LỜI CẢM ƠN!

Trước hết em xin bày tỏ lòng biết ơn sâu sắc nhất tới cô giáo hướng dẫn Tiến sĩ Hồ Thị Hương Thơm đã tận tình giúp đỡ em rất nhiều trong suốt quá trình tìm hiểu nghiên cứu và hoàn thành báo cáo tốt nghiệp.

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

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

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

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

Em xin chân thành cảm ơn!

Hải phòng, ngày… tháng…năm 2013

Sinh viên thực hiện

MỤC LỤC

DANH MỤC BẢNG - HÌNH

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. Với việc sử dụng mạng internet toàn cầu để thông tin, liên lạc ngày càng tăng trong mọi lĩnh vực chính trị, quân sự, quốc phòng, kinh tế, thương mại… Vấn đề được đặt ra đó là sự an toàn của dữ liệu. Một công nghệ phần nào giải quyết được vấn đề trên là giấu tin mật, nó cho phép giấu thông tin mật vào trong các nguồn thông tin khác, làm ẩn đi sự tồn tại của thông mật. Trong đồ án này em xin trình bày một kỹ thuật giấu tin đó là kỹ thuật giấu tin CPT trên ảnh nhị phân, gồm các chương sau:

Chương 1. Khái niệm tổng quan: Trình bày tổng quan kỹ thuật giấu tin trong ảnh, cấu trúc ảnh BITMAP và phương pháp đánh giá PSNR (peak signal-to-noise ration) ảnh trước và sau khi giấu tin.

Chương 2. Kỹ thuật giấu tin CPT trên ảnh nhị phân: Giới thiệu và trình bày kỹ thuật giấu và tách tin CPT.

Chương 3. Cài đặt thử nghiệm: Trình bày một số giao diện của chương trình và thử nghiệm kỹ thuật giấu tin CPT trên ảnh nhị phân, đưa ra nhận xét đánh giá.

KỹthuậtgiấutinCPT trênảnhnhịphân

Chương 1. KHÁI NIỆM TỔNG QUAN

1.1. Tổng quan kỹ thuật giấu tin trong ảnh

1.1.1.Khái niệm

Giấu tin là kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác.

Giấu tin trong ảnh là kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong ảnh mà khó phát hiện bằng kỹ thuật thông thường.

Mục đích:

-Mục đích của giấu tin có hai vấn đề chính đó là:

+ Bảo mật cho dữ liệu được đem giấu.

+ Bảo mật cho chính đối tượng được đem giấu thông tin.

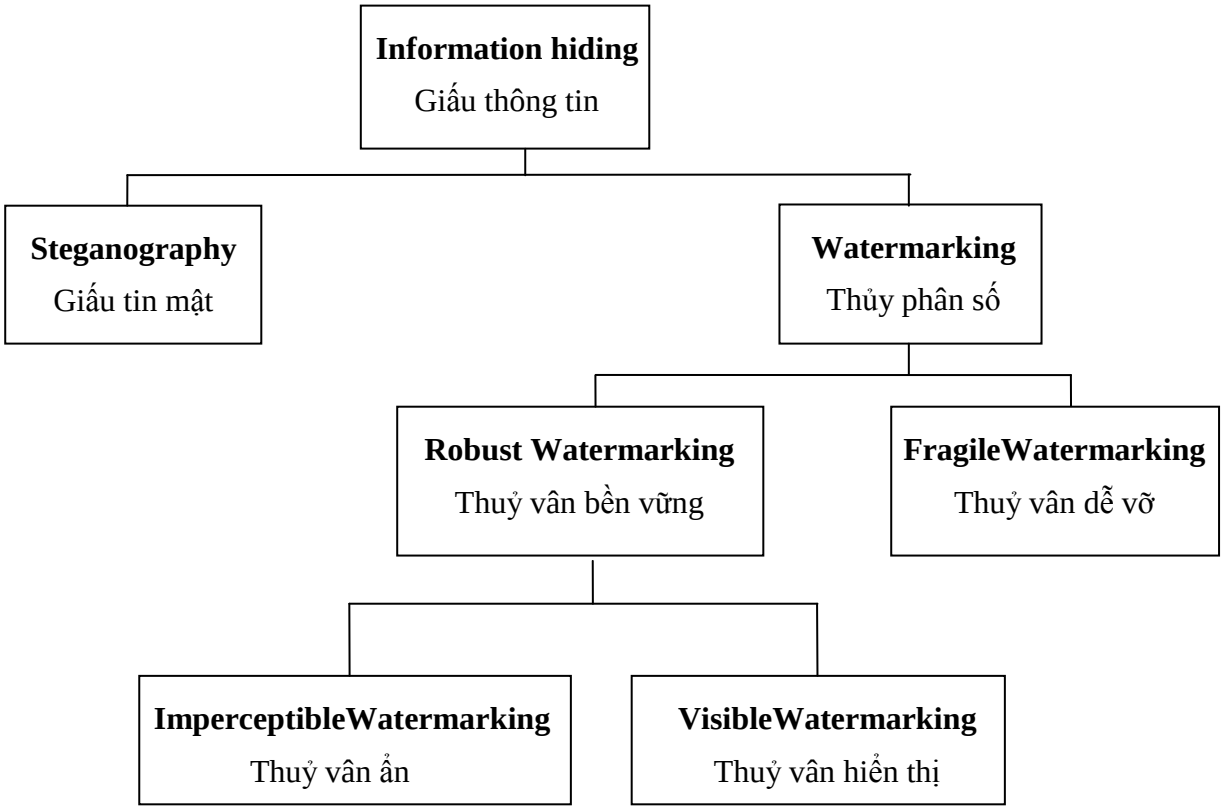
- Ngày nay kỹ thuật giấu tin được nghiên cứu để phục vụ các mục đích tích cực như: bảo vệ bản quyền các tài liệu số hóa (dùng thuỷ vân số), hay giấu các thông tin bí mật về quân sự và kinh tế. . .

-Sự phát triển của công nghệ thông tin đã tạo ra những môi trường giấu tin mới vô cùng tiện lợi và phong phú. Người ta có thể giấu tin trong các văn bản, hình ảnh, âm thanh. Cũng có thể giấu tin ngay trong các khoảng trống hay các phân vùng ẩn của môi trường lưu trữ như đĩa cứng, đĩa mềm. Các gói tin truyền đi trên mạng cũng là môi trường giấu tin thuận lợi. Các tiện ích phần mềm cũng là môi trường lý tưởng để gài các thông tin quan trọng để xác nhận bản quyền.

1.1.2. Phân loại giấu tin

Có thể phân loại kỹ thuật giấu tin làm hai hướng:

- ❖ Giấu tin mật (Steganography).
- ❖ Thủy vân số (Watermarking).



Hình 1. 1. Sơđồ phân loại kỹ thuật giấu tin.

- *Giấu tin mật (Steganograph)* quan tâm tới việc giấu các tin sao cho thông tin giấu được càng nhiều càng tốt và quan trọng là người khác khó phát hiện được một đối tượng có bị giấu tin bên trong hay không bằng kỹ thuật thông thường.

- *Thủy vân số (Watermarking)* đánh giấu vào đối tượng nhằm khẳng định bản quyền sở hữu hay phát hiện xuyên tạc thông tin. Thủy vân số được phân thành 2 loại thủy vân bền vững và thủy vân dễ vỡ.

- ***Thuỷ vân bền vững (Robust Watermarking):*** thường được ứng dụng trong các ứng dụng bảo vệ bản quyền. Thuỷ vân được nhúng trong sản phẩm như một hình thức dán tem bản quyền. Trong trường hợp này, thuỷ vân phải tồn tại bền vững cùng với sản phẩm nhằm chống việc tẩy xoá, làm giả hay biến đổi phá huỷ thuỷ vân. Thủy vân bền vững có hai loại:

  - ✓ *Thuỷ vân ẩn (Visible Watermarking):* cũng giống như giấu tin, bằng mắt thường không thể nhìn thấy thuỷ vân.
  - ✓ *Thuỷ vân hiện (Imperceptible Watermarking):* là loại thuỷ vân được hiện ngay trên sản phẩm và người dùng có thể nhìn thấy được.

- *Thủy vân dễ vỡ (Fragile Watermarking):* là kỹ thuật nhúng thuỷ vân vào trong ảnh sao cho khi phân bố sản phẩm trong môi trường mở nếu có bất cứ một phép

biến đổi nào làm thay đổi đối tượng sản phẩm gốc thì thuỷ vân đã được giấu trong đối tượng sẽ không còn nguyên vẹn như trước khi giấu nữa (dễ vỡ).

Bảng 1. 1. So sánh giữa giấu tin mật và thủy vân số.

	Giấu tin mật	**Thủy vân số**
Mục đích	- Che giấu sự hiện hữu của thông điệp. - Thông tin che giấu độc lập với vỏ bọc.	- Thêm vào thông tin bản quyền. - Che giấu thông tin gắn với đốitượng vỏ bọc.
Yêu cầu	- Không phát hiện được thôngđiệp bị che giấu. - Dung lượng tin được giấu.	- Tiêu chuẩn bền vững.
Tấn công thành công	- Phát hiện ra thông điệp bí mật bị che giấu.	- Thủy phân bị phá vỡ.

1.1.3. Yêu cầu thiết yếu đối với một hệ thống giấu tin mật

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

- Tính vô hình: nghĩa là với người quan sát bằng mắt thường không thể phát hiện được ảnh có chứa thông tin ẩn trong đó. Đây là một tính chất cực kỳ quan trọng đối với kỹ thuật giấu tin mật.

- Khả năng nhúng: lượng thông tin cần nhúng càng nhiều càng tốt nhưng không được vi phạm tính chất khác của kỹ thuật giấu tin mật.

- Khả năng không thể dò tìm được: là khả năng chống lại việc xác định ảnh đó có hay không có thông tin ẩn bằng các kỹ thuật thống kê toán học thông thường.

1.1.4. Mô hình kỹ thuật giấu tin và tách tin cơ bản

Các thành phần chính của một hệ giấu tin và tách tin trong ảnh số gồm:

-Bản tin mật (Secret Message): có thể là văn bản hoặc tệp ảnh hay bất kỳ một tệp nhị phân nào, vì quá trình xử lý đều chuyển chúng thành chuỗi các bit.

-Ảnh phủ (hay ảnh gốc) (Cover Data): là ảnh được dùng để làm môi trường nhúng tin mật.

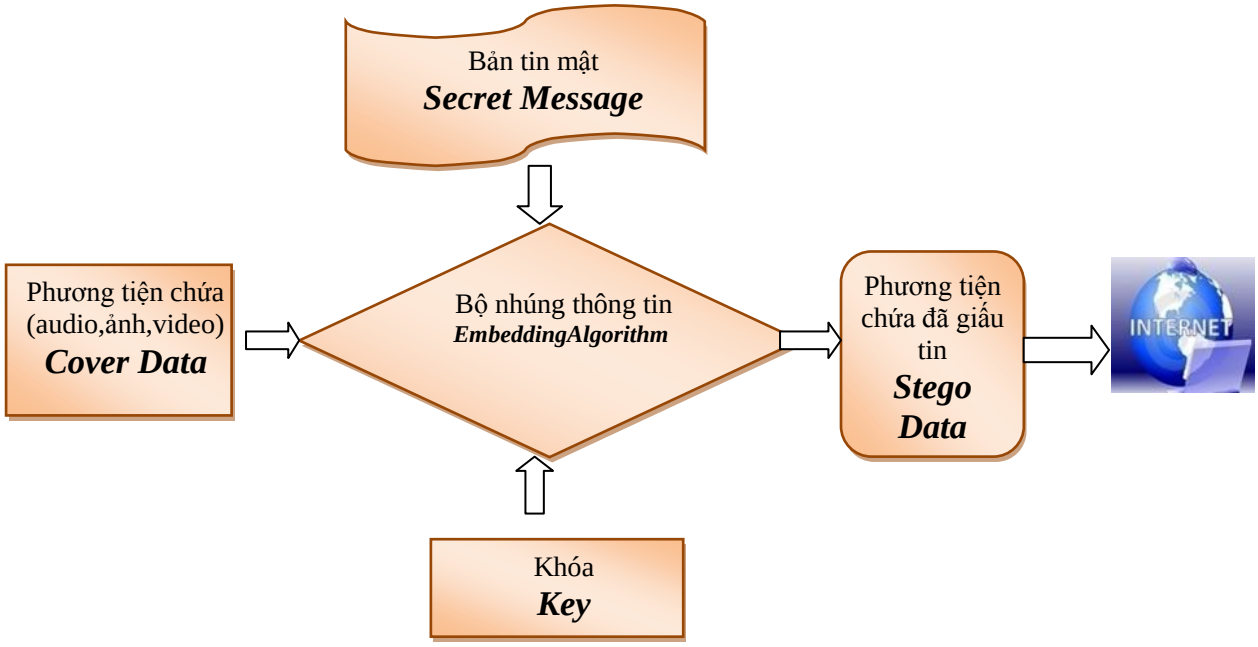
-Khoá bí mật K (Key): khoá viết mật tham gia vào quá trình giấu tin để tăng tính bảo mật.

