BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

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

KỸ THUẬT GIẤU TIN TRÊN K BIT LSB CỦA ẢNH

ĐỒ ÁN TỐT NGHIỆP HỆ ĐẠI HỌC CHÍNH QUY

Ngành: Công nghệ thông tin

Sinh viên thực hiện : Nguyễn Diễm Hương

Giáo viên hướng dẫn : TS. Hồ Thị Hương Thơm

Mã sinh viên : 121277

HẢI PHÒNG - 2012

LỜI CẢM ƠN

Em xin chân thành cảm ơn tất cả các thầy cô trong khoa Công nghệ thông tin Trường ĐHDL Hải Phòng, những người đã nhiệt tình giảng dạy và truyền đạt những kiến thức cần thiết trong suốt thời gian em học tập tại trường để em có thể hoàn thành tốt quá trình học tập của mình.

Đặc biệt, em xin gửi lời cảm ơn chân thành và sâu sắc đến Tiến sĩ Hồ Thị Hương Thơm, người đã trực tiếp hướng dẫn tận tình chỉ bảo em trong suốt quá trình làm đồ án tốt nghiệp.

Với sự hiểu biết còn hạn chế cộng với vốn kiến thức còn phải học hỏi nhiều nên bài báo cáo của em không thể tránh khỏi những thiếu sót, em rất mong có được sự góp ý của các thầy cô giáo và các bạn để kết quả của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải Phòng, ngày… tháng… năm 2012

Sinh viên thực hiện

Nguyễn Diễm Hương

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

Ở đây ta tìm hiểu về một kỹ thuật đã và đang được nghiên cứu và ứng dụng rất mạnh mẽ ở nhiều nước trên thế giới đó là kỹ thuật giấu tin (data hiding). Đây là kỹ thuật mới và phức tạp, nó đang được xem như một công nghệ chìa khoá cho vấn đề bảo vệ bản quyền, chứng thực thông tin và điều khiển truy cập… ứng dụng trong an toàn và bảo mật thông tin. Trong đồ án này tìm hiểu kỹ thuật giấu tin trên k bit LSB của ảnh.

Nội dung được trình bày trong 3 chương:

Chương 1. Một số khái niệm tổng quan

Chương 2. Kỹ thuật giấu tin trên k-LSBs

Chương 3. Cài đặt và thử nghiệm

Chương 1. MỘT SỐ KHÁI NIỆM TỔNG QUAN

1. 1. Cấu trúc của ảnh Bitmap

BMP là một định dạng tập tin hình ảnh khá phổ biến. Các tập tin đồ họa lưu dưới dạng BMP thường có đuôi là .BMP hoặc .DIB (Device Independent Bitmap).

Các thuộc tính tiêu biểu của một tập tin ảnh BMP (và file ảnh nói chung) là:

- Số bit trên mỗi điểm ảnh (bit per pixel), thường được ký hiệu bởi n. Một ảnh BMP n-bit có 2^n màu. Giá trị n càng lớn thì ảnh càng có nhiều màu, và càng rõ nét hơn. Giá trị tiêu biểu của n là 1 (ảnh đen trắng), 4 (ảnh 16 màu), 8 (ảnh 256 màu), 16 (ảnh 65536 màu) và 24 (ảnh 16 triệu màu). Ảnh BMP 24-bit có chất lượng hình ảnh trung thực nhất.
- Chiều cao của ảnh (height), chiều rộng của ảnh (width), điểm ảnh (pixel).

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

Ảnh bitmap được chia thành ba dạng: ảnh nhị phân (ảnh đen trắng), ảnh đa mức xám, ảnh màu.

1. 1. 1. Ảnh đen trắng

Là ảnh mà mỗi điểm ảnh chỉ thể hiện một trong hai trạng thái 0 và 1 để biểu diễn trạng thái điểm ảnh đen hay trắng.

Hình 1.1. Ví dụ về ảnh đen trắng

1. 1. 2. Ảnh đa cấp xám

Là ảnh mà mỗi điểm ảnh được biểu diễn bởi một giá trị và đó là cường độ sáng của điểm ảnh.

Hình 1.2. Ví dụ về ảnh đa cấp xám

1. 1. 3. Ảnh màu

Là ảnh mà mỗi điểm ảnh được biểu diễn bởi ba đại lượng R, G, B. Số lượng màu có thể của loại ảnh này lên tới 265^3 màu khác nhau. Nhưng số lượng màu trên thực tế của một ảnh nào đó thường khá nhỏ.

Với ảnh có số màu lớn thì các điểm ảnh không tổ chức dưới dạng bảng màu, khi đó giá trị của các điểm ảnh chính là giá trị của các thành phần màu R, G, B. Tùy theo chất lượng ảnh mà quyết định số bit để biểu diễn cho mỗi màu thường là 24 bit, hoặc 32 bit. Với ảnh 24 bit mỗi thành phần màu được biểu diễn bởi một byte (8 bit).

Hình 1.3. Ví dụ về ảnh màu

1. 1. 4. Ý nghĩa của các phần trong tệp ảnh Bitmap

- Bitmap Header: Mô tả thông tin chung về tệp định dạng bitmap, độ lớn của phần này cố định với mọi tệp bitmap.
- Bitmap Infor: Mô tả thông tin về ảnh được lưu trữ, độ lớn của phần này cố định.
- Pallete Table: Bảng màu của ảnh bitmap, độ lớn của phần này có thể bằng 0 (không có bảng màu) đối với ảnh đen trắng và ảnh màu có số lượng màu lớn hơn 256 màu.

- Data: Thông tin về từng điểm ảnh, độ lớn của phần này phụ thuộc vào kích thước ảnh.

1. 2. Tổng quan về kỹ thuật giấu tin

1. 2. 1. Sơ lược về lịch sử giấu tin

Ý tưởng về che giấu thông tin đã có từ hàng nghìn năm về trước nhưng kĩ thuật này được dùng chủ yếu trong quân đội và trong các cơ quan tình báo. Mãi cho tới vài thập niên gần đây, giấu thông tin mới nhận được sự quan tâm của các nhà nghiên cứu và các viện công nghệ thông tin với rất nhiều công trình nghiên cứu. Cuộc cách mạng số hóa thông tin và sự phát triển nhanh chóng của mạng truyền thông là nguyên nhân chính dẫn đến sự thay đổi này. Những phiên bản sao chép hoàn hảo, các kĩ thuật thay thế, sửa đổi tinh vi cộng với sự lưu thông trên mạng của các dữ liệu đa phương tiện đã sinh ra rất nhiều những vấn đề nhức nhối về nạn ăn cắp bản quyền, phân phối bất hợp pháp, xuyên tạc trái phép… đây là lúc công nghệ giấu tin được chú ý và phát triển.

