LỜI CẢM ƠN

Em xin bày tỏ lòng biết ơn sâu sắc nhất tới giáo viên hướng dẫn là PGS.TS Trịnh Nhật Tiến, thầy đã tận tình hướng dẫn và giúp đỡ em rất nhiều trong quá trình tìm hiểu và nghiên cứu để em có thể hoàn thành tốt đề tài tốt nghiệp của mình.

Em xin gửi lời cảm ơn đến Ban giám hiệu và các Thầy cô giáo của Trường Đại học Dân Lập Hải Phòng đã giảng dạy chúng em trong suốt 4 năm học, cung cấp cho chúng em những kiến thức chuyên môn cần thiết và quý báu giúp chúng em hiểu rõ hơn các lĩnh vực nghiên cứu để hoàn thành đề tài được giao.

Xin cảm ơn các bạn bè và gia đình đã động viên cổ vũ, đóng góp ý kiến, trao đổi trong suốt quá trình học tập cũng như làm tốt nghiệp, giúp em hoàn thành đề tài đúng thời hạn.

Hải Phòng, tháng 6 năm 2009

Sinh viên

Nguyễn Thị Mai

MỤC LỤC

GIỚI THIỆU

Công nghệ thông tin và đặc biệt là sự phát triển của hệ thống mạng máy tính đã tạo nên môi trường mở và là phương tiện trao đổi, phân phối tài liệu một cách tiện lợi, nhanh chóng. Tuy nhiên cũng đặt ra một vấn đề về bảo vệ tài liệu, ngăn chặn việc đánh cắp và sao chép tài liệu một cách bất hợp pháp. Vấn đề an toàn và bảo mật thông tin hiện nay luôn nhận được sự quan tâm đặc biệt của nhiều nhà nghiên cứu trong nhiều lĩnh vực. Một giải pháp đang được sử dụng và tỏ ra hiệu quả cho việc đảm bảo an toàn thông tin là giấu tin vào đối tượng khác. Đối tượng được áp dụng để chứa tin phổ biến nhất là ảnh. Giải pháp giấu tin được đưa ra nhằm hai mục tiêu chính đó là bảo mật cho thông tin được đem giấu (giấu tin mật) và bảo mật cho chính đối tượng được dùng để chứa tin (thủy vân số).

Giấu tin mật (steganography) là một lĩnh vực khoa học và nghệ thuật giấu thông tin trong đa phương tiện. Hệ thống steganography giấu các thông tin mật số vào trong đối tượng số khác mà khó bị phát hiện bằng kỹ thuật thông thường. Trước kia con người sử dụng ẩn các hình xăm hoặc mực vô hình để truyền thông điệp mật. Ngày nay nhờ có máy tính và công nghệ mạng công việc truyền thông tin mật trở nên dễ dàng và hiệu quả hơn.

Thủy vân trên ảnh số (watermarking) là kỹ thuật nhúng một lượng thông tin số vào một bức ảnh số sao cho người không được phép, khó có thể lấy được thông tin ra khỏi ảnh mà không phá hủy chính ảnh gốc. Trong kỹ thuật thủy vân số thì thông tin nhúng được gọi là thủy vân. Thủy vân có thể là một chuỗi các ký tự hay một hình ảnh nào đó.

Tuy nhiên kỹ thuật giấu tin làm nảy sinh một nguy cơ khác là lợi dụng việc giấu tin để thực hiện hành vi bất hợp pháp như truyền kế hoạch tấn công khủng bố, những sản phẩm văn hóa không lành mạnh,… Từ đó đặt ra vấn đề làm thế nào để phát hiện ảnh có giấu tin hay không, thông tin chứa trong đó là gì. Hiện nay có một số phương pháp giấu tin và phát hiện tin đang được nghiên cứu rộng rãi. Đồ án của em nhằm tìm hiểu về một số thuật toán giấu tin và phát hiện ảnh có giấu tin.

DANH SÁCH CÁC TỪ VIẾT TẮT

DCT	Discrete Consine Transform	Phép biến đổi cosin rời rạc
IDCT	Inverted Discrete Consine Transform	Phép biến đổi consin rời rạc ngược
LSB	Least Significant Bit	Bit ít quan trọng nhất
PoV	Pair of Values	Cặp giá trị
RS	Regular – Singular	Kỹ thuật chính quy - đơn
IMG	Image	Ảnh đen trắng img
PCX	Personal Computer Exchange	Ảnh xám PCX
GIF	Graphics Interchange Format	Định dạng ảnh đồ họa GIF
BMP	Bitmap	Ảnh không nén Bitmap
JPEG	Joint Photographic Expert Group	Ảnh nén JPEG
RLC	Run Length Coding	Phương pháp nén dữ liệu ảnh loạt dài RLC
LZW	Lampel Ziv Welch	Phương pháp nén dữ liệu ảnh LZW
DES	Data Encryption Standard	Chuẩn mã dữ liệu
Audio		Âm thanh
Video		Âm thanh và hình ảnh nhìn thấy

Chương 1. CÁC KHÁI NIỆM CƠ BẢN

1.1 KHÁI NIỆM MÃ HÓA

1/. ***Mã hóa*** là quá trình chuyển thông tin có thể đọc được (gọi là ***bản rõ***) thành thông tin **"khó"** có thể đọc được theo cách thông thường (gọi là ***bản mã***). Đó là một trong những kỹ thuật để bảo mật thông tin.

2/. ***Giải mã*** là quá trình chuyển thông tin ngược lại từ ***bản mã*** thành ***bản rõ***.

3/. ***Thuật toán mã hóa*** hay ***giải mã*** là thủ tục tính toán để thực hiện mã hóa hay giải mã.

4/. ***Khóa mã hóa*** là một giá trị làm cho thuật toán mã hóa thực hiện theo cách riêng biệt và sinh ra bản mã riêng. Thông thường khóa càng lớn thì bản mã càng an toàn. Phạm vi các giá trị có thể có của khóa được gọi là ***Không gian khóa***.

5/. ***Hệ mã hóa*** là tập các thuật toán, các khóa nhằm che giấu thông tin, cũng như làm rõ nó. Có thể chia hệ mã hóa thành hai loại chính đó là hệ mã hóa khóa đối xứng và hệ mã hóa khóa bất đối xứng.

Hệ mã hóa khóa đối xứng là hệ mã hóa mà biết được khóa lập mã thì có thể "dễ" tính được khóa giải mã và ngược lại. Đặc biệt một số hệ mã hóa có khóa lập mã và khóa giải mã trùng nhau ($k_e = k_d$), như hệ mã hóa "dịch chuyển" hay DES. Hệ mã hóa khóa đối xứng còn gọi là ***Hệ mã hóa khóa bí mật,*** hay ***khóa riêng,*** vì phải giữ bí mật cả 2 khóa. Sự mã hóa và giải mã của hệ thống mã hóa khóa đối xứng biểu thị bởi:

$$E_k: P \rightarrow C \text{ và } D_k: C \rightarrow P$$

Hệ mã hóa khóa phi đối xứng là hệ mã hóa có khóa lập mã và khóa giải mã khác nhau ($k_e \neq k_d$), biết được khóa này cũng **"khó"** tính được khóa kia. Hệ mã hóa này còn được gọi là **Hệ mã hóa khóa công khai** vì:

+ ***Khóa lập mã*** cho ***công khai***, gọi là ***khóa công khai (Public key)***

+ ***Khóa giải mã*** giữ bí mật, còn gọi là ***khóa riêng (Private key)*** hay ***khóa bí mật***

1.2 KHÁI NIỆM GIẤU TIN

1.2.1 Khái niệm

1/. Môi trường giấu tin (cover multimedia) (hay còn gọi là vật mang tin) là đối tượng được dùng để giấu tin như văn bản, ảnh, audio, video…

Giấu tin trong ảnh:

Thông tin sẽ được giấu vào dữ liệu ảnh nhưng chất lượng ảnh ít thay đổi và "khó" biết được đằng sau ảnh đó mang những thông tin có ý nghĩa gì.

Trong ảnh thông tin được giấu một cách vô hình. Nó là một cách truyền thông tin mật cho nhau mà người khác không thể biết được.

Giấu tin trong audio:

Giấu tin trong audio lại phụ thuộc vào hệ thống thính giác. 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.

Giấu tin trong video:

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

2/. Dữ liệu sẽ được giấu (information) là một lượng thông tin mang ý nghĩa nào đó, tùy thuộc vào mục đích của người sử dụng.

3/. Giấu thông tin là nhúng mẩu tin mật vào một vật mang tin khác, sao cho mắt thường "khó" phát hiện ra mẩu tin mật đó, mặt khác khó nhận biết được vật mang tin đã được giấu một tin mật.