-Bộ nhúng thông tin (Embedding Algorithm): Những chương trình, thuật toán nhúng tin.

-Ảnh mang (Stego Data): là ảnh sau khi đã nhúng tin mật vào đó.

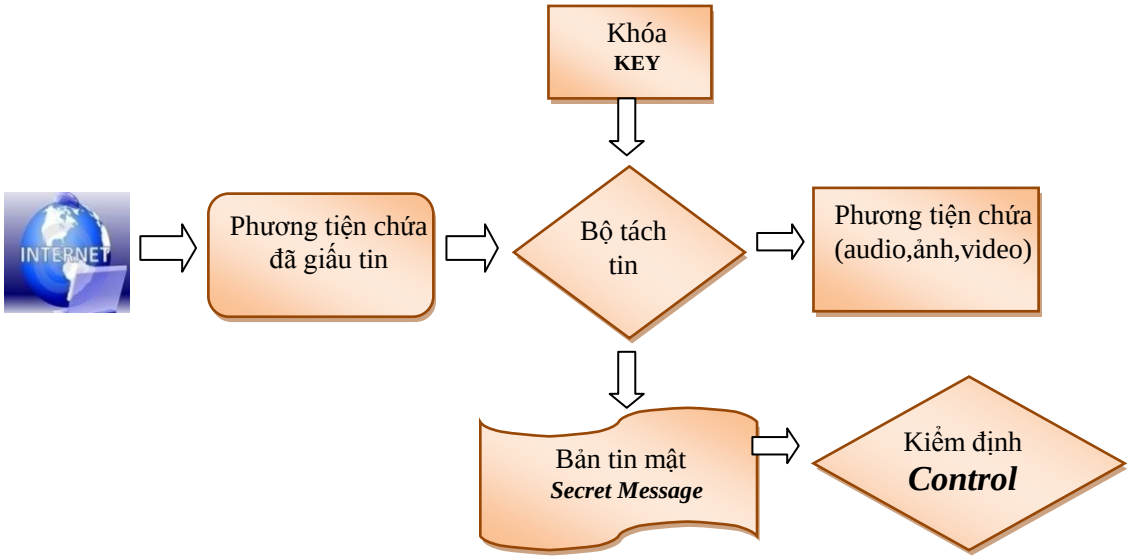
-Kiểm định (Control):kiểm tra thông tin sau khi được giải mã.

Mô hình của kỹ thuật giấu tin và tách tin cơ bản được mô tả như sau:



Hình 1. 2. Lược đồ chung cho quá trình giấu tin.

Hình 1. 2 biểu diễn quá trình giấu tin cơ bản. Phương tiện chứa bao gồm các đối tượng được dùng làm môi trường giấu tin như: text, audio, video, ảnh, bản tin mật là một lượng thông tin mang một ý nghĩa nào đó như ảnh, logo, đoạn văn bản… tuỳ 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 những chương trình, triển khai các thuật toán để giấu tin và được thực hiện với một khoá bí mật giống như các hệ mật mã cổ điển. Sau khi giấu tin, ta thu được phương tiện chứa bản tin đã giấu và phân phối sử dụng trên mạng.



Hình 1. 3. Lược đồ chung cho quá trình tách tin.

Hình 1.3 mô tả việc tách thông tin đã giấu. Sau khi nhận được đối tượng phương tiện chứa có giấu thông tin, quá trình tách tin được thực hiện thông qua bộ nhúng thông tin cùng với khoá của quá trình nhúng. Kết quả thu được gồm phương tiện chứa gốc và bản tin mật đã được giấu. Bước tiếp theo bản tin mật thu được sẽ được xử lý kiểm định so sánh với thông tin giấu ban đầu.

1.1.5. Môi trường giấu tin

1. 1. 5. 1. Giấu tin trong ảnh

Hiện nay giấu thông tin trong ảnh là một bộ phận chiếm tỷ lệ lớn 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: xác định xuyên tạc thông tin, bảo vệ quyền tác giả…Thông tin sẽ được giấu cùng 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 nhĩa. Ngày nay khi ảnh số được sử dụng rất phổ biến thì giấu thông tin trong ảnh đã mang lại nhiều những ứng dụng quan trọng trên các lĩnh vực đời sống xã hội. Ví dụ như các nước phát triển chữ ký tay đã được số hóa 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 dung lưu trữ chứ ký trong ảnh nhị phân rồi gắn vào vị trí nào đó trong tệp văn bản để đảm bảo tính an toàn của thông tin.

1. 1. 5. 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 thông tin là đảm bảo tính chất ẩn của thông tin được giấu đồng thời không làm ảnh hưởng tới chất lượng của dữ liệu. Để đảm bảo yêu cầu này ta lưu ý rằng kỹ thuậtgiấu 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 hệ phục thuộc vào hệ thống tính 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 giải 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 của các giải 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 tới 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. 5. 3. Giấu tin trong video

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

1. 1. 5. 4. Giấu tin trong dạng văn bản 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 hóa 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, video, audio. Gần đây đã có một số nghiên

cứu giấu tin trong cơ sở dữ liệu quân hệ, các gói IP truyền trên mạng, chắc chắn sau này còn phát triển tiếp cho các môi trường dữ liệu số khác.

1.1.6. Một số ứng dụng của kỹ thuật giấu tin

Giấu tin trong ảnh số ngày càng được ứng dụng rộng rãi trong nhiều lĩnh vực. Các ứng dụng có sử dụng đến giấu tin trong ảnh số có thể là: ***Bảo vệ bản quyền tác giả*** (Copyright Protection), ***Điểm chỉ số*** (fingerprinting), ***Gán nhãn***(Labelling), ***Giấu thông tin mật*** (Steganography)…

- *Bảo vệ bản quyền:*Là ứng dụng cơ bản nhất của kỹ thuật thuỷ vân số (watermarking) - một dạng của phương pháp giấu tin. Một thông tin nào đó mang ý nghĩa sở hữu quyền tác giả (người ta gọi nó là thuỷ vân - watermark) sẽ được nhúng vào trong các sản phẩm, thuỷ vân đó chỉ có một mình người chủ sở hữu hợp pháp các sản phẩm đó có và được dùng làm minh chứng cho bản quyền sản phẩm. Giả sử có một thành phẩm dữ liệu dạng đa phương tiện như ảnh, âm thanh, video cần được lưu thông trên mạng. Để bảo vệ các sản phẩm chống lại hành vi lấy cắp hoặc làm nhái cần phải có một kỹ thuật để "dán tem bản quyền" vào sản phẩm này. Việc dán tem hay chính là việc nhúng thuỷ vân cần phải đảm bảo không để lại một ảnh hưởng lớn nào đến việc cảm nhận sản phẩm. Yêu cầu kỹ thuật đối với ứng dụng này là thuỷ vân phải tồn tại bền vững cùng với sản phẩm, muốn bỏ thuỷ vân này mà không được phép của người chủ sở hữu thì chỉ còn cách là phá huỷ sản phẩm.

- *Điểm chỉ số:*Mục tiêu của điểm chỉ số là để chuyển thông tin về người nhận (chứ không phải chủ sở hữu) sản phẩm phương tiện số nhằm xác định đây là bản sao duy nhất của sản phẩm. Về mặt ý nghĩa điểm chỉ số tương tự như số xê ri của phần mềm.

- *Gán nhãn:*Tiêu đề, chú giải và nhãn thời gian cũng như các minh hoạ khác có thể được nhúng vào ảnh, ví dụ đính tên người lên ảnh của họ hoặc đính tên vùng địa phương lên bảng đồ. Khi đó nếu sao chép ảnh thì cũng sẽ sao chép cả các dữ liệu nhúng trong nó. Và chỉ có chủ sở hữu của tác phẩm, người có được khoá mật (Stego-Key) mới có thể tách ra và xem các chú giải này. Trong một cơ sở dữ liệu ảnh, người ta có thể nhúng các từ khoá để các động cơ tìm kiếm có thể tìm nhanh một bức ảnh. Nếu ảnh là một khung ảnh cho cả một đoạn phim, người ta có thể gán cả thời điểm diễn ra sự kiện để đồng bộ hình ảnh vớiâm thanh. Người ta cũng có thể gán số lần ảnh được xem để tính tiền thanh toán theo số lần xem.

- *Giấu thông tin mật:* Trong nhiều trường hợp sử dụng mật mã có thể gây ra sự chú ý ngoài mong muốn. Ngoài ra việc sử dụng công nghệ mã hoá có thể bị hạn chế một

số kỹ thuật giấu tin trong ảnh mầu hoặc cấm sử dụng. Ngược lại việc giấu tin trong môi trường nào đó rồi gửi đi trên mạng ít gây sự chú ý. Có thể dùng nó để gửi đi một bí mật thương mại, một bản vẽ hoặc các thông tin nhạy cảm khác.

1.2. Cấu trúc ảnh BITMAP

Bảng 1. 2. Cấu trúc ảnh bitmap.

Bitmap Header (54 byte)
Color Palette
Bitmap Data

Mỗi file ảnh Bitmap gồm 3 phần theobảng sau:

1.2.1. Bitmap header

Thành phần bitcount (Bảng 1. 3 Thông tin về Bitmap header) của cấu trúc Bitmap header cho biết số bit dành cho mỗi điểm ảnh và số lượng màu lớn nhất của ảnh.

Bảng 1. 3. Thông tin về Bitmap header.

Byte thứ	Ý nghĩa	Giá trị
1-2	Nhận dạng file	‘BM’ hay 19778
3-6	Kích thước file	Kiểu long trong Turbo C
7-10	Dự trữ	Thường mang giá trị 0
11-14	Byte bắt đầu vùng dữ liệu	Offset của byte bắt đầu vùng dữ liệu
15-18	Số byte cho vùng thông tin	4 byte
19-22	Chiều rộng ảnh BMP	Tính bằng pixel
23-26	Chiều cao ảnh BMP	Tính bằng pixel
27-28	Số Planes màu	Cố định là 1
29-30	Số bit cho 1 pixel (bitcount)	Có thể là 1, 4, 8, 16, 24 tùy theo loại ảnh
31-34	Kiểu nén dữ liệu	0: Không nén 1: Nén runlength 8bits/pixel 2: Nén runlength 4bits/pixel
35-38	Kích thước ảnh	Tính bằng byte
39-42	Độ phân giải ngang	Tính bằng pixel/metter
43-46	Độ phân giải dọc	Tính bằng pixel/metter

47-50	Số màu sử dụng trong ảnh	
51-54	Số màu được sử dụng khi hiện thị ảnh	

1.2.2. Palette màu

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

Bảng 1. 4. Bảng màu của ảnh Bitmap.

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

1.2.3. Bitmap data

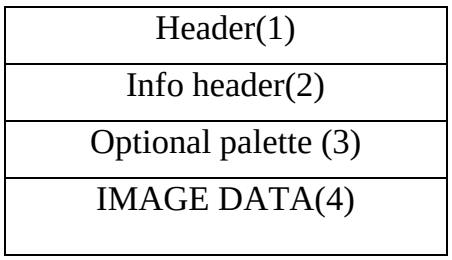
Phần này nằm ngay sau phần Palete màu của ảnh BMP. Đây là phần chứa giá trị màu của điểm ảnh trong ảnh BMP. Các dòng ảnh được lưu từ dưới lên trên, các điểm ảnh được lưu từ trái sang phải. Giá trị của mỗi điểm ảnh là một chỉ số trỏ tới phần tử màu tương ứng trong Palete màu.

