tin an ninh ngày càng khó khăn. Vấn đề phát hiện và phân loại các đối tượng dữ liệu trên môi trường truyền thông công cộng là vấn đề cấp thiết hiện nay. Trong đồ án này nghiên cứu một số kỹ thuật phát hiện và ước lượng thông điệp có giấu tin trên miền LSB của ảnh màu và ảnh cấp xám.

Nội dung của đề tài được trình bày trong 3 chương:

Chương 1: Một số kỹ thuật giấu tin trên miền LSB của ảnh

Chương 2: Một số kỹ thuật phát hiện và ước lượng thông điệp giấu trong ảnh

Chương 3: Kết quả thực nghiệm

CHƯƠNG I. MỘT SỐ KỸ THUẬT GIẤU TIN TRÊN MIỀN LSB CỦA ẢNH

1.1. Tổng quan về giấu tin.

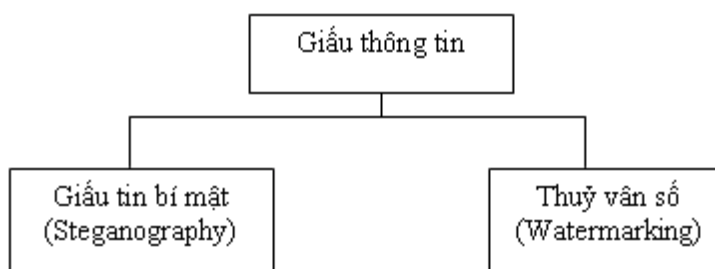
1.1.1. Định nghĩa giấu tin.

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

1.1.2. Mục đích của giấu tin: có 2 mục đích của giấu thông tin.

- Bảo mật cho những dữ liệu được giấu

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.



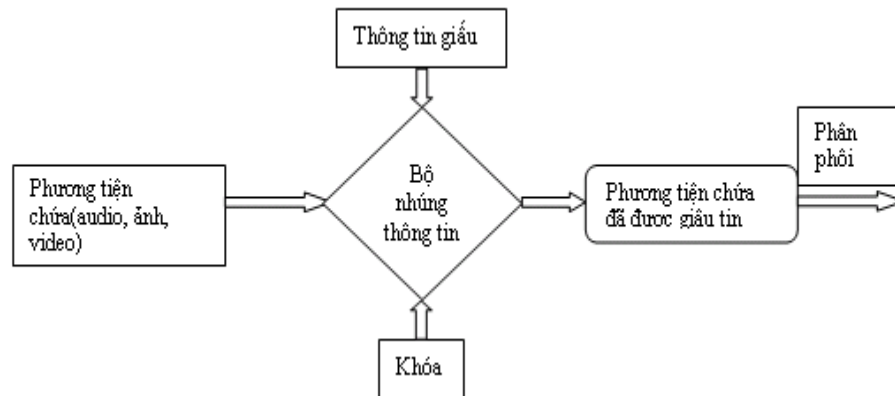
Hình 1: Hai lĩnh vực chính của kỹ thuật giấu thông tin.

- 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 dấu (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 thủy 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 sau:



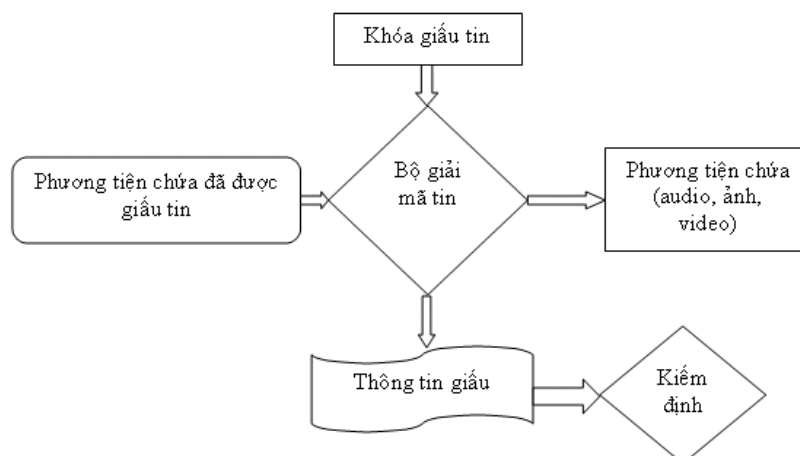
Hình 2: Lược đồ chung cho quá trình giấu tin.

- Thông tin cần giấu tùy 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.



Hình 3: Lược đồ chung cho quá trình giải mã

Hình vẽ trên 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.

1.1.4. Phân loại kỹ thuật giấu tin theo môi trường.

1.1.4.1. Giấu tin trong ảnh

- Hiện nay giấu thông tin trong ảnh là một bộ phận chiếm tỷ lệ lớn nhất trong các chương trình ứng dụng, các phần mềm, hệ thống giấu tin trong đa phương tiện bởi lượng thông tin được trao đổi bằng ảnh là rất lớn và hơn nữa giấu thông tin trong ảnh cũng 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... Thông tin sẽ được giấu cùng với dữ liệu ảnh nhưng chất lượng ảnh ít thay đổi và chẳng ai biết được đằng sau ảnh đó mang những thông tin có ý nghĩa. Ngày nay khi ảnh số đã được sử dụng rất phổ biến thì giấu thông tin trong ảnh đã đem lại nhiều những ứng dụng quan trọng trên các lĩnh vực trong đời sống xã hội. Ví dụ như ở các nước phát triển chữ ký tay đã được số hoá và lưu trữ sử dụng như là hồ sơ cá nhân của các dịch vụ ngân hàng tài chính.

- Phần mềm WinWord của Microsoft cũng cho phép người dùng lưu trữ chữ ký trong ảnh nhị phân rồi gắn vào vị trí nào đó trong file văn bản để đảm bảo tính an toàn của thông tin.

- 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.

1.1.4.2. Giấu tin trong audio.

- Giấu thông tin trong audio mang những đặc điểm riêng khác với giấu thông tin trong các đối tượng đa phương tiện khác. Một trong những yêu

cầu cơ bản của giấu tin là đảm bảo tính chất ẩn của thông tin được giấu đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu. Để đảm bảo yêu cầu này ta lưu ý rằng kỹ thuật giấu thông tin trong ảnh phụ thuộc vào hệ thống thị giác của con người – HSV (Human Vision System) còn kỹ thuật giấu thông tin trong audio lại phụ thuộc vào hệ thống thính giác HAS (Human Auditory System).

- Một vấn đề khó khăn ở đây là hệ thống thính giác của con người nghe được các tín hiệu ở các dải tần rộng và công suất lớn nên đã gây khó dễ đối với các phương pháp giấu tin trong audio. Nhưng tai con người lại kém trong việc phát hiện sự khác biệt các dải tần và công suất có nghĩa là các âm thanh to, cao tần có thể che giấu được các âm thanh nhỏ thấp một cách dễ dàng.

- Vấn đề khó khăn thứ hai đối với giấu tin trong audio là kênh truyền tin, kênh truyền hay băng thông chậm sẽ ảnh hưởng đến chất lượng thông tin sau khi giấu. Giấu thông tin trong audio đòi hỏi yêu cầu rất cao về tính đồng bộ và tính an toàn của thông tin. Các phương pháp giấu thông tin trong audio đều lợi dụng điểm yếu trong hệ thống thính giác của con người.

1.1.4.3. 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 dần trải theo tần số của dữ liệu gốc. Nhiều nhà nghiên cứu đã dùng những hàm cosin riêng và các hệ số truyền sóng riêng để giấu tin. Trong các thuật toán khởi nguồn thì thường các kỹ thuật cho phép giấu các

ảnh vào trong video nhưng thời gian gần đây các kỹ thuật cho phép giấu cả âm thanh và hình ảnh vào video.