1. 2. 2. Khái niệm giấu tin

"Giấu tin" là một kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác. Kỹ thuật giấu tin nhằm hai mục đích: một là bảo mật cho dữ liệu được đem giấu, hai là bảo vệ cho chính đối tượng mang tin giấu. Hai mục đích khác nhau này dẫn đến hai kỹ thuật chủ yếu của giấu tin. Đó là giấu tin mật (Steganography) và thủy vân số (Watermarking).

- Kỹ thuật giấu tin mật (Steganography): Với mục đích đảm bảo an toàn và bảo mật thông tin được giấu. Các kỹ thuật giấu tin mật tập trung vào việc sao cho thông tin giấu được nhiều và người khác khó phát hiện ra thông tin có được giấu trong hay không.
- Kỹ thuật thủy vân số (Watermarking): Với mục đích bảo mật cho chính các đối tượng giấu tin. Đảm bảo một số các yêu cầu như: tính bền vững, khẳng định bản quyền sở hữu hay phát hiện xuyên tạc thông tin…

Nói chung giấu tin trong đa phương tiện là tận dụng "độ dư thừa" của phương tiện giấu để thực hiện việc giấu tin mà người ngoài cuộc "khó" cảm nhận được có thông tin giấu trong đó.

1. 2. 3. Môi trường giấu tin

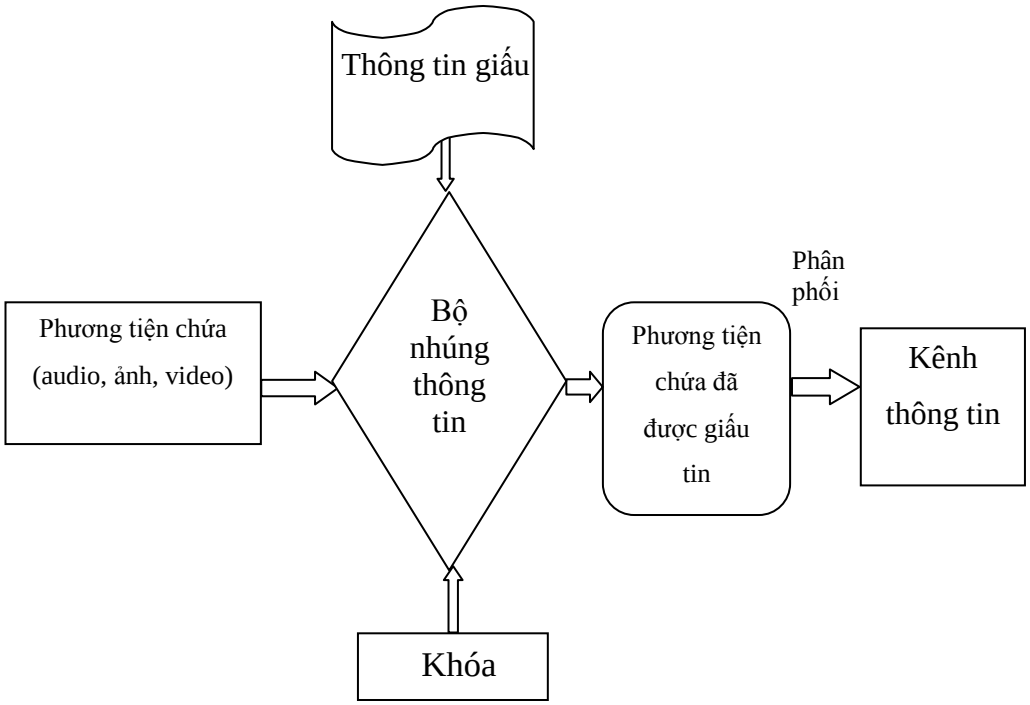
Bao gồm giấu tin trong ảnh, trong audio, trong video, trong văn bản dạng text… Hiện nay, giấu tin trong ảnh chiếm tỉ lệ lớn nhất hệ thống giấu tin trong đa phương tiện.

1. 2. 4. Mô hình kỹ thuật giấu thông tin cơ bản

Để thực hiện giấu tin cần xây dựng được các thủ tục giấu tin. Các thủ tục này sẽ thực hiện nhúng thông tin cần giấu vào môi trường giấu tin. Các thủ tục giấu tin thường được thực hiện với một khóa giống như các hệ mật mã để tăng tính bảo mật. Sau khi giấu tin ta thu được đối tượng chứa thông tin giấu và có thể phân phối đối tượng đó trên kênh thông tin.

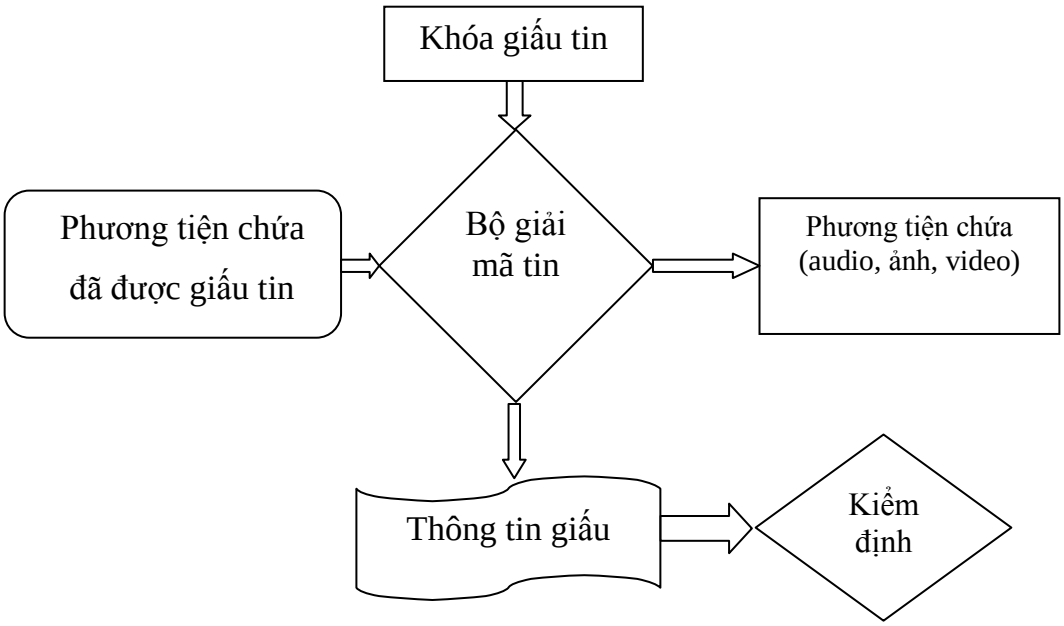
Giấu thông tin vào phương tiện chứa và tách lấy thông tin là hai quá trình trái ngược nhau và có thể mô tả qua sơ đồ khối của hệ thống trong đó:

- Thông tin cần giấu tuỳ theo mục đích của người sử dụng, nó có thể là thông điệp (với các tin bí mật) hay các logo, hình ảnh bản quyền.
- Phương tiện chứa: các file ảnh, text, audio… là môi trường để nhúng tin.
- Bộ nhúng thông tin: là những chương trình thực hiện việc giấu tin.
- Đầu ra: là các phương tiện chứa đã có tin giấu trong đó.