1.2.4. Ảnh nhị phân

Ảnh nhị phân là ảnh kỹ thuật số mà chỉ có hai giá trị có thể cho mỗi pixel. Thông thường hai màu sắc được sử dụng cho một ảnh nhị phân là hai màu đen và trắng mặc dù có thể sử dụng bất kì hai màu sắc khác. Các màu sắc được sử dụng cho đối tượng trong hình là màu nền trước khi phần còn lại của hình ảnh là màu nền.

- Ảnh nhị phân được gọi là nhị cấp hoặc hai cấp. Điều này có nghĩa là mỗi điểm ảnh được lưu giữ như là một bit (0 hoặc 1).
- Ứng dụng chính của ảnh nhị phân được dùng theo tính logic để phân biệt đối tượng ảnh với nền hay để phân biệt điểm biên với điểm khác.
- Ảnh nhị phân thường được lưu trữ trong bộ nhớ như là một ảnh bitmap, một mảng đóng gói của các bit.
- Ảnh nhị phân được lưu trữ như là một ảnh định dạng bitmap hay ảnh định dạng IMG.

Sự đơn giản của định dạng tệp tin BMP, và sự phổ biến của nó trong windows và các hệ điều hành khác, cũng như thực tế là định dạng này cũng tương đối tốt, làm cho nó trở thành một định dạng hình ảnh rất phổ biến, chương trình xủ lí từ nhiều hệ điều hành có thể đọc và viết.



Hình 1. 4.Cấu trúc ảnh bitmap của ảnh nhị phân

(1). BITMAPFILEHEADER(14 byte): là phần chứa các thông tin về kiểu ảnh, kích thước, độ phân giải, số bit dùng cho một pixel, cách mã hóa, vị trí bảng màu …

(2). BITMAPINFOHEADER: là nơi lưu trữ thông tin chi tiết về các hình ảnh bitmap, mà sẽ được sử dụng để hiển thị hình ảnh trên màn hình.

(3). OPTINAL PALETE: là một khối byte (một bảng) danh sách các màu có sẵn để sử dụng trong chỉ mục màu sắc cụ thể của ảnh.

(4). IMAGE DATA: là nơi lưu trữ mô tả dữ liệu của ảnh. Điểm ảnh được lưu trữ "ngược lại" đối với hình ảnh bình thường bằng raster, bắt đầu ở góc trái bên dưới, từ trái sang phải, và sau đó liên tiếp bởi hàng từ đáy lên đỉnh của hình ảnh.

1.3. Phương pháp đánh giá PSNR(peak signal-to-noise ratio)

PSNR là phương pháp đánh giá độ nhiễu của ảnh trước và sau khi giấu tin, đơn vịđo là logarithm decibel. Thông thường PSNR càng cao thì độ nhiễu của ảnh trước và sau khi giấu tin càng thấp. Giá trị PSNR được coi là tốt ở vào khoảng 35dB và nhỏ hơn 20dB là không chấp nhận được. Hiện nay PSNR được dùng rộng rãi trong kỹ thuật đánh giá chất lượng hình ảnh và video.

Cách đơn giản nhất là định nghĩa thông qua trung bình lỗi bình phương (MSE – mean squared error) được dùng cho ảnh 2 chiều có kích thước $m \times n$ trong đó I và Klà ảnh gốc và ảnh được khôi phục tương ứng:

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

PSNR được định nghĩa bởi:

$$\text{PSNR} = 10*\log_{10}\left(\frac{MAX_1^2}{MSE}\right) = 20*\log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right)$$

Ở đây, MAX(I) là giá trị tối đa của điểm ảnh trên ảnh I. Khi các điểm ảnh được biểu diễn bởi 8 bit, thì giá trị của nó là 255.Trường hợp tổng quát, điểm ảnh được biểu diễn bởi B bit, MAX(I) là 2^B-1. Với ảnh màu biểu diễn 3 giá trị RGB trên 1 điểm ảnh, các tính toán cho PSNR tương tự ngoại trừ việc tính MSE là tổng của 3 giá trị (tính trên 3 kênh màu RGB) chia cho kích thước của ảnh và chia cho 3.

Với ảnh nhị phân các điểm ảnh trên ảnh nhị phân được biểu diễn bởi 2 bit 0 hoặc 1, nên giá trị của MAX(I) = 1.

Chương 2. GIẤU TIN TRONG ẢNH NHỊ PHÂN

2.1. Giới thiệu tổng quan giấu tin trong ảnh nhị phân

Đối tượng làm môi trường chứa tin của thuật toán này là ảnh nhị phân đen trắng dạng bitmap. Ảnh nhị phân đen trắng bao gồm các điểm ảnh chỉ có màu đen hoặc trắng (tương ứng với bit 0 hoặc bit 1). Để giấu dữ liệu, ta sẽ tách ma trận điểm ảnh (pixel) thành ma trận bit F kích thước *mxn* rời nhau, và giấu tin trên mỗi ma trận đó, Bởi vậy các thuật toán chỉ cần quan tâm tới phương pháp giấu dữ liệu trên ma trận F.

Một số thuật toán giấu tin trên ảnh nhị phân nổitiếng hiện nay như:Wu-Lee[2], CPT[3], CPTE[5]. Các thuật toán này đều dựa trên thao tác biếnđổi ma trận bit.

2.2. Một số kỹ thuật giấu tin trên ảnh nhị phân điển hình

2. 2.1. Giấu tin theo khối bit (CB)

Ý tưởng cơ bản của kỹ thuật này là chia ảnh gốc thành các khối nhỏ và trong mỗi khối nhỏ sẽ giấu 1 bit thông tin. Quá trình giấu tin:

Với một ảnh gốc kích thước MxN, chia phần thông tin ảnh thành các khối nhỏ có kích thước m×n, số các khối nhỏ sẽ là (M×N)/(m×n) khối.Vì ảnh là đen trắng nên mỗi khối là một ma trận hai chiều m dòng, n cột các phần tử có giá trị 0 hoặc 1.

Chọn các khối chưa giấu tin để thực hiện giấu tin, các khối được chọn cho đến khi giấu hết các thông tin cần giấu hoặc khi đã chọn hết các khối.

Với mỗi khối ảnh F kích thước m×n và bit đang cần giấu b, tiến hành biến đổi F thành F’ để giấu bit b sao cho:

$$SUM(F') \bmod 2 = b$$

Như vậy, mỗi lần giấu một bit, có thể xảy ra hai trường hợp: SUM (F) mod 2 = b, khi đó ta giữ nguyên khối ảnh. Ngược lại chọn ngẫu nhiên một bit trong khối F và tiến hành đảo giá trị của bit này để được khối ảnh mới F’.

Quá trình tách tin: Khi nhận được ảnh đã giấu tin, việc giải mã tin sẽ thực hiện theo các bước:

Chia ảnh thành các khối có kích thước giống kích thước khối đã sử dụng khi thực hiện giấu, đây chính là khoá để giải mã.

Với mỗi khối ảnh đã giấu tin F' được chọn theo thứ tự như quá trình giấu tin, thực hiện tách lấy bit thông tin đã giấu theo công thức: b = SUM(F') mod 2.

Như vậy, sau khi xét hết các khối đã giấu, ta thu được một chuỗi bit, chuỗi này là thông tin nhị phân đã giấu cần phải lấy ra.

Lược đồ giấu tin CB có thể giấu được 1 bit thông tin vào một khối kích thước m×n bit mà chỉ thay đổi tối đa 1 bit trong đó.

2. 2. 2.Lược đồ giấu tin của M. Y. Wu và J. H. Lee (WL)

Kỹ thuật giấu tin theo khối bit CB thể hiện độ an toàn không cao với việc sử dụng duy nhất kích thước khối là khoá cho quá trình giấu tin, ảnh chứa thông tin giấu cũng dễ bị phát hiện do kỹ thuật có thể sẽ đảo bit trong các khối ảnh toàn màu đen hoặc toàn màu trắng dẫn tới sự bất thường ở vị trí bit đảo so với các điểm lân cận trong khối.

Kỹ thuật giấu thông tin trong ảnh đen trắng do M.Y.Wu và J.H.Lee vẫn dựa trên tư tưởng giấu một bit thông tin vào một khối ảnh gốc nhưng đã khắc phục được phần nào những tồn tại nêu trên bằng cách đưa thêm khoá K cho việc giấu tin và đưa thêm các điều kiện để đảo bit trong mỗi khối, theo điều kiện đó các khối ảnh gốc toàn màu đen hoặc toàn màu trắng sẽ không được sử dụng để giấu tin.

Quá trình biến đổi khối ảnh F thành F' để giấu 1 bit b được thực hiện sao cho:

$$SUM(K \hat{} F') \bmod 2 = b$$

Công thức này cũng được sử dụng cho quá trình tách, lấy tin đã giấu.

Lược đồ giấu tin WL có thể giấu được 1 bit thông tin vào một khối m×n bit và chỉ phải thay đổi tối đa 1 bit trong đó.

2. 2. 3. Lược đồ giấu tin của Chen-Pan-Tseng

Trên cơ sởthuật toán Wu-Lee như đã trình bày trên, các tác giả Yu Yuan Chen, Hsiang Kuang Pan và Yu Chee Tseng đã phát triển một kỹ thuật giấu tin mới hay còn gọi là CPT. Kỹ thuật này sử dụng một ma trận khoá K và một ma trận trọng số W trong quá trình giấu và tách thông tin.

Quá trình biến đổi khối ảnh F thành F' kích thước m×n để giấu r bit thông tin $b_1b_2\ldots b_r$ được thực hiện sao cho:

$$SUM((F' \oplus K) \otimes W) \equiv b_1b_2 \ldots b_r \pmod{2^r}.$$

Công thức trên được sử dụng để tách chuỗi bit đã giấu $b_1b_2. . .b_r$ từ khối ảnh F'.

Lược đồ CPT cho phép giấu r bit thông tin vào một khối ảnh nhị phân kích thước m×n (với $2^r < m \times n$) bằng cách chỉ thay đổi nhiều nhất 2 bit trong khối ảnh gốc.

Trong phần tiếp theo sẽ đi vào trình bày chi tiết kỹ thuật giấu tin nhị phân CPT.

2. 3. Kĩ thuật giấu tin CPT cho ảnh nhị phân

2. 3. 1. Ý tưởng của kĩ thuật

Việc giấu tin vào ảnh nhị phân thực sự là một thách thức không nhỏ. Thuật toán giấu bit tin vào khối ảnh nhị phân được M. Y. WU và J. H. LEE đề xuất trong [2]. Tuy nhiên, mỗi khối chỉ giấu được không nhiều thông tin và khả năng bảo mật cũng không được tốt. Trong nghiên cứu [3], trên cơ sở phát triển ý tưởng của nhóm M. Y. WU và J. H. LEE, các tác giả Y. Y. Chen, H. Pan, Y. Tseng (CPT) đề xuất một phương pháp giấu thông tin trong ảnh nhị phân, theo đó, ảnh được chia thành nhiều khối F có cùng kích thước m×n. Cho phép giấu được tối đa $r = \log_2(mn+1)$ bit dữ liệu vào khối ảnh kích thước m×n mà chỉ cần thay đổi nhiều nhất 2 bit trong khối ảnh.

2. 3. 1. 1. Ma trận trọng số

Chương trình giấu tin phụ thuộc rất nhiều vào ma trận trọng số W để đại diện cho dữ liệu nhúng. Phần này sẽ được làm rõ thông qua ví dụ dưới đây. Giả sử ma trận K và W có kích cỡ 3x3. Sau đây, chúng ta xét một khối con F_i có kích cỡ 3x3 của ma trận F. Vậy làm thế nào để nhúng r = 2 bit dữ liệu vào F_i.

$$F_i = \begin{bmatrix}1 & 1 & 0\\ 1 & 0 & 0\\ 1 & 1 & 0\end{bmatrix} K = \begin{bmatrix}0 & 1 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\end{bmatrix} W = \begin{bmatrix}1 & 2 & 3\\ 1 & 2 & 3\\ 1 & 2 & 3\end{bmatrix}$$

Trước tiên, chúng ta sẽ thực hiện một phép toán XOR giữa F_i và K

$$F_i \oplus K = \begin{bmatrix}1 & 1 & 0\\ 1 & 0 & 0\\ 1 & 1 & 0\end{bmatrix} \oplus \begin{bmatrix}0 & 1 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 1\end{bmatrix}$$

Tiếp theo, thực hiện nhân chập trên hai ma trận($F_i \oplus K$) và W. Ta được:

$$(F_i \oplus K) \otimes W = \begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 1\end{bmatrix} \otimes \begin{bmatrix}1 & 2 & 3\\ 1 & 2 & 3\\ 1 & 2 & 3\end{bmatrix} = \begin{bmatrix}1 & 0 & 3\\ 0 & 2 & 0\\ 1 & 0 & 3\end{bmatrix}$$

Tính tổng của biểu thức trên ta có:

$$SUM((F_i \oplus K) \otimes W) = 1 + 3 + 2 + 1 + 3 = 10$$

Chúng ta giấu 2 bit dữ liệu b_1b_2 vào F_i. Giả sử sau khi giấu, F_i được thay đổi thànhF_i' sao cho:

$$SUM((F_i' \oplus K) \oplus W) \equiv b_1b_2 \pmod 4 \quad (2.1)$$

Với biểu thức này, người nhận có thể lấy được b_1b_2bởi phép tính $SUM((F_i' \oplus K) \otimes W) \bmod 4$.