1.1.4.4 . 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 gì dữ liệu đa phương tiện như ảnh, audio, video. Gần đây đã có một số nghiên cứu giấu tin trong cơ sở dữ liệu quan hệ, các gói IP truyền trên mạng chắc chắn sau này còn tiếp tục phát triển tiếp.

1.1.5. Phân loại theo cách thức tác động lên các phương tiện.

- Phương pháp chèn dữ liệu: Phương pháp này tìm các vị trí trong file dễ bị bỏ qua và chèn dữ liệu cần giấu vào đó, cách giấu này không làm ảnh hưởng gì tới sự thể hiện các file dữ liệu ví dụ như được giấu sau các ký tự EOF.

- Phương pháp tạo các phương tiện chứa: Từ các thông điệp cần chuyển sẽ tạo ra các phương tiện chứa để phục vụ cho việc truyền thông tin đó, từ phía người nhận dựa trên các phương tiện chứa này sẽ tái tạo lại các thông điệp.

1.1.6. Phân loại theo các mục đích sử dụng.

- Giấu thông tin bí mật: đây là ứng dụng phổ biến nhất từ trước đến nay, đối với giấu thông tin bí mật người ta quan tâm chủ yếu tới các mục tiêu:

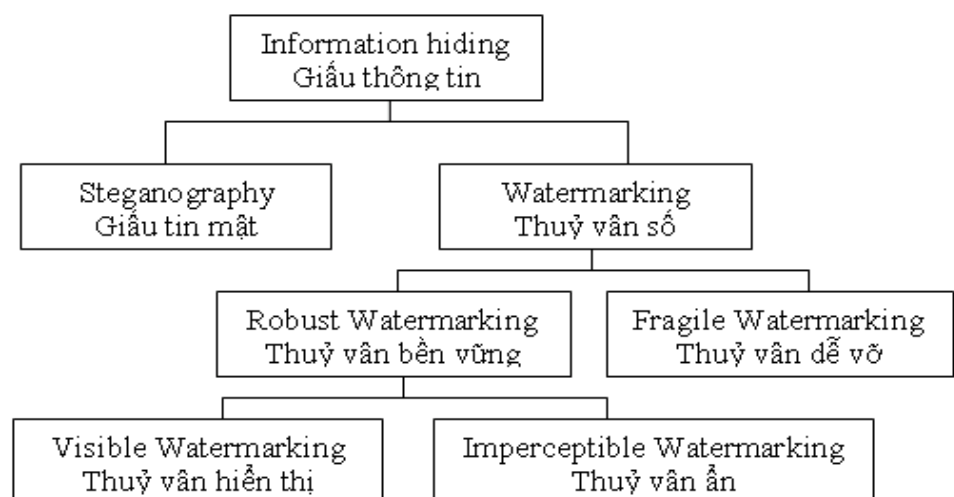
- + Độ an toàn của giấu tin - khả năng không bị phát hiện của giấu tin.
- + Lượng thông tin tối đa có thể giấu trong một phương tiện chứa cụ thể mà vẫn có thể đảm bảo an toàn.
- + Độ bí mật của thông tin trong trường hợp giấu tin bị phát hiện.

- Giấu thông tin bí mật không quan tâm tới nhiều các yêu cầu bền vững của phương tiện chứa, đơn giản là bởi người ta có thể thực hiện việc gửi và nhận nhiều lần một phương tiện chứa đã được giấu tin.

- Giấu thông tin thuỷ vân: do yêu cầu bảo vệ bản quyền, xác thực... nên giấu tin thuỷ vân có yêu cầu khác với giấu tin bí mật. Yêu cầu đầu tiên là các dấu hiệu thuỷ vân đủ bền vững trước các tấn công vô hình hay cố ý gỡ bỏ nó.

Thêm vào đó các dấu hiệu thuỷ vân phải có ảnh hưởng tối thiểu (về mặt cảm nhận) đối với các phương tiện chứa. Như vậy các thông tin cần giấu càng nhỏ càng tốt.

Tuỳ theo các mục đích khác nhau như bảo vệ bản quyền, chống xuyên tạc nội dung, nhận thực thông tin,... thuỷ vân cũng có các yêu cầu khác nhau



Hình 4: Phân loại các kỹ thuật giấu tin

Che giấu thông tin nói chung có rất nhiều ứng dụng tuỳ theo từng hoàn cảnh cụ thể. Giấu thông tin bí mật góp phần thực hiện “tàng hình” các phiên liên lạc, một sự bổ sung lý tưởng cho công tác bảo mật thông tin.

1.2. Tổng quan về ảnh BMP.

1.2.1. Khái niệm về ảnh đen trắng, ảnh màu, ảnh cấp xám.

➤ *Ảnh đen trắng.*

Đó là những bức ảnh mà mỗi điểm ảnh chỉ là những điểm đen hoặc trắng, được quy định bằng một bit. Nếu bit mang giá trị là 0 thì điểm ảnh là điểm đen, còn nếu mang giá trị là 1 thì điểm ảnh là điểm trắng. Do đó để biểu diễn một điểm ảnh đen trắng ta có thể dùng một ma trận nhị phân, là ma trận mà mỗi phần tử chỉ nhận một trong hai giá trị là 0 hoặc 1.

➤ *Ảnh màu*

Quá trình giấu tin vào ảnh màu cũng tương tự như với ảnh đen trắng nhưng trước hết ta phải chọn từ mỗi điểm ảnh ra bit có trọng số thấp nhất (LSB) để tạo thành một ảnh nhị phân gọi là ảnh thứ cấp. Sử dụng ảnh thứ cấp này như ảnh môi trường để giấu tin, sau khi biến đổi ảnh thứ cấp ta trả nó lại ảnh ban đầu để thu được ảnh kết quả.

➤ *Ảnh đa cấp xám*

Đối với ảnh đa cấp xám bảng màu của nó đã có sẵn, tức là những cặp màu trong bảng màu có chỉ số chênh lệch càng ít thì càng giống nhau. Vì vậy đối với ảnh đa cấp xám bit LSB của mỗi điểm ảnh là bit cuối cùng của mỗi điểm ảnh.

Quá trình tách bit LSB của ảnh đa cấp xám và thay đổi các bit này bằng thuật toán giấu tin trong ảnh đen trắng sẽ làm chỉ số của điểm màu bị thay đổi tăng hoặc giảm 1 đơn vị, do đó điểm ảnh mới sẽ có độ sáng tối của ô màu liền trước hoặc liền sau ô màu của điểm ảnh cũ. Bằng mắt thường rất khó có thể nhận thấy sự thay đổi về độ sáng tối này.

➤ *Ảnh nhỏ hơn hoặc bằng 8 màu*

Những ảnh thuộc loại này gồm có 16 màu (4 bit màu) và ảnh 256 màu (8 bit màu). Khác với ảnh màu, ảnh xám với số bit nhỏ hơn hoặc bằng 8 bit không phải luôn luôn được sắp xếp màu bảng màu.

Những màu ở liền kề nhau trong bảng màu có thể rất khác nhau chẳng hạn như màu đen với màu trắng vẫn có thể được xếp cạnh nhau.

Vì vậy việc xác định bit LSB của ảnh loại này rất khó. Nếu ta chỉ làm như đối với ảnh xám, tức là vẫn lấy bit cuối cùng của mỗi điểm ảnh để tạo thành ảnh thứ cấp thì mỗi thay đổi 0 $\rightarrow$ 1 hoặc 1 $\rightarrow$ 0 trên ảnh thứ cấp có thể làm cho ảnh màu của điểm ảnh cũ và mới tương đương ứng thay đổi rất nhiều dù chỉ số màu của chúng cũng tăng hoặc giảm 1 mà thôi.

