BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

------- o0o -------

KỸ THUẬT GIẤU TIN THUẬN NGHỊCH TRONG ẢNH MMPOUA

ĐỒ ÁN TỐT NGHIỆP HỆ ĐẠI HỌC CHÍNH QUY

Ngành: Công nghệ thông tin

Sinh viên thực hiện: Bùi Văn Nhất

Giáo viên hướng dẫn: TS. Hồ Thị Hương Thơm

Mã sinh viên: 121280

HẢI PHÒNG - 2012

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 2012

Sinh viên thực hiện

Bùi Văn Nhất

MỤC LỤC

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 đã tìm hiểu một kỹ thuật giấu tin văn bản trong hình ảnh là kỹ thuật giấu tin thuận nghịch tránh vượt ngưỡng trong ảnh MMPOUA(minimum\maximum preserved overflow\underflow avoid-ance). Đồ án được tổ chức gồm ba chương như 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 thuận nghịch trong ảnh MMPOUA: Giới thiệu và trình bày kỹ thuật giấu và tách tin MMPOUA.

Chương 3. Cài đặt thử nghiệm: Trình bày một số giao diện của chương trình và thử nghiệm kỹ thuật giấu tin thuận nghịch trong ảnh MMPOUA, đưa ra nhận xét đánh giá.

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.

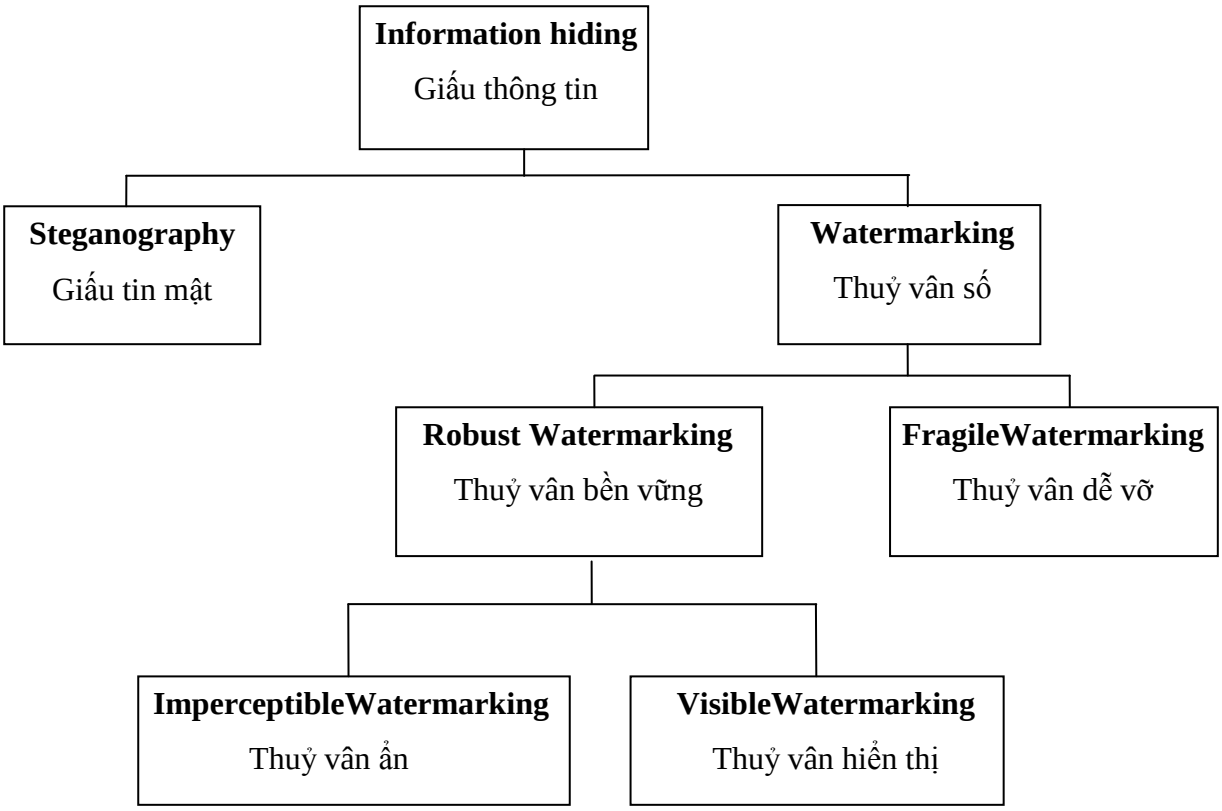
- Ngày nay kỹ thuật giấu tin được nghiên cứu để phục vụ các mục đích tích cực như: bảo vệ bản quyền các tài liệu số hóa (dùng thuỷ vân số), hay giấu các thông tin bí mật về quân sự và kinh tế...

- 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. Sơ đồ phân loại kỹ thuật giấu tin.

- ***Giấu tin mật (Seganograph)*** 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 (Watermaking)*** 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 đối tượng vỏ bọc.
Yêu cầu	- Không phát hiện được thông điệp 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.	- Watermaking 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.

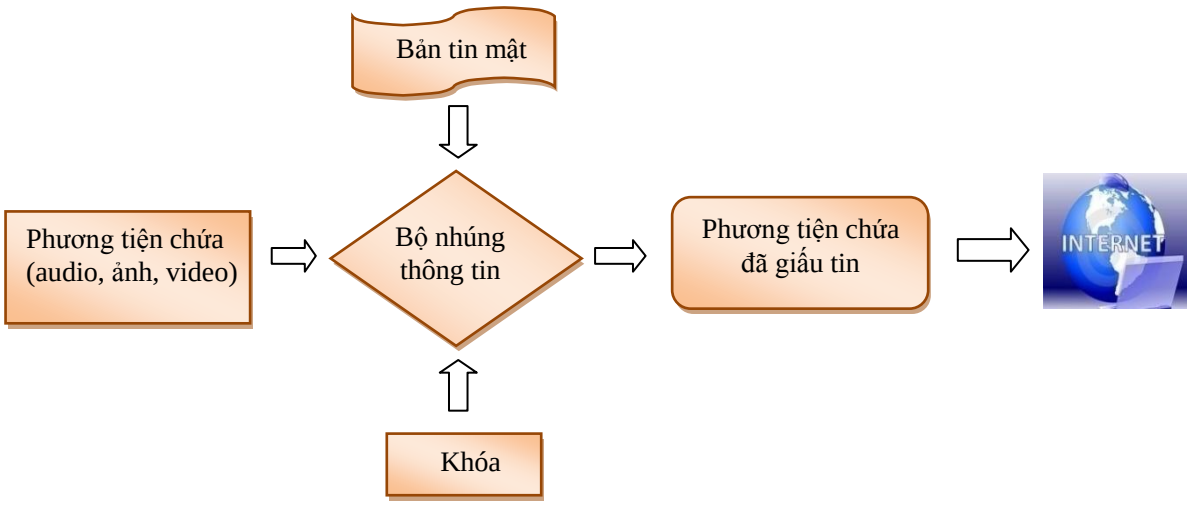
- ***Khả năng không thể dò tìm được:*** là khả năng chống lại việc xác định ảnh đó có hay không có thông tin ẩn bằng các kỹ thuật thống kê toán học thông thường.

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:

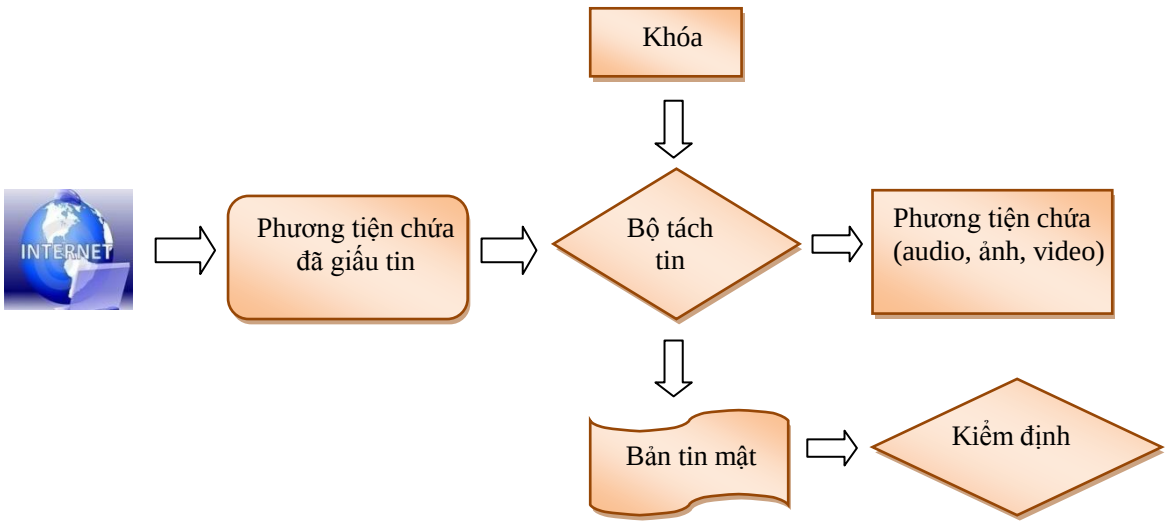
- ***Bản tin mật (Secret Message):*** có thể là văn bản hoặc tệp ảnh hay bất kỳ một tệp nhị phân nào, vì quá trình xử lý đều chuyển chúng thành chuỗi các bit.
- ***Ảnh phủ (hay ảnh gốc) (Cover Data):*** là ảnh được dùng để làm môi trường nhúng tin mật.
- ***Khoá bí mật K (Key):*** khoá viết mật tham 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 thuật giấu thông tin trong ảnh phụ thuộc vào hệ thống thị giác của con người – HSV (Human Vision System) còn kỹ thuật giấu thông tin trong audio lại 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 với âm 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 theo bảng 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.

1.3. 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 vị đo 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 K là ảnh gốc và ảnh được khôi phục tương ứng:

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

PSNR được định nghĩa bởi:

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

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.

Chương 2. KỸ THUẬT GIẤU TIN THUẬN NGHỊCH TRONG ẢNH MMPOUA

2.1. Giới thiệu

Giới thiệu: Kỹ thuật giấu tin thuận nghịch tránh vượt ngưỡng được Ching-Yu Yang và Wu-Chih Hu đề xuất vào tháng 8 năm 2011.

Ý tưởngcủa kỹ thuật giấu tin:

Ý tưởng của kỹ thuật giấu tin thuận nghịch tránh vượt ngưỡng được mô tả như sau:

- Bước đầu là chia nhỏ ma trận điểm ảnh thành các ma trận nhỏ có kích cỡ 3x3. Xác định những điểm ảnh nhỏ nhất (hoặc lớn nhất) trong ma trận nhỏ 3x3 và cố định chúng, những điểm ảnh này có tác dụng giữ cố định khối ma trận và ngăn ngừa sự cố vượt ngưỡng.
- Sau đó tiến hành giảm hay thay đổi giá trị điểm ảnh bằng cách trừ giá trị các điểm ảnh còn lại cho điểm ảnh có giá trị nhỏ nhất (hoặc lớn nhất) rồi nén điểm ảnh và cô lập những điểm ảnh thỏa mãn (theo yêu cầu thuật toán). Chuỗi bit thông điệp sẽ được giấu vào những điểm ảnh đã giảm hay thay đổi giá trị, trừ những điểm ảnh cô lập và những điểm ảnh có giá trị lớn nhất hoặc nhỏ nhất.

