MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

DANH MỤC CHỮ VIẾT TẮT, TIẾNG ANH

Chữ viết tắt	Diễn giải	Ý nghĩa
BMP	Bitmap	Định dạng tệp tin hình ảnh BMP.
DIB	Device Independent Bitmap	Thiết bị độc lập ảnh bitmap.
TIFF	Tagged Image File Format	Được gắn thẻ định dạng tệp in ảnh.
GIF	Graphics Interchange Format	Định dạng Trao đổi Hình ảnh.
IMG	Image	Ảnh IMG.
	Embedding	Kỹ thuật nhúng.
	Embedded data	Kỹ thuật nhúng tin.
	Watermarking	Là thủy vân số, thủy ấn.
	Host data	Tin gốc.
	Filtering	Thực hiện lọc.
	Lossy compressio	Nén mất dữ liệu .
	Fingerprinting	Nhận dạng vân tay, điểm chỉ.
PSNR	Peak Signal to Noise Ratio	Tỷ số tín hiệu đỉnh trên nhiễu.
MSE	Mean squared error	Bình phương trung bình lỗi.
	Lossy compression	Nén có mất mát dữ liêu.

MỞ ĐẦU

Mục đích của đề tài là che giấu thông tin vào trong ảnh nhị phân, khi nhìn bằng mắt thường sẽ khó phát hiện ra ảnh có giấu tin hay không vì sự thay đổi của ảnh sau khi giấu tin là ít nhất. Thuật toán sử dụng việc thay đổi nhiều nhất 1 phần tử trong khối đang xét. Thuật toán này không chỉ nhằm giấu tin với độ hiển thị của thông tin được giấu là thấp mà nó còn đảm bảo khả năng có thể thuận nghịch cho ảnh sau khi giấu tin.

Với thuật toán này ảnh sau khi giấu tin sẽ được khôi phục lại như ảnh ban đầu. Điều này rất quan trọng đối với những sản phẩm bản quyền cần được chứng thực và xác thực bằng giấu vân tay. Sau khi xác định sản phẩm được chứng thực ta có thể lấy lại ảnh gốc mà không có sự thay đổi nào trên ảnh gốc.

Trong báo cáo này sẽ trình bày một thuật toán mới, cải tiến từ thuật toán trong [1], cũng dựa trên tính chẵn lẻ của các khối bit, nhưng có sử dụng thêm một ma trận khóa để tăng cường tính bảo mật cho thuật toán giấu tin. Khi nhận được ảnh có tin giấu, người nhận cần phải có thêm ma trận khóa mới có thể trích rút được thông tin. Đồng thời để có thể lấy lại ảnh gốc phải có ma trận định vị. Khối bit được sử dụng không chỉ cố định là 3×3 mà có thể là m×n bất kỳ. Ngoài ra chất lượng ảnh sau khi giấu còn được nâng cao hơn do trong thuật toán mới này, những khối toàn màu đen hoặc toàn màu trắng sẽ không được sử dụng để giấu tin.

Cấu trúc báo cáo bao gồm phần mở đầu và bốn chương nội dung:

- Chương 1: Giới thiệu tổng quan về giấu tin trong ảnh, định nghĩa về giấu tin trong ảnh cũng như phân loại kỹ thuật giấu tin cho ta thấy cái nhìn khái quát về giấu tin trong ảnh.
- Chương 2: Nghiên cứu cấu trúc ảnh bitmap, tìm hiểu hệ thống các khối trong ảnh bitmap. Mỗi một khối sẽ có những chức năng riêng lưu trữ các giá trị của điểm ảnh.
- Chương 3: Kỹ thuật giấu tin cho ảnh nhị phân, giới thiệu về kỹ thuật được trình bày trong báo cáo, chương này đưa ra các bước thực hiện của thuật toán.
- Chương 4: Cài đặt và thử nghiệm, thực hiện cài đặt trên máy tính sử dụng phần mềm matlap R2008b. Thử nghiệm giấu tin trên 42 ảnh bitmap với kích cỡ khác nhau và đưa ra đánh giá PSNR.

Chương 1. TỔNG QUAN VỀ GIẤU TIN TRONG ẢNH

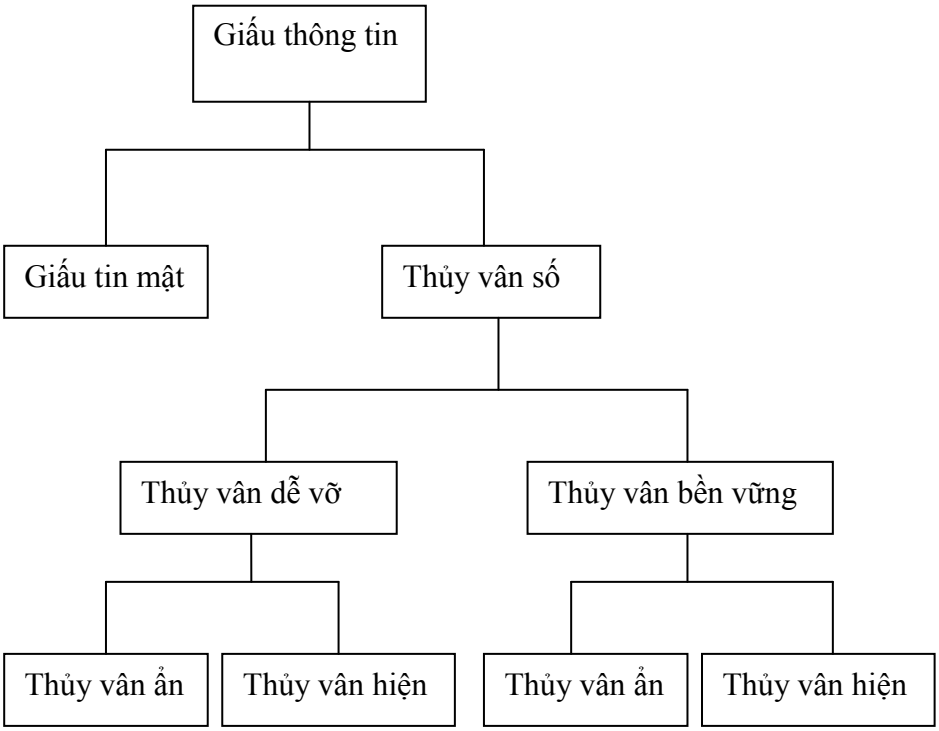
1.1. Khái niệm cơ bản về giấu tin trong ảnh

Giấu thông tin là kỹ thuật nhúng (embedding) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu ảnh số khác [3].

1.2. Phân loại các kỹ thuật giấu tin trong ảnh

Có thể chia lĩnh vực giấu tin thành hai hướng lớn là [2]:

- Thủy vân số (watermarking).
- Giấu tin mật (steganography).



Hình 1.1. *Phân loại các kĩ thuật giấu tin (Fabien A.P. Patitcolaset al., 1999)*

1.2.1. Thủy vân số

Watermarking là kỹ thuật nhúng một biểu tượng vào trong ảnh môi trường để xác định quyền sở hữu ảnh môi trường, chống sự giả mạo và xuyên tạc thông tin. Kích thước của biểu tượng thường nhỏ (từ vài bit tới vài nghìn bit).

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

- Thủy vân dễ vỡ: Là kỹ thuật nhúng thủy vân vào trong một đối tượng (sản phẩm) và nếu có bất kỳ phép biến đổi nào làm thay đổi sản phẩm gốc thì thủy vân đã được giấu trong đối tượng sẽ không còn nguyên vẹn như trước khi giấu.