Tiếp theo, chúng ta phải làm thế nào để sửa đổi F_i để đảm bảo (2.1), nghĩa là ta phải thay đổi vài bit trong F_i. Khi $SUM (F_i \oplus K) \otimes W \equiv 2$, nếu $b_1.b_2 = 2$ thì không cần thiết phải sửa đổi F_i. Nếu không, một vài bit(s) sẽ được thay đổi. Quan sát thấy nếu chúng ta đảo bit $(F_i)_j$ thì $(F_i \oplus K)_{j,k}$ sẽ bị thay đổi. Nếu $(F_i \oplus K)_{j,k}$ được đảo bit từ 0 đến 1, thì SUM sẽ tăng $w_{j,k}$, nếu không sẽ giảm $w_{j,k}$. Giả sử, chúng ta thay đổi $[F_i]_{1,1}$, SUM sẽ giảm $w_{1,1}$=1, và nếu chúng ta thay đổi $[F_i]_{1,2}$ thì SUM sẽ giảm $w_{1,2}$ = 2. Nó không khó để chúng ta xác định cần phải đảo một bit trong F_i để tăng hoặc giảm SUM bằng 1,2 hoặc 3 trong ví dụ này.

*Định nghĩa 1:*Một ma trận W kích cỡ *mxn* là một ma trận trọng số, nếu mỗi phần tử thuộc $(1,2, ...,2^r - 1)$ xuất hiện ít nhất một lần trong W, nghĩa là $\{[W]_{i,j}, i=1..m, j= 1..n\} = \{1,2, ...,2^r - 1\}$.

Ý nghĩa của định nghĩa sẽ rõ ràng như sau, (cho phép dễ dàng xây dựng một W khi khởi tạo thuật toán giấu tin), ta đặt 2^r-1 ≤*mxn*. Ngoài ra, còn nhiều sự lựa chọn khác cho W. Đầu tiên, chúng ta có thể chọn 2^r-1 phần tử trong Wthuộc $\{1,2,...,2^r\text{-}1\}$. Số còn lại *mxn*-(2^r-1) phần tử có thể được chỉ định ngẫu nhiên. Như vậy, số lượng các lựa chọn cho W là:

$$C_{2^r-1}^{mn} * (2^r - 1)! * (2^r - 1)^{mn-(2^r-1)}$$

W là một ma trận trọng số và F_i là một khối con của ảnh đầu vào F. Sau đây, chúng ta có thể nhúng r bit dữ liệu, $b_1b_2\ldots b_r$ vào F_i bằng cách thay đổi nhiều nhất 2 bit trong F_i. Mục tiêu là thay đổi F_i thành F_i' để đảm bảo:

$$SUM ((F' \oplus K) \otimes W) = b_1b_2\ldots b_r \pmod{2^r} \quad (2.2)$$

<u>*Bổ đề 1:*</u> Với mỗi $w = 1..2^{r-1}$mà $w \neq 2^{r-1}$thì mệnh đề sau đúng:

$$S_w = \varnothing \text{ta có} S_{2^r\text{-}w} \neq \varnothing$$

Chứng minh: Giả sử $S_w = \varnothing$:Từ định nghĩa 1, có ít nhất một bit $[W]_{j,k} = w$. Điều này có nghĩa là $[F_i]_{j,k} = 1$. Mặt khác, đảo bit$[F_i]_{j,k}$tổng tăng lên đến w, tập hợp S_w sẽ không rỗng. Nếu chúng ta bổ sung $[F_i]_{j,k}$tổng giảm xuống w hoặc tương đương với việc tăng $2^r - w \pmod{2^r}$. Như vậy tậpS_{2^r-w}không rỗng. Chú ý rằng ngoại trừ trường hợp $w = 2^{r-1}$thì $w=2^r - w$.

Bổ đề 2: Tập hợp $S_{2^{r-1}} \neq \varnothing$

Chứng minh: Từ định nghĩa 1, $[W]_{j,k} = 2^{r-1}$có ít nhất một bitthì $2^{r-1} = -2^{r-1} \pmod{2^r}$nếu $[F_i]_{j,k} \cap K_{j,k} = 0$ hay bằng 1. Nếu chúng ta đảo bit $[F_i]_{j,k}$thì tổng sẽ tăng hoặc giảm 2^{r-1}. Do đó, bổ đề được chứng minh.

*Bổ đề 3:*Quá trìnhđảo bit trên khối F thành khối F' sao cho:SUM ((F' $\oplus$ K) $\otimes$ W) = $b_1 b_2 \ldots b_r \pmod{2^r}$ thì luôn luôn thành công và có nhiều nhất 2 bit của F_i được sửa đổi để giấu vào r bit dữ liệu.

Chứng minh: Chúng ta kiểm tra một loạt các giá trị của h và tìm thấy một h đủ điều kiện. Trước tiên, chúng ta kiểm tra S_d. Nếu $S_d \neq \varnothing$ thì h=1. Mặt khác, $S_d = \varnothing$ nghĩa là $S_{-d} \neq \varnothing$theobổ đề 1.Tiếp theo chúng ta kiểm tra S_{2d}. Nếu $S_{2d} \neq \varnothing$ thì h= 2. Mặt khác$S_{2d} = \varnothing$nghĩa là $S_{-2d} \neq \varnothing$theo bổ đề1. Tiếp theo chúng ta kiểm tra S_{3d}. Nếu $S_{3d} \neq \varnothing$ thì h=3. Mặt khác$S_{3d} = \varnothing$nghĩa là $S_{-3d} \neq \varnothing$.Chúng ta có thể lặp lại quá trình này để kiểm traS_{4d}, S_{5d},.v.v… Nếu như những lần kiểm tra này tiếp tục sai chúng ta sẽ kiểm traS_{2^r-1}. Như vậy, bổ đề 2 đảm bảo rằngS_{2^r-1}không rỗng do đó bổ đề được chứng minh.

Yêu cầu này có thể được chứng minh bằng một quy tắc đơn giản trong lý thuyết số, nói rằng {d mod 2^r, 2d mod 2^r , 3d mod 2^r,…} phải chứa tất cả hoặc chỉ những con số mà là bội số của gcd(d,2^r) mà nhỏ hơn 2^r. Khi 2^{r-1}là một bội số của gcd(d,2^r) thìS_{2^r-1}cuối cùng sẽ được kiểm tra.

2. 3. 2. Thuật toán giấu tin

Từ các phân tích trên có thể viết tóm lược thuật toán giấu tin như sau:

Khóa bí mật K là một ma trận nhị phân có cùng kích thước với khối ảnh F_i (là ma trận con của F) (số khả năng lựa chọn K là 2^{mn}).

Ma trận trọng số W cũng có cùng kích thước với khóa K, có các phần tử thuộc{1, 2, . . , 2^{r-1}} và các phần tử này phải xuất hiện ít nhất một lần trong W (số khả năng lựa chọn W: $C_{mn}^{2^{r-1}} * (2^r - 1)! * (2^r - 1)^{mn-(2^r-1)}$)

Nội dung thuật toán:

Đầu vào: Ảnh nhị phân F, cần giấu r bit thông tin $b_1b_2...b_r$ vào F.

Đầu ra: Ảnh nhị đã giấu tin F'.

Thuật toán gồm 4 bước:

Bước 1: Chia ma trận F thành các ma trận con $F_1...F_n$ kích thước bằng K và W. Thực hiện tính ma trận trên mỗi khối F: $T_1 = F_1 \oplus K$ (Phép toán XOR), tương tự với $F_2...F_n$

Bước 2: Tính tổng SUM($T \otimes W$) (Phép $\otimes$ nhân chập từng phần tử)

Bước 3: Với mọi w = 1, . . . , 2^{r-1}, tập hợp S_w được xác định:

$S_w = \{(j, k)|((W[j, k]=w) \text{ and } (T[j, k]=0)) \text{ or } ((W[j, k]= 2^r-w) \text{ and } (T[j, k])=1))\}$

S_w là tập hợp các tọa độ (j, k) của F sao cho khi đảo bit F[j, k] thì SUM ở bước 2 tăng lên w đơn vị (theo mod 2^r).

Bước 4: Đảo bit trên khối F thành khối F' sao cho:

$$SUM ((F' \oplus K) \otimes W) = b_1b_2...b_r \pmod{2^r}$$

Xử lý đảo bit trên F như sau:

Kí hiệu : $d = (b_1b_2...b_r)_2 - SUM((F \oplus K) \otimes W) \pmod{2^r}$.

Đảo bit trên F để được F' sao cho SUM($T \otimes W$) tăng lên d.

* Nếu d = 0: Không cần thay đổi F

* Nếu $d \neq 0$: Có hai khả năng xảy ra:

- Nếu $S_d \neq \varnothing$: Chọn phần tử (j, k) thuộc S_d rồi đảo bit $F_{[j, k]}$

- Nếu $S_d = \varnothing$: Thực hiện theo các bước:

→ Tìm số tự nhiên h nhỏ nhất để $S_{hd} \neq \varnothing$ và $S_{d - hd} \neq \varnothing$.

→ Chọn (j, k) thuộc S_{hd}; (u, v) thuộc S_{d-hd} rồi đảo bit đồng thời $F_{[j, k]}$ và $F_{[u, v]}$, SUM($T \otimes W$) sẽ tăng lên [hd + (d - hd)] = d.

2. 3. 3. Thuật toán tách tin

Nội dung thuật toán:

Đầu vào: Ảnh nhị phânchứa tin F'

Đầu ra: Thông tin b giấu trong F'

Thuật toán gồm 4 bước:

Bước 1: Chia ma trận F' thành các ma trận con $F'_1 \ldots F'_n$ kích cỡ bằng kích cỡ của K và W. Tính ma trận $T'_i = F'_i \oplus$ K (Phép toán XOR)