➤ *Ảnh hightcolor (16 bit màu)*

Ảnh 16 bit màu thực tế chỉ sử dụng 15 bit cho mỗi điểm ảnh trong đó 5 bit biểu diễn cường độ tương đối của màu đỏ, 5 bit biểu diễn cường độ tương đối của màu xanh lam, 5 bit biểu diễn cường độ tương đối của màu xanh lơ. Còn lại một bit không dùng đến là bit cao nhất của byte thứ hai trong mỗi cặp thứ hai byte biểu diễn một điểm ảnh, đó chính là bit LSB của ảnh 16 bit màu. Việc thay đổi giá trị của những bit này sẽ không hề ảnh hưởng tới màu sắc của từng điểm ảnh trong môi trường.

➤ *Ảnh true color (24 bit màu)*

Ảnh true color sử dụng 3 byte cho mỗi điểm ảnh, mỗi byte biểu diễn một thành phần trong cấu trúc RGB. Trong mỗi byte các bit cuối cùng của mỗi byte trong phần dữ liệu ảnh là các bit LSB của ảnh true color.

Để tăng lượng thông tin giấu được vào ảnh môi trường, từ mỗi byte của ảnh true color ra sẽ lấy nhiều hơn một bit để tạo thành ảnh thứ cấp. Thông thường cũng chỉ nên lấy nhiều nhất 4 bit cuối cùng của mỗi byte để ảnh kết quả không bị nhiễu đáng kể, khi đó lượng thông tin tối đa có thể giấu trong ảnh cũng tăng lên gấp bốn lần so với lượng thông tin tối đa giấu được trong ảnh đó nếu chỉ lấy 1 bit cuối cùng ở từng byte.

1.2.2. Cấu trúc ảnh BMP

Để thực hiện việc giấu tin trong ảnh, trước hết ta phải nghiên cứu cấu trúc của ảnh và có khả năng xử lý được ảnh tức là phải số hoá ảnh. Quá trình số hoá các dạng ảnh khác nhau và không như nhau. Có nhiều loại ảnh đã được chuẩn hoá như: JPEG, PCX, BMP... Sau đây là cấu trúc ảnh *.BMP.

Mỗi file ảnh BMP gồm 3 phần:

- ✓ BitmapHeader (54 byte)
- ✓ Palette màu (bảng màu)
- ✓ BitmapData (thông tin ảnh)

Cấu trúc cụ thể của ảnh:

- Palette màu (bảng màu): bảng màu của ảnh, chỉ những ảnh lớn hơn hoặc bằng 8 bit màu mới có Palette màu.

- BitmapData (thông tin ảnh): phần này nằm ngay sau phần palette 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 từ trái sang phải. Giá trị của mỗi điểm ảnh là một chỉ số trỏ tới phần tử màu tương ứng của palette màu.

BitmapHeader (54 byte)

Byte	Đặt tên	Ý nghĩa	Giá trị
1 - 2	ID	Nhận dạng file	'BMP' hay 19778
3 - 6	File_Size	Kích thước File	Kiểu Long trong turbo C
7 - 10	Reserved	Dành riêng	Mang giá trị 0
11 - 14	OffsetBit	Byte bắt đầu vùng dữ liệu	Offset của byte bắt đầu vùng dữ liệu
15 - 18	Isizes	Số byte cho vùng info	40 byte
19 - 22	Width	Chiều rộng của ảnh BMP	Tính bằng pixel
23 - 26	Height	Chiều cao của ảnh BMP	Tính bằng pixel
27 - 28	Planes	Số planes màu	Cố định là 1
29 - 30	bitCount	Số bit cho một pixel	Có thể là 1,4,6,16,24
31- 34	Compression	Kiểu nén dữ liệu	0: Không nén 1: Nén runlength 8bits/pixel 2: Nén runlength 4bits/pixel
35 - 38	ImageSize	Kích thước ảnh	Tính bằng byte
39 - 42	XpelsPerMeter	Độ phân giải ngang	Tính bằng pixel/metr
43 - 46	YpelsPerMeter	Độ phân giải dọc	Tính bằng pixel/metr

47 – 50	ColorsUsed	Số màu sử dụng trong ảnh	
51 – 54	ColorsImportant	Số màu được sử dụng khi hiện ảnh	

- Thành phần BitCount của cấu trúc BitmapHeader 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 trị 0 thì điểm ảnh là đen, bit mang giá trị 1 điểm ảnh là điểm trắng.

4: Bitmap là ảnh 16 màu, mỗi điểm ảnh được biểu diễn bởi 4 bit.

8: Bitmap là ảnh 256 màu, mỗi điểm ảnh biểu diễn bởi 1 byte.

16: Bitmap là ảnh highcolor, mỗi dãy 2 byte liên tiếp trong bitmap biểu diễn cường độ tương đối của màu đỏ, xanh lá cây, xanh lơ của một điểm ảnh.

24: Bitmap là ảnh true color (2^{24} màu), mỗi dãy 3 byte liên tiếp trong bitmap biểu diễn cường độ tương đối của màu đỏ, xanh lá cây, xanh lơ (RGB) của một điểm ảnh.

- Thành phần ColorUsed của cấu trúc BitmapHeader xác định số lượng màu của palette màu 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.

1.2.3. Cấu trúc ảnh PNG

Là một dạng hình ảnh sử dụng phương pháp nén dữ liệu mới – không làm mất đi dữ liệu gốc. PNG được tạo ra nhằm cải thiện và thay thế định dạng ảnh GIF với một định dạng hình ảnh không đòi hỏi phải có giấy phép sáng chế sử dụng. PNG được hỗ trợ bởi thư viện tham chiếu libpng, một thư viện nền độc lập bao gồm các hàm của C để quản lý các hình ảnh PNG.

Những tập tin PNG thường có phần mở rộng là PNG và đã được gán kiểu chuẩn MIME là image/png.

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 2 dấu xuống dòng, ở giữa là 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. 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.

Về cơ bản, định dạng PNG đem lại cho ta những ưu thế vượt trội hơn so với các định dạng phổ thông khác hiện nay như JPG, GIF, BMP...Những ưu thế tỏ rõ sức mạnh hơn khi được sử dụng trong môi trường đồ họa web.

- ✓ Giảm thiểu dung lượng: Trong tất cả các định dạng ảnh phổ thông hiện nay thì hình ảnh PNG có thể coi là dung lượng nhỏ nhất. Điều này rất quan trọng khi sử dụng PNG trong môi trường web.
- ✓ Độ sâu của màu: Ảnh PNG hỗ trợ đến true color 48bit màu. Trong khi đó ảnh gif chỉ ở mức 256 màu.

1.3. Khái niệm 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 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... 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.

1.4. Một số kỹ thuật về giấu thông tin trong LSB.

1.4.1 Kỹ thuật giấu FlipEmbed

Ý tưởng: Là tách các bit quan trọng LSB của pixel ảnh, sao đó tại mỗi bit sẽ giấu một thông điệp.

Thuật toán:

Input:

- + Một file ảnh màu hoặc ảnh cấp xám C
- + Một chuỗi thông điệp giấu M
- + Một bộ khởi tạo bước đi giả ngẫu nhiên

Output:

- + Một file ảnh đã giấu tin S

Các bước thực hiện giấu thông điệp:

- Chuyển thông điệp cần giấu M sang dạng nhị phân.
- Đọc header của ảnh để lấy thông tin ảnh, đọc bảng màu. Sau đó đọc toàn bộ dữ liệu ảnh vào một mảng hai chiều để sử dụng cho việc giấu tin.
- Tách các bit cao (trừ bit LSB) của pixel được chọn ghép với bit thông điệp cần giấu. Quá trình được thực hiện lần lượt từ trên xuống cho đến khi giấu hết các bit thông điệp vào trong ảnh.

Các bước lấy thông điệp

Lấy từ bộ khởi tạo bước đi từ trên xuống đã thiết lập trong quá trình giấu để chọn vị trí pixel theo trình tự đã giấu. Tách LSB của các pixel theo bước đi từ trên xuống dưới được chọn chính là bit thông điệp đã giấu.