2.2. Kỹ thuật giấu tin thuận nghịch trong ảnh MMPOUA

Kỹ thuật giấu tin thuận nghịch tránh vượt ngưỡng gồm thuật toán bảo toàn nhỏ nhất và bảo toàn lớn nhất. Hai thuật toán này triển khai kỹ thuật giấu tin cơ bản là giống nhau. Tuy nhiên, thuật toán bảo toàn lớn nhất thay thế thuật toán bảo toàn nhỏ nhất dưới điều kiện: thuật toán bảo toàn nhỏ nhất không đủ khả năng điều khiển giấu tin thuận nghịch tránh vượt ngưỡng.

2.2.1. Thuật toán bảo toàn nhỏ nhất(Minimun Preserved Algorithm)

2.2.1.1. Thuật toán giấu tin:

- ***Đầu vào:*** Ảnh C có kích thước nxn. Chuỗi bit thông điệp cần giấu b_s, hai ngưỡng β, γ và hệ số k.

- ***Đầu ra:*** Ảnh C đã giấu tin.

- ***Các bước thực hiện:***

  + Bước một: Tách nhỏ ma trận điểm ảnh thành các ma trận nhỏ kích cỡ 3x3. Xác định điểm ảnh có giá trị nhỏ nhất trong ma trận nhỏ, giả sử điểm ảnh đó có giá trị P_{min}. Cố định điểm ảnh có giá trị P_{min} và trừ giá trị các điểm ảnh còn lại cho P_{min} theo công thức: $\{\hat{P}_{ij}\} = \{P_{ij}\} - P_{min}$.

  + Bước hai: Giá trị điểm ảnh $\hat{P}_{ij}$ sẽ thay đổi giá trị mới $\tilde{P}_{ij} = \hat{P}_{ij} - \gamma$ nếu $\hat{P}_{ij} > \gamma$, những điểm ảnh có giá trị được thay đổi được đánh cờ tương ứng theo bản đồ điểm ảnh với $B_{ij} = 1$, ngược lại sang bước ba.

  + Bước ba: Tiến hành cô lập những điểm ảnh thỏa mãn $\hat{P}_{ij} \geq \beta$ theo công thức: $\widetilde{P_{ij}} = \hat{P}_{ij} + (2^k - 1) * \beta$ với $\hat{P}_{ij} \in \{\hat{P}_{ij}, \widetilde{P_{ij}}\}$.

  + Bước bốn: Giấu chuỗi bit dữ liệu b_s vào những điểm ảnh đã giảm (hoặc đã thay đổi) c_r, sao cho thỏa mãn $0 \leq c_r < \beta$, nhân c_r với 2^k được $\widehat{c_r}$. Sau đó cộng bít b_s vào $\widehat{c_r}$, cuối cùng cộng P_{min} với $\widehat{c_r}$ và $\hat{P}_{ij}$ theo công thức: $\widehat{c_r} = \widehat{c_r} + P_{min}$, $\hat{P}_{ij} = \hat{P}_{ij} + P_{min}$. Quá trình được lặp lại cho tới khi giấu hết các bit thông điệp.

2.2.1.2. Thuật toán tách tin:

- ***Đầu vào:*** Ảnh mang tin D có kích cỡ nxn. Hai ngưỡng β, γ và hệ số k.

- ***Đầu ra:*** Chuỗi bit thông điệp và ảnh gốc.

- ***Các bước thực hiện:***

  + Bước một: Tách nhỏ ma trận điểm ảnh thành các ma trận nhỏ kích cỡ 3x3. Xác định điểm ảnh có giá trị nhỏ nhất trong ma trận nhỏ,

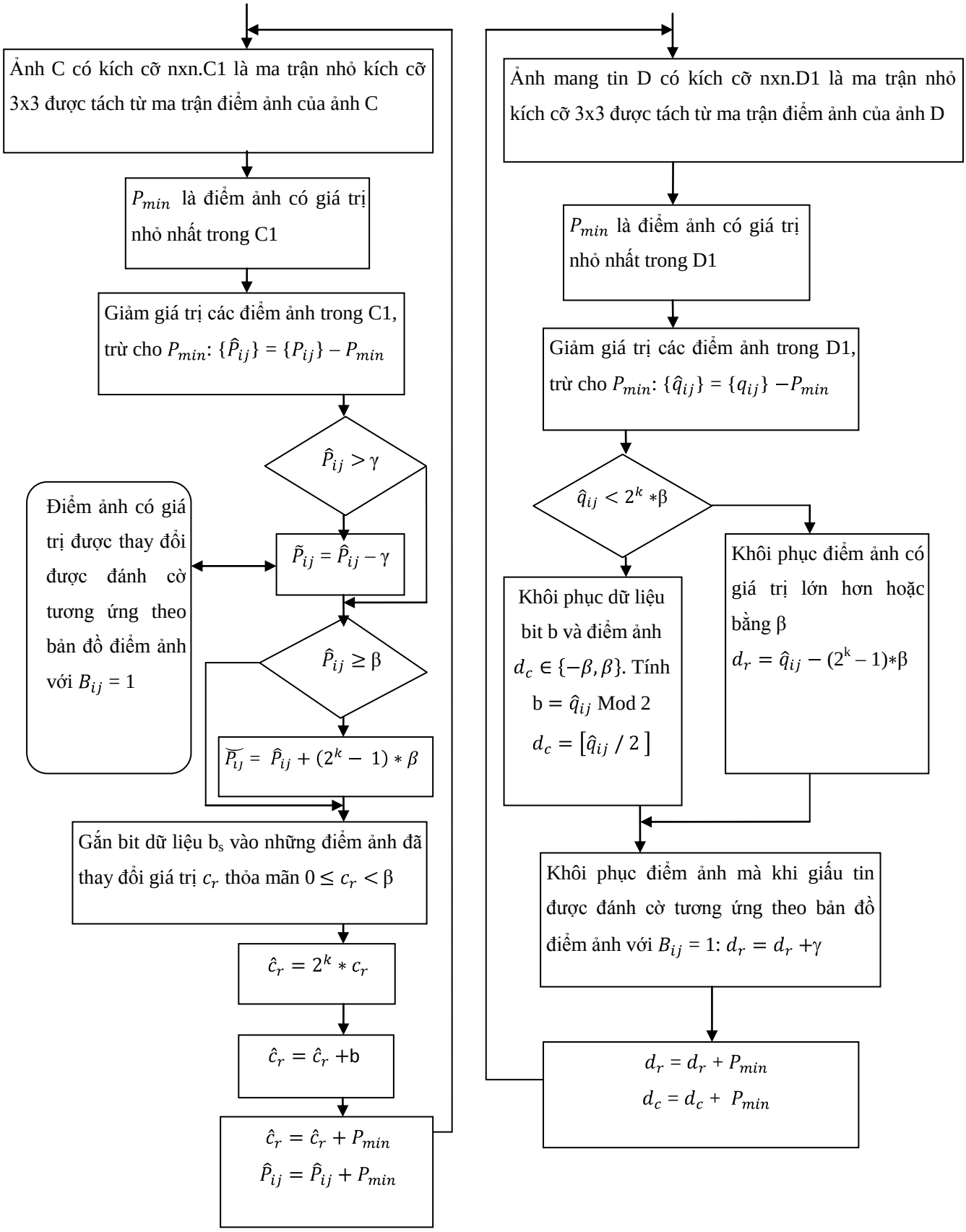
giả sử điểm ảnh đó có giá trị P_{min}. Cố định điểm ảnh có giá trị P_{min} và trừ giá trị các điểm ảnh còn lại cho P_{min} theo công thức: $\{\hat{q}_{ij}\} = \{q_{ij}\} - P_{min}$.

+ Bước hai: Khôi phục bit thông điệp b và những điểm ảnh $d_c \in \{-\beta, \beta\}$. Tính $b = \hat{q}_{ij} \text{ Mod } 2$ và $d_c = \lfloor \hat{q}_{ij} / 2 \rfloor$ nếu $\hat{q}_{ij} < 2^k * \beta$. Ngược lại khôi phục những điểm ảnh có giá trị lớn hơn hoặc bằng β theo công thức sau: $d_r = \hat{q}_{ij} - (2k - 1) * \beta$.

+ Bước ba: Khôi phục lại những điểm ảnh khi giấu tin được đánh cờ tương ứng theo bản đồ điểm ảnh với $B_{ij} = 1$ theo công thức: $d_r = d_r + \gamma$.

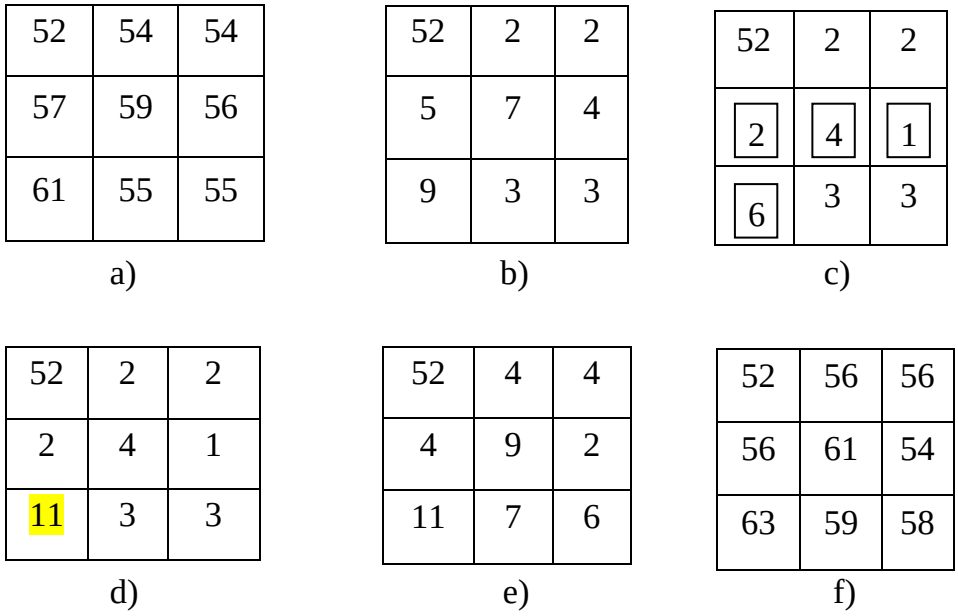
+ Bước bốn: Cộng P_{min} vào d_r và d_c theo công thức: $d_r = d_r + P_{min}$, $d_c = d_c + P_{min}$. Quá trình xử lý dừng lại cho tới khi tách hết các bit thông điệp.

2.2.1.3. Lưu đồ giấu tin và tách tin



Hình 2.1. Lược đồ tiến trình thuật toán bảo toàn nhỏ nhất. Trái: Bộ giấu tin. Phải: Bộ tách tin.

2.2.1.4. Ví dụ minh họa



Hình 2.2. Ví dụ giấu bit thông điệp sử dụng thuật toán bảo toàn nhỏ nhất.

Hình 2.2 mô tả ví dụ sử dụng thuật toán bảo toàn nhỏ nhất để giấu tin với chuỗi bit thông điệp là: 0001010. Hình 2.2 (a) ma trận gốc 3x3, hình 2.2 (b) ma trận được thay đổi, hình 2.2 (c) ma trận bị nén, hình 2.2 (d) ma trận bị cô lập, hình 2.2 (e) ma trận đã giấu bit, hình 2.2 (f) ma trận giấu tin. Hệ số k được sử dụng ở đây là 1, β và γ có giá trị theo thứ tự là 5 và 3. Hình 2.1 (a) minh họa ma trận gốc có kích cỡ 3x3. Hình 2.1 (b) mô tả việc giảm giá trị điểm ảnh của ma trận bằng cách trừ giá trị điểm ảnh trong hình 2.1 (a) cho điểm ảnh có giá trị nhỏ nhất của ma trận là 52. Hình nhữ nhật bao quanh những điểm ảnh trong hình 2.1 (c) là cờ đánh giấu sự thay đổi giá trị của điểm ảnh, thỏa mãn điều kiện giá trị điểm ảnh đó lớn hơn 3 và được đặt giá trị là 1 tương ứng trong bản đồ điểm ảnh. Hình2.1 (d) mô tả điểm ảnh bị cô lập nếu lơn hơn hoặc bằng 5 bằng cách lấy giá trị điểm ảnh đó cộng với $(2^k - 1) * \beta$. Hình 2.1 (e) mô tả ma trận đã được giấu bit. Cuối cùng, hình 2.1 (f) mô tả ma trận giấu tin bằng cách cộng giá trị của điểm ảnh nhỏ nhất tới các điểm ảnh trong ma trận trừ điểm ảnh có giá trị nhỏ nhất trong hình 2.1 (e).