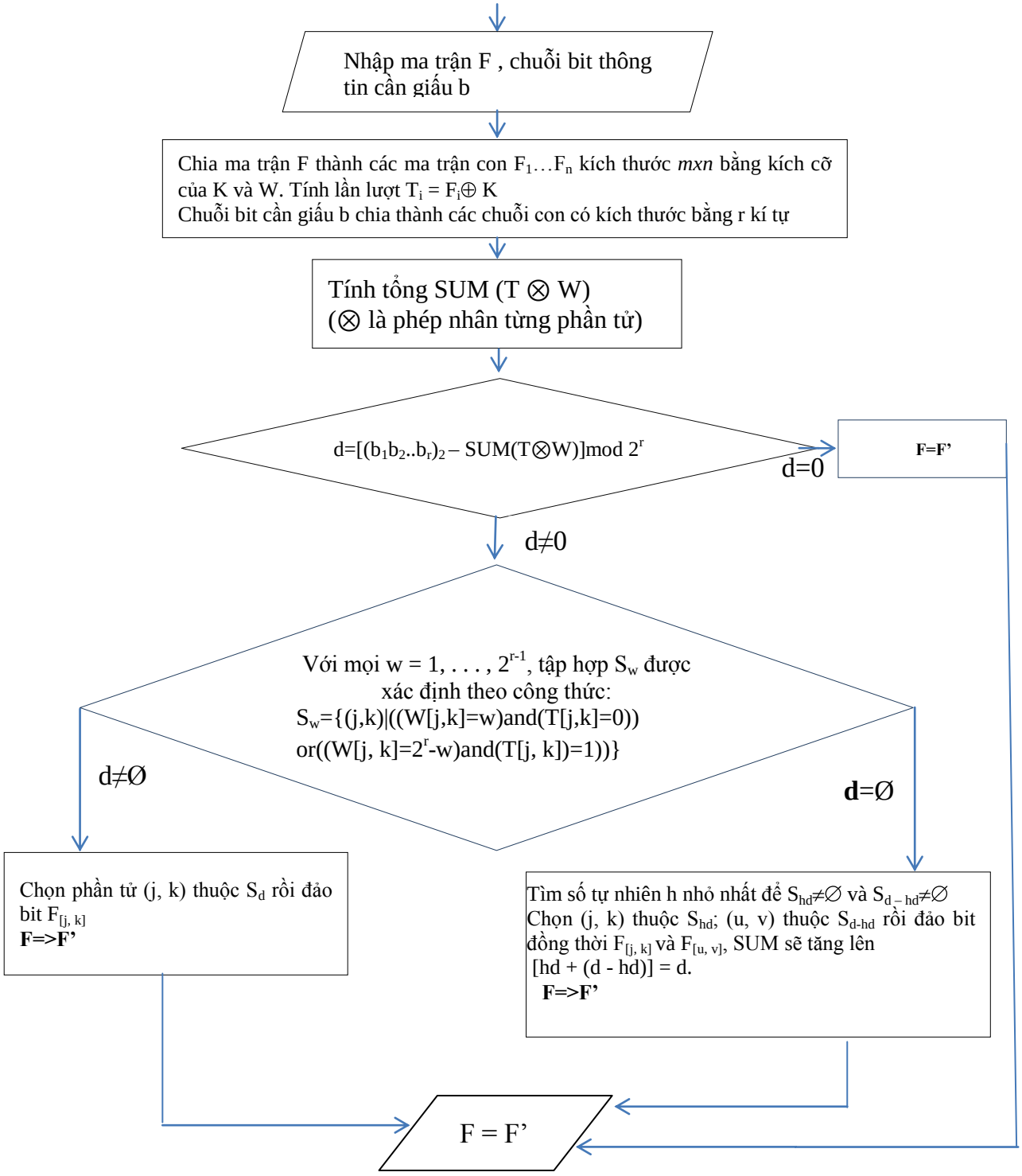
Bước 2: Tính tổng SUM($T'_i \otimes$ W) (Phép $\otimes$ nhân chậptừng phần tử)

*Bước 3:*Tính b bằng công thức

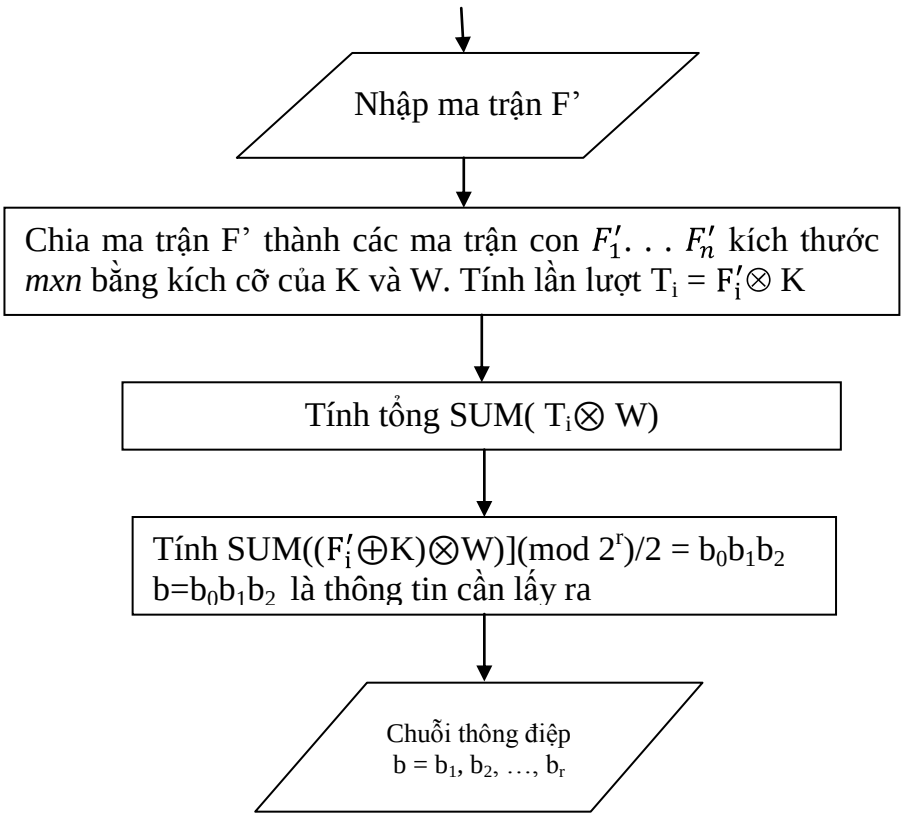
$$\text{SUM}((F'_i \oplus \text{K}) \otimes \text{W})](\text{mod } 2^r)/2 = b_0 b_1 b_2$$

$b=b_0b_1b_2$ là thông tin cần lấy ra.

Hình 2.1, 2.2 Lưu đồ tổng quát quá trình giấu và tách tin ảnh nhị phân



Hình 2. 1.Sơ đồ quá trình giấu tin



Hình 2. 2. Sơ đồ quá trình tách tin

2. 3. 4. Ví dụ quá trình giấu và tách tin

F K W

1	1	0	0	0	1	0	0
1	0	0	0	1	1	0	0
0	0	0	0	0	1	1	1
0	0	1	0	0	1	0	1
0	1	0	0	0	1	0	0
1	1	0	0	1	0	0	1
0	0	1	0	0	1	1	1
0	1	1	1	0	0	0	1

0	1	0	1
0	1	0	0
1	1	0	1
0	0	0	0

13	12	15	8
7	4	3	10
1	2	9	6
11	14	5	1

r= 3

Thông điệp giấu là chuỗi nhị phân: 001 110 011 001 được tách thành các chuỗi con kích thước r = 3.

Thực hiện chạy chậm giấu tin:

Chia F thành 4 ma trận con F_1, F_2, F_3, F_4 cùng kích thước với F và W. Thực hiện tính ma trận trên mỗi khối: $T = F \oplus K$

$F_1 \oplus K$ $F_2 \oplus K$

1	0	0	1	0	0	0	1
1	1	0	0	1	0	0	0
1	1	0	1	1	0	1	0
0	0	1	0	0	1	0	1
0	0	0	1	0	0	0	1
1	0	0	0	1	1	0	1
1	1	1	1	1	0	1	0
0	1	1	1	0	0	0	1

$F_3 \oplus K$ $F_4 \oplus K$

Tính tổng S = SUM (T ⊗ W)

- S_1 = SUM ($T_1 \otimes$ W) = 46

  d1 = $(001)_2$ - S_1 =1 – 46= -45= -45(mod 8) =3

  d1=3, $S_{d1}= F_{2,3}$

  Vậy phải đảo bit $F_{2,3}$ ta được F'_1:

1	1	0	0
1	0	1	0
0	0	0	0
0	0	1	0

  Kiểm tra Sum[($F'_1 \oplus$K)⊗W](mod 2^r) =49 mod(8)= 1 =$(001)_2$, vậy áp dụng đã đúng.

- S_2= SUM ($T_2 \otimes$ W) = 40

  d2 = $(010)_2$ – 40 = -38 = -38 mod(8) = 2

  d2 = 2 , S2 = $F_{3,2}$

  Vậy phải đảo bit $F_{3,2}$ ta được F'_2

0	1	0	0
1	1	0	0
0	0	1	1
0	1	0	1

  Kiểm tra Sum[($F'_2 \oplus$K)⊗W)](mod 2^r) = 42 mod(8)= 2 =$(010)_2$, vậy áp dụng đã đúng.

- S_3= SUM ($T_3 \otimes$ W) = 53

  d3 = $(000)_2$ – 53 = -53 = -53 mod 8 = 3

  d3 = 3 , $S_3 = F_{2,3}$

  Chọn $F_{2,3}$ để đảo bit, vậy F'_3 là

0	1	0	0
1	1	1	0
0	0	1	0
0	1	1	1

  Kiểm tra Sum[($F'_3 \oplus$K)$\otimes$W)](mod 2^r) = 56 mod(8)= 0 =$(000)_2$, vậy áp dụng đã đúng.

- S_4= SUM ($T_4 \otimes$ W) = 40

  d4 = $(001)_2$ – 40 = -39 = -39 mod 8 = 1

  d1 = 1 , $S_1 = \varnothing$

  h=2 => $S_2 = F_{3,2}$, $S_{-1} = S_7 = \varnothing$

  h=3 => $S_3 = F_{2,3}$, $S_{-2} = S_6 = F_{3,4}$

  Vậy ta phải đảo bit $F_{2,3}$, $F_{3,4}$ để đượcF'_4

0	1	0	0
1	0	1	1
0	1	1	0
0	0	0	1

Kiểm tra Sum[($F'_4 \oplus$K)$\otimes$W)](mod 2^r) = 39 mod(8)= 1 =$(001)_2$, vậy áp dụng đã đúng.

Vậy F sau khi đã giấu tin là:

1	1	0	0	0	1	0	0
1	0	1	0	1	1	0	0
0	0	0	0	0	0	1	1
0	0	1	0	0	1	0	1
0	1	0	0	0	1	0	0
1	1	1	0	1	0	1	1
0	0	1	0	0	1	1	0
0	1	1	1	0	0	0	1

Chương 3. CÀI ĐẶT VÀ THỬ NGHIỆM

3.1. Môi trường cài đặt

-Ngôn ngữ cài đặt:Ngôn ngữ lập trình Matlab phiên bản 7.5

-Môi trường soạn thảo:Matlab phiên bản 7.5

-Môi trường chạy chương trình:Môi trường giao diện Matlab phiên bản 7.5

-Cấu hình tối thiểu để cài đặt Matlap:

+Intel hoặc AMD x86 processor supporting SSE2

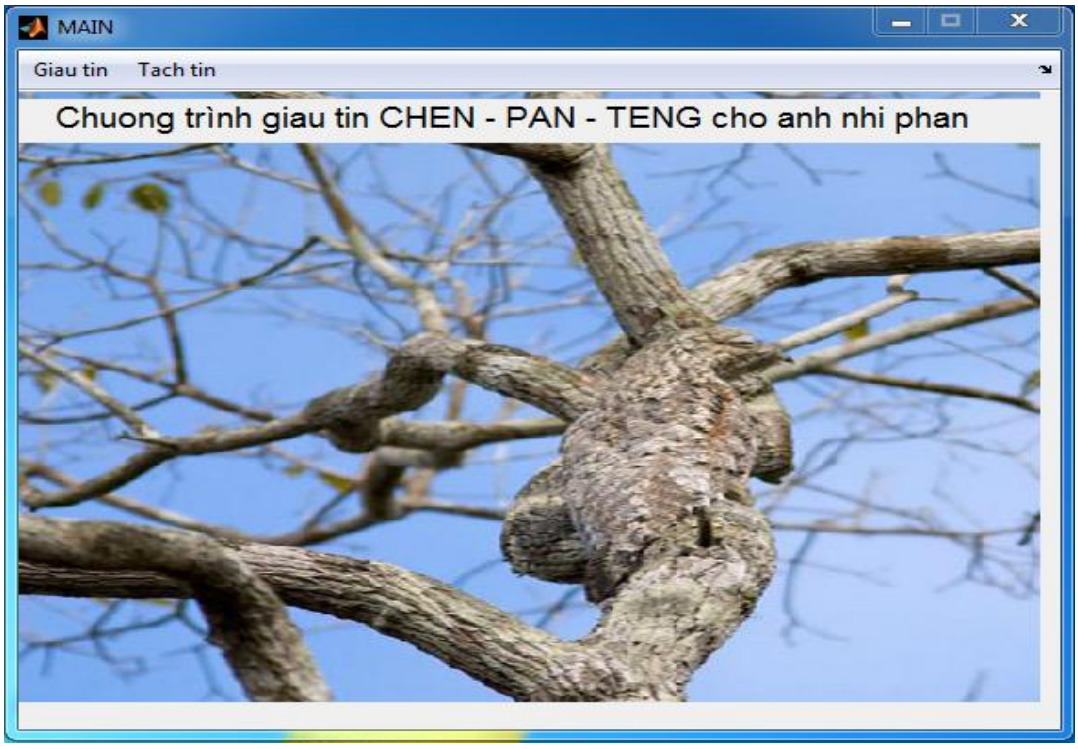
+Windows XP SP2 x64, SP3, …

+Dung lượng ổ cứng từ 1GB tới 5GB

+Bộ nhớ RAM tối thiểu 1GB

3.2. Giao diện chương trình

3.2.1. Giao diện chương trình chính



Hình 3.1. Giao diện chương trình chính

Đầu vào:

- Ảnh nhị phân F có kích thước *mxn.*
- Chuỗi thông điệp cần giấu.