1.4.2. Thuật toán FlipEmbed cải tiến

Ý tưởng: Tạo các bước đi giả ngẫu nhiên để chọn pixel sẽ giấu thông tin, tại pixel được chọn sẽ tách các bit ít quan trọng LSB của pixel ảnh tại điểm đó, sau đó sẽ giấu một bit thông điệp.

Thuật toán:

Input:

- + Một file ảnh màu hoặc ảnh cấp xám C
- + Một chuỗi thông điệp giấu M
- + Một bộ khởi tạo bước đi giả ngẫu nhiên

Output:

- + Một file ảnh đã giấu tin S

Các bước thực hiện giấu thông điệp:

- Chuyển thông điệp cần giấu M sang dạng nhị phân.
- Đọc dữ liệu của ảnh vào mảng 2 chiều.
- Khởi tạo bộ tạo bước đi giả ngẫu nhiên để chọn ra pixel sẽ giấu bit thông điệp.
- Tách các bit cao (trừ bit LSB) của pixel được chọn ghép với bit thông điệp cần giấu. Quá trình được thực hiện cho đến khi giấu hết các bit thông điệp vào trong ảnh.

Các bước lấy thông điệp

Tách LSB của các pixel theo bước đi được chọn chính là bit thông điệp đã giấu.

1.4.3. Kỹ thuật giấu Simemembed

Ý tưởng:

- + Chia miền LSB của ảnh thành nhiều khối có kích thước $m \times n$.

- + Giấu bit thông điệp trên từng khối theo tính đồng chẵn lẻ của các bit số 1 trong khối.

Thuật toán:

Input:

- + C là một file ảnh màu hoặc ảnh cấp xám (chưa giấu tin)

- + M là thông điệp cần giấu

Output:

- + S là một file ảnh đã giấu tin

Cách thức thực hiện giấu:

- Chia phần thông tin ảnh (ma trận 2 chiều điểm ảnh) thành các khối nhỏ có kích thước $m \times n$.

- Mỗi khối nhỏ này sẽ được dùng để giấu một bit thông tin theo quy tắc sau: sau khi giấu thì tổng số bit 1 trong khối và bit thông tin cần giấu sẽ có cùng tính chẵn lẻ.

Các bước tách thông điệp

Chia khối dữ liệu của ảnh theo kích thước dùng để giấu, trong mỗi khối đó tách các LSB của khối đếm số bit 1 nếu số bit 1 là chẵn thì viết bit đầu ra là 0, nếu số bit 1 là lẻ thì viết bit đầu ra là 1.

CHƯƠNG II. MỘT SỐ KỸ THUẬT PHÁT HIỆN VÀ ƯỚC LƯỢNG THÔNG ĐIỆP GIẤU TRONG ẢNH

2.1. Các vấn đề phát hiện ảnh có giấu tin

2.1.1. Phân tích tin ẩn giấu (steganalysis)

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.

Phân tích ảnh có giấu thông tin 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.

2.1.2. Các phương pháp phân tích có thể phân thành 3 nhóm :

- 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. Phương pháp này rất rộng.

- 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.

Trong các phần tiếp theo sẽ trình bày một số phương pháp phát hiện ảnh có giấu tin trên miền LSB bằng thống kê toán học. Các phương pháp này đưa ra độ tin cậy rất cao khi dữ liệu giấu lớn nhưng cũng có một số hạn chế cho một số ảnh có tỷ lệ nhiễu lớn.

2.2. Một số kỹ thuật phát hiện ảnh có giấu tin và ước lượng ảnh có giấu tin

2.2.1 Kỹ thuật phát hiện RS (Regular Singular)

Thuật toán này được đề xuất bởi nhóm tác giả J. Fridrich, M. Goljan, and R. Du. Đây là một kỹ thuật phát hiện khá tin cậy cho trường hợp ảnh giấu thông điệp ngẫu nhiên trên các miền.

Ý tưởng

Chia miền giá trị của ảnh thành các nhóm có miền giá trị đều đặn (R-Regular), miền giá trị dị thường (S-Singular). Ta thấy rằng với một ảnh có giấu tin thì tổng số của các miền R rất gần với tổng số của miền S.

Thuật toán phát hiện

Input:

+ C là một file ảnh màu hoặc ảnh cấp xám (đã được giấu tin)

+ M là mặt nạ

Output:

+ Đánh giá S là một file ảnh đã giấu tin hay chưa giấu tin

Cách bước thực hiện

Đặt C là ảnh test với các giá trị của nó thuộc $P=\{0, \dots, 255\}$. Sau đó chia C thành các nhóm G khác nhau mỗi nhóm có n pixel $G=(x_1, \dots, x_n)$.

Để thực hiện việc phân dữ liệu ảnh thành miền có giá trị đều đặn và miền giá trị dị thường ta sử dụng các hàm phụ trợ:

+ Hàm Hamming xác định khoảng cách giữa các điểm trong một tập

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \quad (1)$$

+ Một ánh xạ F xác định trên tập P gọi là Flipping nếu $F^2 = I$ trong đó I là một ánh xạ đồng nhất. Ta sử dụng hai tập ánh xạ F1 và F-1 như sau:

$$\begin{aligned} F1: 0 \leftrightarrow 1, 2 \leftrightarrow 3, \dots, 254 \leftrightarrow 255, \quad F-1: -1 \leftrightarrow 0, 1 \leftrightarrow 2, \dots, 253 \leftrightarrow \\ 254, \quad 255 \leftrightarrow 256 \end{aligned} \quad (2)$$

Ta có công thức $F-1(x)=F1(x+1)-1$ với tất cả các x

=> Nhóm G được quyết định là thuộc nhóm nào trong 3 nhóm (Regular Group (R), Singular Group (S), Unusable Group (U)) khi và chỉ khi:

$$G \in R \Leftrightarrow f(F_M(G)) > f(G)$$

$$G \in S \Leftrightarrow f(F_M(G)) < f(G)$$

$$G \in U \Leftrightarrow f(F_M(G)) = f(G)$$

+ Với M là một mặt lạ phụ trợ chứa các giá trị -1, 0, 1 để trộn các Pixel trong nhóm. $F_M(G)$ được xác định như sau:

$$F_M(G) = \{F_{M(1)}(x_1), F_{M(2)}(x_2), \dots, F_{M(n)}(x_n)\} \text{ với } x_i \in G$$

- Đặt R_M là số nhóm của R, S_M là số nhóm của S, U_M là số nhóm của U. Chúng ta có:

- Theo giả thuyết thống kê của phương pháp này đó là trong một ảnh điển hình (chưa giấu thông tin) thì giá trị của R_M gần bằng giá trị của R_{-M} và tương tự giá trị của S_M gần bằng giá trị của S_{-M} .

$$R_M \cong R_{-M} \text{ và } S_M \cong S_{-M} \quad (3)$$

- Sự ngẫu nhiên của LSB gây ra sự khác nhau giữa R_M và S_M . Khi độ dài của thông điệp giấu trong LSB càng tăng lên thì nó làm cho R_M và R_{-M} càng rất khác nhau, tương tự S_M càng khác S_{-M} trong khi đó R_M và S_M có giá trị rất gần nhau. Tức là với ảnh có giấu thông tin ẩn trong LSB của ảnh thì