+ Thủy vân ẩn: Cũng giống như giấu tin, bằng mắt thường không thể phát hiện thủy vân ẩn.

+ Thủy vân hiện: Là loại thủy vân hiện ngay trên sản phẩm và có thể phát hiện sự tồn tại của thủy vân.

1.2.2. Giấu tin mật

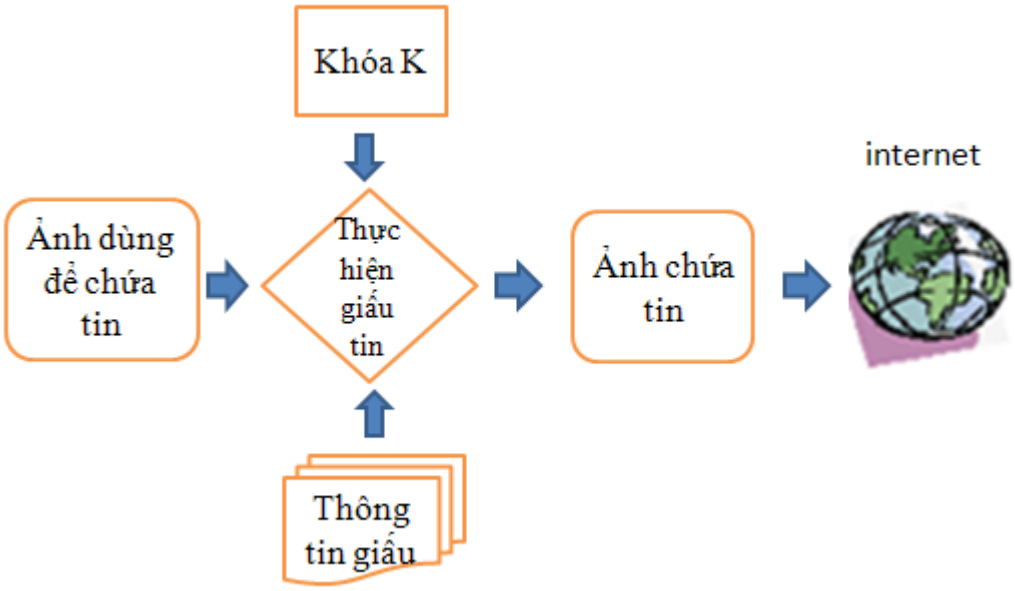
Steganography (giấu tin, viết phủ) là lĩnh vực nghiên cứu việc nhúng các mẩu tin mật vào một môi trường phủ. Trong quá trình giấu tin để tăng bảo mật có thể người ta dùng một khoá viết mật khi đó người ta nói về Intrinsic Steganography (dấu tin có xử lý). Khi đó để giải mã người dùng cũng phải có khoá viết mật đó.

Giấu tin mật quan tâm đến các ứng dụng sao cho người khác khó phát hiện nhất việc có tin được giấu và nếu có phát hiện tin được giấu thì việc giải tin cũng khó thực hiện nhất. Một yêu cầu nữa đối với kỹ thuật này là lượng tin giấu vào trong ảnh cũng là lớn nhất.

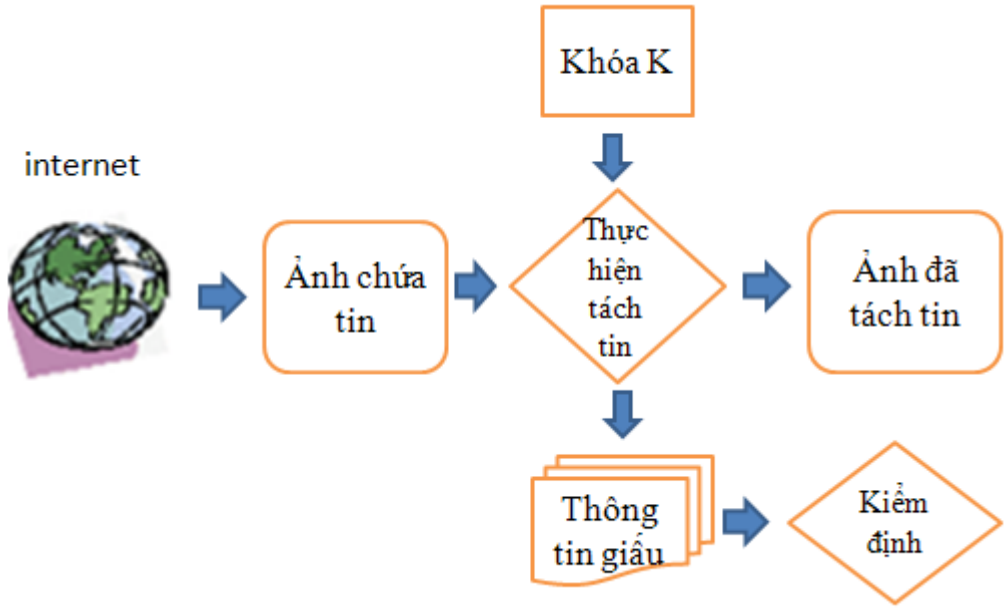
1.3. Mô hình kỹ thuật giấu tin

Hệ thống giấu tin nói chung bao gồm 2 phần chính: quá trình giấu tin và quá trình tách tin (hình 1.2 và hình 1.3) [3].

Giai đoạn giấu tin, các thông tin khoá (công khai hoặc bí mật) và dấu tin được chèn vào ảnh gốc để được ảnh có bản quyền. Giai đoạn tách tin, dữ liệu khoá (bí mật) và ảnh giấu tin (ảnh có chứa tin) sẽ làm dữ liệu cơ sở để tách tin từ ảnh có bản quyền.



Hình 1.2. *Quá trình giấu tin*



Hình 1.3. *Quá trình tách tin*

Thông tin về quá trình giấu tin và quá trình tách tin:

- Thông tin giấu: có thể là văn bản hoặc tệp ảnh hay bất kỳ một tệp nhị phân nào, vì quá trình xử lý chúng ta đều chuyển chúng thành chuỗi các bit.
- Ảnh dùng để chứa tin: là ảnh được dùng để làm môi trường nhúng tin mật.
- Khoá K: khoá mật tham gia vào quá trình giấu tin, tăng tính bảo mật.
- Ảnh chứa tin: là ảnh sau khi đã nhúng tin mật vào đó.

- Ảnh đã tách tin: là ảnh sau khi đã tách thông điệp.
- Kiểm định: kiểm tra chất lượng ảnh sau khi giấu và kiểm tra tính toàn vẹn của thông tin đã được giấu.

1.4. Mục đích của kỹ thuật giấu tin trong ảnh

Dựa vào phân loại các kỹ thuật giấu tin ta có 2 hướng chính đó là thủy vân số và giấu tin mật. Mỗi loại lại có những mục đích tương ứng như sau:

- Thứ nhất: bảo mật cho chính đối tượng được dùng để giấu tin (thủy vân số).

Kỹ thuật thủy vân số: đây là kỹ thuật nhằm bảo mật và xác thực cho chính đối tượng được giấu tin. Các ứng dụng cơ bản nhất là bảo vệ bản quyền, phát hiện xuyên tạc thông tin.

- Thứ hai: bảo mật cho thông tin được giấu (giấu tin mật).