Hình 1.4. Lược đồ chung cho quá trình giấu tin

Tách thông tin từ các phương tiện chứa diễn ra theo quy trình ngược lại với đầu ra là các thông tin đã được giấu vào phương tiện chứa. Phương tiện chứa sau khi tách lấy thông tin có thể được sử dụng, quản lý theo những yêu cầu khác nhau.



Hình 1.5. Lược đồ chung cho quá trình giải mã

Sau khi nhận được đối tượng phương tiện chứa có giấu thông tin, quá trình giải mã được thực hiện thông qua một bộ giải mã tương ứng với bộ nhúng thông tin cùng với khoá của quá trình nhúng. Kết quả thu được gồm phương tiện chứa gốc và thông tin đã giấu. Bước tiếp theo thông tin đã giấu sẽ được xử lý kiểm định so sánh với thông tin ban đầu.

1. 2. 5. Các phương pháp giấu tin

➢ Các phương pháp giấu tin trong ảnh hiện nay đều thuộc vào một trong ba nhóm:

- Giấu tin trong miền quan sát: Ý tưởng chính của phương pháp này là lấy từng bit của tin mật rải nó lên ảnh vỏ bọc, thay đổi bit có trọng số thấp của ảnh bằng các bit của tin mật để ít ảnh hưởng đến chất lượng ảnh, và mắt người khó cảm nhận được sự thay đổi của ảnh đã giấu tin.
- Các phương pháp dựa vào kỹ thuật biến đổi ảnh, ví dụ biến đổi từ miền không gian sang miền tần số.
- Các phương pháp sử dụng mặt nạ che giấu.

➢ Nếu phân chia các phương pháp theo định dạng ảnh thì có hai nhóm chính:

- Nhóm phương pháp phụ thuộc định dạng ảnh.
- Nhóm phương pháp độc lập với định dạng ảnh.

Các phương pháp nhóm thứ hai có nhiều ưu điểm hơn về tính bền vững, nhưng lượng thông tin giấu được sẽ ít hơn và cài đặt cũng sẽ phức tạp hơn.

➢ Nếu phân chia các phương pháp theo đặc điểm kỹ thuật có:

- Phương pháp thay thế.
- Phương pháp xử lý tín hiệu.
- Các phương pháp mã hóa: Lượng hóa; Mã hóa sửa lỗi.
- Các phương pháp thống kê – kiểm thử giải thuyết.
- Phương pháp sinh mặt nạ.

1. 2. 6. Đặc trưng và tính chất của kỹ thuật giấu tin trong ảnh

Khi giấu thông tin trong ảnh, thông tin sẽ được giấu cùng với dữ liệu ảnh nhưng chất lượng ảnh ít thay đổi và gần như khi nhìn bình thường vào ảnh đó chúng ta không thể phát hiện ra rằng đằng sau ảnh là khối thông tin được ẩn trong đó. Và một đặc điểm của giấu thông tin trong ảnh đó là thông tin được giấu một cách vô hình, nó là một cách truyền thông tin mật cho nhau mà người khác không thể biết được bởi sau khi giấu thông tin thì chất lượng ảnh gần như không thay đổi.

Kỹ thuật giấu tin trong ảnh thường chú ý những đặc trưng và các tính chất cơ bản sau đây:

➢ Phương tiện có chứa dữ liệu tri giác tĩnh: Dữ liệu gốc ở đây là dữ liệu tĩnh, dù đã giấu thông tin vào trong ảnh hay chưa thì khi ta xem ảnh bằng thị giác, dữ liệu ảnh không thay đổi theo thời gian, điều này khác với dữ liệu âm thanh và dữ liệu băng hình vì khi ta nghe hay xem thì dữ liệu gốc sẽ thay đổi liên tục với tri giác của con người theo các đoạn, các bài hay các cảnh…

➢ Kỹ thuật giấu phụ thuộc ảnh: Kỹ thuật giấu tin khác nhau tùy theo các loại ảnh khác nhau (ảnh đen trắng, ảnh xám, ảnh màu).

➢ Kỹ thuật giấu tin lợi dụng tính chất hệ thống thị giác của con người: Dữ liệu ảnh được quan sát bằng hệ thống thị giác của con người nên các kỹ thuật giấu tin phải đảm bảo một yêu cầu cơ bản là những thay đổi trên ảnh phải rất nhỏ sao cho

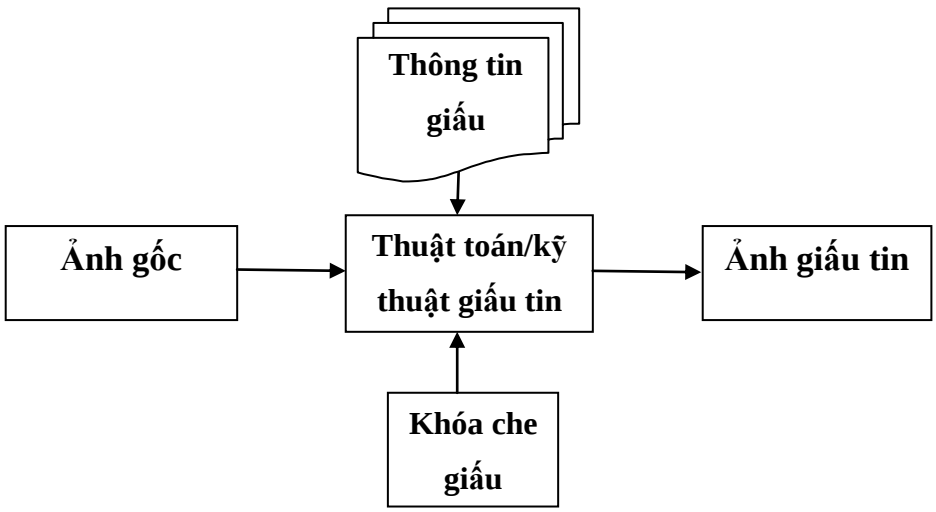
bằng mắt thường khó nhận thấy được sự thay đổi đó vì có như thế thì mới đảm bảo cho được độ an toàn cho thông tin giấu.