Đầu ra:

-Ảnh nhị phân F’ đã được giấu tin.

Chức năng giấu tin:

-Giấu tin trên thuật toán Chen-Pan-Tseng

- Giấu vào chuỗi kí tự: do người dùng nhập vào từ bàn phím

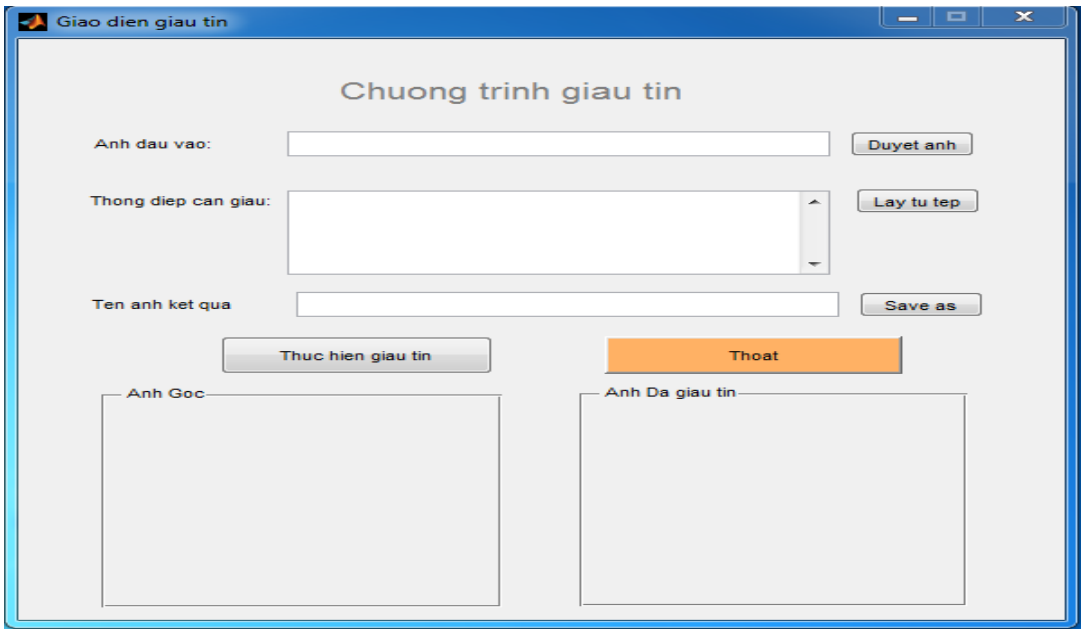
-Giấu vào tệp văn bản: Cho phép chọn một tệp văn bản định dạng *.txt để giấu vào ảnh

Chức năng tách tin:

-Tách tin dựa trên thuật toán Chen-Pan-Tseng theo ảnh đã giấu tin từ trước.

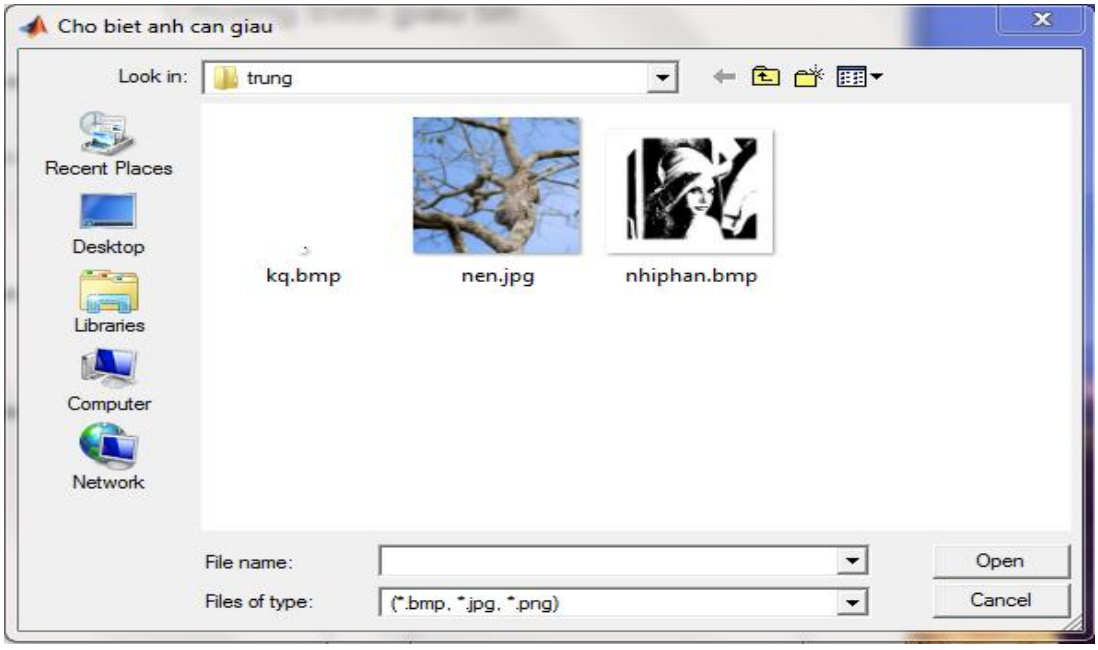
-Tách chuỗi thông điệp đã giấu và lưu dưới dạng tệp *.txt

3.2.2. Giao diện chức năng giấu tin



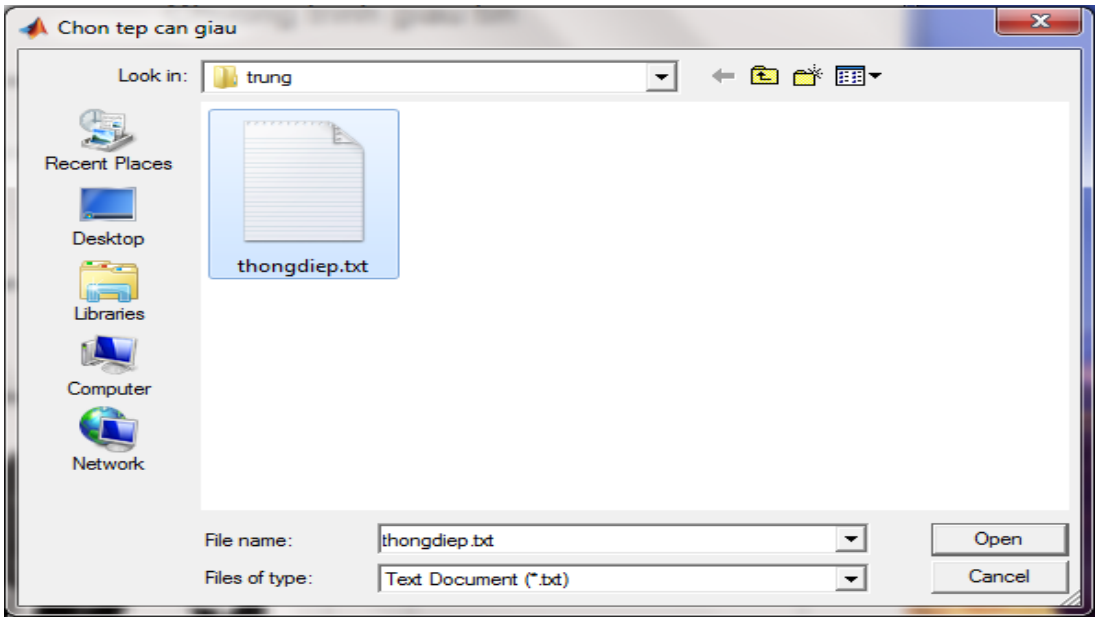
Hình 3.2. Giao diện chức năng giấu tin

Từ giao diện chính của chương trình chúng ta chọn ảnh cần giấu tin bằng cách nhấn vào button “Duyệt ảnh”.Khi đó chương trình sẽ mở ra hộp thoại duyệt ảnh.



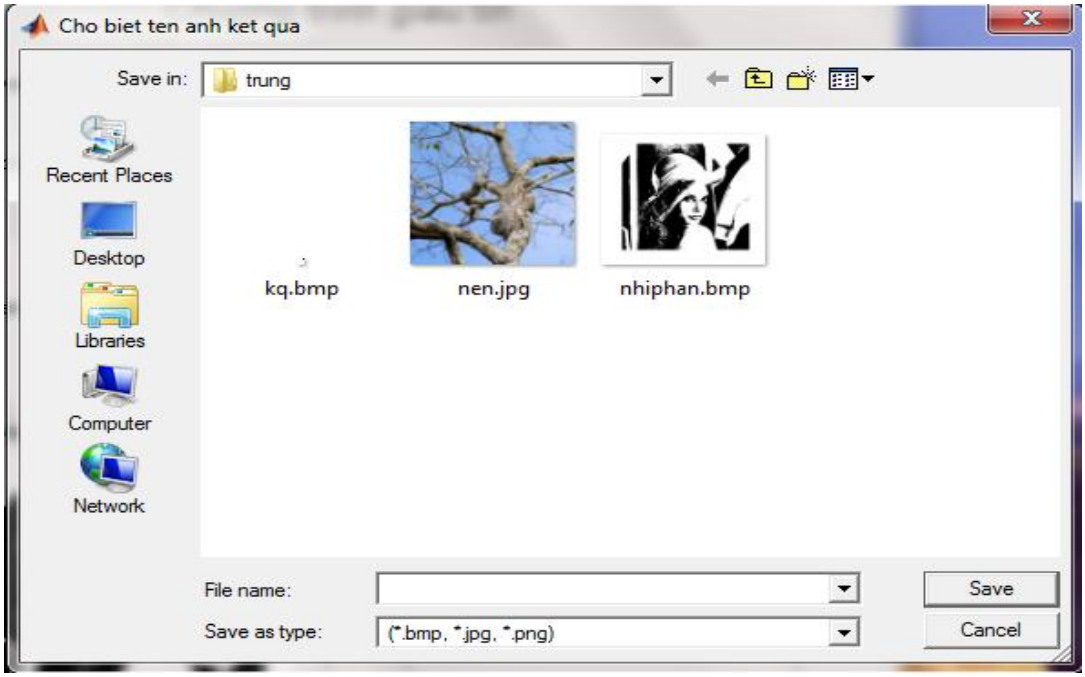
Hình 3.3. Hộp thoại chọn ảnh nhị phân cần giấu tin

Chúng ta sẽ chọn ảnh nhị phân bất kì để thực hiện giấu tin vào ảnh đó. Sau khi chọn ảnh nhị phân xong, ta nhập thông diệp vào từ bàn phím hoặc lấy thông điệp từ tệp *.txt bất kì để giấu tin.