Kỹ thuật giấu tin mật: với mục đích bảo mật cho thông tin được giấu kỹ thuật này đưa ra nhằm 2 mục tiêu chính là thông tin được giấu số lượng lớn và rất khó phát hiện ra thông tin có được giấu vào ảnh hay không.

1.5. Các yêu cầu đối với giấu tin trong ảnh

Những yêu cầu cơ bản đối với giấu tin cho ảnh là:

- Tính ẩn của giấu tin được chèn vào ảnh: Sự hiện diện của giấu tin trong ảnh không làm ảnh hưởng tới chất lượng của ảnh đã chèn tin.
- Tính bền của giấu tin: Cho phép các tin có thể tồn tại được qua các phép biến đổi ảnh, biến dạng hình học hay các hình thức tấn công cố ý khác.
- Tính an toàn: không thể xoá được tin ra khỏi ảnh trừ khi ảnh được biến đổi tới mức không còn mang thông tin

Tính ẩn của tin là một yêu cầu rất quan trọng của phương pháp giấu tin.

1.6. Thủy vân số thuận nghịch trong ảnh nhị phân

Thủy vân số thuận nghịch là kỹ thuật giấu thông điệp, giấu biểu tượng mà sau khi khôi phục thông điệp trong quá trình tách tin, ta có thể khôi phục lại xấp xỉ hoặc giống ảnh gốc ban đầu.

Một số tác giả [6, 7, 8] phân loại kỹ thuật giấu tin thuận nghịch thành 2 loại:

- Kỹ thuật dựa vào trải phổ cộng (addtive spead spectrum).

- Kỹ thuật dựa trên tính năng nén của ảnh (image fearture compression): có khả năng thủy vân số thuận nghịch cao.

1.6.1. Kỹ thuật dựa vào trải phổ cộng

Loại đầu tiên [9, 10] sử dụng kĩ thuật trải phổ cộng. Trong những kĩ thuật này, một tín hiệu trải phổ tương ứng với dữ liệu được nhúng là được chồng vào (thêm vào) tín hiệu gốc. Trong việc giải mã, các dữ liệu ẩn được phát hiện và các tín hiệu thêm vào sẽ bị loại bỏ (trừ đi) để phục hồi tín hiệu gốc. Trong kĩ thuật này, sự giải nén the payload (tải trọng) rất mạnh, theo nghĩa là the payload có thể được giải nén thậm chí nếu ảnh được ẩn đã bị sửa đổi một chút. Tuy nhiên, trong trường hợp này, ảnh gốc sẽ không thể khôi phục lại được.

1.6.2. Kỹ thuật dựa trên tính năng nén của ảnh

Loại thứ hai [6, 7, 11] ghi đè một phần của tín hiệu gốc với dữ liệu được nhúng vào. Hai loại thông tin phải được nhúng vào: Dữ liệu nén của phần được ghi đè và dữ liệu the net payload (để cho phép hồi phục tín hiệu gốc). Trong quá trình giải mã, thông tin ẩn sẽ được tách ra, dữ liệu the payload sẽ được hồi phục, và dữ liệu được nén sẽ được sử dụng để hồi phục lại tín hiệu gốc. Những kĩ thuật này không gây ra tình trạng salt-and-pepper artifacts, vì những phần được sửa đổi thường là những bits ít được kể đến nhất hoặc những sóng có hệ số tần số cao mà không gây ra sự biến dạng cảm quan. Những kĩ thuật này thường cung cấp khả năng che giấu dữ liệu nhiều hơn loại đầu tiên.

Hãy xem xét, ví dụ, các dữ liệu ẩn mà ảnh che giấu được chia thành các khối, và một bit dữ liệu được chèn vào mỗi khối bằng cách trộn (nếu cần thiết) điểm ảnh với khả năng hiển thị thấp nhất. Những khối với số chẵn (lẻ) của những điểm ảnh đen có bít 0 (1) được nhúng vào. Trong kĩ thuật này, ảnh gốc không thể phục hồi được thậm chí nếu những tỉ suất ban đầu của những điểm ảnh đen được biết, vì điểm ảnh được lộn lại một cách chính xác bên trong mỗi khối không thể nào định vị được nếu không có một ma trận định vị các điểm đã lộn lại đó.

Chương 2. NGHIÊN CỨU CẤU TRÚC ẢNH BITMAP

2.1. Cấu trúc ảnh Bitmap

Một tập tin BMP điển hình thông thường chứa những khối dữ liệu sau:

Bảng 2.1. Các khối dữ liệu trong một tập tin BMP

Tên khối	Ý nghĩa
BMP File Header	Lưu trữ thông tin tổng hợp về file BMP.
Bitmap Infomation	Lưu trữ thông tin chi tiết về ảnh bitmap.
Color Palette	Lưu trữ định nghĩa của màu được sử dụng cho bitmap.
Bitmap Data	Lưu trữ từng pixel của hình ảnh thực tế.

2.1.1. BMP File Header (14 byte)

Đây là khối bytes ở phần đầu tập tin, sử dụng để định danh tập tin. Ứng dụng đọc khối bytes này để kiểm tra xem đó có đúng là tập tin BMP không và có bị hư hỏng không.

Bảng 2.2. Chi tiết khối bytes tiêu đề tập tin BMP

Offset	Size	Mục đích
0000h	2 bytes	Magic number sử dụng để định nghĩa tập tin BMP: 0x42 0x4D(mã hexa của kí tự B và M). Các mục dưới đây có thể được dùng: • BM - Windows 3.1x, 95, NT, ... etc • CI - OS/2 Color Icon • CP - OS/2 Color Pointer
0002h	4 bytes	Kích thước của tập tin BMP theo byte.
0006h	2 bytes	Dành riêng; giá trị thực tế phụ thuộc vào ứng dụng tạo ra hình ảnh.
0008h	2 bytes	Dành riêng; giá trị thực tế phụ thuộc vào ứng dụng tạo ra hình ảnh.
000Ah	4 bytes	offset, địa chỉ bắt đầu các byte dữ liệu ảnh bitmap.

2.1.2. Bitmap Information (DIB header: 40 byte)

Khối bytes này nói cho ứng dụng biết các thông tin chi tiết về hình ảnh, sẽ được sử dụng để hiển thị hình ảnh trên màn hình. Bảng sau miêu tả chi tiết cấu trúc tiêu đề DIB. Tất cả các giá trị được lưu trữ như là unsigned interger, trừ khi lưu ý một cách rõ ràng.

Bảng 2.3. Chi tiết khối bytes thông tin tập tin BMP

Offset	Size	Mục đích
Eh	4	Kích thước của tiêu đề(40 bytes).
12h	4	Chiều rộng bitmap tính bằng pixel (signed interger).
16h	4	Chiều cao bitmap tính bằng pixel (signed interger).
1Ah	2	Số lượng các mặt phẳng màu sắc được sử dụng. Phải được thiết lập bằng 1.
1Ch	2	Số bit trên mỗi pixel, là độ sâu màu của hình ảnh. giá trị điển hình là 1, 4, 8, 16, 24 và 32.
1Eh	4	Phương pháp nén được sử dụng. Xem bảng tiếp theo để có danh sách các giá trị có thể.
22h	4	Kích thước hình ảnh. Đây là kích thước của dữ liệu bitmap(xem bên dưới), và không nên nhầm lẫn với kích thước tập tin.
26h	4	Độ phân giải theo chiều ngang của hình ảnh(signed interger).
2Ah	4	Độ phân giải theo chiều dọc của hình ảnh(signed interger).
2Eh	4	Số lượng màu trong bảng màu.
32h	4	Số lượng các màu sắc quan trọng được sử dụng, hoặc 0 khi màu sắc nào cũng đều là quan trọng, thường bị bỏ qua.