1.2.2 So sánh giữa giấu tin và mã hóa

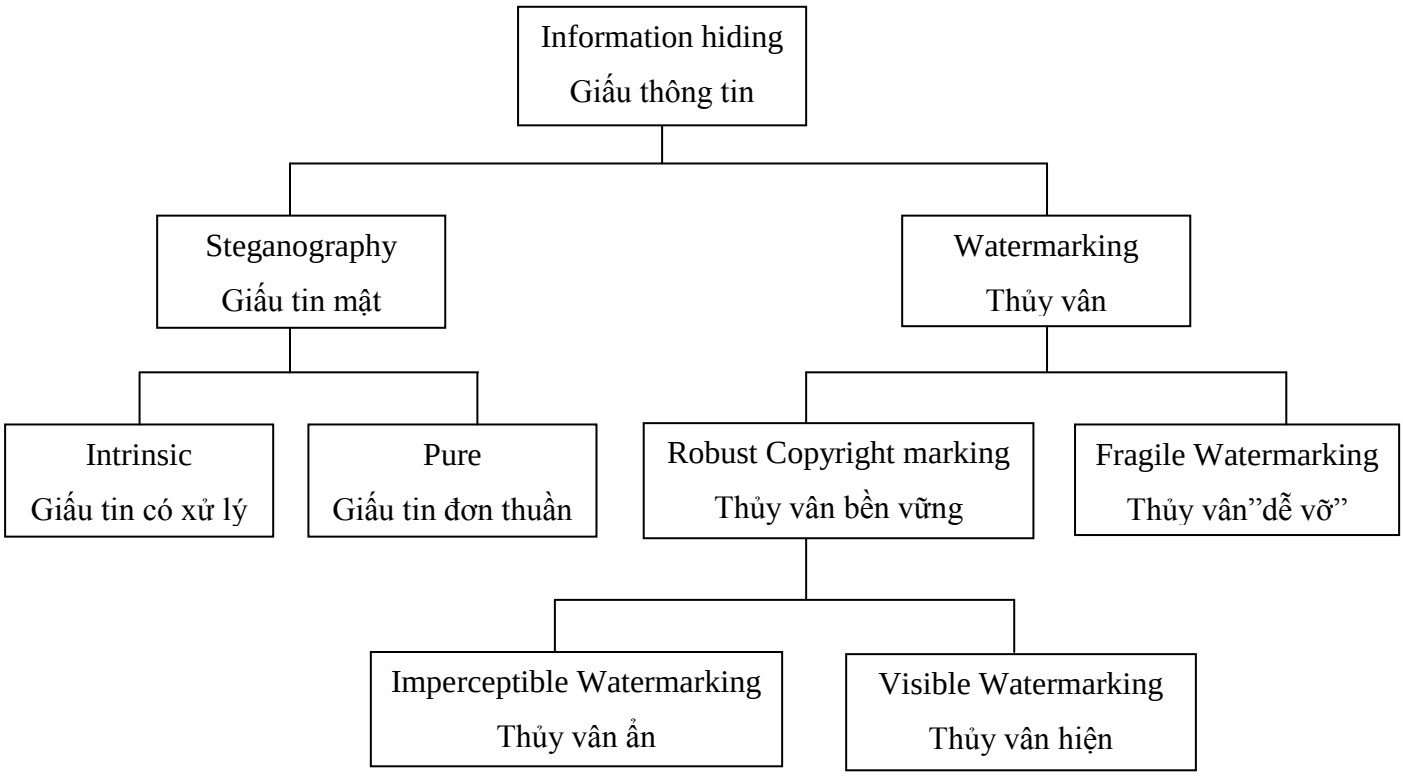
Giống nhau: cùng mục đích là để đối phương "khó" phát hiện ra tin cần giấu.

Khác nhau: "Mã hóa" là giấu đi "ý nghĩa" của thông tin.

"Giấu tin" là giấu đi "sự hiện diện" của thông tin.

1.3 PHÂN LOẠI CÁC KỸ THUẬT GIẤU TIN

Có thể chia kỹ thuật giấu tin ra làm 2 loại lớn đó là thủy vân (watermarking) và giấu tin mật (steganography).



Hình 1. Phân loại các kỹ thuật giấu tin

1/. Thủy vân số (Watermarking): Giấu mẩu tin ngắn, nhưng đòi hỏi độ bền vững cao của thông tin cần giấu (trước các biến đổi thông thường của tệp dữ liệu môi trường).

- Thủy vân bền vững: thường được ứng dụng trong bảo vệ bản quyền. Thủy vân được nhúng trong sản phẩm như một hình thức dán tem bản quyền. Trong trường hợp này, thủy vân phải tồn tại bền vững cùng với sản phẩm nhằm chống việc tẩy xóa, làm giả hay biến đổi phá hủy thủy vân.

- Thủy vân dễ vỡ: Là kỹ thuật nhúng thủy vân vào trong một đối tượng (sản phẩm) sao cho khi phân bố sản phẩm (trong môi trường mở) nếu có bất kỳ phép biến đổi nào làm thay đổi sản phẩm gốc thì thủy vân đã được giấu trong đối tượng sẽ không còn nguyên vẹn như trước khi giấu.
- Thủy vân ẩn: Cũng giống như giấu tin, bằng mắt thường không thể nhìn được thủy vân ẩn.
- Thủy vân hiện: Là loại thủy vân hiện ngay trên sản phẩm và mọi người đều có thể nhìn thấy được.

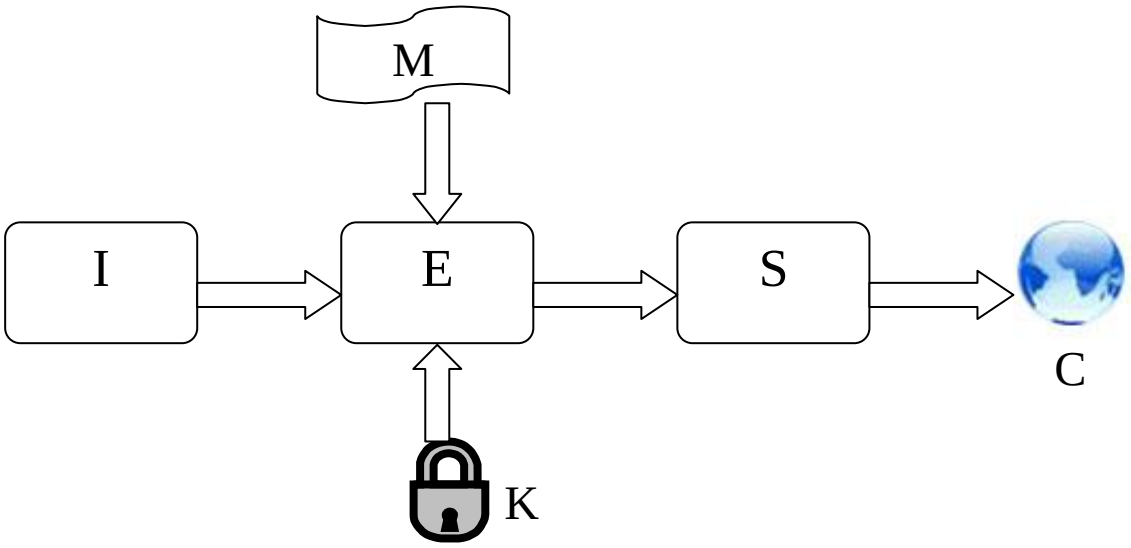
2/. Giấu tin mật (Steganography): Che giấu bản tin (đòi hỏi độ mật cao và dung lượng càng lớn càng tốt) vào môi trường (đối tượng) gốc.

Phân biệt giữa Steganography và watermarking

Steganography	Watermarking
– Tập trung vào việc giấu được càng nhiều tin càng tốt, ứng dụng trong truyền dữ liệu mật. – Cố gắng làm ảnh hưởng ít nhất đến chất lượng của đối tượng gốc để không bị chú ý đến dữ liệu đã được giấu trong đó. – Thay đổi đối tượng gốc cũng làm cho dữ liệu giấu bị sai lệch (ứng dụng trong xác thực thông tin). – Bảo mật cho dữ liệu cần giấu. Khía cạnh này tập trung vào kỹ thuật giấu tin mật, tức là giấu tin sao cho giấu được nhiều và người khác khó phát hiện ra thông tin được giấu trong đó.	– Không cần giấu nhiều thông tin, chỉ cần lượng thông tin nhỏ đặc trưng cho bản quyền của người sở hữu. – Trong trường hợp thủy vân nhìn thấy thì thủy vân sẽ hiện ra. – Thủy vân phải bền vững với mọi tấn công có chủ đích hoặc không có chủ đích vào sản phẩm. – Thủy vân số đánh dấu vào chính đối tượng, nhằm khẳng định bản quyền sở hữu hay phát hiện xuyên tạc thông tin.

1.4 MÔ HÌNH KỸ THUẬT GIẤU TIN

Mô hình kỹ thuật giấu tin cơ bản được trình bày trên hình vẽ sau:



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

Hình vẽ trên biểu diễn quá trình giấu thông tin cơ bản. Đối tượng được dùng làm môi trường để giấu tin như văn bản, ảnh, audio, video,… Dữ liệu giấu là một lượng thông tin mang ý nghĩa nào đó, tùy thuộc vào mục đích của người sử dụng. Thông tin sẽ được giấu vào trong phương tiện chứa nhờ một bộ nhúng, bộ nhúng là chương trình, những thuật toán để giấu tin và được thực hiện với khóa bí mật giống như các hệ mật mã cổ điển. Sau khi giấu tin, ta thu được phương tiện chứa đã mang thông tin và phân phối sử dụng trên mạng.

Trên hình vẽ:

- Secret Message (M): thông tin cần giấu.
- Cover Data (I): dữ liệu phủ, môi trường sẽ giấu tin.
- Embeding Algorithm (E): thuật toán nhúng tin.
- Key (K): Khóa bí mật, sử dụng trong giấu tin.
- Stego Data (S): dữ liệu mang tin mật, hay môi trường đã chứa tin mật.
- Control (C): Kiểm tra thông tin sau khi tách tin.

1.5 MỘT SỐ ỨNG DỤNG

1/. Bảo vệ bản quyền tác giả

Là ứng dụng cơ bản nhất của kỹ thuật thủy vân số - một dạng của phương pháp giấu tin. Một thông tin nào đó mang ý nghĩa quyền sở hữu tác giả (người ta gọi là thủy vân - watermark) sẽ được nhúng vào trong sản phẩm, thủy vân đó chỉ một mình người chủ sở hữu hợp pháp sản phẩm đó có, và được dùng làm minh chứng cho bản quyền sản phẩm. Yêu cầu kỹ thuật đối với ứng dụng này là thủy vân phải tồn tại bền vững cùng với sản phẩm, muốn bỏ thủy vân này mà không được phép của người chủ sở hữu, thì chỉ có cách là phá hủy sản phẩm.

2/. Xác thực thông tin hay phát hiện xuyên tạc thông tin (authentication and tamper detection)

Một tập các thông tin sẽ được giấu trong phương tiện chứa sau đó được sử dụng để nhận biết xem dữ liệu trên phương tiện gốc đó có bị thay đổi hay không.

3/. Dấu vân tay hay dán nhãn (fingerprinting and labeling)

Thủy vân trong ứng dụng này để nhận diện người gửi hay người nhận của một thông tin nào đó.

4./ Điều khiển truy cập (copy control)

Thủy vân trong trường hợp này để điều khiển truy cập đối với thông tin. Các thiết bị phát hiện ra thủy vân thường được gắn sẵn vào trong hệ thống đọc ghi.

Ví dụ như hệ thống quản lý sao chép DVD đã được ứng dụng ở Nhật. Ứng dụng loại này yêu cầu thủy vân phải được bảo đảm an toàn và sử dụng phương pháp phát hiện thủy vân đã giấu mà không cần thông tin gốc.

5/. Giấu tin mật (steganography)

Là ứng dụng giấu một lượng thông tin mật, quan trọng vào bên trong một đối tượng gốc nhằm che giấu, truyền thông bí mật điểm – điểm. Các thông tin giấu được (trong trường hợp này) càng nhiều càng tốt. Việc giải mã (tách tin) để nhận được thông tin, cũng không cần phương tiện chứa (gốc) ban đầu.