$$R_M \cong S_M$$

$$R_M \neq R_{-M} (R_{-M} > R_M)$$

$$S_M \neq S_{-M} (S_M > S_{-M})$$

2.2.2. Kỹ thuật ước lượng bằng RS

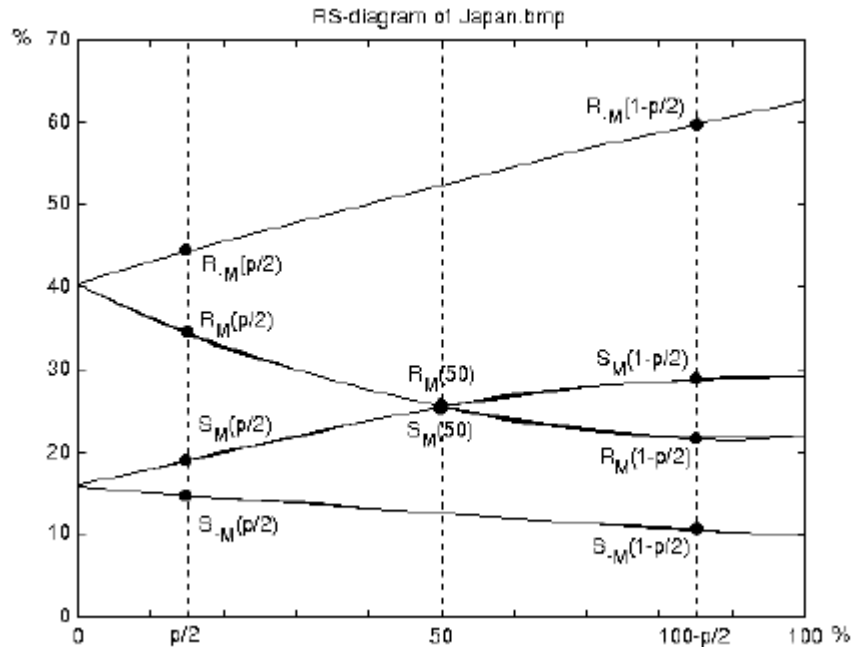
Chúng tôi cho phép kí hiệu số miền đều đặn cho mặt nạ M như R_M (trong % tất cả các miền). Tương tự như thế, S_M cũng được kí hiệu có liên quan số miền dị thường. Ta có $R_M + S_M \leq 1$ và $R_{-M} + S_{-M} \leq 1$ cho mặt nạ là âm. Các giả thiết thống kê về phương pháp phát hiện đó là một trong những hình ảnh tiêu biểu, giá trị của R_M xấp xỉ bằng giá trị của R_{-M} , và cũng tương tự cho S_M và S_{-M} : $R_M \approx R_{-M}$ và $S_M \approx S_{-M}$ (4)

Giả thiết này có thể được tìm ra chứng minh bằng cách xem xét tỉ mỉ biểu thức (2). Áp dụng các thao tác trộn hàm F_{-1} cũng giống như hàm F_1 tới một ảnh màu, có thể thay đổi vị trí bằng 1.

Cho một hình ảnh tiêu biểu, đây không phải là một lý do tại sao khẳng định số nhóm R và S thay đổi đáng kể khi thay đổi vị trí màu sắc bằng 1. Các giả thiết này được xác minh bằng các thực nghiệm cho các hình ảnh được chụp với máy ảnh kỹ thuật số cho những định dạng mất thông tin và không bị mất thông tin. Nó cũng làm tốt cho việc xử lý ảnh với các thao tác xử lý ảnh thông thường và cho hầu hết các hình ảnh đã được quét. Tuy nhiên, là vi phạm sau khi thay đổi miền LSB trong mỗi quan hệ (2). Ví dụ phát hiện miền LSB.

Sự ngẫu nhiên của miền LSB tập trung vào sự khác biệt giữa R_M và S_M tới 0 như độ dài thông điệp m được nhúng tăng lên. Sau khi trộn LSB của 50% pixels (Đó là những gì sẽ xảy ra sau khi nhúng một cách ngẫu nhiên bit thông điệp vào mỗi điểm ảnh), thu được $R_M \approx S_M$. Điều này tương đương với việc nói rằng, khả năng nhúng miền LSB không mất thông tin là 0. Điều bất ngờ đó là ảnh hưởng của miền LSB thay đổi ngẫu nhiên cũng làm ảnh hưởng trực tiếp trên R_{-M} và S_{-M} . Chúng làm tăng sự khác biệt cùng với độ dài thông điệp m được nhúng. Đồ thị cho thấy R_M , S_M , R_{-M} , S_{-M} có chức năng như là số

điểm ảnh được trộn với LSB xuất hiện trong hình 5 (biểu đồ RS). Giải thích riêng cho việc làm tăng sự khác biệt giữa R_M và S_M là sự bỏ qua cho tính không bền vững.



Hình 5: Đồ thị RS cho một hình ảnh tiêu biểu. Trục x có liên quan số điểm ảnh được trộn với LSB, trục y có liên quan số miền đều đặn và dị thường với mặt nạ M và $-M$, $M = [0 \ 1 \ 1 \ 0]$.

Nguồn gốc của phương pháp phát hiện mới (phương pháp RS) là ước tính bốn đường cong của biểu đồ RS và tính toán khác, sự giao nhau của chúng bằng cách sử dụng ngoại suy. Thông thường hình dạng của bốn đường cong trong biểu đồ gần như là các đường thẳng hoàn toàn đối với ảnh gốc. Những thực nghiệm chứng tỏ đường cong R_M và S_M là được biểu diễn với những đường thẳng hợp lý, trong khi “bên trong” đường cong R_M và S_M có thể được biểu diễn gần đúng hơn với phương trình bậc 2. Các tham số của đường cong có thể xác định từ các điểm đánh dấu trong hình 5.

Nếu có một ảnh đã giấu tin cùng với một thông điệp độ dài chưa biết p (trong % của những điểm ảnh) được nhúng rải rác ngẫu nhiên vào trong LSB của điểm ảnh. Theo ước lượng ban đầu số nhóm R và S tương ứng với các điểm $R_M(p/2)$, $S_M(p/2)$, $R_{-M}(p/2)$, và $S_{-M}(p/2)$ (nhìn vào Hình 1). Nhân tố

của một nửa sự việc đó là bởi vì, giả định thông điệp là một chuỗi bit ngẫu nhiên trung bình chỉ có một nửa các pixels sẽ được trộn. Nếu trộn LSB của tất cả các pixels trong ảnh và tính toán được số nhóm R và S , sẽ thu được bốn điểm $R_M(1-p/2)$, $S_M(1-p/2)$, $R_{-M}(1-p/2)$, $S_{-M}(1-p/2)$ (nhìn ở hình 1). Bằng cách thay đổi ngẫu nhiên miền LSB của ảnh giấu thông tin, sẽ thu được trung điểm $R_M(1/2)$ và $S_M(1/2)$. Có thể gắn các đường thẳng qua các đỉnh $R_{-M}(p/2)$, $R_{-M}(1-p/2)$ và $S_{-M}(p/2)$, $S_{-M}(1-p/2)$. Các điểm $R_M(p/2)$, $R_M(1/2)$, $R_M(1-p/2)$ và $S_M(p/2)$, $S_M(1/2)$, $S_M(1-p/2)$ xác định được hai parabol.

Nó có thể tránh được thời gian sử dụng thống kê dự toán của trung điểm $R_M(1/2)$ và $S_M(1/2)$ tại cùng thời điểm, muốn làm cho độ dài thông điệp tăng lên hợp lý bằng cách chấp nhận thêm hai điều kiện (tự nhiên):

- Điểm giao nhau của đường cong R_M và R_{-M} như điểm giao nhau của đường cong S_M và S_{-M} có cùng trục tọa độ x . Bản chất đây là một phiên bản mạnh theo giả thiết của chúng tôi (2).

- Giao điểm đường cong R_M và S_M tại $m = 50\%$, hay $R_M(1/2) = S_M(1/2)$. Giả thiết này tương đương với việc nói rằng khả năng thu nhận của miền LSB ngẫu nhiên được nhúng mà không mất thông tin là 0 [1].

Những giả thiết đã được xác minh qua thực nghiệm cho cơ sở dữ liệu lớn của các hình ảnh BMPs, JPEGs chưa được xử lý và những hình ảnh BMP đã xử lý.

Sự biến đổi nó có thể xuất phát từ một công thức đơn giản cho độ dài thông điệp p bí mật. Sau khi định lại kích thước trục x từ mức $p/2 \rightarrow 0$ và $100-p/2 \rightarrow 1$, giao điểm của trục tọa độ x là một nghiệm của phương trình bậc hai.