2.1.3. Bảng màu (Color Palette)

Với (4*x bytes), x là số màu của ảnh: định nghĩa các màu sẽ được sử dụng trong ảnh.

Bảng màu xuất hiện sau tiêu đề BMP và tiêu đề DIB. Vì vậy, offset là kích cỡ của tiêu đề BMP cộng với kích thước của tiêu đề DIB.

Có tất cả 2^24 màu RGB khác nhau, nhưng các loại Bitmap 1bit (2 màu, hoặc chuẩn Windows là trắng-đen), 4 bits (16 màu), 8 bits (256 màu) không thể khai thác hết, nên chỉ liệt kê các màu được dùng trong file. Mỗi màu trong bảng màu được mô tả bằng 4 bytes. (BlueByte, GreenByte, RedByte, ReservByte).

2.1.4. Dữ liệu ảnh (lưu dữ liệu ảnh)

Dữ liệu ảnh được lưu từng điểm cho đến hết hàng ngang (từ trái sang phải), và từng hàng ngang cho đến hết ảnh (từ dưới lên trên).

Đối với mỗi điểm ảnh loại màu Indexed, ta cần 1, 4 hoặc 8 bits để đặc trưng cho điểm đang xét ứng với màu thứ mấy trong bảng màu.

Thí dụ:

Giá trị 0111 (=7) trong loại BMP 4 bits cho biết điểm đó có màu 7 (màu xám theo "chuẩn" Windows). Riêng loại 24 bits, không mô tả màu bằng thứ tự trên bảng màu (nếu liệt kê hết bảng màu của nó thì đã tốn cả Gigabyte bộ nhớ và đĩa), mà người ta liệt kê luôn giá trị RGB của 3 màu thành phần.

2.2. Giới thiệu về ảnh nhị phân

Ảnh nhị phân được lưu trữ như là một ảnh định dạng bitmap hay ảnh định dạng IMG.

Ảnh IMG là ảnh đen trắng chỉ bao gồm 2 màu: màu đen và màu trắng. Người ta phân mức đen trắng đó thành L mức. Nếu sử dụng số bit B=8 bít để mã hóa mức đen trắng (hay mức xám) thì L được xác định: L=2B. Trong bài này ta nghiên cứu ảnh nhị phân nên B=1, nghĩa là chỉ có 2 mức: mức 0 và mức 1. Mức 1 ứng với màu sáng, còn mức 0 ứng với màu tối.

Một số dạng ảnh hay sử dụng sau: BMP, TIF, GIF, DIB, IMG.

Ví dụ: Biểu diễn về ảnh nhị phân:

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

Chương 3. KĨ THUẬT GIẤU TIN THUẬN NGHỊCH CHO ẢNH NHỊ PHÂN

Thủy vân số thuận nghịch là kỹ thuật giấu thông điệp, giấu biểu tượng mà sau khi khôi phục thông điệp trong quá trình tách tin, ta có thể khôi phục lại xấp xỉ hoặc giống ảnh gốc ban đầu.

3.1. Giới thiệu thuật toán giấu tin cho ảnh nhị phân

Qua quá trình tìm hiểu và nghiên cứu đề tài "thủy vân số thuận nghịch cho ảnh nhị phân" em đã thu thập được một số tài liệu liên quan. Sau đây em sẽ đề cập tới kỹ thuật mà em sử dụng để trình bày trong đợt làm đồ án này. Đó là thuật toán giấu tin có thuận nghịch cho ảnh nhị phân sử dụng tính chẵn lẻ của các khối bit [1].

3.1.1. Tư tưởng của thuật toán

Báo cáo trình bày một thuật toán để giấu tin trong ảnh nhị phân sử dụng tính chẵn lẻ của các khối bit. Thuật toán có thể giấu được một bit vào mỗi khối ảnh bằng cách thay đổi nhiều nhất một phần tử của khối đó, xác định điểm thay đổi bằng cách dùng ma trận láng giềng và khóa K. Tính bảo mật và chất lượng ảnh sau khi giấu tin của thuật toán này khá cao. Kỹ thuật này có thể thuận nghịch cho ảnh nhị phân có nghĩa là trong quá trình tách tin ta có thể khôi phục lại ảnh sau khi được giấu tin giống với ảnh gốc ban đầu.

3.1.2. Một số định nghĩa của thuật toán

- **Định nghĩa 1**

  Phép toán ^ là phép AND từng phần tử của hai ma trận cùng cấp.

Với A, B là các ma trận cùng cấp m×n, ta có C = A^B cũng là ma trận cấp m×n trong đó C[j,k] = A[j,k] AND B[j,k], với j = 1, 2, …, m, k = 1, 2, …, n.

- **Định nghĩa 2**

  Phép toán SUM(F) tính tổng các phần tử của ma trận F.

- **Định nghĩa 3**

  Phần tử láng giềng của phần tử F[j,k] là phần tử F[u,v] thỏa mãn điều kiện:

$$\begin{cases} 1 \le |u-j| + |v-k| \le 2 \\ |u-j| < 2 \\ |v-k| < 2 \end{cases}$$

❖ **Định nghĩa 4**

Ma trận láng giềng của ma trận F cấp m×n là ma trận N cấp m×n trong đó N[j,k] là số phần tử láng giềng thuộc khối F của F[j,k] mà có giá trị khác với F[j,k].

Ví dụ:

$$\text{Nếu } F = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \qquad \text{thì } N = \begin{bmatrix} 2 & 2 & 1 \\ 2 & 5 & 2 \\ 0 & 2 & 2 \end{bmatrix}$$

❖ **Định nghĩa 5**

Ma trận định vị LM: đánh dấu sự thay đổi của các bit khi đã đảo ngược lại.

3.2. Kỹ thuật giấu tin trong ảnh nhị phân

3.2.1. Dữ liệu vào

+ F: Ảnh nhị phân được dùng để giấu tin

+ m và n: Kích thước của khối con F_i của F

+ K: Ma trận nhị phân cấp m×n với các giá trị được lựa chọn ngẫu nhiên

+ B: Dãy bit cần giấu vào F

F là một ma trận nhị phân và được phân hoạch thành các khối F_i cấp m×n. Mỗi khối F_i sẽ được sử dụng để giấu một bit b của B bằng cách thay đổi nhiều nhất một phần tử trong F_i.

Ma trận K là khoá bí mật, được thỏa thuận giữa người gửi và người nhận.

3.2.2. Dữ liệu ra

+ F': Ảnh nhị phân chứa dãy bit B, trong đó mỗi khối F'_i cấp m×n là một phân hoạch của F' giấu một bit b của B và F'_i khác F_i nhiều nhất là một bit.

+ LM: Ma trận định vị các điểm ảnh đã bị đảo bit. Ma trận này sẽ giúp thuận nghịch cho ảnh nhị phân được giấu tin.

3.2.3. Các bước của thuật toán giấu tin

3.2.3.1. Quá trình giấu tin

- **Đầu vào:**

- Ảnh gốc

- Khóa K

- Ảnh thông điệp

- **Đầu ra:**

- Ảnh chứa thông điệp

- Ma trận định vị

- **Các bước thực hiện giấu tin:**

Bước 1:

+ Tính SUM(F_i)

+ Nếu SUM(F_i) = 0 hoặc SUM(F_i) = mn thì bỏ qua không giấu tin vào khối F_i này, chuyển sang xét khối F_i tiếp theo.