1.6 TÍNH CHẤT, ĐẶC TRƯNG CỦA GIẤU TIN TRONG ẢNH

1.6.1 Phương tiện chứa có dữ liệu tri giác tĩnh

Dữ liệu gốc ở đây là dữ liệu ảnh tĩnh, dù đã giấu thông tin vào trong ảnh hay chưa, thì khi người ta xem ảnh bằng thị giác, dữ liệu ảnh không thay đổi theo thời gian. Khác với dữ liệu audio hay video, khi nghe hay xem, thì dữ liệu gốc sẽ thay đổi liên tục với tri giác của con người theo các đoạn hay các bài, các ảnh,…

1.6.2 Giấu tin phụ thuộc ảnh

Kỹ thuật giấu tin phụ thuộc vào các loại ảnh khác nhau. Chẳng hạn đối với ảnh đen trắng, ảnh xám hay ảnh màu, ta có những kỹ thuật riêng do các loại ảnh với đặc trưng khác nhau. Ảnh nén và ảnh không nén cũng áp dụng những kỹ thuật giấu tin khác nhau, vì ảnh nén có thể làm mất thông tin khi nén ảnh…

1.6.3 Giấu tin lợi dụng khả năng thị giác của con người

Giấu tin trong ảnh cũng gây ra những thay đổi trên dữ liệu ảnh gốc. Dữ liệu ảnh được quan sát bằng hệ thống thị giác con người, nên các kỹ thuật giấu tin phải đảm bảo yêu cầu cơ bản là những thay đổi trên ảnh phải rất nhỏ, sao cho bằng mắt thường không thể nhận ra được sự thay đổi đó, vì có như thế thì mới đảm bảo được độ an toàn cho thông tin giấu.

1.6.4 Giấu tin không làm thay đổi kích thước ảnh

Các phép toán giấu tin sẽ được thực hiện trên dữ liệu của ảnh. Dữ liệu ảnh bao gồm cả phần header (là nơi lưu các thông tin về tệp, kích thước, và địa chỉ offset về vùng dữ liệu), bảng màu (có thể có) và dữ liệu ảnh. Khi giấu tin, các phương pháp giấu đều biến đổi giá trị của các bit trong dữ liệu ảnh trước hay sau khi giấu tin, là như nhau.

1.6.5 Đảm bảo chất lượng ảnh sau khi giấu tin

Đây là yêu cầu quan trọng đối với giấu tin trong ảnh. Sau khi giấu tin bên trong, ảnh phải đảm bảo yêu cầu không bị biến đổi, để có thể không bị phát hiện dễ dàng so với ảnh gốc.

1.7 CÁC ĐỊNH DẠNG ẢNH THÔNG DỤNG

Ảnh thu được sau quá trình số hóa có nhiều loại khác nhau, phụ thuộc vào kỹ thuật số hóa ảnh. Sau đây là một số định dạng ảnh thông dụng.

1.7.1 Định dạng ảnh: IMG (Image)

Ảnh IMG là ảnh đen trắng, mỗi điểm ảnh được thể hiện bởi 1 bit. Toàn bộ ảnh chỉ gồm các điểm sáng và tối tương ứng với giá trị 1 hoặc 0.

Tỉ lệ nén của kiểu định dạng này là khá cao. Ảnh IMG được nén theo từng dòng. Mỗi dòng bao gồm các gói (Pack). Các dòng giống nhau được nén thành một gói.

1.7.2 Định dạng ảnh: PCX (Personal Computer Exchange)

Định dạng ảnh PCX là một trong những định dạng loại cổ điển nhất. Nó sử dụng phương pháp mã hóa loạt dài RLC để nén dữ liệu ảnh. Quá trình nén và giải nén được thực hiện trên từng dòng ảnh. Thực tế, phương pháp giải nén PCX kém hiệu quả hơn so với kiểu IMG.

Định dạng ảnh PCX thường được dùng để lưu trữ ảnh vì thao tác đơn giản, cho phép nén và giải nén nhanh. Tuy nhiên vì cấu trúc của nó cố định, nên trong một số trường hợp nó làm tăng kích thước lưu trữ.

1.7.3 Định dạng ảnh: GIF (Graphics Interchanger Format)

Định dạng ảnh GIF do hãng Computer Incorporated (Mỹ) đề xuất lần đầu tiên vào năm 1990. Với định dạng GIF, khi số màu trong ảnh càng tăng, thì ưu thế của định dạng GIF càng nổi trội. Những ưu thế này có được là do GIF tiếp cận các thuật toán LZW (Lampel Ziv Welch) (dựa vào sự lặp lại của một nhóm điểm, người ta xây dựng từ điển lưu các chuỗi ký tự có tần suất lặp lại cao và thay thế bằng từ mã tương ứng mỗi khi gặp lại chúng). Dạng ảnh GIF cho chất lượng cao, độ phân giải đồ họa tốt, cho phép hiển thị trên hầu hết các phần cứng đồ họa.

1.7.4 Định dạng ảnh: BMP (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 kỳ phần cứng nào. Tên file mở rộng mặc định của một file ảnh Bitmap là BMP, nét vẽ được thể hiện là các điểm ảnh. Qui ước màu đen, trắng tương ứng với các giá trị 0, 1. Ảnh BMP được sử dụng trên Microsoft Windows và các ứng dụng chạy trên Windows từ version 3.0 trở lên. BMP thuộc loại ảnh mảnh.

Có rất nhiều định dạng ảnh thuộc kiểu bitmap như BMP, PCX, TIFF, GIF, JPEG, TGA, PNG, PCD…Mỗi file ảnh BMP gồm bốn phần:

- Bitmap Header (14 bytes): giúp nhận dạng tập tin bitmap.
- Bitmap Information (40 bytes): chứa một số thông tin chi tiết giúp hiển thị ảnh.
- Palette màu (4*x bytes), x là số màu của ảnh: định nghĩa các màu sẽ được sử dụng trong ảnh.
- Bitmap Data: Chứa dữ liệu ảnh.

Đặc điểm nổi bật nhất của định dạng BMP là tập tin ảnh thường không được nén bằng bất kỳ thuật toán nào. Khi lưu ảnh, các điểm ảnh được ghi trực tiếp vào tập tin - một điểm ảnh sẽ được mô tả bởi một hay nhiều byte tùy thuộc vào giá trị n của ảnh. Do đó, một hình ảnh lưu dưới dạng BMP thường có kích cỡ rất lớn, gấp nhiều lần so với các ảnh được nén (chẳng hạn GIF, JPEG hay PNG).

1.7.5 Định dạng ảnh: JPEG (Joint Photographic Expert Group)

Một nhóm các nhà nghiên cứu đã phát minh ra định dạng này, để hiển thị các hình ảnh đầy đủ màu hơn (full-colour) cho định dạng di động, mà kích thước file lại nhỏ hơn. Giống như ảnh GIF, JPEG cũng được sử dụng nhiều trên Web.

Lợi ích của JPEG hơn GIF là nó có thể hiển thị hình ảnh với màu chính xác (true-colour) (có thể lên đến 16 triệu màu). Điều đó cho phép JPEG được sử dụng tốt nhất cho hình ảnh chụp và hình ảnh minh họa có số lượng màu lớn.

Nhược điểm chính của định dạng JPEG là chúng được nén bằng thuật toán lossy (mất dữ liệu). Điều này có nghĩa rằng hình ảnh sẽ bị mất một số chi tiết khi chuyển sang định dạng JPEG. Đường bao giữa các khối màu có thể xuất hiện nhiều điểm mờ, và các vùng sẽ mất sự rõ nét.

Nói cách khác, định dạng JPEG thực hiện bảo quản tất cả thông tin màu trong hình ảnh đó. Tuy nhiên với các hình ảnh chất lượng màu cao (high-colour) như hình ảnh chụp, thì điều này sẽ không ảnh hưởng gì.

Ảnh JPEG không thể làm trong suốt hoặc chuyển động, trong trường hợp này ta sẽ sử dụng định dạng GIF (hoặc định dạng PNG để tạo trong suốt).

Tạo ảnh JPEG Fast-Loading:

Giống như với các ảnh GIF, để tạo hình JPEG nhỏ đến mức có thể (tính theo bytes) để website tải nhanh hơn. Điều chỉnh chính để thay đổi kích thước file JPEG được gọi là quality, và thường có giá trị từ 0 tới 100%, khi 0% thì chất lượng là thấp nhất (nhưng kích thước file là nhỏ nhất), và 100% thì chất lượng cao nhất (nhưng kích thước file là lớn nhất). 0% chất lượng JPEG sẽ nhìn rất mờ khi so sánh với ảnh gốc. Còn 100% chất lượng JPEG thường không phân biệt được so với ảnh gốc.

1.8 CÁC TIÊU CHÍ ĐÁNH GIÁ KỸ THUẬT GIẤU TIN TRONG ẢNH SỐ

1.8.1 Tính vô hình

Như đã nêu, kỹ thuật giấu thông tin trong ảnh phụ thuộc rất nhiều vào hệ thống thị giác của con người. Tính vô hình hay không cảm nhận được (imperceptible) của mắt người thường giảm dần ở những vùng ảnh có màu xanh tím, thủy vân ẩn thường được chọn giấu trong vùng này.

1.8.2 Khả năng giấu thông tin

Khả năng giấu thông tin (Hiding Capacity) hay lượng thông tin giấu được (dung lượng) trong một ảnh được tính bằng tỉ lệ giữa lượng thông tin giấu và kích thước của ảnh. Các thuật toán giấu tin đều cố gắng đạt được mục tiêu giấu được nhiều tin và gây nhiễu không đáng kể. Thực tế, người ta luôn phải cân nhắc giữa dung lượng tin cần giấu với các tiêu chí khác như chất lượng (Quality), tính bền vững (Robustness) của thông tin giấu.

1.8.3 Chất lượng của ảnh có giấu thông tin

Chất lượng của ảnh có giấu tin được đánh giá qua sự cảm nhận của mắt người. Nên chọn những ảnh có nhiễu, có những vùng góc cạnh hoặc có cấu trúc, làm ảnh môi trường vì mắt thường ít nhận biết được sự biến đổi, khi có tin giấu, trên những ảnh này.