2.2.2. Thuật toán bảo toàn lớn nhất(Maximun Preserved Algorithm)

Quá trình giấu tin với thuật toán bảo toàn lớn nhất cơ bản cũng tương tự như thuật toán bảo toàn nhỏ nhất.

2.2.2.1 Thuật toán giấu tin:

- ***Đầu vào:*** Ảnh C có kích thước nxn. Chuỗi bit thông điệp cần giấu b_s, hai ngưỡng β, γ và hệ số k.
- ***Đầu ra:*** Ảnh C đã giấu tin.
- ***Các bước thực hiện:***

  + Bước một: Tách nhỏ ma trận điểm ảnh thành các ma trận nhỏ kích cỡ 3x3. Xác định điểm ảnh có giá trị lớn nhất trong ma trận nhỏ, giả sử điểm ảnh đó có giá trị P_{max}. Cố định điểm ảnh có giá trị P_{max} và trừ giá trị các điểm ảnh còn lại cho P_{max} theo công thức: $\{\widehat{P}_{ij}\} = \{P_{ij}\} - P_{max}$.

  + Bước hai: Giá trị điểm ảnh $\widehat{P}_{ij}$ sẽ thay đổi giá trị mới $\widetilde{P}_{ij} = \widehat{P}_{ij} + \gamma$ nếu $\widehat{P}_{ij} < -\gamma$, những điểm ảnh có giá trị được thay đổi được đánh cờ tương ứng theo bản đồ điểm ảnh với $B_{ij} = 1$, ngược lại sang bước ba.

  + Bước ba: Tiến hành cô lập những điểm ảnh thỏa mãn $\widehat{P}_{ij} \leq -\beta$ theo công thức: $\widetilde{P}_{ij} = \widehat{P}_{ij} - (2^k - 1) * \beta$ với $\widehat{P}_{ij} \in \{\widehat{P}_{ij}, \widetilde{P}_{ij}\}$.

  + Bước bốn: Giấu chuỗi bit dữ liệu b_s vào những điểm ảnh đã giảm (hoặc đã thay đổi) c_1, sao cho nó thỏa mãn $-\beta \leq c_1 < 0$, nhân c_1 với 2^k được $\hat{c}_1$. Sau đó trừ bít b_s cho $\hat{c}_1$, cuối cùng cộng P_{max} với $\hat{c}_1$ và $\hat{P}_{ij}$ theo công thức: $\widehat{c_1} = \widehat{c_1} + P_{max}$, $\hat{P}_{ij} = \hat{P}_{ij} + P_{max}$. Quá trình được lặp lại cho tới khi giấu hết các bit thông điệp.

2.2.2.2. Thuật toán tách tin:

- ***Đầu vào:*** Ảnh mang tin D có kích cỡ nxn. Hai ngưỡng β, γ và hệ số k.

- ***Đầu ra:*** Chuỗi bit thông điệp và ảnh gốc.

- ***Các bước thực hiện:***

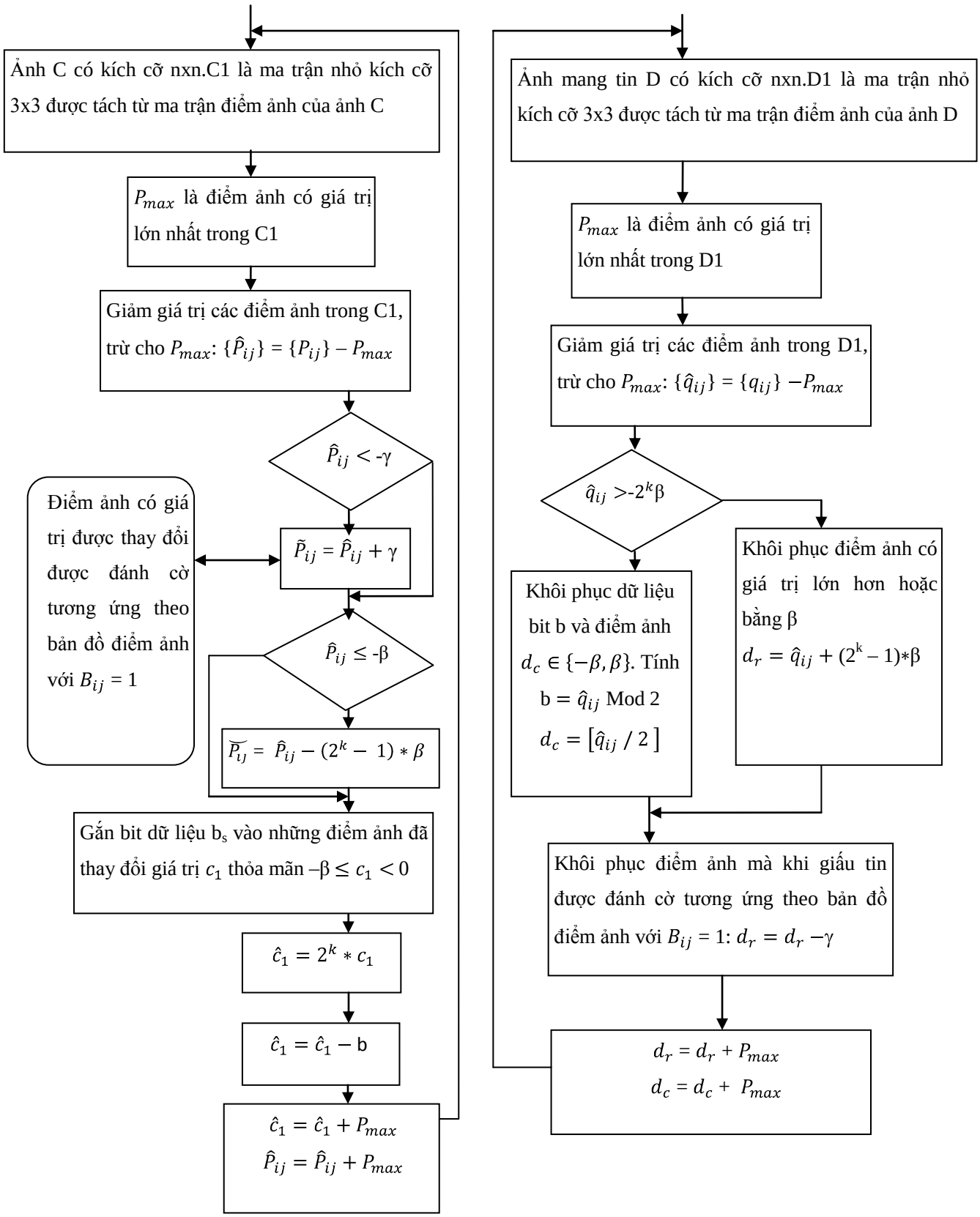
+ Bước một: Tách nhỏ ma trận điểm ảnh thành các ma trận nhỏ kích cỡ 3x3. Xác định điểm ảnh có giá trị nhỏ nhất trong ma trận nhỏ, giả sử điểm ảnh đó có giá trị P_{max}. Cố định điểm ảnh có giá trị P_{max} và trừ giá trị các điểm ảnh còn lại cho P_{max} theo công thức: $\{\hat{q}_{ij}\} = \{q_{ij}\} - P_{max}$.

+ Bước hai: Khôi phục dữ liệu bit b và những điểm ảnh d_c thỏa mãn điều kiện $d_c \in \{-\beta, \beta\}$. Tính $b = \hat{q}_{ij}$ Mod 2 và $d_c = \lceil \hat{q}_{ij} / 2 \rceil$ nếu thỏa mãn $\hat{q}_{ij} > -2^k * \beta$. Ngược lại khôi phục những điểm ảnh có giá trị lớn hơn hoặc bằng β theo công thức: $d_r = \hat{q}_{ij} + (2k - 1) * \beta$.

+ Bước ba: Khôi phục lại những điểm ảnh khi giấu tin được đánh cờ tương ứng theo bản đồ điểm ảnh với $B_{ij} = 1$ theo công thức: $d_r = d_r - \gamma$.

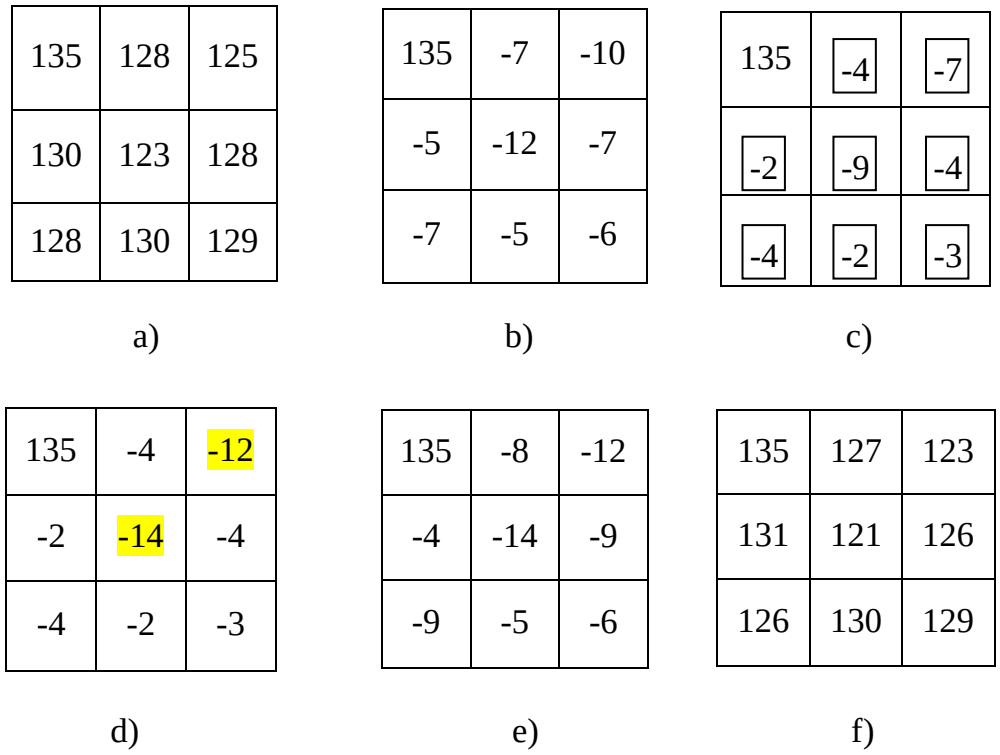
+ Bước bốn: Cộng P_{max} vào d_r và d_c: $d_r = d_r + P_{max}, d_c = d_c + P_{max}$. Quá trình xử lý cho tới khi tách hết các bit thông điệp.

2.2.2.3 Lưu đồ giấu và tách tin



Hình 2.3. Lược đồ tiến trình thuật toán bảo toàn lớn nhất. Trái: Bộ giấu tin. Phải: Bộ tách tin.

2.2.2.4. Ví dụ minh họa



Hình 2.4. Ví dụ giấu bit thông điệp sử dụng thuật toán bảo toàn lớn nhất.