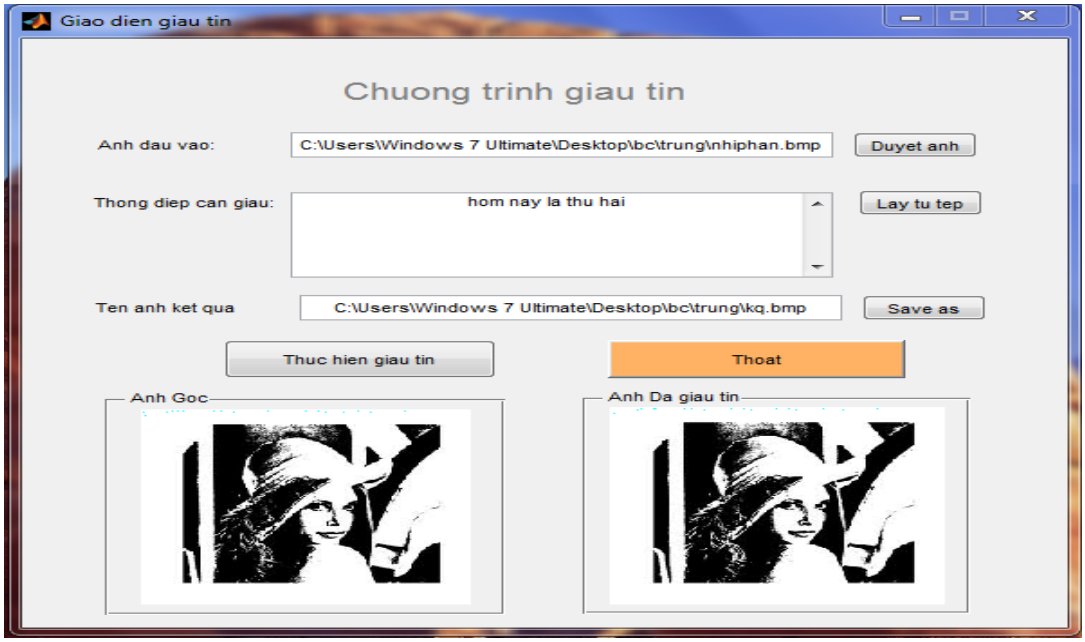


Hình 3.4. Hộp thoại chọn tệp thông điệp

Chúng ta cần chọn nơi sẽ lưu thông điệp sau khi đã giấu tin vào bằng cách chọn “Save as” từ giao diện



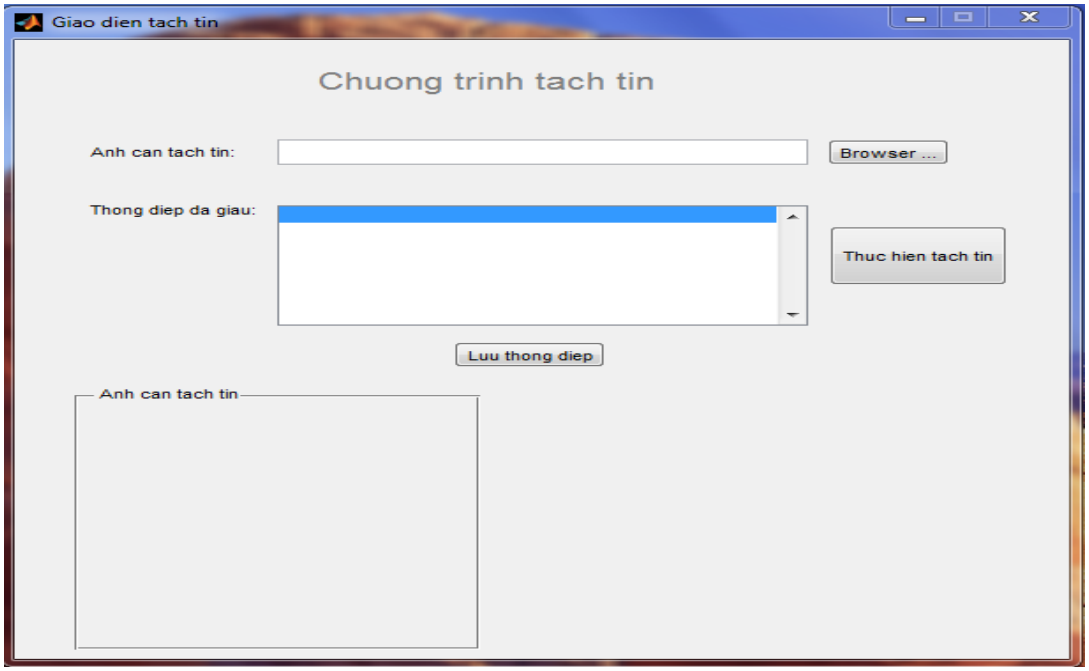
Hình 3.5. Hộp thoại cho biết tên ảnh sau khi đã giấu tin



Hình 3.6. Giao diện sau khi giấu tin

Sau khi đã lựa chọn xong đầu vào và đầu ra cho chương trình, chúng ta chọn nút "thực hiện giấu tin". Chương trình sẽ thực hiện và đưa ra kết quả ảnh đã giấu tin ngay trên giao diện của chương trình

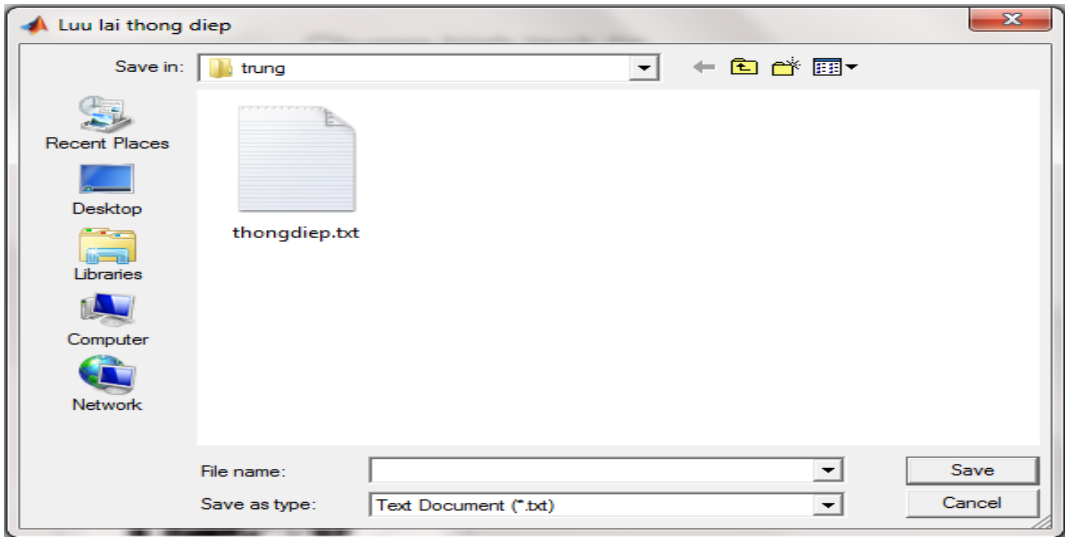
3.2.3. Giao diện chức năng tách tin



Hình 3.7. Giao diện chức năng tách tin

Bước đầu cần cho biết ảnh mang tin bằng cách chọn "Browser" để lấy giá trị đầu vào của ảnh. Sau đó ta tiến hành tách tin bằng cách nhấn button "Thực hiện tách tin".

Sau khi đã tách tin xong, chúng ta tiến hành lưu lại thông điệp bằng cách chọn button "Lưu thông diệp"



Hình 3.8. Hộp thoại chọn lưu thông điệp

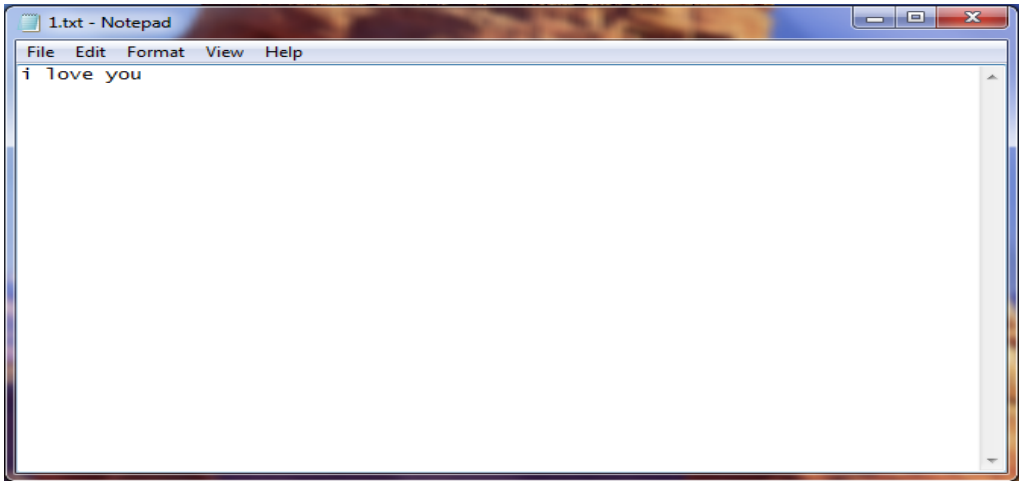
Chúng ta gõ tên của tệp thông điệp cần lưu lại và chọn "Save" để tiến hành lưu lại trên máy tính.

3.3. Kết quả thực nghiệm và nhận xét

3.3.1. Kết quả thực nghiệm

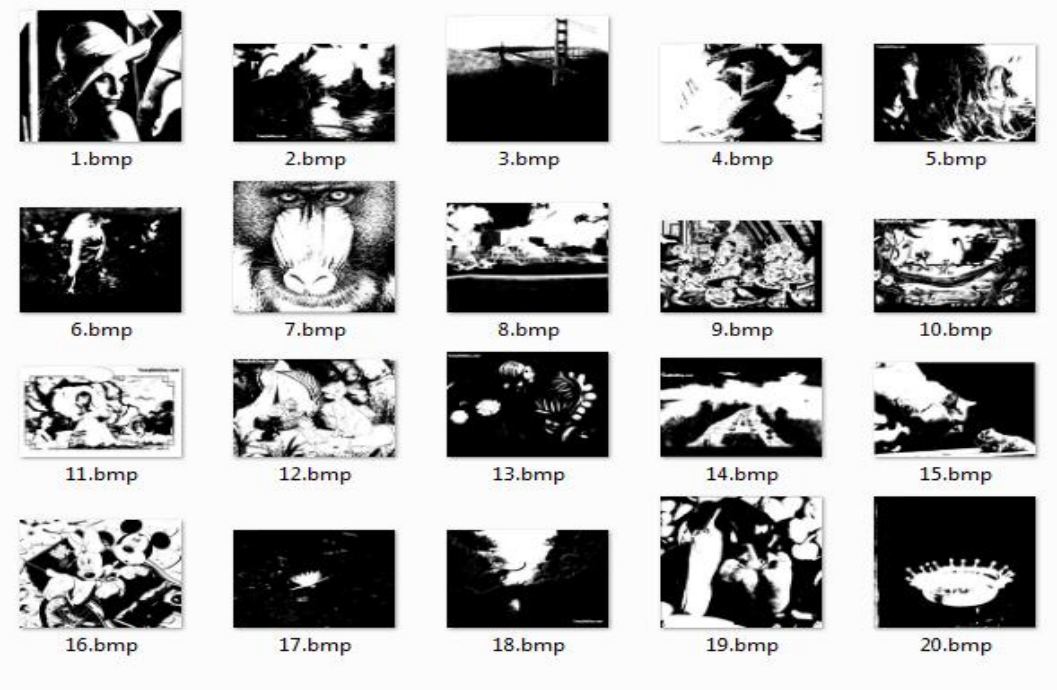
Thực nghiệm này sẽ đưa ra khả năng giấu tin khi sử dụng kỹ thuật giấu tin CPT với ảnh nhị phân.