1.8.4 Tính bền vững của thông tin được giấu

Tính bền vững thể hiện qua việc các thông tin giấu không bị thay đổi khi ảnh mang tin phải chịu tác động của các phép xử lý ảnh như nén, lọc, biến đổi, tỉ lệ,…

1.8.5 Thuật toán và độ phức tạp tính toán

Cần nắm được một số kiến thức cơ bản về cấu trúc của ảnh để chọn ra thuật toán tìm miền ảnh thích hợp cho việc giấu tin. Độ phức tạp của thuật toán mã hóa và giải mã là yếu tố quan trọng để đánh giá các phương pháp giấu tin trong ảnh. Yêu cầu về độ phức tạp tính toán phụ thuộc vào từng ứng dụng. Những ứng dụng theo hướng Watermark thường có thuật toán phức tạp hơn hướng Steganography.

1.9 CÁC HƯỚNG TIẾP CẬN CỦA GIẤU TIN TRONG ẢNH

1.9.1 Tiếp cận trên miền không gian của ảnh

Đây là hướng tiếp cận cơ bản và tự nhiên trong số các kỹ thuật giấu tin. Miền không gian ảnh là miền dữ liệu ảnh gốc, tác động lên miền không gian ảnh chính là tác động lên các điểm ảnh, thay đổi trực tiếp giá trị của các điểm ảnh. Đây là hướng tiếp cận tự nhiên, bởi vì khi nói đến việc giấu tin trong ảnh người ta thường nghĩ ngay đến việc thay đổi giá trị các điểm ảnh nguồn. Một phương pháp phổ biến của hướng tiếp cận này là phương pháp tác động đến bit ít quan trọng nhất của mỗi điểm ảnh.

Ý tưởng cơ bản của phương pháp tác động đến bit ít quan trọng nhất (LSB – Least Significant Bit) của các điểm ảnh là chọn ra từ mỗi điểm ảnh các bit ít có ý nghĩa nhất về mặt tri giác, để sử dụng cho việc giấu tin. Việc bit nào được coi là ít tri giác nhất và bao nhiêu bit có thể được lấy ra để thay thế đều phụ thuộc vào khả năng hệ thống thị giác của con người và nhu cầu về chất lượng ảnh trong các ứng dụng.

1.9.2 Tiếp cận trên miền tần số của ảnh

Trong một số trường hợp cách khảo sát trực tiếp ở trên cũng gặp phải khó khăn nhất định hoặc rất phức tạp và hiệu quả không cao, do đó ta có thể dùng phương pháp khảo sát gián tiếp thông qua các kỹ thuật biến đổi. Các biến đổi này làm nhiệm vụ chuyển miền biến số độc lập sang miền khác, và như vậy tín hiệu và hệ thống rời rạc sẽ được biểu diễn trong miền mới với các biến số mới.

Mỗi cách biến đổi sẽ có những thuận lợi riêng, tùy từng trường hợp mà sử dụng biến đổi nào. Sau khi khảo sát, biến đổi xong các tín hiệu và hệ thống rời rạc trong miền các biến số mới này, nếu cần thiết có thể dùng các biến đổi ngược để đưa chúng về miền biến số độc lập.

Phương pháp khảo sát gián tiếp sẽ làm đơn giản rất nhiều các công việc gặp phải khi dùng phương pháp khảo sát trực tiếp trong miền biến số độc lập tự nhiên. Có nhiều phép biến đổi, trong đó phổ biến là biến đổi Fourier DFT, biến đổi Cosin rời rạc DCT, biến đổi sóng nhỏ DWT…

Chương 2. MỘT SỐ PHƯƠNG PHÁP GIẤU TIN TRONG ẢNH

Để thực hiện việc giấu thông tin trong môi trường ảnh, trước hết cần số hóa các bức ảnh theo những chuẩn phổ biến như JPEG, PCX, GIF,…

2.1 GIẤU TIN BẰNG THAY THẾ BIT CÓ TRỌNG SỐ THẤP NHẤT

LSB (Least Significant Bit) là bit có ảnh hưởng ít nhất tới việc quyết định màu sắc của mỗi điểm ảnh, vì vậy khi ta thay đổi ít nhất tới việc quyết định màu sắc của mỗi điểm ảnh, vì vậy khi ta thay đổi bit này thì màu sắc của điểm ảnh mới sẽ gần như không khác biệt so với điểm ảnh cũ.

LSB của một điểm ảnh có vị trí tương tự như chữ số hàng đơn vị của một số tự nhiên, khi bị thay đổi, giá trị chênh lệch giữa số cũ và số mới sẽ ít nhất, so với khi ta thay đổi giá trị của chữ số hàng chục hoặc hàng trăm. 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 ảnh của ảnh đó.

Mục đích của phương pháp là chọn ra các bit ít quan trọng (ít làm thay đổi chất lượng của ảnh nền) và thay thế chúng bằng các bit thông tin cần giấu. Để khó bị phát hiện, thông tin giấu thường được nhúng vào những vùng mắt người kém nhạy cảm với màu sắc. Với ảnh 24 bit, mỗi màu được chứa trong 3 byte, theo thứ tự từ trái sang phải, byte đầu tiên chứa giá trị biểu thị cường độ màu lam (B), byte thứ hai chứa giá trị biểu thị cường độ màu lục (G), byte thứ ba chứa giá trị biểu thị cường độ màu đỏ (R). Như vậy, mỗi màu được xác định bởi một số nguyên có giá trị trong khoảng 0 – 255.

2.1.1 Phương pháp giấu tin

Tư tưởng của thuật toán là chọn ngẫu nhiên một điểm ảnh, với mỗi điểm ảnh, chọn ngẫu nhiên một byte màu, sau đó giấu bit tin vào bit màu có trọng số thấp nhất. Để tăng tính bảo mật, thông tin thường được nhúng vào các vùng trong ảnh mà mắt người kém nhạy cảm. Đối với ảnh 24 bit màu, mỗi điểm ảnh được chứa trong 3 byte, như vậy mỗi màu được xác định bởi 1 số nguyên có giá trị trong miền từ 1 đến 256. Thuật toán thay thế k bit có trọng số nhỏ nhất sử dụng trong ảnh 24 bit màu, có thể biểu diễn qua các bước sau:

B1: Thông tin cần giấu được biểu thị bởi luồng bit, và luồng bit này được chia nhỏ thành các cụm k bit: E_iB, E_iG, E_iR.

Điểm ảnh thứ i ký hiệu H_i chứa 24 bit được tách ra làm 3 byte riêng B_i, G_i, R_i ứng với màu xanh lục, xanh lam, đỏ. Từ các byte này, lại tách ra các khối k bit cuối kí hiệu B_ik, G_ik, R_ik.

Là bước giải rác tin. Thông tin có thể được mã hóa, sau đó lại tạo một hàm băm ngẫu nhiên. Tham số seed là hạt giống để sinh ra các số ngẫu nhiên. Nếu dùng cùng một hạt giống, sẽ sinh ra các chuỗi số ngẫu nhiên giống nhau, là điểm chọn để giấu tin trong ảnh. Quá trình rải tin phải được kiểm tra để chọn ra những điểm chưa có tin giấu. Đặc tính của hàm Collection là không lưu các giá trị trùng lặp, nên điểm sinh ra sẽ là duy nhất.

B2: Thay thế B_ik, G_ik, R_ik bởi các giá trị tương ứng E_iB, E_iG, E_iR

Mỗi điểm ảnh mới nhận được, ký hiệu H_i' sẽ mang 3 × (8 - k) bit có trọng số cao cho thông tin về ảnh, và 3 × k bit trọng số thấp cho thông tin giấu. Gọi ảnh nhận được sau khi thay thế là H'.

Là bước giấu thông tin ảnh. Mỗi lần chọn 1 byte thông tin, trích từng bit từ 1 đến 8, giấu bit tin vào điểm ảnh chưa dùng. Có thể giấu tối đa 3 bit tin trong 1 điểm ảnh.

B3: Tách các thông tin bằng cách tách từ mỗi điểm ảnh 3 cụm k bit từ các byte B_i, G_i, R_i, và chắp lại thành bản tin giấu.

Kỹ thuật này tuy đơn giản, nhưng nếu bản tin trước khi giấu đã được mã hóa và trật tự giấu tin được chọn theo một quy luật nào đó, thì việc tách thông tin từ H' sẽ không đơn giản.

2.1.2 Phương pháp tách tin

B3.1 Cung cấp hạt giống seed như B1, tìm điểm ảnh và byte có chứa tin. Trích bit tin mật.

B3.2 Ghép các bit tin mật thành từng byte, chắp các byte thành bản tin đã giấu.

B3.3 Tách tin, thu được thông tin giấu.

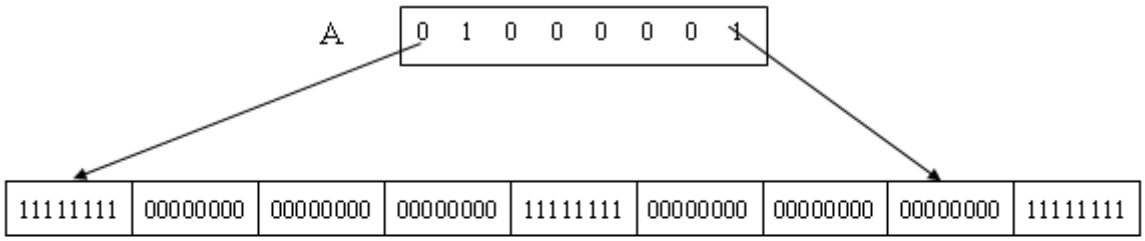
Ví dụ:

Giả sử, cần giấu tin là chữ A vào một vùng ảnh với mỗi điểm ảnh có các màu kề nhau gồm lam, lục và đỏ:

Số hóa thông tin và ảnh gốc, kết quả thu được trong bảng sau:

Ký hiệu	Giá trị thập phân	Giá trị nhị phân
A	65	01000001
Màu lam (B, G, R)	(255,0,0)	11111111, 00000000, 00000000
Màu lục (B, G, R)	(0, 255, 0)	00000000, 11111111, 00000000
Màu đỏ (B, G, R)	(0,0,255)	00000000, 00000000, 11111111

Thực hiện giấu tin vào ảnh theo kỹ thuật LSB, lật bit bên phải nhất



Kết quả giấu thông tin theo kỹ thuật LSB

11111110	00000001	00000000	00000000	11111110	00000000	00000000	00000001	11111111

2.1.3 Phân tích thuật toán

1/. Đánh giá thuật toán

Thuật toán giấu tin được coi là an toàn nếu thông tin được giấu không bị phát hiện hoặc thời gian phát hiện được thông tin giấu là đủ lâu, bảo đảm được bí mật.