Hình 2.4 mô tả ví dụ sử dụng thuật toán bảo toàn lớn nhất để giấu tin với chuỗi bit thông điệp là: 0001010. Hình 2.4 (a) ma trận gốc 3x3, hình 2.4 (b) ma trận được thay đổi, hình 2.4 (c) ma trận bị nén, hình 2.4 (d) ma trận bị cô lập, hình 2.4 (e) ma trận đã giấu bit, hình 2.4 (f) ma trận giấu tin. Hệ số k được sử dụng ở đây là 1, β và γ có giá trị theo thứ tự là 5 và 3. Hình 2.4 (a) minh họa ma trận gốc có kích cỡ 3x3. Hình 2.4 (b) mô tả việc giảm giá trị điểm ảnh của ma trận bằng cách trừ giá trị điểm ảnh trong hình 2.4 (a) cho điểm ảnh có giá trị lớn nhất của ma trận là 135. Hình nhữ nhật bao quanh những điểm ảnh trong hình 2.4 (c) là cờ đánh giấu sự thay đổi giá trị của điểm ảnh, thỏa mãn điều kiện giá trị điểm ảnh đó nhỏ hơn -3 và được đặt giá trị là 1 tương ứng trong bản đồ điểm ảnh. Hình 2.4 (d) mô tả điểm ảnh bị cô lập nếu nhỏ hơn hoặc bằng -5 bằng cách lấy giá trị điểm ảnh đó trừ cho $(2^k - 1) * \beta$. Hình 2.4 (e) mô tả ma trận đã được giấu bit. Cuối cùng, hình 2.4 (f) mô tả ma trận giấu tin bằng cách cộng giá

trị của điểm ảnh nhỏ nhất tới các điểm ảnh trong ma trận trừ điểm ảnh có giá trị nhỏ nhất trong hình 2.4 (e).

2.3. Vấn đề vượt ngưỡng

Thông thường, khi đặt hệ số k =1, tức là phép chia modulo-2 được sử dụng trong thuật toán bảo toàn nhỏ nhất hoặc bảo toàn lớn nhất. Khi đó kỹ thuật giấu tin thuận nghịch có thể tránh được sự cố vượt ngưỡng. Tuy nhiên nếu có một điểm ảnh trong ma trận có giá trị bằng 255 hoặc 0, sự cố vượt ngưỡng có thể xảy ra khi đang giấu bit. Để khắc phục vấn đề này, kỹ thuật giấu tin có sử dụng 2 ngưỡng là ϕ_1 và ϕ_2. Nếu một điểm ảnh trong ma trận có giá trị lớn hơn ϕ_1, thì khi đó thuật toán bảo toàn nhỏ nhất được dùng để cô lập điểm ảnh đó. Điểm ảnh được cô lập không tham gia giấu bit, mà có tác dụng tránh vượt ngưỡng nhằm hạn chế độ nhiễu của ảnh sau khi giấu tin. Nếu nhiều hơn một điểm ảnh cô lập sẽ đánh dấu chỉ số các điểm đó trong ma trận. Ngược lại, nếu một điểm ảnh trong ma trận có giá trị nhỏ hơn ϕ_2, khi đó thuật toán bảo toàn lớn nhất sẽ được dùng để cô lập điểm ảnh đó.

Trong kỹ thuật giấu tin, chi phí sử dụng trong quá trình ép điểm ảnh không có điểm ảnh cô lập là: $[\frac{M}{n}]$ x $[\frac{N}{n}]$ x $n^2 \leq$ M x N bit. Khi có điểm ảnh cô lập thì chi phí thêm B_S x N_b bit, B_S và N_b là số điểm ảnh cô lập và số bit, tương ứng với chỉ số mỗi điểm ảnh cô lập trong ma trận. Cụ thể, B_S với độ dài 15 bit đủ để đánh chỉ số điểm ảnh cô lập trong ma trận có kích cỡ nxn vì: $[\frac{M}{n}]$ x $[\frac{N}{n}] < 2^{15}$ nếu $n \geq 3$. Kết quả, chi phí bit dùng trong kỹ thuật giấu tin có điểm ảnh cô lập là: $([\frac{M}{n}]$ x $[\frac{N}{n}]$ x $n^2)$ + (B_N x N_b). Tuy nhiên, khi $B_S > \frac{1}{N_b}[\frac{M}{n}]$ x $[\frac{N}{n}]$, những điểm ảnh cô lập trong ma trận áp dụng cách giải quyết trên không khả thi. Trong trường hợp này, thay vì sử dụng B_S và N_b, kỹ thuật sẽ đánh giấu chỉ số $[\frac{M}{n}]$ x $[\frac{N}{n}]$ những điểm ảnh cô lập trong ma trận tương ứng một vị trí trong ma trận. Tổng số chi phí sử dụng là:

$$([\frac{M}{n}] \text{ x } [\frac{N}{n}] \text{ x } n^2) + ([\frac{M}{n}] \text{ x } [\frac{N}{n}]) = (1 + \frac{1}{n2}) \text{ x } [\frac{M}{n}] \text{ x } [\frac{N}{n}] \text{ bit.}$$

Chương 3. CÀI ĐẶT VÀ THỬ NGHIỆM

3.1. Môi trường cài đặt

- Ngôn ngữ cài đặt: Ngôn ngữ lập trình Matlab phiên bản 7.0.

- Môi trường soạn thảo: Matlab phiên bản 7.0.

- Môi trường chạy chương trình: Môi trường giao diện Matlab phiên bản 7.0.

- Cấu hình tối thiểu để cài đặt Matlab phiên bản 7.0.

  + Bộ vi xử lý Pentium hoặc Pentium Pro.

  + Windows 95 hoặc NT.

  + Dung lượng ổ cứng từ 25Mb cho tới hơn 1Gb.

  + Bộ nhớ Ram tối thiểu 128Mb.

3.2. Giao diện chương trình

Kỹ thuật giấu tin thuận nghịch trong ảnh MMPOUA triển khai trên hai thuật toán bảo toàn nhỏ nhất và bảo toàn lớn nhất. Về bản chất hai thuật toán cơ bản giống nhau về cách xử lý giấu tin nên bày một thuật toán bảo toàn lớn nhất.

3.2.1. Giao diện chính chương trình

Hình 3.1. Giao diện chính chương trình

Đầu vào:

- Ảnh gốc C có kích thước m $_x$ n.
- Chuỗi thông điệp cần giấu.
- Hai ngưỡng β, γ và hệ số k.

Đầu ra:

- Ảnh C đã giấu tin.

Chức năng chính của chương trình:

Giấu tin:

- Giấu tin trên hai thuật toán: Hoặc bảo toàn nhỏ nhất hoặc bảo toàn lớn nhất.
- Giấu chuỗi ký tự: Giấu một chuỗi thông điệp bất kỳ do người dùng nhập vào từ bàn phím.
- Giấu tệp văn bản: Cho phép người dùng chọn một tệp văn bản dạng file *. txt để giấu vào ảnh.

Tách tin:

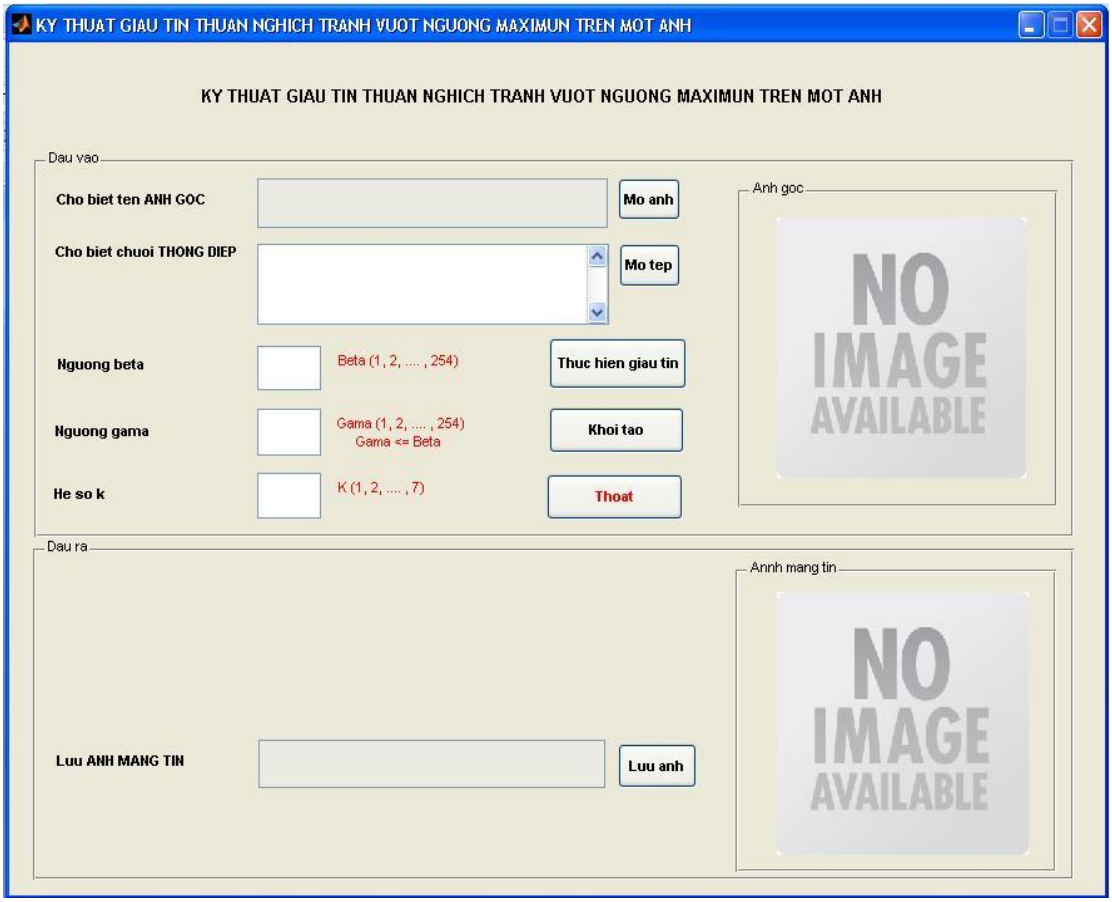
- Tách tin trên hai thuật toán: hoặc bảo toàn nhỏ nhất hoặc bảo toàn lớn nhất tùy theo ảnh đã giấu là giấu theo thuật toán bảo toàn nhỏ nhất hoặc bảo toàn lớn nhất.
- Tách chuỗi thông điệp nhúng từ ảnh đã giấu và lưu ra dạng file *. txt.

3.2.2. Giao diện chi tiết các modul chương trình

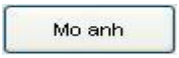
3.2.2.1. Giao diện chức năng giấu tin

Từ giao diện chính của chương trình ta chọn menu “Giau tin” và chọn chức năng “Giau theo cuc dai”.

Giao diện của chức năng “Giau theo cuc dai”.



Hình 3.2. Giao diện giấu tin theo thuật toán bảo toàn lớn nhất.

Nhập các giá trị đầu vào để xử lý giấu tin. Bước đầu, chọn ảnh nhúng tin (Cho biet ten ANH GOC) ta chọn nút 

. Khi đó chương trình sẽ mở ra hộp thoại tìm kiếm ảnh, ảnh được chọn là "baboon.png".

Hình 3.3. Hộp thoại chọn ảnh.