+ Nếu 0 < SUM(F_i) < mn thì chuyển sang bước 2 để giấu tin.

Bước 2:

+ Tính S = SUM(F_i ^ K)

+ Nếu S = b (mod 2) thì đã đạt bất biến, do đó trường hợp này giấu được một bit vào F_i mà không cần phải biến đổi F_i.

+ Đánh dấu LM = 0;

+ Nếu S ≠ b (mod 2) thì cần chuyển sang bước 3 để xác định phần tử thích hợp nhất.

Bước 3:

+ Xây dựng ma trận láng giềng N_i của ma trận F_i.

+ Xác định phần tử N_i[j,k] có giá trị lớn nhất trong ma trận N_i có K[j,k] = 1.

+ Thay đổi phần tử F_i[j,k].

+ Nếu N_i[j,k] có giá trị lớn nhất và K[j,k] = 1 thì ta thay đổi F_i[j,k] ta sẽ nhận được F'_i[j,k].

+ Đánh dấu LM[j,k] = 1.

3.2.3.2. Quá trình khôi phục thông tin giấu

- **Đầu vào:**

- Ảnh chứa thông điệp

- Ma trận định vị

- Khóa K

- **Đầu ra:**

- Thông điệp

- Ảnh khôi phục

- **Các bước thực hiện tách tin:**

Để khôi phục thông tin cần: ảnh nhị phân F’ có chứa tin giấu và ma trận khóa K cấp m×n.

Bước 1:

Chia F’ thành các khối F'_i cấp m×n, sau đó thực hiện tuần tự trên các khối F'_i các công việc ở bước 2.

Bước 2:

Tính SUM(F'_i)

+ Nếu SUM(F'_i) = 0 hoặc SUM(F'_i) = mn thì chuyển sang khối F'_i tiếp theo vì trong khối F'_i này không có tin giấu.

+ Nếu 0 < SUM(F'_i) < mn thì chứng tỏ trong khối F'_i này có tin giấu, và ta cần khôi phục lại bit thông tin này.

Bước 3:

Tính giá trị b = SUM(F'_i^K) mod 2, và b chính là bit đã được giấu trong F'_i.

+ Nếu LM = 0 thì khối F'_i này giữ nguyên giá trị các bit. Nếu LM = 1 thì đảo bit tương ứng.

*** Nhận xét:**

Việc lựa chọn khóa K là hoàn toàn ngẫu nhiên, do đó số khả năng lựa chọn có thể lên đến 2mn. Khi K càng có nhiều bit 0 thì xác suất để các phần tử $N_i[j,k]$ có giá trị lớn nhất trong ma trận láng giềng mà có K[j,k] = 1 càng nhỏ, vì thế sẽ hạn chế khả năng lựa chọn phần tử tốt nhất để thay đổi. Tất nhiên, nếu K gồm toàn bit 0 thì ta không thể sử dụng nó trong thuật toán này để giấu tin được.

Chương 4. CÀI ĐẶT VÀ THỬ NGHIỆM CHƯƠNG TRÌNH

4.1. Môi trường cài đặt

- Chương trình của thuật toán được cài đặt và thử nghiệm trên máy tính. Trong đề tài này em sử dụng ngôn ngữ lập trình Matlab phiên bản R2008b.

- Cấu hình cho MathWorks Matlab R2008b.

➢ **Yêu cầu hệ thống:** tối thiểu

- Base OS: Windows
- OS Version: XP SP3
- Processor: Pentium IV - or Greater
- RAM: 512 MB - 1GB recommended
- Solaris: 512 MB - 1GB recommended
- Hard Disk Total Size: 625 MB (chỉ sử dụng MATLAB)

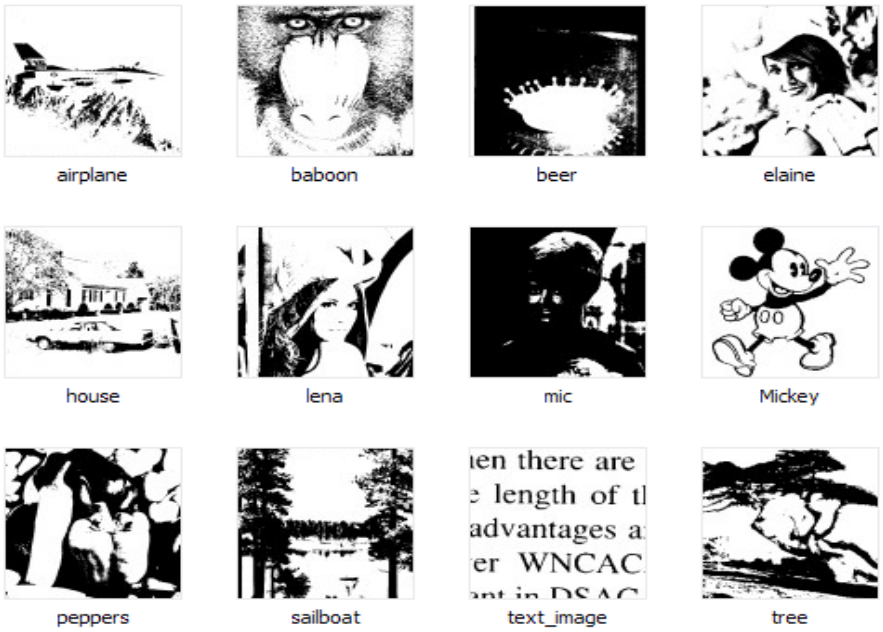
➢ **Yêu cầu hệ thống:** cần thiết

- Base OS: Windows
- OS Version: XP SP3
- Processor: Pentium IV - or Greater
- RAM: 1 GB or Greater
- Solaris: 1 GB or Greater
- Hard Disk Total Size: 40 GB

4.2. Dữ liệu ảnh thử nghiệm

Môi trường thử nghiệm trên ảnh nhị phân bitmap: 12 ảnh chuẩn và 30 ảnh chụp bất kỳ [12]. Em đã sử những ảnh màu và ảnh xám chuyển sang ảnh nhị phân để sử dụng trong đề tài này.

❖ **Tập dữ liệu thử nghiệm chuẩn:** Tập dữ liệu thử nghiệm gồm 12 ảnh chuẩn kích thước 512×512 trong hình 4.1.



Hình 4.1. *Gồm 12 ảnh bitmap chuẩn*

❖ **Tập ảnh dữ liệu thử nghiệm bất kì**

Hình 4.2. *Gồm 30 ảnh bitmap chụp với mọi kích cỡ khác nhau*

4.3. Đo độ đánh giá PSNR

Chất lượng ảnh sau khi tin giấu được đánh giá thông qua giá trị của tỷ số PSNR (Peak Signal to Noise Ratio) tỷ số tín hiệu đỉnh trên nhiễu.

Nó được định nghĩa thông qua bình phương trung bình lỗi MSE (mean squared error) cho hai hình ảnh gốc và ảnh kết quả là I và K có kích thước m×n:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \tag{4.1}$$

PSNR được định nghĩa :

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \end{aligned} \tag{4.2}$$

MAX_I là giá trị tối đa của pixel trên ảnh. Đối với ảnh nhị phân thì $MAX_I = 1$.

4.4. Một số giao diện chương trình

Giao diện của kỹ thuật khá thân thiện giúp người sử dụng dễ dàng thao tác với chương trình. Trong đề tài này em sử dụng phiên bản mới nhất của Matlab hoàn thiện hơn và khá tiện ích.