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0 \quad (5)$$

$$d_0 = R_M(p/2) - S_M(p/2), \quad d_1 = R_M(1-p/2) - S_M(1-p/2),$$

$$d_{-0} = R_{-M}(p/2) - S_{-M}(p/2), \quad d_{-1} = R_{-M}(1-p/2) - S_{-M}(1-p/2).$$

Độ dài thông điệp p là được tính toán từ nghiệm của x , có giá trị tuyệt đối nhỏ nhất của phương trình. Được tính bằng:

$$p = x/(x-1/2). \quad (6)$$

Do không gian có phần hạn chế, bỏ qua phép tính của những công thức toán học. Nó thỏa mãn để nói rằng các đường thẳng được xác định bởi số nhóm R và S tại $p/2$ và $1-p/2$.

2.2.3. Kỹ thuật ước lượng bằng RS cải tiến.

2.2.3.1. Diễn giải phương trình của ước lượng độ dài thông điệp RS

Theo hình .5 R_M , S_M là tuyến tính trong khi R_M và S_M có thể được mô phỏng bởi hai phương trình bậc 2. chúng tôi sẽ diễn giải phương trình (5), mà không được chứng minh trong kỹ thuật ước lượng độ dài thông điệp RS.

Trước hết, chúng tôi sử dụng một phép biến đổi tọa độ $T_1: [p/2, 1-p/2] \rightarrow [0, 1]$, và tọa độ 0, $p/2$, $1/2$, $1-p/2$ trong hệ thống tọa độ ban đầu sẽ được chuyển sang $p/(p-2)$, 0, $1/2$, 1 trong hệ thống tọa độ mới.

Trong hệ thống tọa độ mới, những điểm $(0, R_M(p/2))$ và $(1, R_M(1-p/2))$ quyết định phương trình:

$$R_M(x) = [R_M(1-p/2) - R_M(p/2)]x + R_M(p/2) \quad (7)$$

Tương tự như vậy, $S_M(x)$ quyết định bởi những điểm $(0, S_M(p/2))$ và $(1, S_M(1-p/2))$.

$$S_M(x) = [S_M(1-p/2) - S_M(p/2)]x + S_M(p/2) \quad (8)$$

$S_M(x)$ có thể quyết định bởi những điểm $(0, S_M(p/2))$, $(1/2, S_M(p/2))$ và $(1, S_M(1-p/2))$

$$S_M(x) = 2[S_M(p/2) + S_M(1-p/2) - 2S_M(1/2)]x^2 + [-S_M(1-p/2) - 3S_M(p/2) + 4S_M(1/2)] + S_M(p/2) \quad (9)$$

$R_M(x)$ có thể quyết định bởi những điểm $(0, R_M(p/2))$, $(1/2, R_M(p/2))$ và $(1, R_M(1-p/2))$

$$R_M(x) = 2[R_M(p/2) + R_M(1-p/2) - 2R_M(1/2)]x^2 + [-R_M(1-p/2) - 3R_M(p/2) + 4R_M(1/2)] + R_M(p/2) \quad (10)$$

Theo giả thiết (3), $R_M(x)$ và R_M giao nhau tại $x = 0$ trong hệ thống tọa độ ban đầu, vì thế $x = p/(p-2)$ là trong hệ thống tọa độ mới, và có thể tính toán

$$2[R_M(p/2) + R_M(1 - p/2) - 2R_M(1/2)]x^2 + [-R_M(1 - p/2) - 3R_M(p/2 + 4R_M(1/2))] + R_M(p/2) = [R_M(1 - p/2) - R_M(p/2)]x + R_M(p/2) \quad (11)$$

Tương tự như vậy, S_{-M} và S_M cũng giao nhau tại $p/(p-2)$, sau đó:

$$2[S_M(p/2) + S_M(1 - p/2) - 2S_M(1/2)]x^2 + [-S_M(1 - p/2) - 3S_M(p/2 + 4S_M(1/2))] + S_M(p/2) = [S_M(1 - p/2) - S_M(p/2)]x + S_M(p/2) \quad (12)$$

Từ (11) trừ (12) mang lại

$$2[R_M(p/2) - S_M(p/2) + R_M(1-p/2) - S_M(1 - p/2)]x^2 + [R_M(p/2) - S_M(p/2) - R_M(1 - p/2) - S_M(1 - p/2) - R_M(1 - p/2) - S_M(1 - p/2) - 3R_M(p/2) - S_M(p/2)]x + R_M(p/2) - S_M(p/2) - R_M(p/2) - S_M(p/2) \quad (13)$$

Giả sử

$$\begin{aligned} d_0 &= R_M(p/2) - S_M(p/2), & d_1 &= R_M(1-p/2) - S_M(1-p/2), \\ d_{-0} &= R_{-M}(p/2) - S_{-M}(p/2), & d_{-1} &= R_{-M}(1-p/2) - S_{-M}(1-p/2). \end{aligned}$$

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0$$

2.2.3.2. Sự linh hoạt của thuật toán phát hiện RS

Sự chính xác của RS là dựa trên các giả thiết (3) hoặc (4). Một giả thiết không được nắm giữ thì phương trình bậc hai (5) sẽ không được giữ. Vì vậy, khi tỷ lệ được nhúng là thấp, những sai sót trong giả thiết sẽ tạo nên sự không chính xác. Và khi không có thông điệp được nhúng trong ảnh, tỷ lệ báo động sai là cao. Trong phần này, sẽ phân tích thêm trên giả thiết (3), và một thuật toán ước lượng tỷ lệ thực tế được nhúng một cách chính xác. Mặt nạ M $[0 \ 1 \ 1 \ 0]$ cố định: là sử dụng trong phương pháp quy ước RS. Tuy nhiên, thực tế $R_M(0)$ là không hoàn toàn bằng với $R_{-M}(0)$ đối với mặt nạ này. Điều ban đầu sai có thể dẫn đến ước lượng sai nghiêm trọng. Trong thuật toán mới này, cần thiết lập một mặt nạ bằng cách lựa chọn các loại N mặt nạ khác nhau. Ví dụ, một trong những 4_tuple mặt nạ trong các mặt nạ thiết lập có thể được kí hiệu bởi M_i $i = 1, 2, \dots, N$.

Giả sử $\varepsilon_{R_{M_i}} = R_{-M_i}(0) - R_{M_i}(0)$ và $\varepsilon_{S_{M_i}} = S_{-M_i}(0) - S_{M_i}(0)$, vậy phương

trình (5) sẽ được chuyển sang

$$2(a_{1M_i} + d_{0M_i})x^2 + (a_{-0M_i} - d_{-1M_i} - d_{1M_i} - 3d_{0M_i})x + d_{0M_i} - d_{-0M_i} = \varepsilon_{R_{M_i}} + \varepsilon_{S_{M_i}} \quad (14)$$

Theo phương pháp RS, có thể lựa chọn một phiên bản những mặt nạ khác nhau, cho mỗi M_i sẽ nhận được một bộ giá trị của

$R_{M_i} \in [-p/2, p/2], S_{M_i} \in [-p/2, p/2], R_{-M_i} \in [-p/2, p/2], S_{-M_i} \in [-p/2, p/2], R_{M_i} \in [p/2, p/2], S_{M_i} \in [p/2, p/2], R_{-M_i} \in [p/2, p/2], S_{-M_i} \in [p/2, p/2]$. Sau đó có thể tính toán những tham số trong (5) và có được một phương trình tương ứng với M_i tuần tự.

Chỉ khi $|\varepsilon_{R_{M_i}} + \varepsilon_{S_{M_i}}|$ ban đầu là rất gần tới 0, kết quả phát hiện có thể chính xác.