TH1. Giấu ít thông điệp:chuỗi gồm 10 kí tự



Hình 3.9. Chuỗi thông điệp cần giấu

Hình 3.10. Tập ảnh trước khi giấu



Hình 3.11. Tập ảnh sau khi giấu

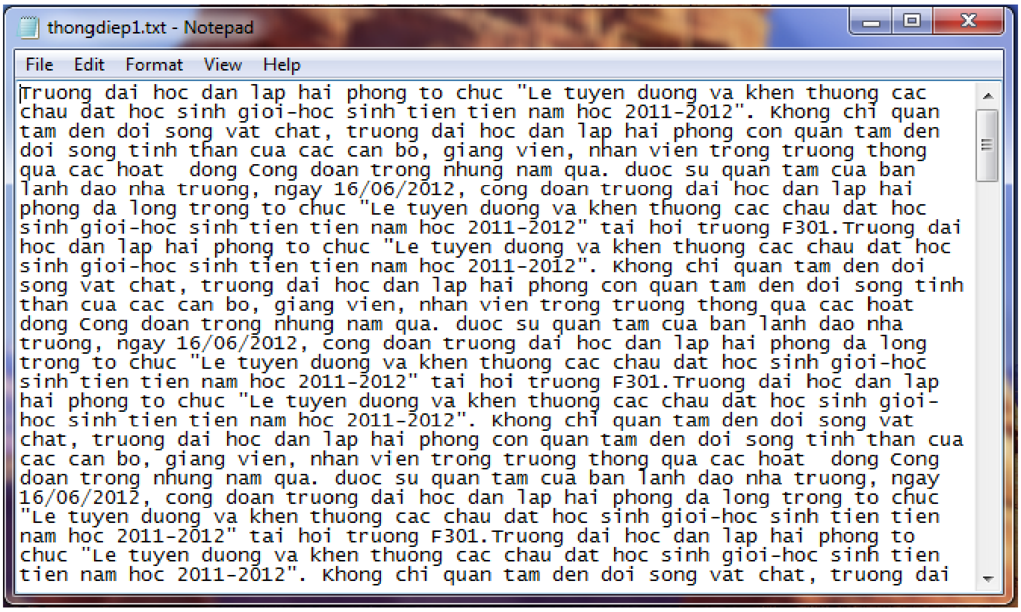
Đánh giá PSNR đơn vị đo là dB

Bảng 3.1. Kết quả đánh giá PSNR trên ảnh nhị phân của kỹ thuật CPT

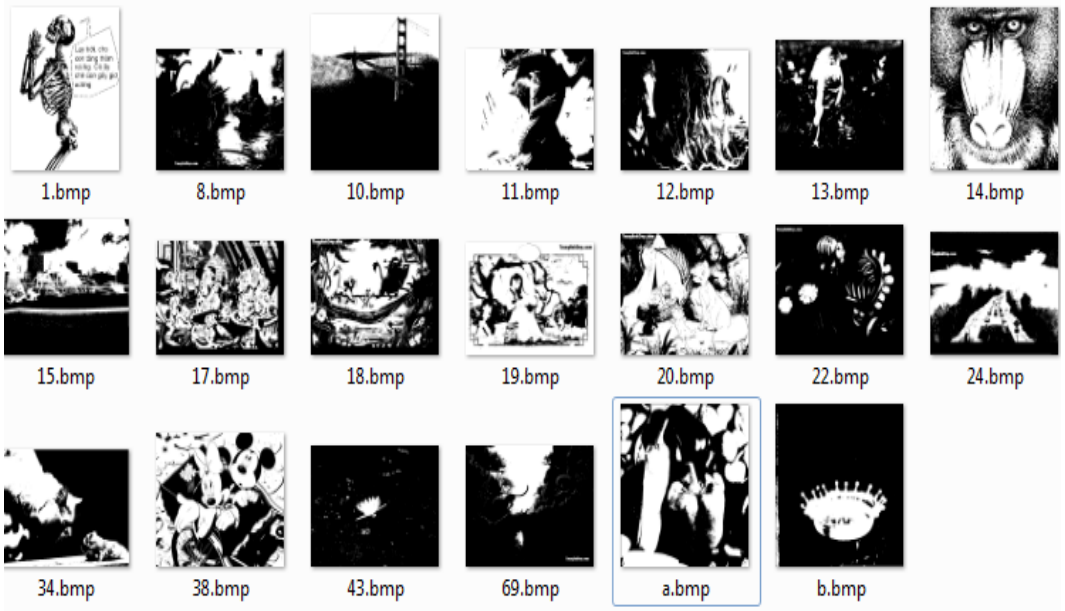
Tên ảnh(kích cỡ ảnh)	**Đánh giá PSNR (dB)**
1.bmp (293x349)	40.3833
8.bmp (700x525)	42.2283
10.bmp (647x619)	42.4087
11.bmp (700x525)	42.0353
12.bmp (700x525)	42.4304
13.bmp (777x624)	43.4318
14.bmp (512x512)	40.7612
15.bmp (746x619)	43.4221
17.bmp (732x510)	41.7414
18.bmp (731x515)	42.5351
19.bmp (700x479)	41.6371
20.bmp (700x525)	42.865

22.bmp (749x603)	43.3258
24.bmp (762x581)	43.0371
34.bmp (700x501)	41.8321
38.bmp (788x647)	43.457
43.bmp (640x480)	41.652
69.bmp (700x525)	42.4304
a.bmp (512x512)	40.7612
b.bmp (512x512)	41.1751
Giá trị trung bình	42.17752

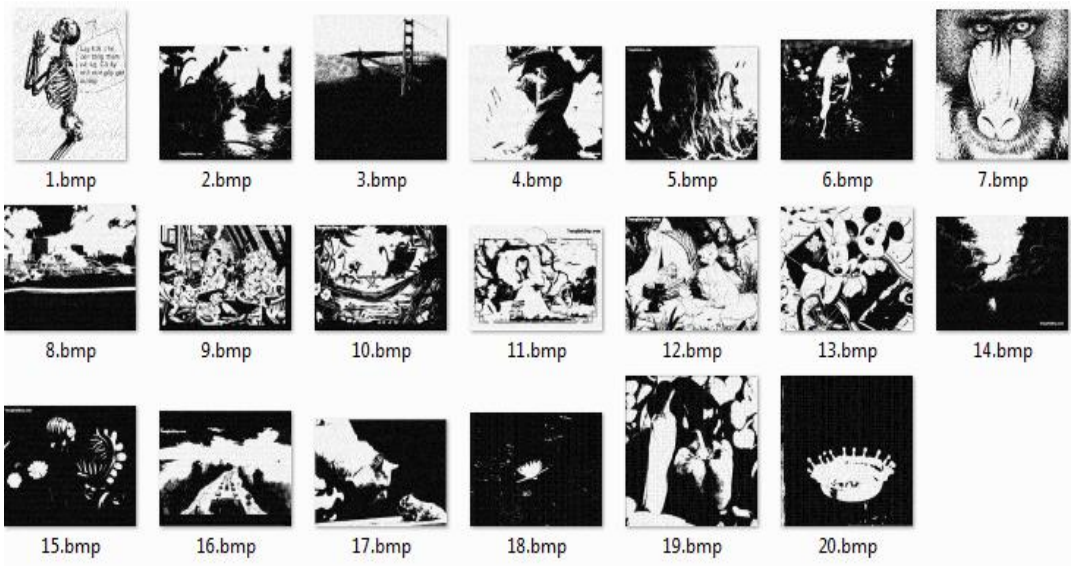
TH2. Giấu nhiều thông điệp: Chuỗi gồm 12004 kí tự



Hình 3.12. Chuỗi thông điệp 12004 ký tự cần giấu



Hình 3.13.Tập ảnh trước khi giấu tin



Hình 3.14. Tập ảnh sau khi giấu tin

Đánh giá PSNR đơn vị đo là dB

Bảng 3.2. Kết quả đánh giá PSNR trên ảnh nhị phân của kỹ thuật CPT

Tên ảnh(kích cỡ ảnh)	**Đánh giá PSNR (dB)**
1.bmp(293x349)	12.7441
8.bmp(700x525)	13.4497

10.bmp(647x619)	13.4916
11.bmp(700x525)	13.5448
12.bmp(700x525)	13.4293
13.bmp(777x624)	13.4113
14.bmp(512x512)	13.2758
15.bmp(746x619)	13.4526
17.bmp(732x510)	13.3116
18.bmp(731x515)	13.4037
19.bmp(700x479)	13.4827
20.bmp(700x525)	13.4215
22.bmp(749x603)	13.457
24.bmp(762x581)	13.501
34.bmp(700x501)	13.4926
38.bmp(788x647)	13.4529
43.bmp(640x480)	13.4688
69.bmp(700x525)	13.4567
a.bmp(512x512)	13.4318
b.bmp(512x512)	13.5084
Giá trị trung bình	13.4094

3.3.2. Nhận xét

Với kết quả thử nghiệm thu được, nếu chuỗi thông điệp nhỏ quan sát bằng mắt thường thì khó có thể phân biệt được ảnh đã giấu và chưa giấu tin, giá trị PSNR trung bình đạt được là khá cao khi giấu tin. Nhưng nếu chuỗi thông điệp lớn giá trị PSNR lại khá thấp, ảnh nhiễu.

Kết quả thử nghiệm trong bảng 3.1, 3.2 cho thấy khả năng giấu tin của mỗi ảnh khác nhau là khác nhau.Những ảnh cùng kích cỡ khả năng giấu của những ảnh đó nằm trong một khoảng giá trị và xấp xỉ bằng nhau.Điều đó chứng tỏ khả năng

giấu phụ thuộc vào giá trị điểm ảnh của ảnh.Một nguyên nhân nữa cũng tác động lớn tới khả năng giấu đó là việc chọn giá trị ma trận khóa K và trọng số W. Vì giá trị điểm ảnh của mỗi ảnh là khác nhau, khả năng giấu của mỗi ảnh được tính liên quan tới K và W nên khi thay đổi giá trị hai ma trận K và W sẽ tạo lên khả năng giấu tin khác nhau.

Thời gian xử lý giấu tin phụ thuộc lớn vào dữ liệu đầu vào như kích thước ảnh gốc, thông điệp giấu lớn hay nhỏ.

Độ an toàn của kỹ thuật cao, phụ thuộc vào giá trị hai ma trận K và W.

Qua thử nghiệm em nhận thấy kỹ thuật giấu tin CPT trong ảnh có những ưu nhược điểm sau:

- Ưu điểm:

  +Khả năng bảo mật cao do ma trận khóa K và trọng số W do người nhận và người gửi biết với nhau. Phải đúng K, W mới có thể lấy được thông tin cần lấy.

  + Độ nhiễu nhỏ, khó phân biệt nếu giấu lượng thông điệp nhỏ.

- Nhược điểm:

  +Phụ thuộc vào ma trận khóa K và trọng số W.

  + Không có bước tính toán khóa giấu tin K và trọng số W để tăng thêm độ an toàn cho dữ liệu.

  + Độ nhiễu của ảnh lớn dễ nhận biết khi dấu lượng bit lớn.

KẾT LUẬN

Kỹ thuật giấu thông tin trong ảnh là hướng nghiên cứu chính của thuật toán giấu thông tin hiện nay và đã đạt được những kết quả khả quan. Đồ án đã trình bày một số khái niệm liên quan đến việc che giấu thông tin trong ảnh số cũng như trình bày kỹ thuật giấu tin CPT trên ảnh nhị phân.

Với kỹ thuật giấu tinCPT trên ảnh nhị phân thì tính vô hình của thông tin sau khi giấu được đảm bảo, thông qua việc sử dụng một ma trận khoá K và một ma trận trọng số W trong quá trình giấu và tách thông tin. Về mặt lý thuyết thì sau khi đã có lượng thông tin được giấu vào trong ảng gốc, nó sẽ để lại dù nhiều, dù ít những dấu vết khác với ảnh gốc ban đầu. Dùngphương pháp đánh giá PSNR để đánh giá chất lượng ảnh trước và sau khi giấu tin kết quả PSNR đạt được là khá cao nếu giấu lượng bit nhỏ, nhưng khá thấp nếu giấu lượng bit lớn. Như vậy kỹ thuật giấu tin CPT đã cho những kết quả không được như mong muốn nếu lượng thông tin cần giấu quá lớn gây nhiễu cho ảnh gốc.

Tuy nhiên, giấu tin mật là vấn đề phức tạp,cộng với khả năng và kinh nghiệm còn hạn chế nên em còn gặp một số khó khăn trong việc tìm hiểu nghiên cứu các kỹ thuật giấu tin CPT trên ảnh nhị phân.

Vì vậy em rất mong nhận được sự đóng góp ý kiến quý báu của các thầy cô giáo cũng như bạn bè để báo của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

[1]. Bùi Thế Hồng (2005); "Về một cải tiến đối với lược đồ giấu dữ liệu an toàn và vô hình trong các bức ảnh hai màu", Tạp chí Tin học và điều khiển học, tập 21, số 4-2005, pp281-292.

[2]. M. Y. Wu and J. H. Lee (1988); "*A Novel Data Embedding Method for Two-Color Facsimile Image*s". In Proceedings of International Symposium on Multimedia Information Processing, Chung-Li, Taiwan, R. O. C, December 1998

[3]. Yu Yuan Chen, Hsiang Kuang Pan and Yu Chee Tseng (2000); "*A Secure Data Hiding Scheme for Two-Color Images*", IEEE Symp. on Computer and Communication.

[4]. Yu Chee Tseng and Hsiang Kuang Pan (2001); "*Secure and Invisible Data Hiding in 2- Color Imag*es", INFORCOM 2001, pp 887-896.

[5]. Phan Trung Huy, Vu Phuong Bac, Nguyen Manh Thang, Truong DucManh, Vu Tien Duc, Nguyen Tuan Nam, "*A New CPT Extension Scheme for High Data EmbeddingRatio in Binary Image*s", the Proceedings of the 1st KSE. Inter. Conf. Hanoi 10/2009. 61-66. IEEE.CS.