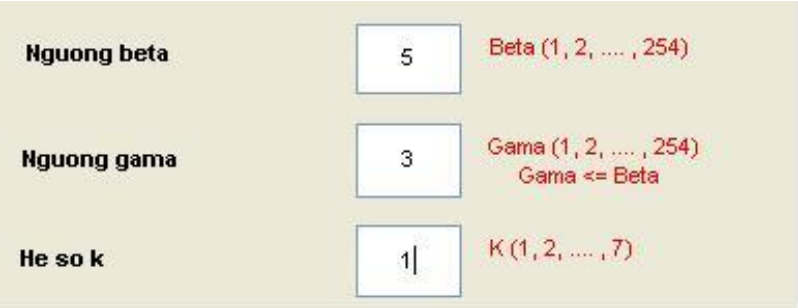
Tiếp theo nhập thông điệp cần giấu vào ảnh. Hoặc ta sẽ nhập trực tiếp thông điệp từ bàn phím vào ô "Cho biet chuoi THONG DIEP":

Hình 3.4. Nhập thông điệp vào ô "Cho biet chuoi THONG DIEP".

Hoặc ta sẽ chọn tệp văn bản định dạng *. txt có sẵn để giấu bằng cách chọn nút Mo tep, khi đó chương trình sẽ mở ra hộp thoại tìm kiếm tệp, tệp được chọn là "nhat. txt".

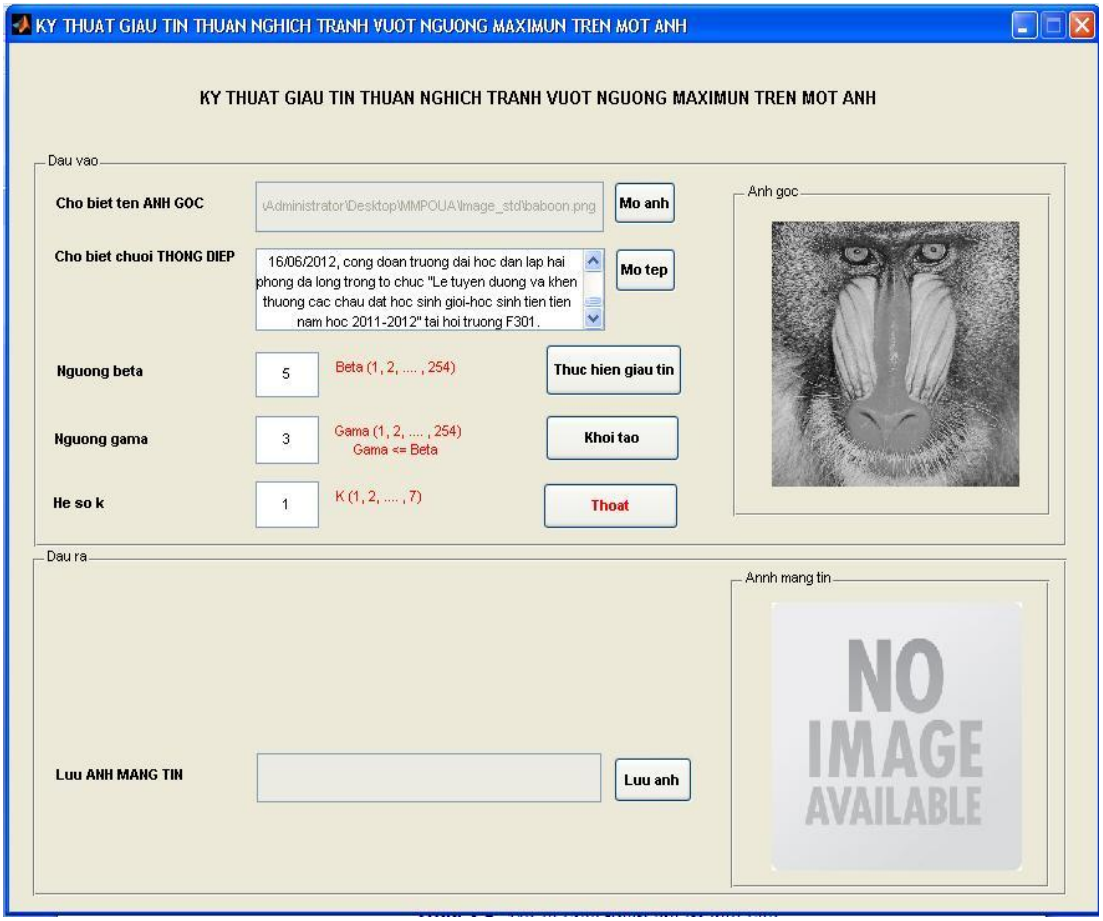
Hình 3.5. Hộp thoại chọn tệp văn bản.

Kế tiếp nhập giá trị hai ngưỡng beta, gama và hệ số k, giá trị càng nhỏ khả năng điều khiển giấu tin tránh vượt ngưỡng và chất lượng ảnh mang tin càng cao. Ví dụ nhập giá trị như hình 3.6.



Hình 3.6. Nhập giá trị hai ngưỡng beta, gama và hệ số k.

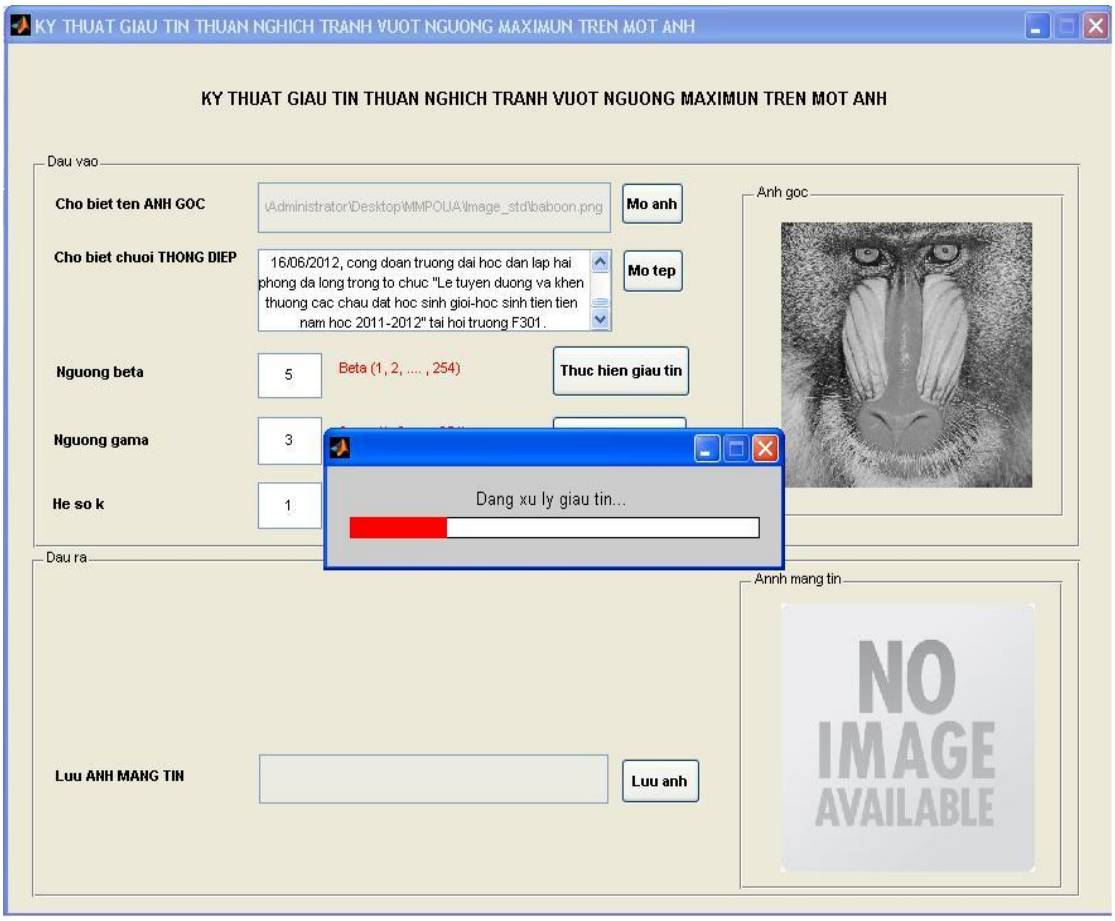
Sau khi nhập xong giá trị đầu vào cho quá trình xử lý giấu tin sẽ được kết quả như hình 3.7.



Hình 3.7. Mô tả việc nhập giá trị đầu vào.

Bước tiếp theo chọn nút 

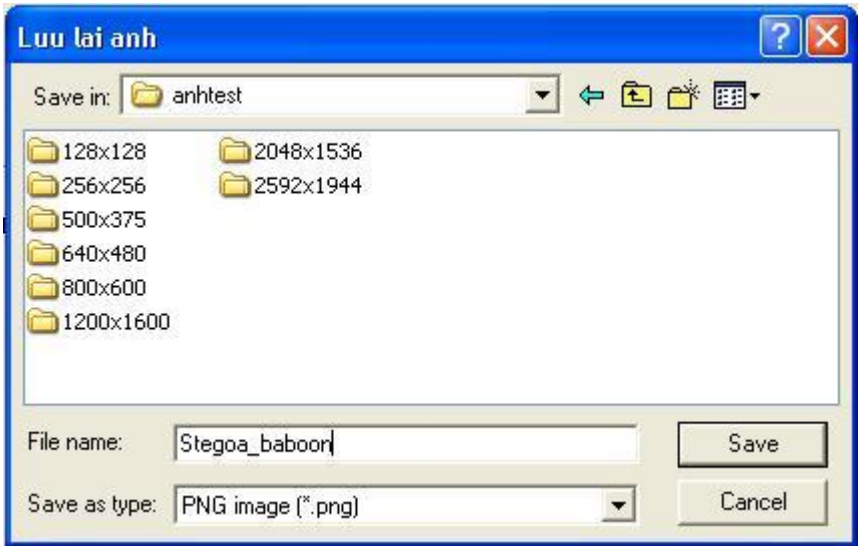
để xử lý giấu tin, hình 3.8 mô tả quá trình xử lý giấu tin.



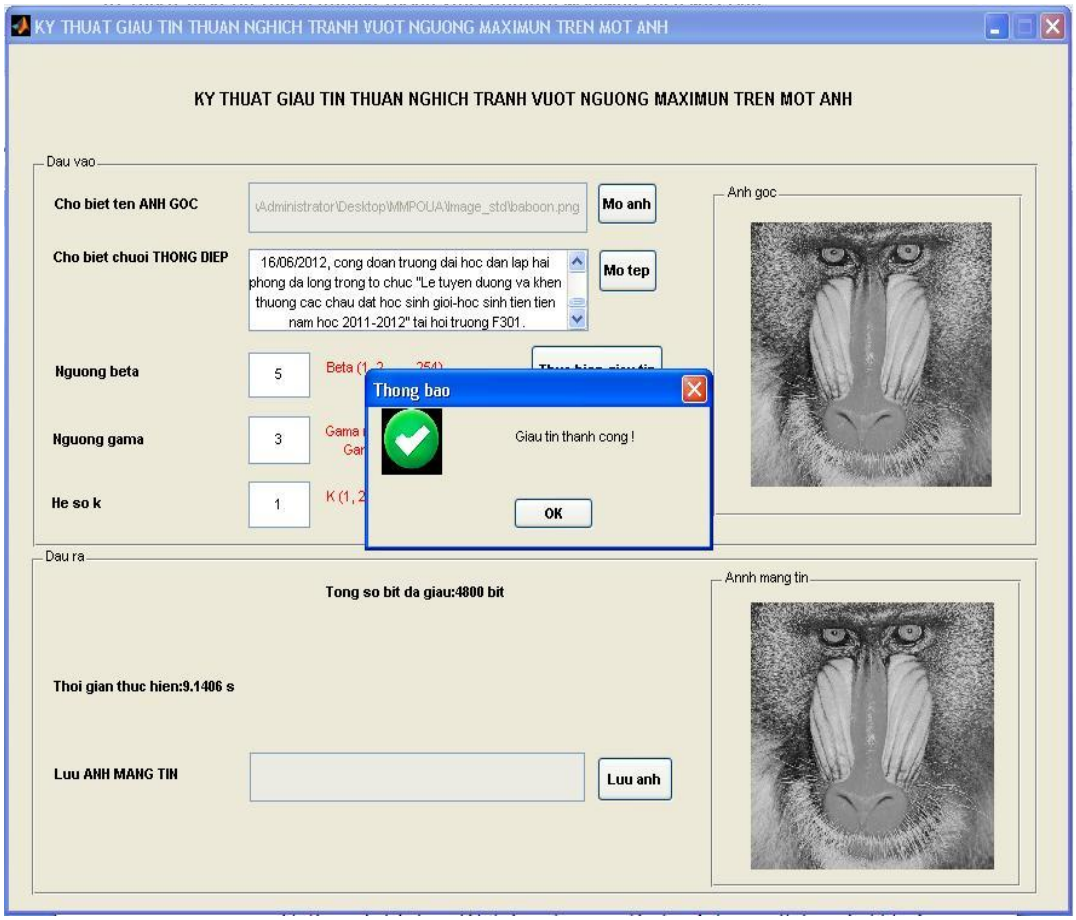
Hình 3.8. Quá trình xử lý giấu tin.