Giả sử

$$a = 2(a_{1M_i} + d_{0M_i}), b = d_{-0M_i} - d_{-1M_i} - d_{1M_i} - 3d_{0M_i}, c = d_{0M_i} - d_{-0M_i}$$

Sau đó bên trái của phương trình (14)

$$2(a_{1M_i} + d_{0M_i})x^2 + (d_{-0M_i} - d_{-1M_i} - d_{1M_i} - 3d_{0M_i})x + d_{0M_i} - d_{-0M_i} \quad (15)$$

Được thay đổi vào $ax^2 + bx + c$, sau khi đã bình phương, nó trở thành

$$a^2x^4 + 2abx^3 + (ac + b^2)x^2 + 2bcx + c^2 \quad (16)$$

Sau đó tính toán khác nhau của (16), đã nhận được

$$4a^2x^3 + 6abx^2 + (ac + 2b^2)x + 2bc \quad (17)$$

Để có được giá trị tối thiểu của $|\varepsilon_{R_{M_i}} + \varepsilon_{S_{M_i}}|$, chúng tôi cho giá trị của (16) bằng 0 như sau:

$$4a^2x^3 + 6abx^2 + (ac + 2b^2)x + 2bc = 0 \quad (18)$$

Lựa chọn một cách thích hợp từ ba gốc của (18) như là p, và thay nó vào trong (15), có thể thu được giá trị của (15) Q_{M_j} hiện tại dưới mặt nạ M_j , tương tự như vậy có thể thu được cái khác Q_{M_j} hiện tại dưới mặt nạ M_i , $i = 1, 2, \dots, N, i \neq j$.

Chọn giá trị tối thiểu từ tất cả các tập hợp của Q, và ghi lại tương ứng với p và mặt nạ. Sau đó mặt nạ này là tối ưu nhất cho hình ảnh hiện thời và p là giá trị ước lượng chính xác nhất.

CHƯƠNG III: KẾT QUẢ THỰC NGHIỆM

3.1. Môi trường cài đặt chương trình

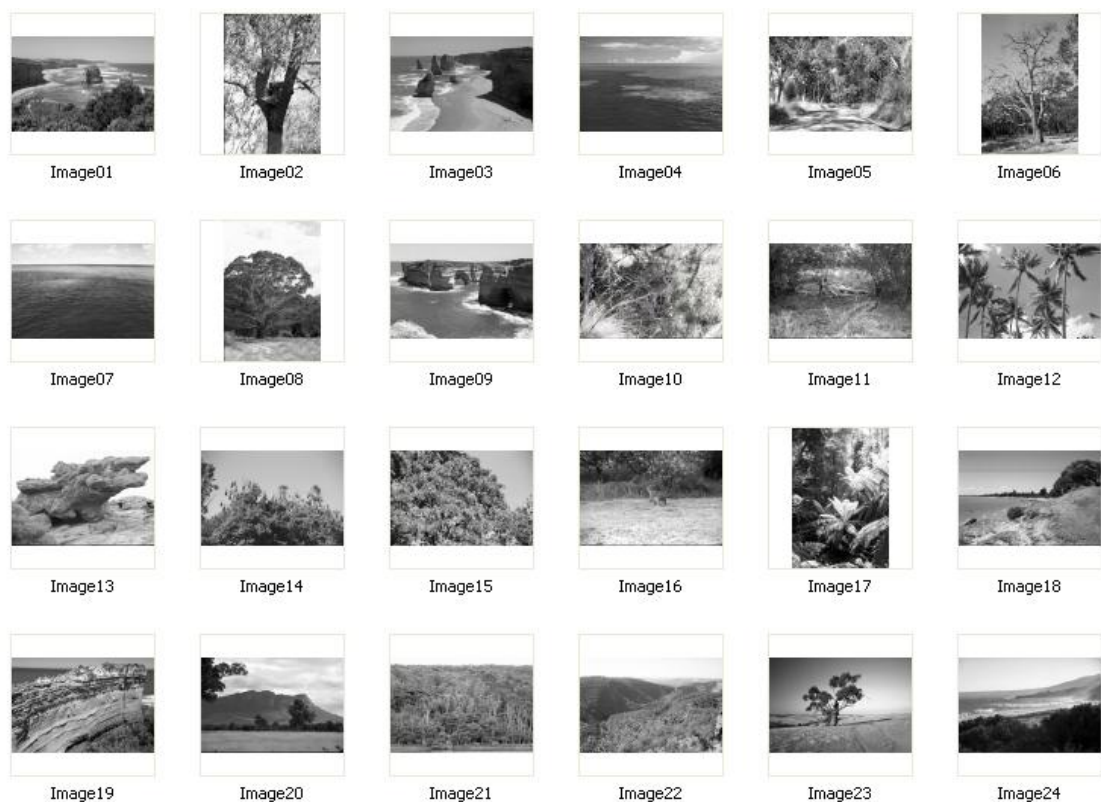
Trong quá trình thực hiện cài đặt chương trình có sử dụng chương trình MATLAB để viết chương trình và đưa ra kết quả.

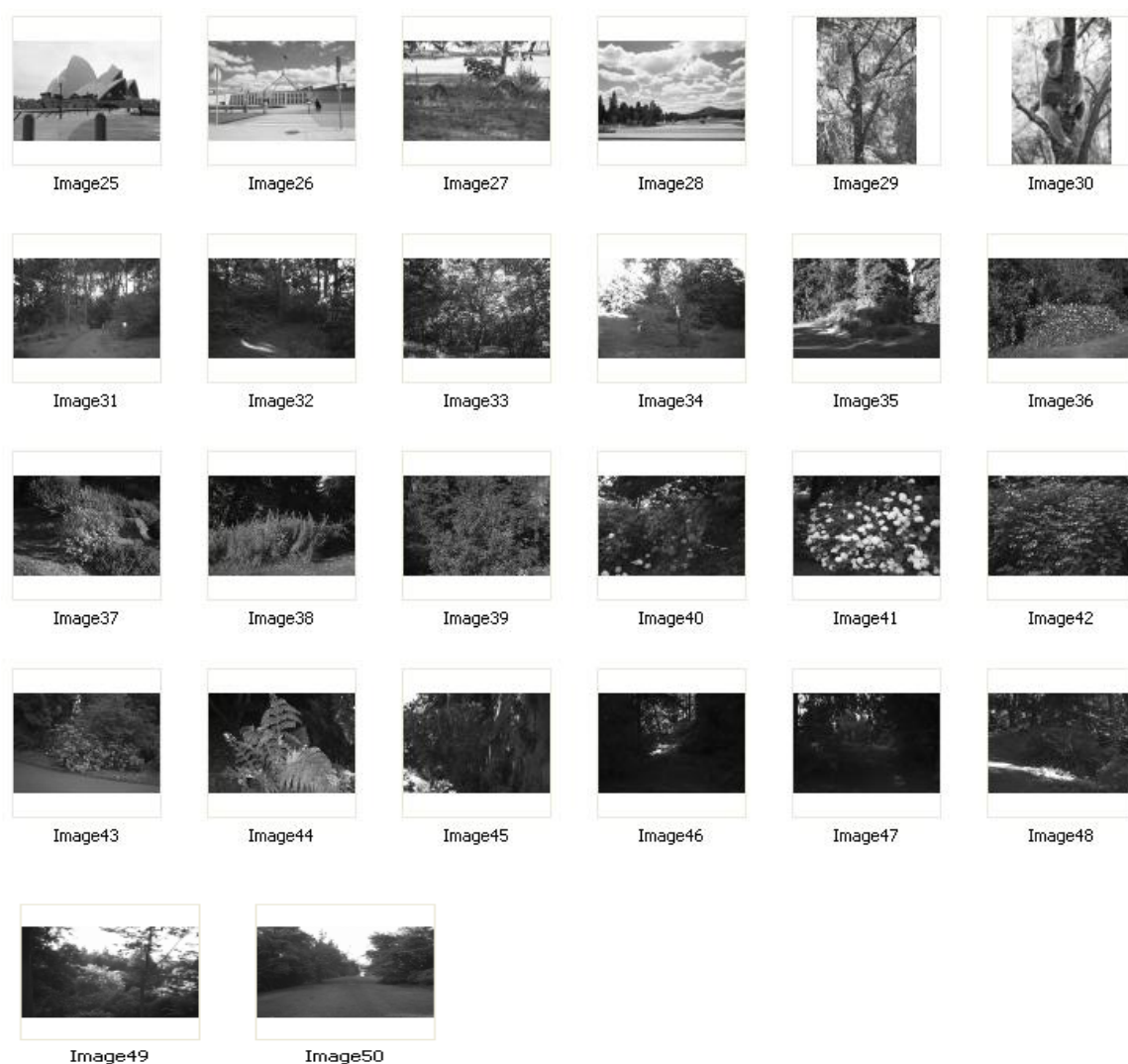
3.2. Cơ sở dữ liệu thử nghiệm

Dữ liệu thực hiện gồm có 100 ảnh JPEG, bao gồm 50 ảnh được chụp từ máy ảnh kỹ thuật số khôi phục sang ảnh bitmap cấp xám bằng trình xử lý photoshop.