4.4.1. Giao diện chính của chương trình

Chương trình giấu tin thuận nghịch cho ảnh nhị phân gồm 4 phần chính sau:

- Hệ thống: chức năng thoát hẳn ra ngoài hệ thống chương trình.
- Giấu tin: thực hiện giấu tin vào ảnh gốc.
- Tách tin: xử lí tách ảnh thông điệp trong ảnh chứa tin giấu.
- Đánh giá PSNR: Tính toán giá trị của PSNR.

Hình 4.3. *Giao diện chính của chương trình*

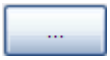
4.4.2. Giao diện giấu tin cho ảnh nhị phân

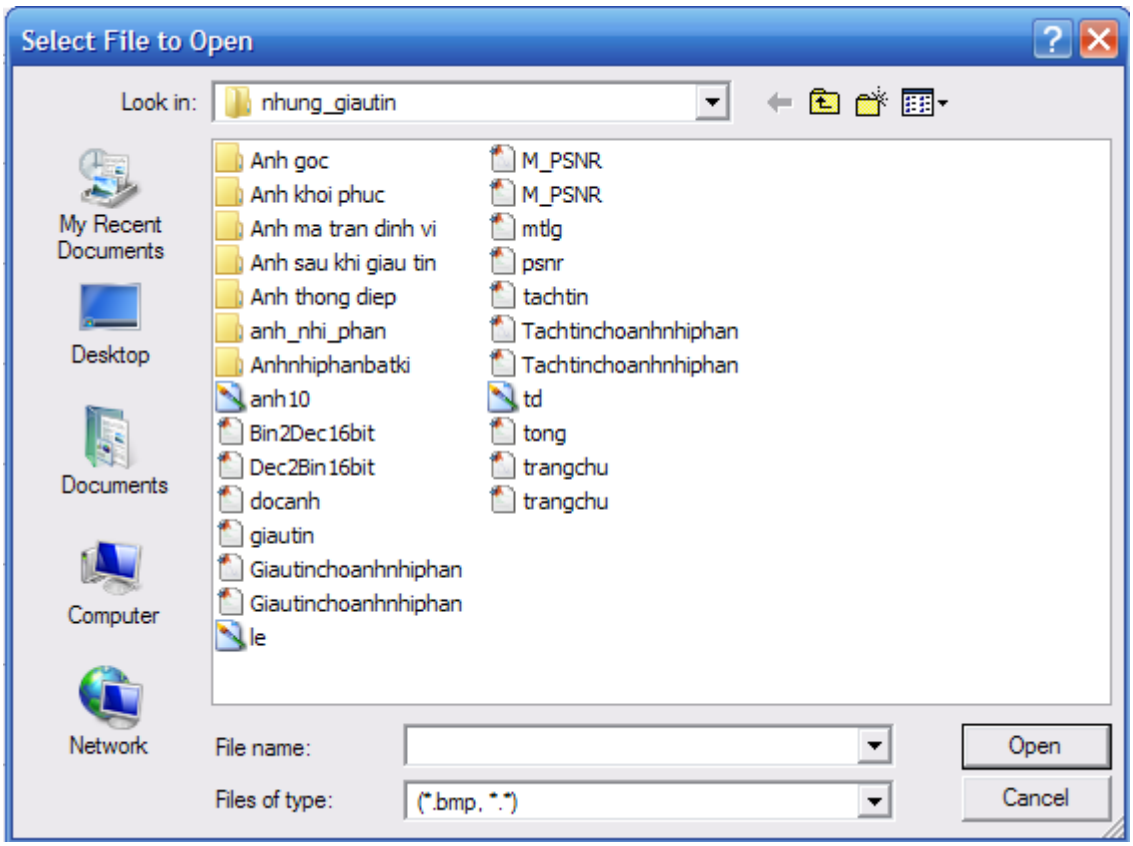
- **Đầu vào:**
  - Chọn ảnh cần giấu
  - Chọn ảnh thông điệp
  - Nhập ma trận khóa K:
    + Nhập số hàng
    + Nhập số cột
- **Đầu ra:**
  - Tên ảnh kết quả
  - Chọn tên ảnh ma trận định vị
- **Các chức năng trong giao diện giấu tin cho ảnh nhị phân:**

- Chọn ảnh cần giấu: chọn ảnh gốc cần giấu tin.

- Chọn ảnh thông điệp: chọn ảnh thông điệp cần giấu.

- Chọn tên ảnh kết quả: chọn tên ảnh chứa thông điệp và thư mục cần chứa ảnh này.

Nhấn vào nút  sẽ hiện lên đường dẫn đến thư mục chứa ảnh cần chọn tương ứng hình 4.4.

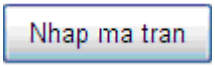


Hình 4.4. *Đường dẫn đến một tệp ảnh trong thư mục*

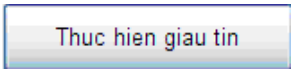
- Nhập ma trận khóa K: ma trận khóa K được nhập vào từ bàn phím với số hàng và số cột phù hợp.

+ Nhập số hàng của ma trận: nhập giá trị số hàng của ma trận khóa K

+ Nhập số cột của ma trận: nhập giá trị số cột của ma trận khóa K

- Nhấn vào nút 

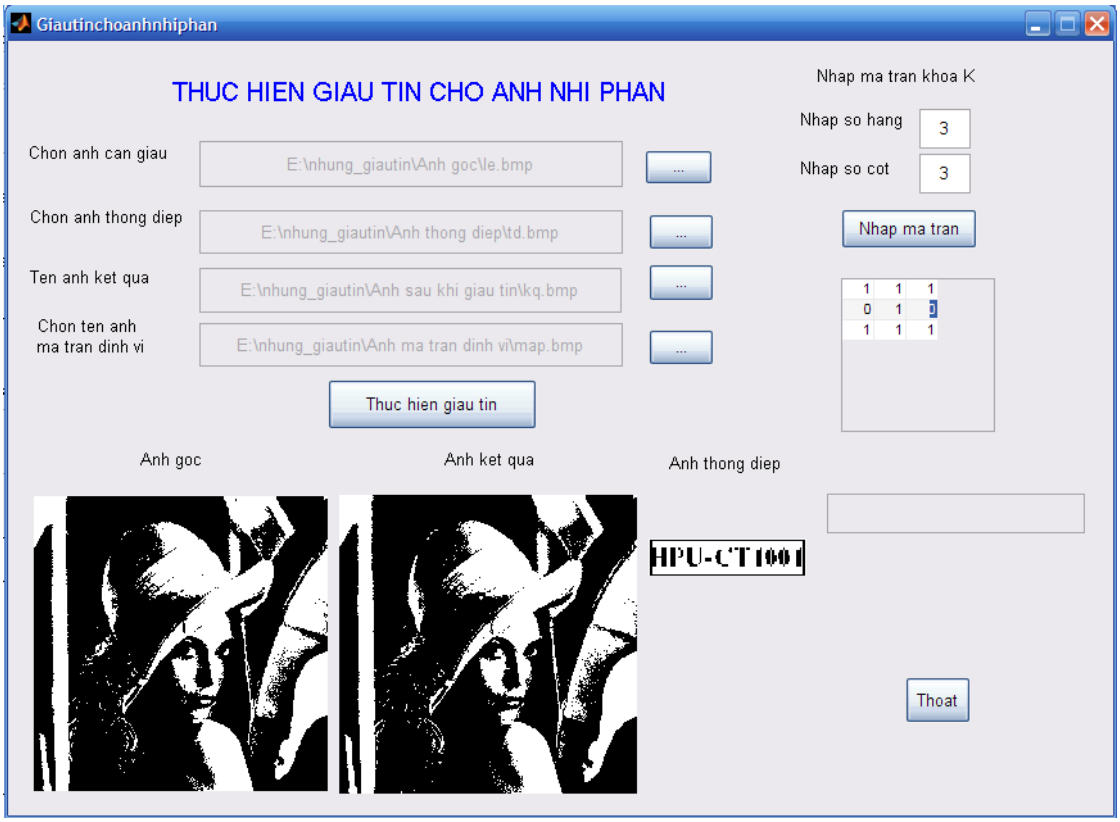
thực hiện nhập ma trận khóa K.