Quá trình xử lý giấu tin kết thúc sẽ có hộp thoại thông báo đã giấu tin thành công như hình 3.10. Sau khi giấu tin thành công chọn nút 

để lưu lại ảnh mang tin. Khi đó một hộp thoại như hình 3.9 được mở ra, chọn đường dẫn, điền tên ảnh cần lưu và chọn "Save" để hoàn tất việc lưu ảnh mang tin.



Hình 3.9. Hộp thoại lưu ảnh.



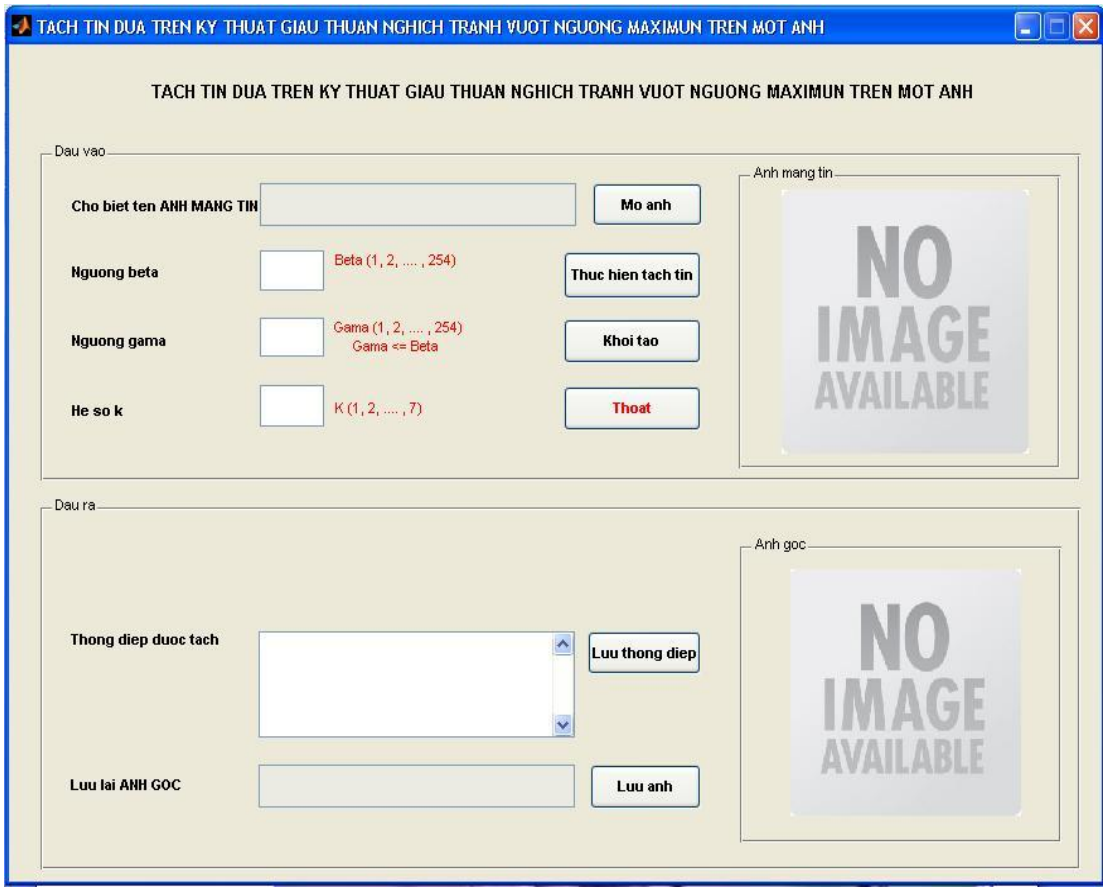
Hình 3.10. Giao diện giấu tin thành công.

Để khởi tạo lại giá trị mới để xử lý giấu tin cho lần sau như hình 3.2 ta chọn nút Khoi tao. Muốn thoát giao diện giấu tin ta chọn nút Thoat.

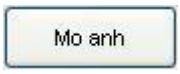
3.2.2.2. Giao diện chức năng tách tin

Từ giao diện chính của chương trình ta chọn menu "Tach tin" và chọn chức năng "Tach theo cuc dai".

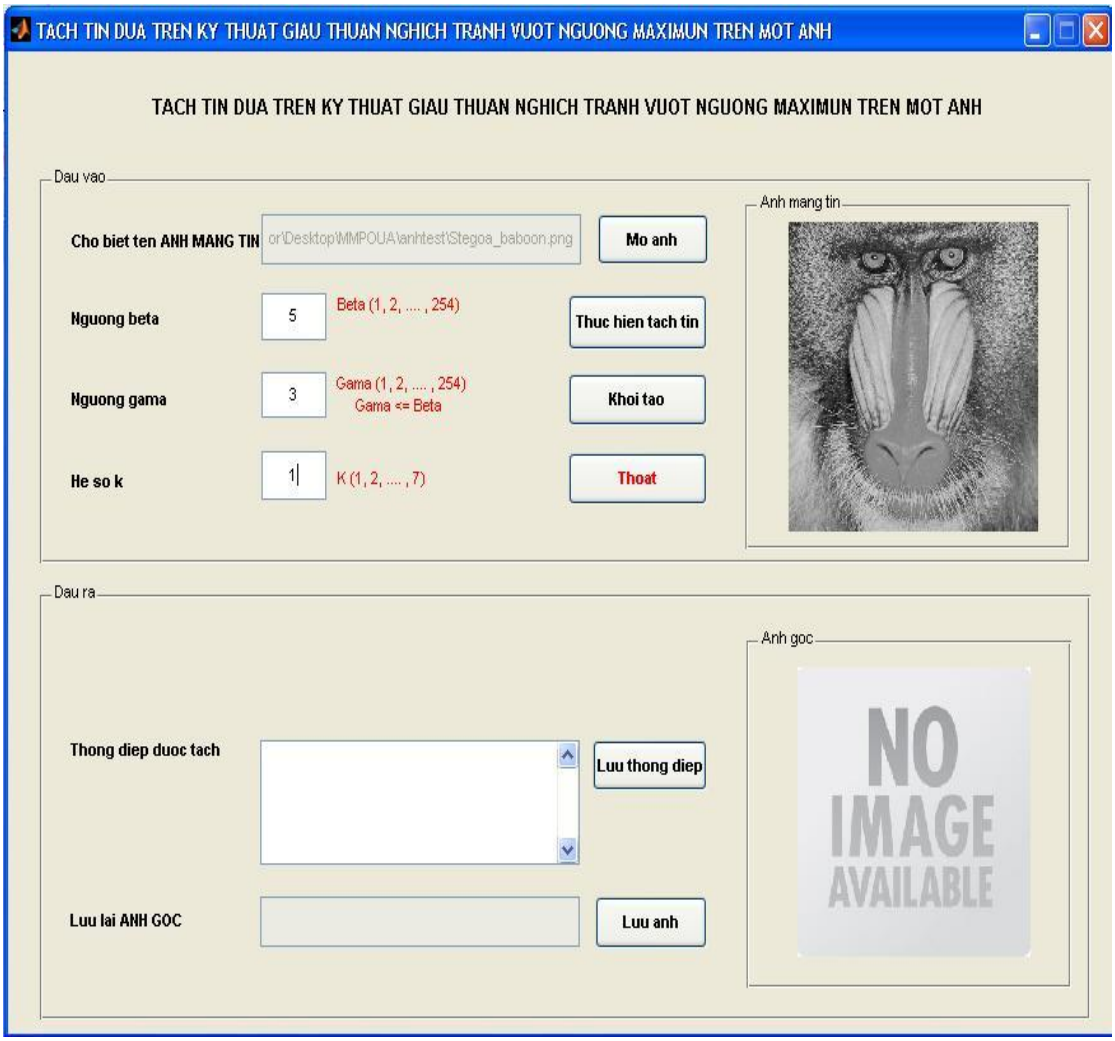
Giao diện của chức năng "Tach theo cuc dai".



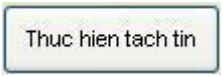
Hình 3.11. Giao diện chức năng tách tin theo cực đại.

Nhập các giá trị đầu vào để tách tin. Bước đầu chọn ảnh cần tách tin (Cho biet ten ANH MANG TIN) ta chọn nút 

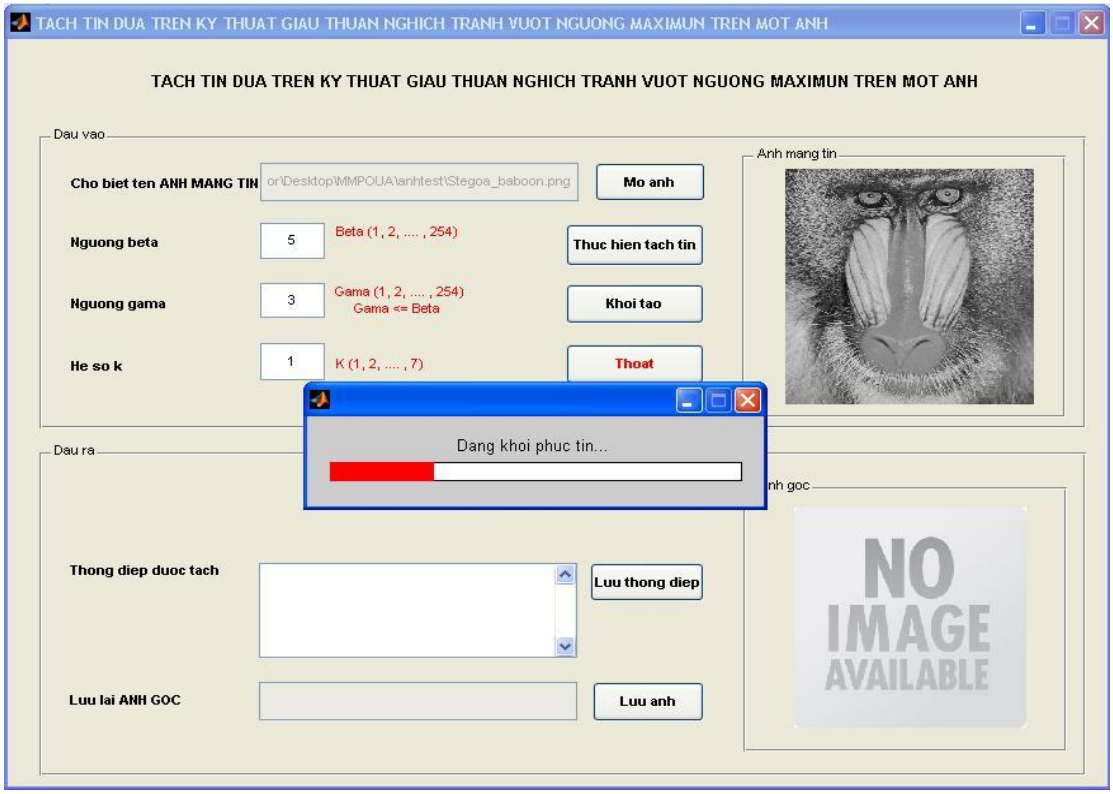
. Khi đó chương trình sẽ mở ra hộp thoại tìm kiếm ảnh như hình 3.3, ảnh chọn là "Stegoa_baboon.png". Kế tiếp nhập giá trị hai ngưỡng beta, gama và hệ số k như hình 3.6. Sau khi nhập xong giá trị đầu vào cho quá trình xử lý giấu tin sẽ được kết quả như hình 3.12.