Chất lượng ảnh sau khi nhúng thủy vân được đánh giá thông qua ước lượng độ dài thông điệp được nhúng ngẫu nhiên thông điệp từ 10% đến 100%. Thực hiện thực nghiệm trên kỹ thuật phát hiện RS và kỹ thuật phát hiện RS cải tiến.

Bảng 3: là bảng đưa ra một số ảnh được sử dụng để phát hiện.





3.3. Bảng kết quả thực nghiệm

3.3.1. Kết quả thử nghiệm trên kỹ thuật RS

Bảng 4: Bảng thông kê wóc lượng độ dài thông điệp bằng kỹ thuật RS

Lượng tin giấu (%)	Kết quả phát hiện đúng	
	Số ảnh phát hiện đúng	Tỉ lệ %
0%	38	76
10%	48	96
20%	46	92
30%	45	90
40%	47	94
50%	48	96
60%	42	84
70%	46	92
80%	49	98
90%	50	100
100%	48	96

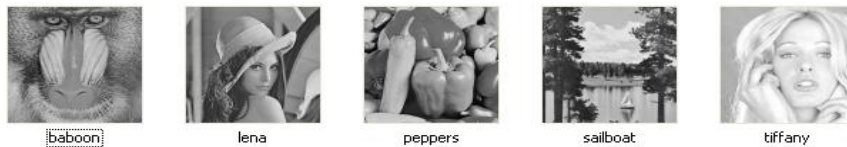
Nhận xét:

Phương pháp phát hiện RS là chính xác hơn cho những thông điệp là rải rác ngẫu nhiên trong ảnh đã được giấu tin hơn là những thông điệp được giấu tuần tự trong ảnh.

Trong mọi trường hợp, ảnh đã được giấu tin đã được phân biệt từ ảnh gốc ban đầu và ước lượng độ dài thông điệp trong phần trăm độ dài thông điệp.

3.3.2. Kết quả thực nghiệm trên kỹ thuật RS cải tiến

Bảng 5: là bảng đưa ra 5 ảnh chuẩn được sử dụng để thống kê trong phương pháp RS cải tiến.



Bảng 6: Là bảng thông kê ước lượng độ dài thông điệp bằng kỹ thuật RS cải tiến.

Lượng tin giấu (%)	5 ảnh chuẩn		50 ảnh chụp từ máy ảnh kỹ thuật số	
	RS	DRS	RS	DRS
0%	1.48	0.26	1.89	0.76
10%	11.66	10.56	8.71	9.45
20%	22.90	20.83	18.91	19.54
30%	32.70	30.07	29.42	29.51
40%	41.90	40.20	39.37	39.52
50%	52.98	50.50	50.56	50.20
60%	59.81	60.00	58.55	58.01
70%	72.07	70.33	72.44	70.87
80%	79.67	79.04	80.61	78.88
90%	91.08	90.19	90.85	89.69
100%	96.95	99.16	97.37	99.78

Nhận xét:

Phương pháp này đã được cải tiến từ phương pháp phát hiện RS truyền thống bằng cách lựa chọn mặt nạ một cách linh hoạt. Phương pháp này có những lợi thế tỉ lệ báo động sai và tỉ lệ mất mát thông tin là rất thấp, tỉ lệ ước lượng được nhúng chính xác hơn và tốc độ phát hiện nhanh hơn.

Lý thuyết suy diễn của phương trình ước lượng độ dài của phương pháp RS cũng được đưa ra.

Đánh giá:

Để so sánh tỉ lệ chính xác của phương pháp DRS và phương pháp truyền thống RS, đã thực hiện thử nghiệm trên 100 ảnh. Để giảm tỉ lệ báo động sai và tỉ mất thông tin, chúng tôi lựa chọn 0.03 ngưỡng dựa trên các thực nghiệm. Tỉ lệ chính xác của các kết quả thực nghiệm đã chỉ ra trên bảng 6. Đối với phương pháp truyền thống RS, phương pháp này có thể tỉ lệ báo động sai là giảm rất nhiều, và vào khoảng 8%. Trong khi đó, tỉ lệ mất thông tin là giảm. từ bảng 6, chúng tôi có thể thấy ước lượng chính xác là cao hơn so với phương pháp truyền thống RS khi tỉ lệ được nhúng là 5%. Nếu tỉ lệ nhúng là cao hơn 5%, thì tỉ lệ mất thông tin của phương pháp DRS tất cả đều bằng 0.

KẾT LUẬN

Việc kết hợp giấu thông tin và công nghệ thông tin là một vấn đề mới đang được nghiên cứu và phát triển để phục vụ nhiều lĩnh vực khác nhau. Trên thế giới người ta đã nghiên cứu nhiều về vấn đề này.

Kỹ thuật giấu thông tin trong ảnh nói chung và giấu thông tin trong ảnh màu nói riêng là một hướng nghiên cứu chính của kỹ thuật giấu thông tin hiện nay và đã đạt được nhiều kết quả khả quan.

Trong đề tài này em đã trình bày một số khái niệm liên quan đến việc che giấu thông tin nói chung và cụ thể là kỹ thuật ước lượng độ dài thông điệp giấu trên bit có trọng số thấp thông qua kỹ thuật phát hiện RS và kỹ thuật phát hiện DIH nói riêng. Do kiến thức còn nhiều hạn chế và hạn chế về thời gian nghiên cứu nên đề tài này không tránh khỏi những thiếu sót, vì vậy em rất mong nhận được sự đóng góp ý kiến của các thầy cô.

Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

- [1]. **Nguyễn Xuân Huy và Trần Quốc Dũng**, “*Giáo trình giấu tin và thủy vân ảnh*”, Thông tin tư liệu, ĐHKHTN, 2003.
- [2]. **Lương Mạnh Ba, Nguyễn Thanh Thủy**, “*Nhập môn xử lý ảnh số*”.
- [3]. **Romana Machado**, “<http://www.stego.com>”, 1996
- [4]. **A Westfeld**, “*Detecting low embedding rates,*” in Proc. Information Hiding Workshop, Springer LNCS 2578, pp. 324–339, 2002.
- [5]. **A. Westfeld and A. Pfitzmann**, “*Attacks on steganographic systems,*” in Proc. Information Hiding Workshop, Springer LNCS 1768, pp. 61–76, 1999
- [6]. **N. F. Johnson and S. Jajodia**, “*Steganalysis of Images Created Using Current Steganography Software.*” Proc. 2nd Information Hiding Workshop, Portland, OR, April 1998
- [7]. **Steganography software for Windows,**

<http://members.tripod.com/steganography/stego/software.html>

- [8]. **J. Fridrich and M. Goljan**, “**Steganalysis of LSB Embedding** *in Color and Grayscale Images*”, *in preparation for the special issue*
- [9]. **S. Katzenbeisser, F. A. P. Petitcolas**, **Information Hiding Techniques for Steganography and Digital Watemarking**, *Artech House, 2000.*