- Nhấn vào nút: 

để thực hiện giấu tin.

- Nhấn nút 

: thoát khỏi giao diện chương trình đang thực thi.



Hình 4.5. *Giao diện giấu tin cho ảnh nhị phân*

4.4.3. Giao diện tách tin cho ảnh nhị phân

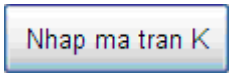
- **Đầu vào:**
  - Chọn ảnh cần tách
  - Nhập tên ma trận định vị
  - Nhập ma trận khóa K
    + Nhập số hàng
    + Nhập số cột
- **Đầu ra:**
  - Tên ảnh khôi phục
  - Ảnh thông điệp sau khi tách
- **Các chức năng trong giao diện tách tin cho ảnh nhị phân:**

  - Chọn ảnh cần tách: chọn ảnh cần tách tin

  - Nhập ma trận khóa K:

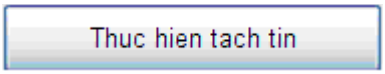
  + Nhập số hàng: nhập số hàng cho ma trận.

  + Nhập số cột: nhập số cột cho ma trận.

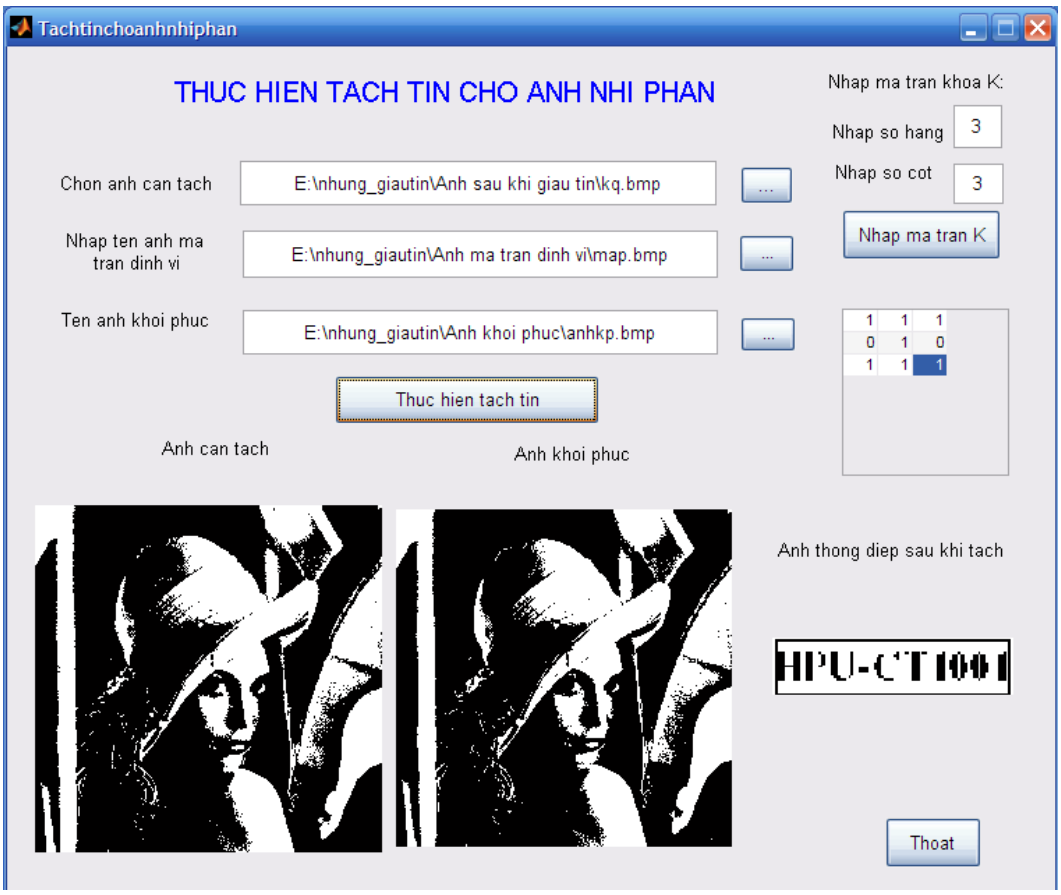
  + Nhấn nút 

hiện ra 1 ma trận với số hằng và số cột đã nhập.

+ Nhập giá trị cho ma trận khóa K.

- Nhấn nút 

: thực hiện tách thông điệp đã được giấu vào ảnh gốc.

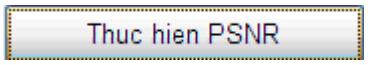


Hình 4.6. *Giao diện tách tin cho ảnh nhị phân*

4.4.4. Giao diện đánh giá PSNR

- **Đầu vào:**
  - Chọn ảnh gốc
  - Chọn ảnh nhúng
- **Đầu ra:**
  - Giá trị đánh giá bằng PSNR
- **Các chức năng trong giao diện đánh giá PSNR cho ảnh nhị phân:**
  - Chọn ảnh gốc: chọn ảnh chưa giấu tin
  - Chọn ảnh nhúng: chọn ảnh đã giấu tin hoặc ảnh đã khôi phục sau khi giấu.

- Nhấn nút  sẽ hiện ra đường dẫn để chọn ảnh tương ứng.

- Thực hiện tính PSNR: nhấn nút 

sẽ hiện ra giá trị đánh giá.

- Hiện số của giá trị PSNR trong ô bên dưới.

Hình 4.7. *Giao diện đánh giá bằng PSNR cho ảnh gốc và ảnh chứa thông điệp*

*** Nhận xét:**

Sau khi đánh giá bằng PSNR cho ảnh gốc và ảnh sau khi giấu tin kết quả của độ đánh giá PSNR>43. Điều này cho thấy ảnh sau khi giấu tin có chất lượng nhìn tuyệt vời, nhìn bằng mắt thường khó có thể nhận biết được ảnh có chứa thông điệp hay không.

Hình 4.8. *Giao diện đánh giá bằng PSNR cho ảnh gốc và ảnh khôi phục*

*** Nhận xét:**

Sau khi đánh giá ảnh gốc và ảnh được khôi phục bằng PSNR cho ra kết quả là hai ảnh là một. Điều đó cho thấy ảnh gốc và ảnh được khôi phục là một. Kỹ thuật này đã thực hiện chính xác sự thuận nghịch cho ảnh nhị phân. Ảnh sau khi giấu tin có thể khôi phục lại như ảnh gốc ban đầu.