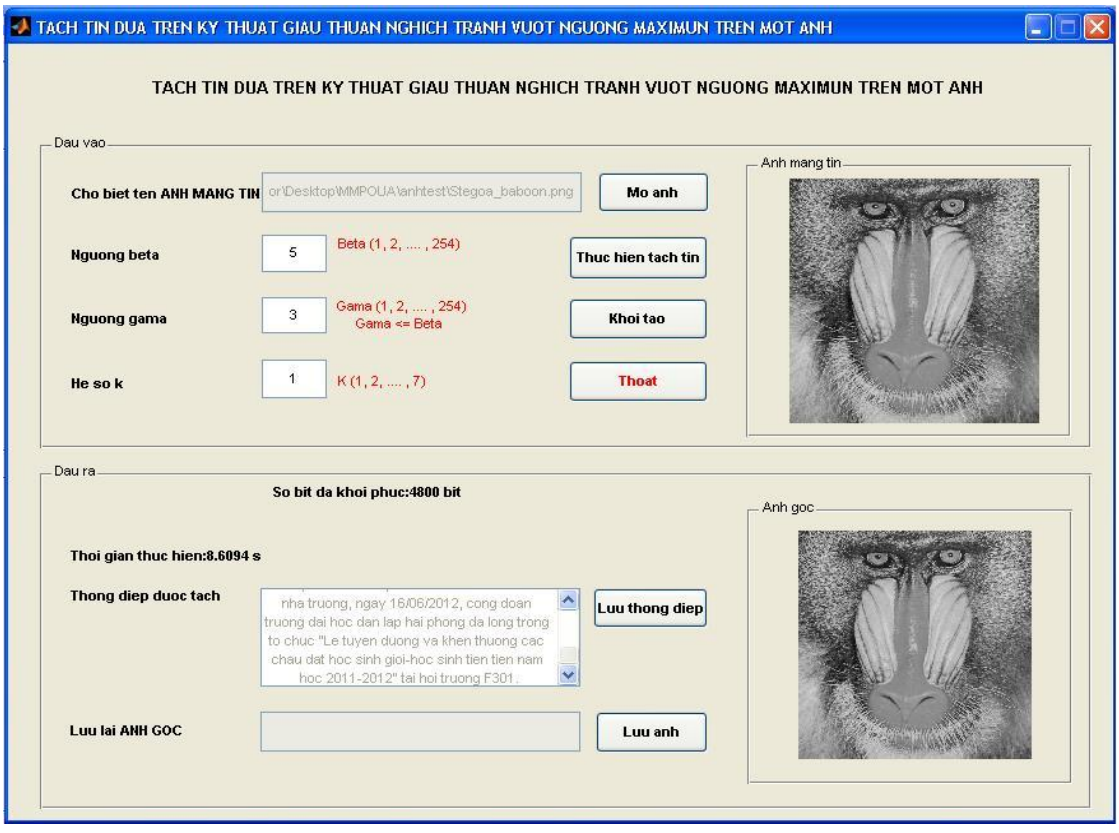
Hình 3.12. Mô tả việc nhập giá trị đầu vào.

Bước tiếp theo chọn nút 

để xử lý tách tin, hình 3.13 mô tả quá trình xử lý tách tin.

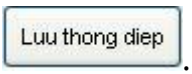


Hình 3.13. Giao diện xử lý tách tin.



Hình 3.14. Giao diện xử lý tách tin thành công.

Quá trình tách tin thành công, thông điệp sẽ hiển thị trong ô "Thong diep duoc tach".

Muốn lưu lại thông được được tách ta chọn nút 

. Khi đó xuất hiện một hộp thoại lưu tệp, nhập tên và chọn "Save". Lưu thông điệp thành công sẽ hiện một hộp thoại thông báo.

Hình 3.15. Hộp thoại thông báo lưu thành công.

Trường hợp muốn lưu lại ảnh gốc ta chọn nút 

và thao tác tương tự như lưu thông điệp được tách. Để khởi tạo lại giá trị mới để xử lý giấu tin cho lần sau như hình 3.11 chọn nút 

. Muốn thoát giao diện giấu tin chọn nút 

.

3.2.3. Giao diện cửa sổ thông tin

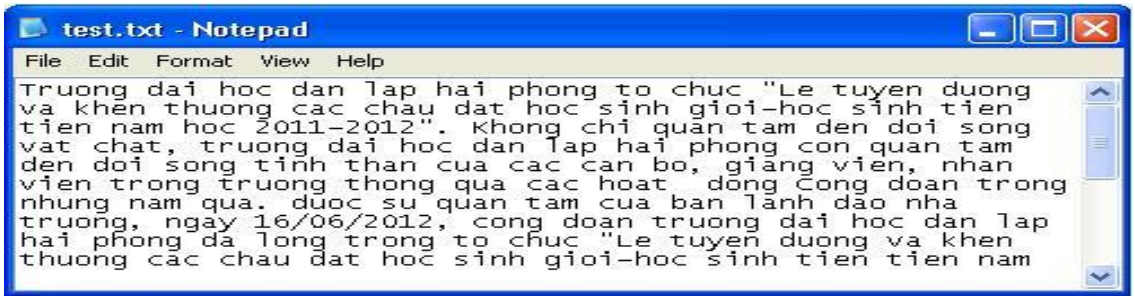
Hình 3.16. Giao diện thông tin sinh viên thực hiện.

3.3. Kết quả thử nghiệm và nhận xét

3.3.1. Kết quả thử nghiệm

Thực nghiệm này sẽ đưa ra khả năng giấu tin khi sử dụng kỹ thuật giấu tin thuận nghịch tránh vượt ngưỡng trong ảnh MMPOUA và độ đánh giá PSNR với ảnh trước và sau giấu tin. Tập ảnh thử nghiệm là ảnh định dạng *.png gồm tập A1 là 9 ảnh cấp xám chuẩn định dạng png có kích thước 512x512. Và tập ảnh A2 là 36 ảnh có ngẫu nhiên gồm ảnh chụp và ảnh tải về trên mạng có kích thước khác nhau được đặt tên từ Image1 tới Image36 được chuyển thành cảnh cấp xám thông qua phần mềm Adobe photoshop CS3.

Chuỗi thông điệp giấu có 9240 bit:



Hình 3.17. Chuỗi thông điệp giấu.

Tập ảnh xám chuẩn A1 trước khi giấu tin:

Hình 3.18. Tập ảnh xám chuẩn A1 trước khi giấu tin.

Tập ảnh xám chuẩn A1 sau khi giấu tin bằng thuật toán bảo toàn lớn nhất:

Hình 3.19. Tập ảnh xám chuẩn A1 sau khi giấu tin.

Tập ảnh xám chuẩn A2 trước khi giấu tin:

Hình 3.20. Tập ảnh xám ngẫu nhiên A2 trước khi giấu tin.

Tập ảnh xám ngẫu nhiên A2 sau khi giấu tin bằng thuật toán bảo toàn lớn nhất:

Hình 3.21. Tập ảnh xám ngẫu nhiên A2 trước khi giấu tin.

Trong thực nghiệm này sử dụng giá trị ngưỡng $\beta = 5$, $\gamma = 3$ và hệ số $k = 1$. Đánh giá PSNR đơn vị đo bằng dB, khả năng giấu đơn vị đo là bit.

Bảng 3.1. Kết quả đánh giá PSNR và khả năng giấu với hai tập ảnh A1 và A2 sử dụng thuật toán bảo toàn lớn nhất và nhỏ nhất.

Tên ảnh (kích cỡ ảnh)	**Sử dụng thuật toán bảo toàn lớn nhất**		**Sử dụng thuật toán bảo toàn nhỏ nhất**	
	Đánh giá PSNR (dB)	**Khả năng giấu (bit)**	**Đánh giá PSNR (dB)**	**Khả năng giấu (bit)**
airplane.png (512 x 512)	53.99	144717	53.8894	140474
baboon.png (512 x 512)	46.7825	50235	46.7647	51277
beer.png (512 x 512)	54.3765	178639	54.6403	179213
elaine.png (512 x 512)	52.721	85327	52.7329	81575
house.png (512 x 512)	54.4775	105467	54.2281	103629
lena.png (512 x 512)	55.2491	140322	55.297	145186
peppers.png (512 x 512)	52.8509	120863	52.6632	120679
sailboat.png (512 x 512)	52.3198	87418	52.4316	92110
tiffany.png (512 x 512)	54.9631	132182	54.9566	130995
Image1.png (1024 x 768)	58.7282	314269	58.4561	309654

Image2.png (305 x 406)	51.0903	70287	X	70771
Image3.png (550 x 413)	53.3572	112179	X	113909
Image4.png (2592 x 1944)	68.4353	3233644	X	3247726
Image5.png (2592 x 1944)	67.7075	2693429	X	2695355
Image6.png (2592 x 1944)	66.1241	2641114	X	2657808
Image7.png (800 x 600)	58.8705	218852	58.906	222398
Image8.png (800 x 600)	57.6615	230387	X	234342
Image9.png (320 x 240)	47.929	31901	X	32037
Image10.png (600 x 480)	55.6333	143714	55.6529	144774
Image11.png (800 x 600)	59.5373	148360	59.582	149396
Image12.png (700 x 700)	57.5005	79941	X	71229
Image13.png (640 x 480)	56.5842	154257	56.6429	154508
Image14.png (469 x 735)	51.7607	61867	X	63923
Image15.png (516 x 384)	53.2632	60342	53.3075	66034
Image16.png (794 x 595)	58.0319	304362	58.0896	306210
Image17.png (540 x 405)	54.1839	89395	54.1491	92820
Image18.png (500 x 394)	55.048	97788	54.9725	98078
Image19.png (600 x 374)	53.5541	86788	53.3481	89383
Image20.png (540 x 405)	54.3891	76096	54.4664	77092
Image21.png (500 x 305)	49.844	47217	50.0856	52280
Image22.png (630 x 374)	55.3679	150577	55.3562	151191
Image23.png (800 x 480)	55.8296	109158	X	116277

Image24.png (660 x 412)	55.5062	153766	55.4922	153082
Image25.png (540 x 337)	53.2715	86606	53.5537	87945
Image26.png (500 x 281)	52.9375	62395	52.9752	61556
Image27.png (442 x 295)	50.1211	46195	X	49001
Image28.png (700 x 438)	58.4609	134488	58.5468	136744
Image29.png (700 x 438)	56.3752	180426	56.4895	179457
Image30.png (400 x 300)	51.9868	55799	52.0131	58062
Image31.png (405 x 304)	47.5426	45491	X	45720
Image32.png (225 x 225)	47.6903	18145	X	17200
Image33.png (720 x 540)	57.9593	165700	57.9137	175154
Image34.png (700 x 525)	59.3081	125166	X	128087
Image35.png (604 x 453)	55.6691	82699	55.5984	89182
Image36.png (1024 x 640)	61.8115	257094	61.7652	258964
Giá trị trung bình	**55.2623**	**302557**	**54.9989**	**304500**

Chú thích:

X: Giấu tin xảy ra vượt ngưỡng.