- Giấu tin trong ảnh tác động lên dữ liệu ảnh nhưng không thay đổi kích thước ảnh: Các thuật toán thực hiện việc giấu thông tin sẽ được thực hiện trên dữ liệu của ảnh. Dữ liệu ảnh bao gồm phần header, bảng màu (có thể có) và dữ liệu ảnh. Do vậy mà kích thước ảnh trước hay sau khi giấu thông tin là như nhau.
- Đảm bảo chất lượng sau khi giấu tin: Đây là một yêu cầu quan trọng đối với giấu tin trong ảnh. Sau khi giấu tin bên trong, ảnh phải đảm bảo được yêu cầu không bị biến đổi để có thể bị phát hiện dễ dàng so với ảnh gốc.
- Thông tin trong ảnh sẽ bị biến đổi nếu có bất cứ biến đổi nào trên ảnh: Vì phương pháp giấu thông tin trong ảnh dựa trên việc điều chỉnh các giá trị của các bit theo một quy tắc nào đó và khi giải mã theo các giá trị đó để tìm được thông tin giấu. Theo đó, nếu một phép biến đổi nào đó trên ảnh làm thay đổi giá trị của các bit thì sẽ làm cho thông tin giấu bị sai lệch. Nhờ đặc điểm này mà giấu thông tin trong ảnh có tác dụng nhận biết và phát hiện xuyên tạc thông tin.
- Vai trò của ảnh gốc khi giải tin: Các kỹ thuật giấu tin phải xác định rõ ràng quá trình lọc ảnh để lấy thông tin giấu cần đến ảnh gốc hay không cần.

1. 2. 7. Mô hình kỹ thuật giấu tin trong ảnh cơ bản

Kỹ thuật giấu tin trong ảnh bao gồm hai quá trình đó là:

- Quá trình 1: Giấu tin vào ảnh



Hình 1.6. Mô hình cơ bản giấu tin

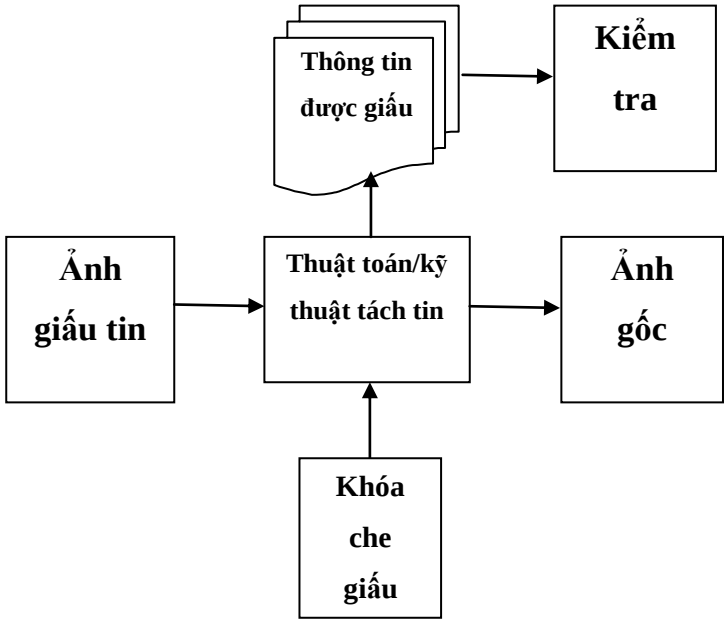
Đầu vào:

- Thông tin giấu: Tùy theo mục đích của người sử dụng mà giấu thông tin ở đây có thể là thông điệp, hình ảnh, video, âm thanh…
- Ảnh gốc: là ảnh được chọn làm môi trường để giấu tin.

Đầu ra:

- Ảnh đã giấu được tin.

➢ Quá trình 2: Tách tin từ ảnh giấu tin



Hình 1.7. Mô hình cơ bản tách tin

Đầu vào:

- Ảnh giấu tin.
- Khóa che giấu.

Đầu ra:

- Thông tin được che giấu.
- Ảnh đã tách tin.

Quá trình giải mã được thực hiện thông qua thuật toán/kỹ thuật tách tin tương ứng với thuật toán/kỹ thuật giấu tin cùng với khóa che giấu của quá trình nhúng. Kết quả thu được gồm ảnh đã tách tin và thông tin đã giấu. Thông tin đã giấu được kiểm tra so sánh với thông tin ban đầu.

1. 2. 8. Các yêu cầu đối với giấu tin trong ảnh

- 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: Chỉ có bên nhận được cấp một khóa và bằng các kỹ thuật tách ảnh phù hợp mới có thể lấy được tin trong ảnh.

1. 3. Đánh giá chất lượng ảnh sau khi giấu tin PSNR

Để đánh giá chất lượng của bức ảnh (hay khung ảnh video) ở đầu ra của bộ mã hoá, người ta thường sử dụng hai tham số: Sai số bình phương trung bình – MSE (mean square error) và phương pháp đề xuất với hệ số tỷ lệ tín hiệu/tín hiệu tạp PSNR (Peak Signal to Noise Ratio).

MSE giữa ảnh gốc và ảnh khôi phục được tính như sau:

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - y_{ij})^2$$

Ở đây: x_{ij} biểu thị giá trị điểm ảnh gốc, và y_{ij} biểu thị giá trị điểm ảnh đã được biến đổi, m và n lần lượt là chiều rộng và chiều cao của ảnh.

PSNR, đơn vị: deciben (dB), thường được sử dụng trong nghiên cứu xử lý hình ảnh: $\mathrm{PSNR} = 10*\log10(\frac{255^2}{\mathrm{MSE}})$

Thông thường, nếu PSNR ≥ 37 dB thì hệ thống mắt người gần như không phân biệt được giữa ảnh gốc và ảnh khôi phục. PSNR càng cao thì chất lượng ảnh khôi phục càng tốt. Khi hai hình ảnh giống hệt nhau, MSE sẽ bằng 0 và PSNR đi đến vô hạn.