Kỹ thuật LSB cho phép giấu tối đa $[\log_2((m \times n)+1)]$ bit dữ liệu vào một khối ảnh kích thước $m \times n$. Hàm f (tỉ lệ giấu tin) được tính theo công thức:

$$f = \frac{\log_2((m \times n)+1)}{m \times n}$$

Vậy f có giá trị giảm theo $m \times n$ (kích thước khối ảnh càng nhỏ thì càng giấu được nhiều tin). Tuy nhiên, độ an toàn của thông tin lại tỉ lệ thuận với kích thước khối ảnh: kích thước khối càng lớn, độ an toàn cho thông tin giấu càng cao.

Vì thế việc chọn kích thước khối giấu tin lớn sẽ làm tăng độ an toàn nhưng lại giảm tỉ lệ tin giấu được và ngược lại, kích thước khối nhỏ sẽ làm tăng tỉ lệ tin giấu nhưng lại làm giảm độ an toàn. Thông thường ta nên chọn kích thước khối sao cho $[\log_2((m \times n)+1)] = 8$ hoặc bằng 4, tức là giấu được tối đa 8 bit hay 4 bit dữ liệu vào mỗi khối ảnh kích thước $m \times n$.

2/. Ưu, nhược điểm của thuật toán

- Ưu điểm: Việc thay thế một, hai hay nhiều hơn nữa các bit LSB của mỗi điểm ảnh sẽ làm tăng dung lượng nhưng làm giảm độ an toàn của thông tin được giấu. Kỹ thuật LSB đơn giản, dễ cài đặt và phát huy hiệu quả tốt trong nhiều ứng dụng.
- Nhược điểm: Kém bền vững trước tác động của các phép xử lý ảnh, nên phương pháp chỉ thích hợp cho giấu tin mà không thích hợp cho thủy vân.

2.2 GIẤU TIN TRÊN MIỀN BIẾN ĐỔI DCT

2.2.1 Biến đổi DCT thuận và nghịch

Vì ảnh gốc có kích thước rất lớn nên trước khi biến đổi DCT, ảnh được phân chia thành các khối, mỗi khối này thường có kích thước 8 x 8 pixel và biểu diễn các mức xám của 64 điểm ảnh, các mức xám này là các số nguyên dương có giá trị từ 0 đến 255. Việc phân khối này sẽ làm giảm được một phần thời gian tính toán các hệ số chung, mặt khác biến đổi cosin đối với các khối nhỏ sẽ làm tăng độ chính xác khi tính toán với dấu phẩy tĩnh, giảm thiểu sai số do làm tròn sinh ra.

Biến đổi DCT là một công đoạn chính trong các phương pháp nén sử dụng biến đổi. Hai công thức ở đây minh hoạ cho 2 phép biến đổi DCT thuận nghịch đối với mỗi khối ảnh có kích thước 8 x 8.

Giá trị $x(n_1, n_2)$ biểu diễn các mức xám của ảnh trong miền không gian, $X(k_1, k_2)$ là các hệ số sau biến đổi DCT trong miền tần số.

$$X(k_1,k_2) = \frac{\varepsilon_{k1}\varepsilon_{k2}}{4}\sum_{n1=0}^{7}\sum_{n2=0}^{7} x(n_1,n_2)\cos\frac{(2n_1+1)k_1\pi}{16}\cos\frac{(2n_2+1)k_2\pi}{16}$$

$$x(n_1,n_2) = \frac{\varepsilon_{k1}\varepsilon_{k2}}{4}\sum_{n1=0}^{7}\sum_{n2=0}^{7} X(k_1,k_2)\cos\frac{(2n_1+1)k_1\pi}{16}\cos\frac{(2n_2+1)k_2\pi}{16}$$

Với $\varepsilon_{k1} = \begin{cases} 1/\sqrt{2} & \text{khi } k_1 = 0 \\ 0 & \text{khi } 1 < k_1 < 8 \end{cases}$ và $\varepsilon_{k2} = \begin{cases} 1/\sqrt{2} & \text{khi } k_2 = 0 \\ 0 & \text{khi } 1 < k_2 < 8 \end{cases}$

2.2.2 Đặc điểm của phép biến đổi DCT trên ảnh hai chiều

+ Thể hiện đặc tính nội dung về tần số của thông tin ảnh. Hệ số góc trên là lớn và đặc trưng cho giá trị trung bình thành phần một chiều gọi là hệ số DC, các hệ số khác có giá trị nhỏ hơn biểu diễn cho các thành phần tần số cao theo hướng ngang và dọc gọi là hệ số AC.

+ Bản thân biến đổi DCT không nén được dữ liệu vì sinh ra 64 hệ số.

+ Theo nguyên lý chung, khi biến đổi chi tiết giữa các điểm ảnh càng lớn theo một hướng nào đó trong khối các điểm ảnh, hướng ngang hoặc dọc hoặc theo đường chéo thì tương ứng theo hướng đó, các hệ số biến đổi DCT cũng lớn.

DCT làm giảm độ tương quan không gian của thông tin trong khối ảnh. Điều đó cho phép biểu diễn thích hợp ở miền DCT do các hệ số DCT có xu hướng có phần dư thừa ít hơn. Hơn nữa, các hệ số DCT chứa thông tin về nội dung tần số không gian của thông tin trong khối. Nhờ các đặc tính tần số không gian của hệ thống nhìn của mắt người, các hệ số DCT có thể được mã hóa phù hợp, chỉ các hệ số DCT quan trọng nhất mới được mã hóa để chuyển đổi.

Khối hệ số DCT có thể chia làm 3 miền: miền tần số thấp, miền tần số cao và miền tần số giữa. Miền tần số thấp chứa các thông tin quan trọng ảnh hưởng đến tri giác. Miền tần số cao thường không mang tính tri giác cao, khi nén JPEG thường loại bỏ thông tin trong miền này.

Trong các thuật toán thủy vân, miền hệ số DCT tần số cao thường không được sử dụng do nó thường không bền vững với các phép xử lý ảnh, hoặc nền ảnh JPEG. Miền tần số thấp cũng khó được sử dụng do một sự thay đổi dù nhỏ trong miền này cũng dẫn đến chất lượng tri giác của ảnh. Vì vậy, miền tần số ở giữa thường hay được sử dụng nhất và cũng cho kết quả tốt nhất.

2.2.3 Kỹ thuật thủy vân sử dụng phép biến đổi DCT

2.2.3.1 Quá trình nhúng thủy vân

Thuật toán dưới đây sẽ sử dụng phương pháp nhúng thuỷ vân trong miền tần số của ảnh, giải tần được sử dụng để chứa tín hiệu thuỷ vân là miền tần số ở giữa của một khối DCT 8x8. Trong đó, các khối DCT 8x8 là những khối ảnh cùng kích thước đã được chọn ra ngẫu nhiên từ ảnh ban đầu và được áp dụng phép biến đổi cosin rời rạc DCT để chuyển sang miền tần số. Mỗi tín hiệu thuỷ vân sẽ được chứa trong một khối.

Input:

- Một chuỗi các bit thể hiện bản quyền
- Một ảnh

Output:

- Một ảnh sau khi thủy vân
- Khóa để giải mã

1/. Các bước thực hiện

Bước 1**:** Ảnh F có kích thước m × n sẽ được chia thành (m × n) / 64 khối 8 ×8, mỗi bit của thủy vân sẽ được giấu trong khối B_k

Bước 2: Chọn một khối bất kì B_k và biến đổi DCT khối đó thu được C_k

$C_k = DCT(B_k)$

Bước 3: Chọn hai hệ số ở vị trí bất kì trong miền tần số giữa của khối C_k, gọi hai hệ số đó là $C_k[i, j] = C_k[p, q]$.

Bước 4: Tính độ lệch $d = ||C_k[i, j]| - |C_k[p, q]|| \bmod a$. Trong đó a là một tham số thỏa mãn $a = 2 (2t + 1)$, với t là một số nguyên dương.

Bước 5: Bit b_k sẽ được nhúng vào khối C_k sao cho thỏa mãn điều kiện sau:

$$\begin{cases} d \geq 2t+1 & \text{Nếu } b_k = 1 \\ d < 2t+1 & \text{Nếu } b_k = 0 \end{cases}$$

Bước 6: Nếu $d < 2t + 1$ và $b_k = 1$ thì trong hệ số DCT $C_k[i,j]$ hoặc $C_k[p,q]$ có giá trị tuyệt đối lớn hơn sẽ bị thay đổi để thỏa $d \geq 2t + 1$ theo công thức sau

$$\text{Max}(|C_k[i, j]|, |C_k[p, q]|) + (\text{INT}(0.75a) - d)$$

Hệ số được chọn sẽ được cộng thêm một lượng là $(\text{INT}(0.75a) - d)$

$$\text{Min}(|C_k[i, j]|, |C_k[p, q]|) - (\text{INT}(0.75a) + d)$$

Hệ số được chọn sẽ được trừ đi 1 lượng là $(\text{INT}(0.75a) + d)$

Bước 7: Nếu $d \geq 2t + 1$ và $b_k = 0$ thì một trong hai hệ số DCT $C_k[i, j]$ hoặc $C_k[p, q]$ có giá trị tuyệt đối lớn hơn sẽ bị thay đổi để thỏa mãn $d < 2t + 1$ theo công thức sau:

$$\text{Max}(|C_k[i, j]|, |C_k[p, q]|) - (d - \text{INT}(0.75a))$$

Hệ số được chọn sẽ bị trừ đi một lượng là $(d - \text{INT}(0.75a)$

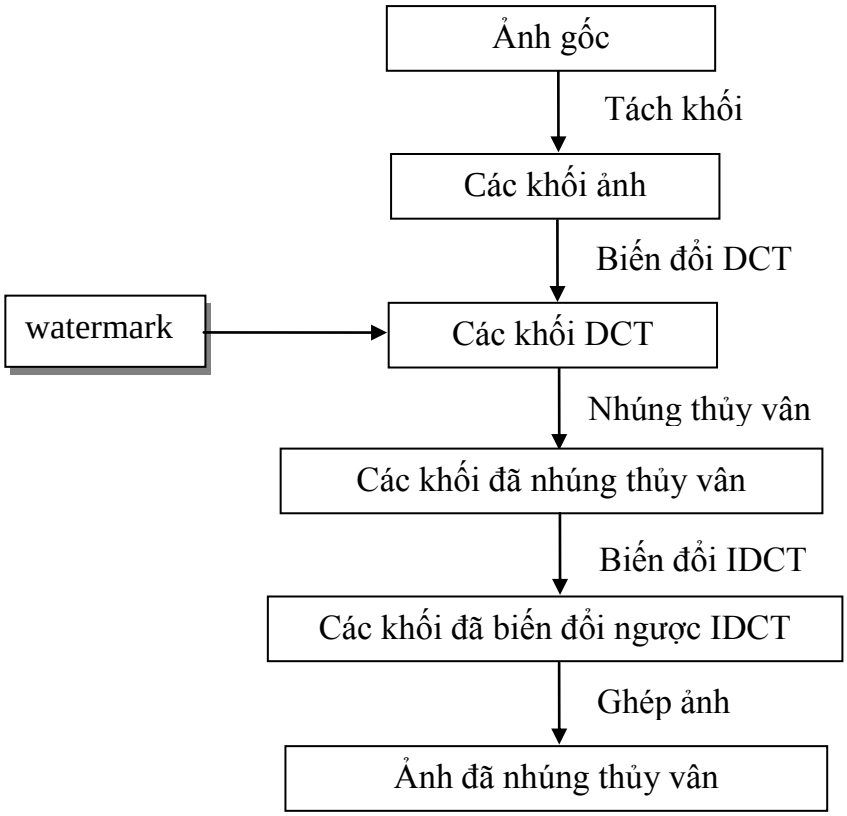
$$\text{Min}(|C_k[i, j]|, |C_k[p, q]|) + (\text{INT}(0.75a) - d)$$