3.3.2. Nhận xét

Với kết quả thử nghiệm thu được, nếu quan sát bằng mắt thường thì khó có thể phân biệt được đâu là ảnh đã giấu tin và chưa giấu tin. Giá trị PSNR trung bình đạt được là khá cao khi giấu lượng bit thông điệp tương đối lớn 9240 bit so với thang đo giá trị trung bình PSNR là 35dB, khi sử dụng thuật toán bảo toàn lớn nhất giá trị PSNR đạt 55.2623, thuật toán bảo toàn nhỏ nhất giá trị PSNR đạt

54.9989. Khả năng giấu trên hai tập ảnh A1 và A2 khá lớn, đạt trung bình 302557 bit với thuật toán bảo toàn lớn nhất, 304500 với thuật toán bảo toàn nhỏ nhất.

Thuật toán bảo toàn lớn nhất và thuật toán bảo toàn nhỏ nhất đều đạt giá trị PSNR và khả năng giấu tương đương nhau. Điểm khác biệt, thuật toán bảo toàn lớn nhất điều khiển giấu tin tránh vượt ngưỡng tốt hơn thuật toán bảo toàn nhỏ nhất.

Kết quả thử nghiệm trong bảng 3.1 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 hai ngưỡng β, γ. Vì giá trị điểm ảnh của mỗi ảnh là khác nhau, khả năng giấu của mỗi ảnh được tính liên quan tới giá trị hai ngưỡng β, γ nên khi thay đổi giá trị hai ngưỡng β, γ sẽ tạo lên khả năng giấu tin khác nhau.

Mối quan hệ giữa hai ngưỡng β, γ là $|\beta| \geq |\gamma| > 0$. Trong đó miền giá trị của ngưỡng β: $1 \leq |\beta| < 254$, từ miền giá trị của ngưỡng β ta có miền giá trị của ngưỡng γ: $1 \leq |\gamma| < 254$. Nếu hai ngưỡng β, γ nằm trong miền giá trị trên thì thuật toán cho kết quả tốt và tối ưu đúng với bản chất thuật toán. Tuy nhiên vẫn có thể chọn giá trị ngưỡng β, γ lớn hơn 255, khi đó chương trình vẫn triển khai giấu tin nhưng không đảm bảo đúng bản chất của thuật toán. Khi giá trị β và γ lớn hơn 255, trong tính toán giấu tin sẽ không có điểm ảnh giảm (hay thay đổi), không có điểm ảnh cô lập để chọn lựa điểm ảnh giấu tin tối ưu, dẫn tới khó kiểm soát tràn ngưỡng, ảnh mang tin có độ nhiễu cao, nói cách khác giá trị PSNR đạt được thấp. Hệ số k sử dụng trong thuật toán giúp điều khiển vượt ngưỡng và tăng độ an toàn cho thuật toán, miền giá trị của k: $1 \leq |k| \leq 7$. Thông thường, giá trị của k = 1 hoặc k = 2 kỹ thuật giấu tin thuận nghịch có thể tránh vượt ngưỡng tốt nhất. Giá trị k=6, k=7 khó điều khiển vượt ngưỡng, chỉ dùng cho một số trưởng hợp ma trận điểm ảnh có giá trị đặc biệt. Giá trị ngưỡng β, γ và hệ số k

càng nhỏ khả năng điều khiển tránh vượt ngưỡng, chất lượng ảnh mang tin càng cao.

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 ngưỡng β, γ và hệ số k. Cụ thể, độ an toàn khi tách tin phụ thuộc vào giá trị: $2^k * \beta$.

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

- Ưu điểm:
  + Kỹ thuật giấu tin đạt giá trị PSNR khá cao nên độ nhiễu của ảnh mang tin tương đối thấp.
  + Khả năng giấu tin tốt.
  + Khắc phục được vấn đề vượt ngưỡng.
- Nhược điểm:
  + Phụ thuộc vào hai ngưỡng β, γ và hệ số k.
  + Không có bước tính toán khóa giấu tin để tăng thêm độ an toàn cho dữ liệu.

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 thuận nghịch trong ảnh MMPOUA.

Với kỹ thuật giấu tin thuận nghịch trong ảnh MMPOUA thì tính vô hình của thông tin sau khi giấu được đảm bảo, thông qua việc chọn hai ngưỡng β, γ và hệ số k phù hợp để những biến đổi không gây ra sự chú ý đáng kể nào. 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. Tuy nhiên sau khi thực hiện kỹ thuật giấu tin, quan sát bằng mắt thường thì khó có thể phân biệt đâu là ảnh gốc đâu là ảnh mang tin. Dùng phương pháp đánh giá PSNR để đánh giá chất lượng ảnh trước và sau khi giấu tin kết quả PSNR đạt được là khá cao, điều đó cho thấy sự biến dạng của ảnh hầu như không có. Như vậy kỹ thuật giấu tin đã cho những kết quả rất triển vọng.

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 thuận nghịch trong ảnh MMPOUA.

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]. Nguyễn Xuân Huy, Trần Quốc Dũng, *Giáo trình giấu tin và thuỷ vân ảnh*, Trung tâm thông tin tư liệu, TTKHTN - CN 2003

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

[3]. Ching-Yu Yang and Wu-Chih Hu, *High-Performance Reversible Data Hiding with Overflow/Underflow Avoidance*, ETRI Journal, Volume 33, Number 4, August 2011.

Một số đồ án tốt nghiệp ngành CNTT từ khóa 7 đến khóa 11 liên quan đến kỹ thuật giấu tin và phát hiện ảnh có giấu tin:

[4]. Dương Uông Hiên_lớp CT701, *"Nghiên cứu kỹ thuật giấu tin mật trên vùng biến đổi DWT"*, tiểu án tốt nghiệp ngành CNTT – 2008.

[5]. Ngô Minh Long – Lớp CT701, *"Phát hiện ảnh có giấu tin trên Bit ít ý nghĩa nhất LSB"*, tiểu án tốt nghiệp ngành CNTT – 2008.

[6]. Đỗ Trọng Phú – CT702, *"Nghiên cứu kỹ thuật giấu tin trên miềm biến đổi DFT"*, tiểu án tốt nghiệp ngành CNTT – 2008.

[7]. Hoàng Thị Huyền Trang – CT802, *"Nghiên cứu kỹ thuật phát hiện ảnh giấu tin trên miền biến đổi của ảnh"*, đồ án tốt nghiệp ngành CNTT – 2008.

[8]. - Nguyễn Thị Kim Cúc – CT801, *"Nghiên cứu một số phương pháp bảo mật thông tin trước khi giấu tin trong ảnh"*, đồ án tốt nghiệp ngành CNTT – 2008.

[9]. *Vũ Tuấn Hoàng* – CT801, "*Nghiên cứu kỹ thuật phát hiện ảnh có giấu tin dựa trên LSB của ảnh cấp xám*", đồ án tốt nghiệp ngành CNTT – 2008.

[10]. Vũ Thị Hồng Phương – CT801, *"Nghiên cứu kỹ thuật giấu tin trong ảnh gif"*, đồ án tốt nghiệp ngành CNTT – 2008.

[11]. Đỗ Thị Nguyệt – CT901, "*Nghiên cứu một số kỹ thuật ước lượng độ dài thông điệp giấu trên bit có trọng số thấp*", đồ án tốt nghiệp ngành CNTT – 2009.

[12]. Mạc như Hiển – CT901, *"Nghiên cứu kỹ thuật giấu thông tin trong ảnh GIF"*, đồ án tốt nghiệp ngành CNTT – 2009.

[13]. Phạm Thị Quỳnh – CT901, *"Nghiên cứu kỹ thuật phát hiện thông tin ẩn giấu trong ảnh JPEG2000"*, đồ án tốt nghiệp ngành CNTT – 2009.

[14]. Phạm Thị Thu Trang – CT901, *"Nghiên cứu kỹ thuật giấu thông tin trong ảnh JPEG2000"*, đồ án tốt nghiệp ngành CNTT – 2009.

[15]. Trịnh Thị Thu Hà – CT901, *"NGHIÊN CỨU KỸ THUẬT PHÁT HIỆN THÔNG TIN ẨN GIẤU TRONG ẢNH GIF "*, đồ án tốt nghiệp ngành CNTT – 2009.

[15]. Vũ Trọng Hùng – CT801, *"Kỹ thuật giấu tin thuận nghịch dựa trên miền dữ liệu ảnh"*, tiểu án tốt nghiệp ngành CNTT – 2009.

[16]. Đỗ Lâm Hoàng – CT1001, *"Nghiên cứu kỹ thuật giấu tin thuận nghịch trên miền dữ liệu ảnh cấp xám"*, đồ án tốt nghiệp ngành CNTT – 2010.

[17]. Nguyễn trường Huy- CT1001, *"Nghiên cứu kỹ thuật giấu tin trên ảnh nhị phân"*, đồ án tốt nghiệp ngành CNTT – 2010.

[18]. Vũ Văn Thành- CT1001, *" Tìm hiểu giải pháp và công nghệ xác thực điện tử sử dụng thủy vân số"*, đồ án tốt nghiệp ngành CNTT – 2010.

[19]. Vũ Văn Tập – CT1001, *"Nghiên cứu kỹ thuật phát hiện ảnh có giấu tin trên miền dữ liệu của ảnh"*, đồ án tốt nghiệp ngành CNTT – 2010.

[20]. Vũ Khắc Quyết – ct1001, *"Nghiên cứu kỹ thuật giấu tin với dung lượng thông điệp lớn"***,** đồ án tốt nghiệp ngành CNTT – 2010.

[21]. Phạm Quang Tùng – CT1001, *"Tìm hiểu kỹ thuật phát hiện ảnh có giấu tin dựa trên phân tích tương quan giữa các bit LSB của ảnh"*, đồ án tốt nghiệp ngành CNTT – 2010.

[22]. Vũ Thị Ngọc – CT1101, *"Nghiên cứu một giải pháp giấu văn bản trong ảnh"*.

[23]. Cao Thị Nhung – CT1101, *"Tìm hiểu kỹ thuật thủy vân số thuận nghịch cho ảnh nhị phân"*, đồ án tốt nghiệp ngành CNTT – 2011.

[24]. Hoàng Thị Thuy Dung – CT1101, *"Kỹ thuật giấu tin trong ảnh dựa trên MBNS (Multiple Base Notational System)"*, đồ án tốt nghiệp ngành CNTT – 2011.

[25]. Vũ Thùy Dung – CT1101, *"Kỹ thuật giấu tin trong ảnh SES (Steganography Evading Statistical analyses)"*, đồ án tốt nghiệp ngành CNTT – 2011.

[26]. Trịnh Văn Thành – CT1101, *"Phát hiện ảnh có giấu tin trên LSB bằng phương pháp phân tích cặp mẫu"*, đồ án tốt nghiệp ngành CNTT – 2011.

[27]. Phạm Văn Đại – CT1101, *"Kỹ thuật giấu tin dựa trên biến đổi Contourlet"*, đồ án tốt nghiệp ngành CNTT – 2011.

[28]. Nguyễn Mai Hương – CT1101, *"Kỹ thuật giấu tin PVD"*, đồ án tốt nghiệp ngành CNTT – 2011.

[29]. Phạm Văn Minh, *"Kỹ thuật phát hiện mù cho ảnh có giấu tin bằng LLRT (Logarithm likelihood Ratio Test)"*, đồ án tốt nghiệp ngành CNTT – 2011.

[30]. Link đến thư viện ảnh chuẩn 512 x 512: USC-SIPI Image Database, Signal and Image Processing Institute, University of Southern California, *http://sipi. usc. edu/services/database/ Database. html*