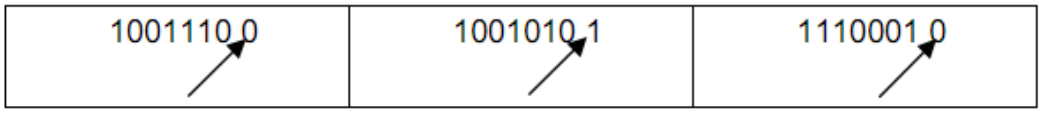
Chương 2. KỸ THUẬT GIẤU TIN TRÊN K BIT LSB CỦA ẢNH

2. 1. Bit ít quan trọng LSB (Least Signification Bit)

Ý tưởng cơ bản của kỹ thuật này là tiến hành giấu tin vào vị trí các bit ít quan trọng LSB đối với mỗi phần tử trong bảng màu.

Đây là phương pháp giấu tin đơn giản nhất, thông điệp dưới dạng nhị phân sẽ được giấu (nhúng) vào các bit LSB – là bit có ảnh hưởng ít nhất tới việc quyết định tới màu sắc của mỗi điểm ảnh. Vì vậy khi ta thay đổi bit ít quan trọng của một điểm ảnh thì màu sắc của mỗi điểm ảnh mới sẽ tương đối gần với điểm ảnh cũ. Ví dụ đối với ảnh 16 bit thì 15 bit là biểu diễn 3 màu RGB của điểm ảnh còn bit cuối cùng không dùng đến thì ta sẽ tách bit này ra ở mỗi điểm ảnh để giấu tin…

Ví dụ: Tách bit cuối cùng trong 8 bit biểu diễn mỗi điểm ảnh của ảnh 256 màu.



Hình 2.1. Mỗi điểm ảnh bểu diễn bởi 8 bit bit cuối cùng được coi là bit ít quan trọng nhất tức là bit bên phải nhất

Trong phép tách này ta coi bit cuối cùng là bit ít quan trọng nhất, thay đổi giá trị của bit này thì sẽ thay đổi giá trị của điểm ảnh lên hoặc xuống đúng một đơn vị, với sự thay đổi nhỏ đó ta hi vọng là cấp độ màu của điểm ảnh sẽ không bị thay đổi nhiều.

Bảng 2.1. Ví dụ giấu chữ A (mã ASCII là 65 hay 01000001) vào trong 8 byte của file gốc

8 byte ban đầu	Byte cần giấu (A)	8 byte sau khi giấu
01001001	0	01001000
11010111	1	11010111
11001100	0	11001100
10110101	0	10110100
00100100	0	00100100

00100101	0	00100100
00100000	0	00100000
00001010	1	00001011

2. 2. Phương pháp giấu tin trên k-LSBs cổ điển

2. 2. 1. Mô tả phương pháp giấu tin trên k-LSBs đơn giản (cổ điển)

Với C là ảnh nguyên bản 8-bit màu xám, kích thước $M_c \times N_c$ điểm ảnh, có dạng:

$$C = \{x_{ij} | 0 \leq i \leq M_c, 0 \leq j \leq N_c, x_{ij} = \{0, 1, 2, \ldots, 255\}\}$$

và M là thông điệp dài n bit biểu diễn dưới dạng:

$$M = \{m_i \mid 0 \leq i < n, m_i \in \{0,1\}\}$$

Giả sử rằng n-bit thông điệp bí mật M được nhúng vào k bit LSB ngoài cùng bên phải của ảnh gốc C. Trước tiên, thông điệp bí mật M được sắp xếp lại để tạo thành một hình ảnh ảo k-bit, biểu diễn M dưới dạng:

$$M' = \{m_i' | 0 \leq i < n', m_i' \in \{0, 1, \ldots, 2^k - 1\}\}$$

Với $n' = M_c \times N_c$. Việc ánh xạ giữa các n-bit thông điệp bí mật $M = \{m_i\}$ và thông điệp nhúng $M' = \{m_i'\}$ có thể được định nghĩa như sau:

$$mi' = \sum_{j=0}^{K-1} m_i \times k + j \times 2^{k-1-j}$$

Thứ hai, tập hợp con n' điểm ảnh $\{x_1, x_2, \ldots, x_n\}$ được chọn từ ảnh gốc C trong 1 chuỗi hành động liên tiếp nhau. Tiến trình nhúng hoàn tất bằng việc thay thế k-LSBs của x_i bởi m_i'. Theo toán học, một giá trị x_i của điểm ảnh được lựa chọn để lưu trữ k-bit thông điệp m_i' được thay đổi khớp với điểm ảnh đã giấu tin x'_i như sau:

$$X'_i = x_i - x_i \bmod 2^k + m'_i$$

Trong tiến trình tách, với ảnh đã giấu tin S, thông điệp nhúng có thể được tách ra mà không đề cập đến ảnh gốc. Sử dụng cùng một trình tự như trong quá trình nhúng, tập hợp các điểm ảnh $\{x'_1, x'_2, \ldots, x'_n, \}$ lưu trữ các bit thông điệp bí

mật được lựa chọn từ ảnh đã giấu tin. K-LSBs của các điểm ảnh được tách ra và nối lại để tái tạo lại thông điệp bí mật. Trong toán học, việc nhúng thông điệp bit m_i có thể được khôi phục bằng:

$$m'_i = x'_i \bmod 2^k$$

2. 2. 2. Tiền xử lý thuật toán giấu và tách tin LSB cổ điển

- Để có thể thực hiện tốt chương trình, trước hết cần bổ sung một số hàm thành phần với mục đích cài đặt chương trình thuận lợi:
  - Hàm chuyển đổi từ chuỗi kí tự sang số nhị phân.
  - Hàm chuyển đổi từ chuỗi số nhị phân sang chuỗi kí tự.
- Tóm tắt thuật toán thay thế LSB đơn giản:

2. 2. 2. 1. Thuật toán giấu

Đầu vào:

- Ảnh gốc cấp xám.
- Thông điệp bí mật.
- Số bit LSB cần mã hóa (2 hoặc 4 bit).

Đầu ra:

- Ảnh mang tin.

Các bước thực hiện:

- Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với m x n phần tử, rồi chuyển ma trận ảnh về mảng 1 chiều I với i phần tử, chuyển các điểm ảnh về dạng nhị phân.
- Bước 2: Biểu diễn thông điệp dưới dạng số nhị phân.
- Bước 3: Cứ 8 bit ảnh tách bỏ số bit LSB ngoài cùng bên phải và ghép phần còn lại với 2 bit nhị phân đầu của thông điệp, kết quả thu được đưa về dạng thập phân rồi gán ngược lại vào I(i).
- Bước 4: Thực hiện lại bước 3 cho đến khi lấy hết các bit của chuỗi nhị phân thông điệp ghép với các bit ảnh. Chuyển đổi ảnh I từ mảng một chiều về mảng 2 chiều m x n phần tử. Được ảnh mới đã giấu tin.