Hệ số được chọn sẽ được cộng thêm một lượng là $(\text{INT}(0.75a) - d)$

Bước 8: Thực hiện phép biến đổi ngược IDCT đối với khối C_k, $B_k = \text{IDCT}(C_k)$.

Bước 9: Ghép các khối ảnh B'_k để được ảnh chứa thủy vân F'.

Quá trình nhúng thủy vân được mô tả qua sơ đồ sau:



2/. Ví dụ:

Giả sử ta cần giấu một bit thủy vân b = 0 vào khối B 8 × 8 được cho dưới đây.

Ta chọn a = 26 = 2(2 × 6 + 1), do đó t = 6.

B =

33	84	66	58	15	159	183	146
28	75	15	37	161	157	136	134
29	59	44	65	192	166	144	139
15	15	15	67	113	123	192	170
88	76	15	102	168	104	199	177
19	10	15	218	140	198	164	141
15	15	15	179	241	235	190	107
15	17	89	181	168	234	190	190

Biến đổi DCT(B) ta thu được khối C như sau:

C =

869	-438	-102	115	18	7	-62	-41
-110	64	143	-18	-78	-62	-2	38
30	-4	-37	-7	-67	8	55	-42
-7	27	22	-10	-3	57	-26	-57
-3	-2	109	-69	-33	41	6	9
-23	-27	-26	9	-29	33	6	-10
12	5	-8	-46	-13	33	38	-42
42	33	5	28	5	-31	-24	40

Trong miền tần số giữa của khối C, ta chọn hai hệ số bất kỳ, giả sử là C[2,3] = 143 và C[6,2] = -27

Tính độ lệch d = ||143| - |-27|| mod 26 = 116 mod 26 = 12

Với bit thủy vân b = 0 thì ta phải thay đổi một trong hai hệ số C[2,3] = 143 hoặc C[6,2] = -27 đã chọn để thu được d < 2t + 1

Vì C[2,3] = 143 có giá trị tuyệt đối lớn hơn C[6,2], theo công thức (2,7) ta tính giá trị mới của C[2,3] là:

C[2,3] = C[2,3] – (d – INT(0.25a)) = 143 – (14 – INT(0.25 × 26)) = 135

Khi đã thay đổi hệ số C[2,3] = 135 ta thực hiện phép biến đổi ngược IDCT(C) và thu được khối B’ như sau:

B’ =

31	83	67	60	17	160	183	143
27	74	16	38	163	158	136	132
28	59	48	66	193	167	144	138
15	15	15	67	114	123	192	169
88	76	15	102	168	104	200	177
20	10	15	27	139	197	165	141
17	16	15	178	240	235	191	109
17	18	88	178	166	232	191	190

2.2.3.2 Quá trình tách thủy vân

Input

- Ảnh đã nhúng thủy vân F'
- Khóa K (nếu có)

Output

- Thủy vân đã nhúng W biểu diễn qua dãy bit b_k

1/. *Các bước thực hiện*

Bước 1: Chia ảnh F' đã nhúng thủy vân thành các khối $B'_{k.}$

Bước 2: Biến đổi DCT các khối $B'_{k.}$

$B_k = DCT(B'_{k.})$

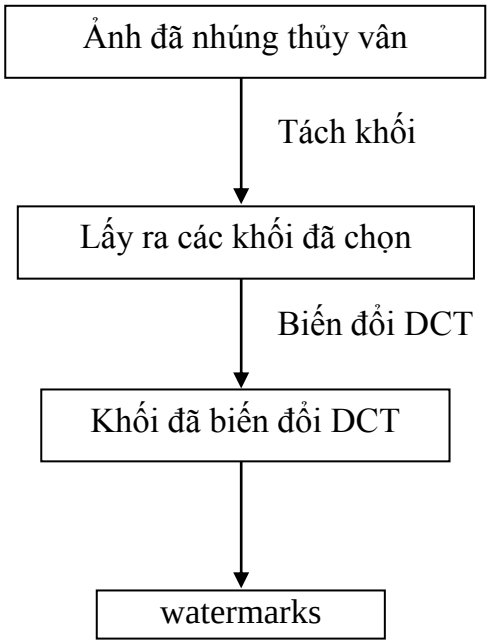
Bước 3: Lấy ra vị trí hai hệ số đã biến đổi $B_k[i,j]$ và $B_k[p,q]$

Bước 4:

Tính $d = | B_k[i,j] - B_k[p,q] |$ mod a với $a = 2(2t+1)$ đã chọn khi nhúng thủy vân.

Bước 5: Nếu $d \geq 2t + 1$ thì được bit $b_k = 1$ ngược lại $b_k = 0$

Bước 6: Ghép các bit b_k tách được từ các khối để được thủy vân đầy đủ W.



2/.Ví dụ:

Với khối B’ ở ví dụ trên, quá trình tách thủy vân như sau:

Ta thực hiện phép biến đổi ngược IDCT của khối B’ để thu được khối B sau:

B =

869	-438	-102	115	18	7	-62	-41
-110	64	135	-18	-78	-62	-2	38
30	-4	-37	-7	-67	8	55	-42
-7	27	22	-10	-3	57	-26	-57
-3	-2	109	-69	-33	41	6	9
-23	-27	-26	9	-29	33	6	-10
12	5	-8	-46	-13	33	38	-42
42	33	5	28	5	-31	-24	40

Ta lấy hai hệ số B[2, 3] = 135 và B[6, 2] = -27

Tính độ lệch d = ||B[2, 3]| - | B[6, 2] || mod 26 = 4.

Ta thấy d < 2t + 1 = 13, vậy bit b = 0 đã được giấu vào khối.

2.2.3.3 Phân tích thuật toán

Kích thước khối ảnh trong thuật toán là 8 × 8, tuy nhiên có thể chọn kích thước khác nhau tùy theo kích thước từng ảnh gốc và kích thước thực tế của thủy vân.

Việc chọn một cặp hệ số trong miền tần số giữa có thể được chọn cố định cho tất cả các khối trong quá trình nhúng thủy vân. Khi đó, thủy vân có thể rất dễ bị phát hiện thông qua việc thử lần lượt các cặp hệ số trong miền tần số giữa. Có thể làm tăng độ an toàn và khó bị phát hiện thủy vân bằng cách đưa ra một thuật toán có sử dụng khóa cho sự lựa chọn cặp hệ số trong miền tần số giữa cho từng khối DCT. Khi đó, vị trí của các cặp hệ số được chọn cho quá trình nhúng thủy vân trong từng khối sẽ được sử dụng phụ thuộc vào khóa của quá trình tách thủy vân. Trong thuật toán này, quá trình tách thủy vân không cần ảnh gốc.

Tham số a trong thuật toán đóng vai trò như là hệ số tương quan giữa tính ẩn và tính bền vững của thủy vân. Khi tăng hệ số a lên thì độ sai lệch của thủy vân giảm đi và như vậy nó bền vững hơn. Tuy nhiên, nếu tăng a thì chất lượng ảnh sau khi giấu tin sẽ giảm. Điều này rất dễ hiểu vì a lớn, nghĩa là phân lớp khoảng cách hai hệ số lớn nên khoảng cách biến đổi của một hệ số để thỏa mãn điều kiện giấu lớn, dẫn đến ảnh hưởng nhiều đến chất lượng ảnh.

Chương 3. MỘT SỐ KỸ THUẬT PHÁT HIỆN ẢNH GIẤU TIN

3.1 KHÁI NIỆM PHÂN TÍCH TIN ẨN GIẤU

Phân tích tin ẩn giấu hay còn gọi là tấn công một hệ giấu tin (steganalysis) là phương pháp để phát hiện, trích rút, phá hủy hay sửa đổi thông tin đã giấu.

Việc phân tích được coi là thành công hay không còn tùy theo ứng dụng. Đối với việc liên lạc bí mật, việc phát hiện và chứng minh một ảnh có chứa tin mật được coi là thành công. Đối với bảo vệ bản quyền số hay chống giả mạo thì việc phân tích được coi là thành công nếu không chỉ phát hiện ra thủy vân mà còn phá hủy hay sửa đổi nó nhưng không làm giảm chất lượng ảnh mang. Đề tài nghiên cứu ứng dụng trên hệ giấu tin mật.

Các kỹ thuật phân tích giấu tin mật hiện tại tập trung vào việc phát hiện ra sự có mặt hay không các thông điệp ẩn trong dữ liệu được quan sát. Bài toán trích chọn ra các thông điệp bí mật là bái toán khó hơn bài toán phát hiện, nhưng bài toán phát hiện làm tiền đề cho việc trích chọn. Như vậy, có thể xác định hai mục tiêu rõ ràng của bài toán phân tích trên hệ giấu tin mật là:

- Phân tích giấu tin bị động (Passive steganalysis): Phát hiện sự hiện diện hay không của thông điệp bí mật trong các dữ liệu được quan sát.
- Phân tích giấu tin chủ động (Active steganalysis): Trích chọn một phiên bản của thông điệp bí mật từ phương tiện chứa tin.