4.5. Kết quả đánh giá PSNR

- **Kết quả đánh giá PSNR của ảnh gốc và ảnh sau khi giấu tin với 12 ảnh bitmap chuẩn.**

Bảng 4.1 Kết quả đánh giá PSNR của 12 ảnh gốc và ảnh sau khi giấu tin

Số thứ tự	Tên ảnh	Đánh giá PSNR
1	airplane.bmp	47.5884
2	baboon.bmp	46.8684
3	beer.bmp	46.8684
4	elaine.bmp	46.8535
5	house.bmp	47.2505
6	lena.bmp	46.4844
7	mic.bmp	40.079
8	Mickey.bmp	47.247
9	peppers.bmp	45.1823
10	sailboat.bmp	45.5264
11	text_image.bmp	47.4996
12	tree.bmp	45.6435
Trung bình		**46.09095**

❖ **Kết quả đánh giá PSNR của ảnh gốc và ảnh sau khi giấu tin với 30 ảnh bất kì.**

Bảng 4.1 Kết quả đánh giá PSNR của 30 ảnh gốc và ảnh sau khi giấu tin

Số thứ tự	Tên ảnh	Đánh giá PSNR
1	h1.bmp	45.0056
2	h2.bmp	42.9391
3	h3.bmp	39.6149
4	h4.bmp	42.692
5	h5.bmp	43.6372
6	h6.bmp	46.2495
7	h7.bmp	44.9905
8	h8.bmp	40.8816
9	h9.bmp	45.6619
10	h10.bmp	45.5852
11	h11.bmp	41.6364
12	h12.bmp	43.8536
13	h13.bmp	47.3519
14	h14.bmp	43.54
15	h15.bmp	43.0212
16	h16.bmp	41.4882
17	h17.bmp	44.0655
18	h18.bmp	42.7813
19	h19.bmp	43.4047
20	h20.bmp	44.7603
21	h21.bmp	44.5472
22	h22.bmp	43.1711
23	h23.bmp	41.2858
24	h24.bmp	44.9624
25	h25.bmp	41.8844
26	h26.bmp	44.7801
27	h27.bmp	43.9919
28	h28.bmp	47.0606
29	h29.bmp	43.05
30	h30.bmp	44.1394
Trung bình		**43.7345**

*** Nhận xét :**

Sau khi đánh giá bằng PSNR, ta nhận được kết quả trung bình khá cao. Điều đó cho thấy giấu tin theo phương pháp này đối với ảnh nhị phân có trực quan là khó nhận biết ảnh đã được giấu tin. Kĩ thuật giấu tin này khá nhanh, chất lượng hình ảnh sau khi giấu tin khá tốt (PSNR>43).

KẾT LUẬN

Trong báo cáo này em đã thực hiện những nhiệm vụ chính sau:

1. Đọc hiểu kỹ thuật giấu tin thuận nghịch cho ảnh nhị phân, nắm rõ tổng quan kỹ thuật giấu tin trong ảnh, nghiên cứu tìm hiểu cấu trúc ảnh bitmap.
2. Cài đặt, thử nghiệm thuật toán bằng chương trình matlab R2008b. Đánh giá bằng PSNR giữa ảnh gốc và ảnh sau khi giấu thông điệp với những tập ảnh có kích thước khác nhau.

Với nhiệm vụ của đợt làm đồ án em trình bày 1 kỹ thuật thủy vân số thuận nghịch cho ảnh nhị phân. Thuật toán có thể giấu một bit vào mỗi khối ảnh m×n bằng cách thay đổi nhiều nhất một phần tử trong khối đó. Thuật toán sử dụng tính chẵn lẻ của các khối bit để xây dựng bất biến, sử dụng một ma trận khóa để tăng tính bảo mật và dùng kỹ thuật thay đổi bit có chọn lọc để nâng cao chất lượng ảnh sau khi giấu. Để lấy lại ảnh như ảnh gốc ban đầu ta sẽ dùng ma trận định vị nhằm khôi phục lại ảnh đã giấu tin. Mỗi khối ảnh m×n được nhập vào bất kì nhằm tăng tính bảo mật cho ảnh chứa thông điệp.

Trong kỹ thuật này em kết hợp giữa 2 loại thủy vân đó là thủy vân ẩn và thủy vân bền vững. Thứ nhất là thủy vân ẩn nhằm sau khi che giấu thông tin người khác khó có thể nhận ra được ảnh này có giấu tin hay không vì ảnh sau khi giấu không thay đổi bao nhiêu so với ảnh gốc (thông qua đánh giá bằng PSNR > 43). Thứ hai là thủy vân bền vững nhằm bảo vệ bản quyền chống xâm phạm dữ liệu, nếu có bất kì sự thay đổi nào trên ảnh cũng làm thay đổi dữ liệu trong ảnh và không thể lấy được thông điệp đã được giấu.

Sau quá trình nghiên cứu và tìm hiểu kĩ thuật giấu tin thuận nghịch cho ảnh nhị phân với thời gian nhất định cùng với sự chỉ bảo tận tình của giáo viên hướng dẫn ThS. Hồ Thị Hương Thơm, em đã hoàn thành đề tài nhận được. Dù có tìm hiểu nhưng kinh nghiệm còn yếu kém không thể tránh khỏi những sai sót nên có gì còn thiếu sót em mong nhận được sự chỉ bảo cũng như góp ý của các thầy cô giáo cùng các bạn để đồ án được hoàn thiện hơn.

Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

Tài liệu Tiếng Việt

[1]. Nguyễn Hiếu Cường (2009), *Một thuật toán mới giấu tin trong ảnh nhị phân sử dụng tính chẵn lẻ của các khối bit*, Trường Đại học Giao thông Vận tải.

[2]. Ngô Thái Hà (2009), *Nghiên cứu kỹ thuật bảo vệ bản quyền các sản phẩm đồ họa vector*, luận văn thạc sĩ khoa học máy tính, Thái Nguyên.

[3]. Nguyễn Trường Huy (2010), *Tìm hiểu kỹ thuật giấu tin cho ảnh nhị phân*, Đồ án tốt nghiệp, Trường Đại học Dân lập Hải Phòng.

[4]. Nguyễn Xuân Huy, Bùi Thế Hồng, Trần Quốc Dũng (2004), *Kỹ thuật thủy vân số trong ứng dụng phát hiện xuyên tạc ảnh*, Kỷ yếu Hội thảo Quốc gia một số vấn đề chọn lọc của Công nghệ Thông tin lần thứ 7. Nhà xuất bản Khoa học kỹ thuật

[5]. Bùi Thế Hồng số (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, 281-292.

Tài liệu tiếng Anh

[6] M. Awrangjeb and M. S. Kankanhalli (2004), *Lossless Water-marking Considering the Human Visual System*, Int. Work-shop on Digital Watermarking, Lecture Notes in Com-puter Science 2939.

[7] M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber (2002), *Reversible Data Hiding*, in Proc. IEEE Int. Conf. on Image Processing.

[8] Y. Q. Shi (2004), *Reversible Data Hiding*, Int. Workshop on Digital Watermarking 2004, Lecture Notes in Com-puter Science 3304.

[9] C. W. Honsinger, P. W. Jones, M. Rabbani, J. C. Stoffel (2001), *Lossless Recovery of an Original Image Containing Em-bedded Data*, US Patent Aug.

[10] J. Fridrich, M. Goljan, R. Du (2001), *Invertible Authentica-tion*, in Proc. SPIE Security and Watermarking of Multime-dia Contents III, San Jose, California, USA.

[11]. Sergio Vicente D. Pamboukian1 (), and Hae Yong Kim2, *reversible data hiding and reversible authentication watermaking for binary images*,

[12]. http://images.google.com.vn/.