2. 2. 2. 2. Thuật toán tách

Đầu vào:

- Ảnh mang tin.

Đầu ra:

- Ảnh đã tách tin.
- Thông điệp mật.

Các bước thực hiện:

- Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với m x n phần tử. Chuyển đổi ma trận ảnh m x n phần tử về mảng 1 chiều I với i phần tử.
- Bước 2: Chuyển các bit ảnh về dạng nhị phân, cứ 8 bit ảnh tách lấy 2 bit ngoài cùng bên phải. Đem ghép các kết quả này lại với nhau.
- Bước 3: Kết quả thu được sử dụng hàm chuyển đổi từ chuỗi số nhị phân về chuỗi kí tự. Sau khi lặp lại quá trình trên số lần bằng số lần duyệt, ta thu được nội dung thông điệp.

❖ Với trường hợp giấu trên 4 bit thông điệp làm tương tự, nhưng tách lấy 4 bit nhị phân đầu của ảnh ghép với 4 bit nhị phân thông điệp.

2. 3. Phương pháp giấu tin trên k-LSBs nâng cao

- Tác giả: Marghny Mohamed, Fadwa Al-Afari và Mohamed Bamatraf.
- Tài liệu sử dụng: Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation (Giấu tin bằng phương pháp thay thế LSB sử dụng khóa hoán vị di truyền tối ưu), Tạp chí Quốc tế Ả Rập Điện tử - Công nghệ, Vol. 2, số 1, tháng 1 năm 2011.

2. 3. 1. Mô tả phương pháp giấu tin trên k-LSBs nâng cao (sử dụng khóa hoán vị)

Đây là phương pháp tối ưu khi k là rất lớn. Những hình ảnh C, và thông điệp bí mật M sẽ được sắp xếp lại hình thành các khối bit (blk) C" và M" tương ứng.

$$C'' = \{c''_i \mid 0 \leq i \leq 2^{blk}-1 | c_i'' \epsilon \{0, 1, 2, \dots, 2^{blk}-1\}\}$$

$$M'' = \{m''_i | 0 \leq i \leq 2^{blk}-1 \mid m''_i \epsilon \{0, 1, 2, \ldots, 2^{blk}-1\}\}$$

Theo toán học, quá trình mã khối sẽ được lấy bằng cách thực hiện trên bit XOR điều hành mỗi khối C'' và M'' như sau:

if ($cipher_i = c''_i$ xor m''_i, $1 \leq i \leq length(M)$ in blk (M_{blk}))

cipher = $\{cipher | 1 \leq i \leq length(M'')$ in blk $| cipher_i = \{0, 1, 2, \ldots, 2^{blk}-1\}\}$

$cipher_i = \{0, 1, 2, \ldots, 2^{blk}-1\}\}$

$i = c''_i$ xor m''_i

end

2. 3. 2. Tiền xử lý thuật toán giấu và tách tin LSB nâng cao

- Để có thể thực hiện tốt chương trình, trước hết cần bổ sung một số hàm thành phần với mục đích cài đặt chương trình thuận lợi:
  - Hàm mã hóa thông điệp.
  - Hàm giải mã thông điệp.
  - Với phương pháp giấu và tách tin nâng cao có quy đổi ta sử dụng bảng sau để quy đổi:

Bảng 2.2. Bảng quy đổi

STT	Kí tự	Mã quy đổi	STT	Kí tự	Mã quy đổi
1	A, a	000001	20	T, t	010100
2	B, b	000010	21	U, u	010101
3	C, c	000011	22	V, v	010110
4	D, d	000100	23	W, w	010111
5	E, e	000101	24	X, x	011000
6	F, f	000110	25	Y, y	011001
7	G, g	000111	26	Z, z	011010
8	H, h	001000	27	0	011011
9	I, i	001001	28	1	011100
10	J, j	001010	29	2	011101
11	K, k	001011	30	3	011110
12	L, l	001100	31	4	011111
13	M, m	001101	32	5	100000
14	N, n	001110	33	6	100001
15	O, o	001111	34	7	100010
16	P, p	010000	35	8	100011
17	Q, q	010001	36	9	100100
18	R, r	010010	37	‘ ‘	100101
19	S, s	010011			

- Tóm tắt thuật toán thay thế k bit LSB nâng cao:

Trường hợp không quy đổi thông điệp:

2. 3. 2. 1. Thuật toán giấu

Đầu vào:

- Ảnh gốc cấp xám.
- Thông điệp bí mật.
- Khóa (8 bit).
- Số bit LSB cần mã hóa trên mỗi điểm ảnh (2 hoặc 4 bit).

Đầu ra:

- Ảnh mang tin.
- Khóa.
- Số bit thông điệp cần mã hóa.

Các bước thực hiện:

- Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với m x n phần tử. Chuyển đổi ma trận ảnh m x n phần tử về mảng 1 chiều I với i phần tử.
- Bước 2: Biểu diễn thông tin giấu dưới dạng chuỗi nhị phân.
- Bước 3: Sử dụng một khóa 8 bit bất kỳ (khóa là kí tự, chuyển khóa về dạng mảng như với thông điệp) đem mã hóa với chuỗi thông điệp bí mật bằng phép XOR: cứ 8 bit khóa đem XOR với 8 bit đầu vào của thông điệp. Thực hiện lại bước này cho đến khi nội dung thông điệp được mã hóa hết.
- Bước 4: Thông điệp đã mã hóa đem giấu vào ảnh tương tự như phương pháp thay thế k bit LSB cổ điển: Là tách lấy 6 bit đầu của bit ảnh đem ghép với 2 bit đầu trong thông điệp rồi chuyển về dạng thập phân và gán ngược lại vào ảnh.
- Bước 5: Thực hiện bước 4 cho đến khi lấy hết các bit của chuỗi nhị phân thông điệp để ghép với các bit ảnh. Chuyển đổi ảnh I từ mảng một chiều về mảng 2 chiều m x n phần tử, được ảnh mới đã giấu tin.

2. 3. 2. 2. Thuật toán tách

Đầu vào:

- Ảnh đã giấu tin.
- Khóa (8 bit).
- Số lần duyệt.
- Số bit thông điệp cần mã hóa.