Trong khuôn khổ bài báo cáo, em tập trung vào giải quyết vấn đề phát hiện sự tồn tại của thông điệp bí mật.

3.2 PHÂN LOẠI PHƯƠNG PHÁP PHÁT HIỆN ẢNH GIẤU TIN

Phân tích trực quan: Đây là phương pháp đơn giản nhất mặc dù kết quả thường không đáng tin cậy. Để phát hiện khả năng một ảnh có giấu tin hay không bằng việc phân tích ảnh một cách trực quan và tìm kiếm những "điểm bất thường". Nhiều phương pháp giấu tin mật, bao gồm cả giấu tin dựa trên LSB và phương pháp dựa trên DCT đều loại bỏ những biến dạng ở những vùng ảnh mịn hoặc thuần nhất một cách dễ nhận thấy. Thật vậy, việc thay đổi bảng màu (của một ảnh màu) dù nhỏ để giấu thông điệp bí mật có thể dẫn đến kết quả là sự thay đổi màu sắc lớn trên ảnh gốc, đặc biệt là nếu ảnh gốc có chứa các màu sắc khác nhau ở mức độ cao. Cũng bởi thực tế là với một ảnh màu tự nhiên, sự thay đổi bit một trong các màu là hiếm.

Phân tích định dạng ảnh: Có nhiều định dạng tệp tin ảnh khác nhau như BMP, GIF, JPEG. Mỗi loại có đặc điểm và cấu trúc định dạng tệp tin khác nhau. Do đó, khi thực hiện giấu tin, chẳng hạn giấu tin theo LSB, sẽ cho sự thay đổi trên ảnh kết quả ở các điểm ảnh khác nhau. Và khi thực hiện phát hiện ảnh giấu tin cũng vậy. Ví dụ như với ảnh JPG: Ảnh JPG sử dụng phép biến đổi DCT để biến đổi liên tiếp các khối điểm ảnh 8 × 8 vào ma trận 64 hệ số DCT. Bit LSB của các hệ số DCT được sử dụng như là các bit dư thừa mà ta sẽ giấu các bit thông điệp ẩn vào trong đó. Sự thay đổi hệ số DCT đơn lẻ sẽ tác động lên tất cả 64 điểm ảnh. Vì lý do đó không thể áp dụng việc phân tích trực quan đối với loại ảnh này.

Phân tích thống kê: Theo Plitzman và Westfeld, lý thuyết thống kê có thể áp dụng để phân tích thống kê các cặp giá trị (cặp giá trị điểm ảnh, cặp các hệ số DCT, cặp các chỉ số bảng màu) để tìm sự khác biệt ở bit LSB. Trước khi giấu tin, trên ảnh chứa thông điệp (cover image), mỗi cặp hai giá trị là phân phối không đều. Sau khi giấu tin, giá trị trong mỗi cặp có xu hướng trở nên bằng nhau. Hơn nữa, nếu các kỹ thuật giấu tin mật giấu các bit thông điệp một cách tuần tự vào các điểm ảnh (hoặc các chỉ số bảng màu hoặc các hệ số DCT) liên tiếp nhau, bắt đầu từ góc trên trái thì ta sẽ quan sát được sự thay đổi đột ngột trong các thống kê. Một số kỹ thuật thống kê sẽ được trình bày trong phần cuối của chương này.

3.3 MỘT SỐ KỸ THUẬT PHÁT HIỆN ẢNH GIẤU TIN

3.3.1 Kỹ thuật phân tích cặp giá trị điểm ảnh

Khái niệm về cặp giá trị (PoV – Pairs of Values) được Pfitzmann và Westfeld đưa ra. Cho một ảnh I. Gọi j là giá trị của điểm ảnh (pixel) trên ảnh I. Nếu I là ảnh đa cấp xám 8 – bit thì $j \in [0,255]$. Nếu j chẵn (j = 2i) thì sau phép lật bit giá trị của j là 2i + 1, nếu j là lẻ (j = 2i+1) thì sau phép lật bit giá trị của j là 2i. Như vậy, nếu một giá trị điểm ảnh ở trong một cặp thì sau khi giấu tin giá trị của nó vẫn nằm trong một cặp có tính chất chẵn lẻ tương tự.

PoV là một cặp hai giá trị điểm ảnh (2i, 2i+1) và hai giá trị trong cặp này chỉ sai khác nhau ở bit thấp nhất.

Trong thuật toán trình bày dưới đây có liên quan đến khái niệm tần số xuất hiện của giá trị điểm ảnh j. Đó là số lần xuất hiện của giá trị điểm ảnh j trên ảnh.

Kỹ thuật PoVs còn được gọi là phương pháp thống kê X^2 (khi bình phương – Chi_squared) và được áp dụng rất thành công đối với việc phát hiện giấu tin mật LSB một cách tuần tự.

Có nhiều kỹ thuật PoV khác nhau như PoV2, PoV2r, PoV3. Trong đó PoV2 và PoV2r chỉ kiểm tra một tập con các điểm ảnh được chọn bởi người dùng. PoV2 kiểm tra phần trăm các điểm ảnh hiện tại (được chọn bởi người dùng) một cách tuần tự, bắt đầu từ góc trên trái của ảnh. PoV2r cũng kiểm tra một cách tuần tự phần trăm các điểm ảnh hiện tại được chọn bởi người dùng nhưng bắt đầu ở một điểm nào đó trên ảnh và sau đó thực hiện phép lật bit cho đến điểm cuối cùng được chọn. PoV3 kiểm tra mỗi tổng phần trăm các điểm ảnh từ 1% đến 100% và trả về xác suất của mỗi tập con các điểm ảnh trên ảnh kiểm tra. Các điểm ảnh cũng được kiểm tra một cách tuần tự, bắt đầu từ góc trên bên trái của ảnh. Thực tế PoV3 kiểm tra các nhóm điểm ảnh theo một trật tự nào đó. Mục dưới đây sẽ trình bày chi tiết kỹ thuật phát hiện tin giấu PoV3.

3.3.1.1 Thuật toán PoV3

Tư tưởng

Với một ảnh I cần kiểm tra, trước tiên ta thống kê tần số của các giá trị điểm ảnh chẵn, lẻ có mặt trong ảnh I. Ta xác định xác suất giấu tin của ảnh thông qua việc áp dụng tiêu chuẩn phân phối χ^2 đối với tần số của các cặp PoV.

Input: Ảnh I cần kiểm tra

Output: P: xác suất giấu tin trong ảnh I

Cách thức thực hiện

Bước 1: Đọc vào ảnh I

Bước 2: Đọc dữ liệu ảnh vào một ma trận $M_{m \times n}$

Bước 3: Khởi tạo giá trị ban đầu cho vecto X, Y.

For each k $\in$ [0, 127]

X[k] = 0; Y[k] = 0.

Bước 4:

Tính X[k] là tần số xuất hiện của các điểm ảnh có giá trị chẵn trên ảnh.

Tính Y[k] là tần số xuất hiện của các điểm ảnh có giá trị lẻ trên ảnh.

Bước 5: Giả sử ta có N cặp PoV

Với mọi k

Nếu (X[k] + Y[k]) $\leq$ 4 thì

X[k] = Y[k] = 0;

N = N – 1;

Bước 6:

For each k

Z[k] = (X[k] + Y[k])/2;

Bước 7: Giả sử ta có N cặp PoV, theo phương pháp thống kê Khi – bình phương với N – 1 bậc tự do ta tính

$$\chi^2_{N-1} = \sum_{k=0}^{127} \frac{(X[k]-Z[k])^2}{Z[k]} \quad (1)$$

Bước 8: Tính P là xác suất của việc giấu tin

$$P = 1 - \frac{1}{2^{\frac{N-1}{2}}\Gamma(\frac{N-1}{2})} \int_0^{\chi^2_{N-1}} e^{\frac{-x}{2}} x^{\frac{N-1}{2}-1} dx \quad (2)$$

3.3.1.2 Phân tích thuật toán

Thông thường đối với ảnh kiểm tra là một ảnh đa cấp xám 8 – bit ta có 256 mức xám khác nhau. Thuật toán xác định các cặp phần tử là các giá trị mức xám chẵn, lẻ nên số lượng các phần tử chẵn, lẻ như vậy có không quá 256/2 = 128 phần tử. Ta xây dựng hai vecto $X(x_0, x_1, \ldots, x_k)$, $Y(y_0, y_1, \ldots., y_k)$ để thống kê tần số xuất hiện các điểm ảnh, với $0 \le k \le 127$. Mỗi phần tử trong X sẽ lưu tần số xuất hiện các điểm ảnh chẵn (X[k] = 2k), mỗi phần tử trong Y sẽ lưu tần số xuất hiện các điểm ảnh lẻ (Y[k] = 2k + 1) với $0 \le k \le 127$.

Ban đầu khởi tạo các phần tử trong X và trong Y đều bằng 0. Sau đó thuật toán thực hiện việc thống kê các giá trị mức xám có trong ảnh cần kiểm tra và tương ứng tăng giá trị của các phần tử trong X[k] và Y[k].

Giả sử rằng ta có N cặp PoV, có k mức chẵn (lẻ) $0 \le k \le 127$

Nếu $X[k] + Y[k] \le 4$ thì X[k] = Y[k] = Z[k] = 0 và N = N – 1.

Nếu ảnh có chứa thông điệp tin ẩn thì X[k] = Z[k] đối với mọi k, trong phương trình (1) χ^2_{N-1} sẽ bé và do đó tích phân $\int_0^{\chi^2_{N-1}} e^{\frac{-x}{2}} x^{\frac{N-1}{2}-1} dx$ sẽ bé và từ (2) suy ra xác suất p sẽ lớn. Ngược lại thì χ^2_{N-1} sẽ lớn suy ra xác suất p sẽ bé. Căn cứ vào sự lớn bé của xác suất p ta sẽ quyết định được ảnh có giấu tin hay không. Hơn nữa Wesfeld và Pfitzmann còn khẳng định rằng nếu ít hơn 100% các điểm ảnh có chứa thông tin được giấu thì xác suất giấu tin sẽ giảm rõ rệt.

3.3.2 Kỹ thuật phân tích đối ngẫu

3.3.2.1 Khái niệm cơ bản trong kỹ thuật đối ngẫu

Kỹ thuật đối ngẫu hay còn gọi là kỹ thuật RS (Regular - Singular) do Fridrich đưa ra. Phương pháp này thực hiện các thống kê về sự thay đổi của các nhóm chính quy (Regular) và nhóm đơn (Singular) trên ảnh để ước lượng độ dài thông điệp đã giấu một cách chính xác. Phương pháp này phù hợp với ảnh màu và ảnh đa cấp xám khi các thông điệp được giấu một cách ngẫu nhiên. Kỹ thuật RS cũng là một số kỹ thuật được dựa trên lý thuyết xác suất thống kê.