Đầu ra:

- Ảnh đã tách tin.
- Thông điệp.

Các bước thực hiện:

- Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với m x n phần tử. Chuyển đổi ma trận ảnh m x n phần tử về mảng 1 chiều I với i phần tử.
- Bước 2: Chuyển các bit ảnh về dạng nhị phân, cứ 8 bit ảnh tách lấy 2 bit ngoài cùng bên phải. Đem ghép các kết quả này lại với nhau.
- Bước 3: Kết quả thu được sử dụng hàm chuyển đổi từ chuỗi số nhị phân về chuỗi kí tự. Sau khi lặp lại quá trình trên số lần bằng số lần duyệt, ta thu được nội dung thông điệp đã mã hóa.
- Bước 4: Sử dụng hàm giải mã thực hiện giải mã thông điệp bằng khóa 8 bit, ta thu được kết quả là nội dung gốc của thông điệp.

❖ Trường hợp chuyển đổi thông điệp về bảng mã đã được quy ước sẵn: Tương tự như trường hợp chuyển đổi kí tự về mã nhị phân của nó, nhưng ở đây khi giấu tin ta sử dụng bảng quy đổi các kí tự và chữ số theo một chuẩn do người lập trình tự định nghĩa. Đến bước tách ta lại quy đổi ngược lại về dạng kí tự và số ban đầu.

2. 4. Ví dụ minh họa

2. 4. 1. Trường hợp giấu và tách tin LSB cổ điển

2. 4. 1. 1. Giấu tin

Giả sử ta có 4 điểm ảnh đầu tiên như sau:

123 197 213 255

Chuyển các điểm ảnh về dạng nhị phân:

01111011 11000101 11010101 11111111

Thông điệp bí mật: chữ ‘a’ có mã ASCII là 97, biểu diễn dưới dạng nhị phân như sau: **01100001**

Cứ 8 bit ảnh, ta lấy 6 bit đầu của điểm ảnh (từ vị trí I_0 đến I_5) ghép với 2 bit thông điệp (từ vị trí a_0 đến a_1) sẽ được:

01111001 11000110 11010100 11111101

2. 4. 1. 2. Tách tin

Lấy 2 bit ngoài cùng bên phải trong mỗi điểm ảnh mới:

011110-01 110001-10 110101-00 111111-01

Ghép lại với nhau được chuỗi nhị phân thông điệp, chính là chữ ‘a’:

0110001

2. 4. 2. Trường hợp giấu và tách tin LSB nâng cao

2. 4. 2. 1. Giấu tin

Giả sử ta có 4 điểm ảnh đầu tiên như sau:

123 197 213 255

Chuyển các điểm ảnh về dạng nhị phân:

01111011 11000101 11010101 11111111

Thông điệp bí mật: chữ ‘a’ có mã ASCII là 97, biểu diễn dưới dạng nhị phân:

01100001

Nhập khóa, cũng là 1 kí tự 8 bit, giả sử là chữ ‘b’, có dạng nhị phân như sau:

01100010

Mã hóa thông điệp chính là dùng phép XOR(a, b) sẽ được:

00000011

Cứ 8 bit ảnh, ta lấy 6 bit đầu của điểm ảnh ghép với 2 bit thông điệp đã mã hóa sẽ được:

01111000 11000100 11010100 11111111

2. 4. 2. 2. Tách tin

Lấy 2 bit ngoài cùng bên phải trong mỗi điểm ảnh mới:

011110-00 110001-00 110101-00 111111-11

Ghép lại với nhau được chuỗi nhị phân thông điệp nhưng đã bị mã hóa:

00000011

Sử dụng hàm mã hóa để lấy lại thông điệp gốc M, bằng cách XOR(M, b) ta được nhị phân của chữ ‘a’: **01100001**

- Trường hợp giấu và tách tin LSB nâng cao có quy đổi, tương tự như trên nhưng không chuyển chữ ‘a’ về dạng nhị phân mà a =>**000001**.