Giả sử ta có một ảnh có M × N điểm ảnh. Tập P là tập tất cả các giá trị điểm ảnh có trên ảnh. Với ảnh đa cấp xám 8 – bit thì P = {0, 1, …., 255}.

Định nghĩa 3.3.1 Một hàm độ khác biệt f trên nhóm G = (x_1, x_2, …, x_n) được định nghĩa như sau:

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

Trong đó x_1, x_2, …, x_n là giá trị các điểm ảnh trên nhóm G. Hàm *f* được xem như là độ trơn của nhóm G.

Việc giấu tin LSB làm tăng nhiễu trên ảnh do đó ta hy vọng rằng giá trị của hàm f sẽ tăng (hoặc giảm) sau khi giấu tin LSB

Định nghĩa 3.3.2 Việc giấu tin LSB sử dụng các kiểu hàm lật (flip) bit $F_m(x)$ với m = -1, 0, 1 và x là giá trị điểm ảnh. Cụ thể như sau:

F_1: $0 \leftrightarrow 1, 2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255$.

F_{-1}: $-1 \leftrightarrow 0, 1 \leftrightarrow 2, 3 \leftrightarrow 4, \ldots, 253 \leftrightarrow 254, 255 \leftrightarrow 256$.

Hay $F_{-1}(x) = F(x+1) - 1$ với mọi x

$F_0(x) = x$, với $\forall x \in P$.

Định nghĩa 3.3.3

Phép lật bit F_1 và F_{-1} được áp dụng lên nhóm G (x_1, x_2, x_3, …., x_n) với một mặt nạ M (M là một n – bộ với các thành phần nhận giá trị -1, 0 hoặc 1) được định nghĩa như sau:

$F_M(G) = (F_{M(1)}(x_1), F_{M(2}(x_2), \ldots . , F_{M(n)}(x_n))$ trong đó $M(i) \in \{-1, 0, 1\}$

Ví dụ: nếu các giá trị các điểm ảnh trong nhóm G là (39, 38, 40, 41) và cho mặt nạ M = (1, 0, 1, 0) thì $F_M(G) = (F_1(39), F_0(38), F_1(40), F_0(41)) = (38, 38, 41, 41)$.

Định nghĩa 3.3.4

Cho một mặt nạ M, phép lật bit F, và hàm khoảng cách f, một nhóm G các điểm ảnh được phân lớp vào một trong ba lớp như sau:

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

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

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

Trong đó R gọi là các nhóm chính quy (Regular), S là các nhóm đơn (Singular) và U là các nhóm không dùng được (Unusable).

Định nghĩa 3.3.5

Ta gọi

R_M là số tương đối các nhóm R với mặt nạ M không âm, $M \in \{0, 1\}$.

S_M là số tương đối các nhóm S với mặt nạ M không âm, $M \in \{0, 1\}$.

R_{-M} là số tương đối các nhóm R với mặt nạ M không dương, $M \in \{-1, 0\}$.

S_{-M} là số tương đối các nhóm S với mặt nạ M không dương, $M \in \{-1, 0\}$.

Ta có R_M xấp xỉ bằng R_{-M}, S_{-M} xấp xỉ bằng S_{-M} và được viết như sau:

$R_M \cong R_{-M}$ và $S_M \cong S_{-M}$

Việc giấu tin LSB tập trung vào sự khác biệt giữa R_M và S_M. Nếu có 50% điểm ảnh bị lật (khi mỗi điểm ảnh bị giấu bit thông điệp) ta thu được $R_M \cong S_M$ nhưng ảnh hưởng của việc giấu tin LSB đến R_{-M} và S_{-M} lại ngược lại. Dưới đây sẽ trình bày các bước cụ thể của kỹ thuật RS trong đó có sử dụng đến các khái niệm và định nghĩa vừa trình bày ở trên.

3.3.2.2 Thuật toán RS

Tư tưởng:

Kỹ thuật RS phân hoạch ảnh cần kiểm tra thành các nhóm điểm ảnh cố định. Mỗi nhóm đó lại được phân lớp vào các nhóm R hay S phụ thuộc vào sự khác biệt giữa các điểm ảnh trong nhóm bị tăng hoặc giảm sau phép lật bit LSB với mặt nạ M. Sau đó tính xác suất của việc giấu tin căn cứ vào số nhóm R, S đó.

Input

- Ảnh I cần kiểm tra
- n: số phần tử của một nhóm
- M_n: mặt nạ là một vecto có phần tử nhận giá trị trong tập {-1, 0, 1}

Output

- P: Xác suất giấu tin trong ảnh I

Cách thực hiện

Bước 1: Đọc vào ảnh I

Bước 2: Đọc giá trị điểm ảnh vào một ma trận $A_{M \times N}$.

Bước 3: $P = P \cup \{x_i\}$ với $x_i \in [0, 255]$.

Bước 4: Chia ảnh thành $M \times N/n$ nhóm khác nhau. Mỗi nhóm n điểm ảnh.
Với mỗi nhóm $G = (x_1, x_2, \ldots, x_n)$ ta thực hiện các bước sau:

Bước 5: Tính hàm $f(G)$

$$f(G) = \sum_{i=1}^{n-1} |x_i - x_{i+1}|$$

Bước 6: Cho mặt nạ $M = \{M(i)\}_{i = 1, \ldots, n}$ với $M(i) \in \{-1, 0, 1\}$. Tính

$F_M(G) = (F_{M(1)}(x_1), F_{M(2)}(x_2), \ldots\ldots, F_{M(n)}(x_n))$

Bước 7: Phân lớp nhóm G

$f(F_M(G)) > f(G)$ thì $R = R \cup G$;

$f(F_M(G)) < f(G)$ thì $S = S \cup G$;

$f(F_M(G)) = f(G)$ thì $U = U \cup G$.

Bước 8: Tính

R_M = số các nhóm R tương ứng với mặt nạ M, M $\in$ {0, 1}.

S_M = số các nhóm S tương ứng với mặt nạ M, M $\in$ {0, 1}.

R_{-M} = số các nhóm R tương ứng với mặt nạ M, M $\in$ {-1, 0}.

S_{-M} = số các nhóm S tương ứng với mặt nạ M, M $\in$ {-1, 0}.

Bước 9:

Nếu | R_M | = | S_M | thì p =1

Ngược lại thực hiện các bước 9 đến bước 12

Bước 10: Tính các hệ số

$d_0 = R_M (p/2) - S_M (p/2)$;

$d_0 = R_M (1 - p/2) - S_M (1 - p/2)$;

$d_{-0} = R_{-M} (p/2) - S_{-M} (p/2)$;

$d_{-1} = R_{-M} (1 - p/2) - S_{-M} (1 - p/2)$;

Bước 11: Tính x_p là nghiệm của phương trình

$2(d_1 + d_0) x_p^2 + (d_{-0} - d_{-1} - d_1 - 3d_0) x_p + d_0 - d_{-0}$.

Bước 12: Tính ước lượng độ dài thông điệp p

$P = x_p / (x_p - 1/2)$.

KẾT LUẬN

Kể từ khi ra đời, giấu tin đã và đang làm tốt vai trò của nó trong nhiều lĩnh vực như bảo vệ thông tin an toàn trong quá trình trao đổi, bảo vệ quyền tác giả trong quá trình phân phối,…Tuy nhiên, có những trường hợp lợi dụng kỹ thuật giấu tin để thực hiện những hành vi bất hợp pháp như tuyên truyền sản phẩm văn hóa không lành mạnh, truyền những thông tin về kế hoạch tấn công khủng bố,…Từ sử dụng sai chức năng của giấu tin ở trên đặt ra vấn đề làm thế nào để phát hiện được phương tiện chứa tin có tiềm ẩn bên trong các tin giấu hay không, và thông tin chứa trong đó là gì nhằm có thể hỗ trợ trong việc ngăn ngừa các thảm kịch xảy ra. Mặt khác việc nghiên cứu khả năng phát hiện thông tin ẩn cũng sẽ làm tăng mức độ an toàn cho kỹ thuật giấu tin, đặc biệt là kỹ thuật giấu tin mật. Bài toán đặt ra là phát hiện có tồn tại tin giấu trong ảnh hay không, cũng như có thể sửa đổi hay phá hủy thông tin đã giấu hay không? Trên thế giới có nhiều cách tiếp cận khác nhau để giải quyết bài toán phát hiện tin giấu. Trong đồ án em đã trình bày một số kỹ thuật giấu tin bằng thay thế bit có trọng số thấp nhất, kỹ thuật thủy vân trên miền biến đổi DCT, và em tìm hiểu về kỹ thuật phát hiện ảnh có giấu tin theo hướng tiếp cận sử dụng lý thuyết xác suất thống kê.

Kết quả chính của đồ án tốt nghiệp là:

1/. Trình bày một số khái niệm cơ bản về mã hóa, giấu tin và các vấn đề liên quan.

2/. Trình bày hai phương pháp giấu tin trong ảnh: giấu tin bằng bit có trọng số thấp nhất, kỹ thuật thủy vân sử dụng phép biến đổi DCT.

3/. Trình bày kỹ thuật phân tích cặp giá trị điểm ảnh PoV3, và kỹ thuật phân tích đối ngẫu RS.

TÀI LIỆU THAM KHẢO

[1] Giáo trình giấu tin và thủy vân ảnh – Nguyễn Xuân Huy – Trần Quốc Dũng.

[2] Luận văn thạc sĩ "Giấu thông tin trong ảnh" – Vũ Thị Chung Thủy – năm 2004.

[3] Luận văn thạc sĩ: "Bảo mật bằng các kỹ thuật mã hóa và giấu tin" – Đinh Ngọc Triều – 2004.

[4] Giáo trình "An toàn dữ liệu" – Trịnh Nhật Tiến.

[5] "Nhập môn xử lý ảnh số"- Lương Mạnh Bá, Nguyễn Thanh Thúy, nhà xuất bản khoa học và kỹ thuật.

[6] Luận văn thạc sĩ "Kỹ thuật giấu tin trong ảnh và nghiên cứu khả năng có thể để phát hiện ảnh có giấu tin" – Nguyễn Thị Phương Hoa.