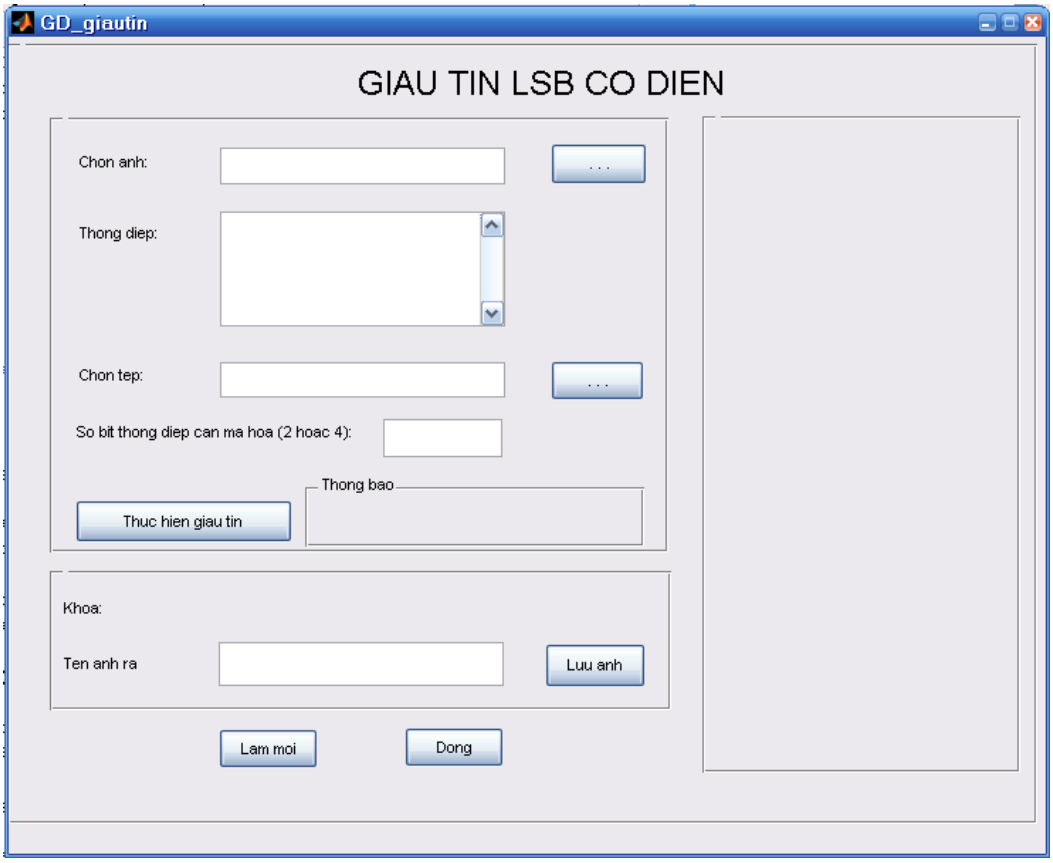
Chương 3. CÀI ĐẶT VÀ THỬ NGHIỆM

3. 1. Môi trường cài đặt

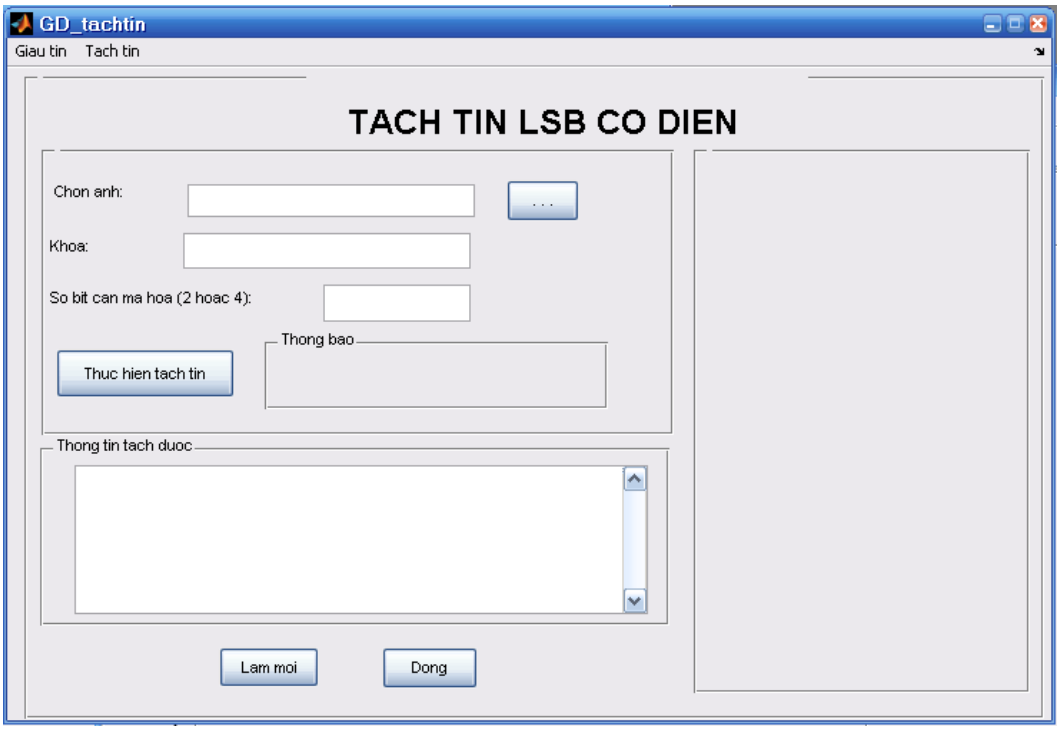
- Ngôn ngữ cài đặt, môi trường soạn thảo và chạy chương trình được thực hiện trên ngôn ngữ lập trình Matlap 2007b.
- Hệ điều hành Window XP và môi trường Net FrameWork 2.0.

Một số giao diện của chương trình:

Hình 3.1. Giao diện chính của chương trình

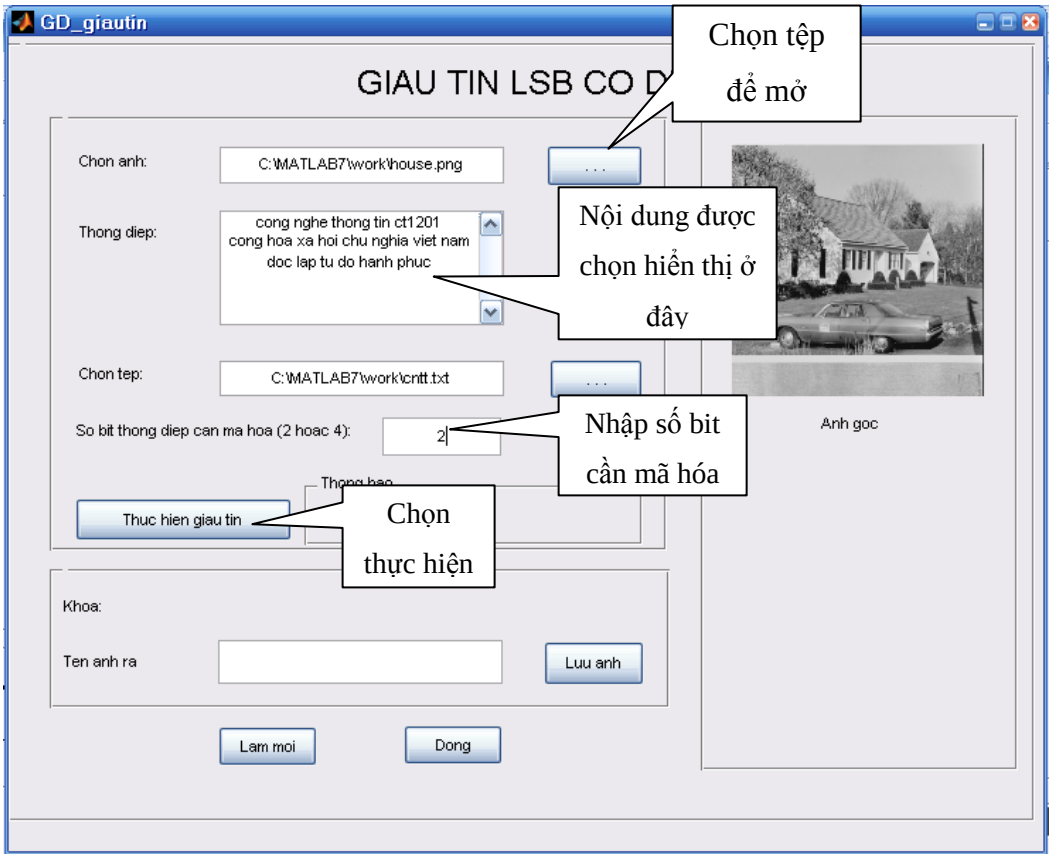


Hình 3.2. Giao diện giấu tin LSB cổ điển



Hình 3.3. Giao diện tách tin LSB cổ điển

➢ Quy trình giấu tin:



Hình 3.4. Giao diện trước khi giấu tin

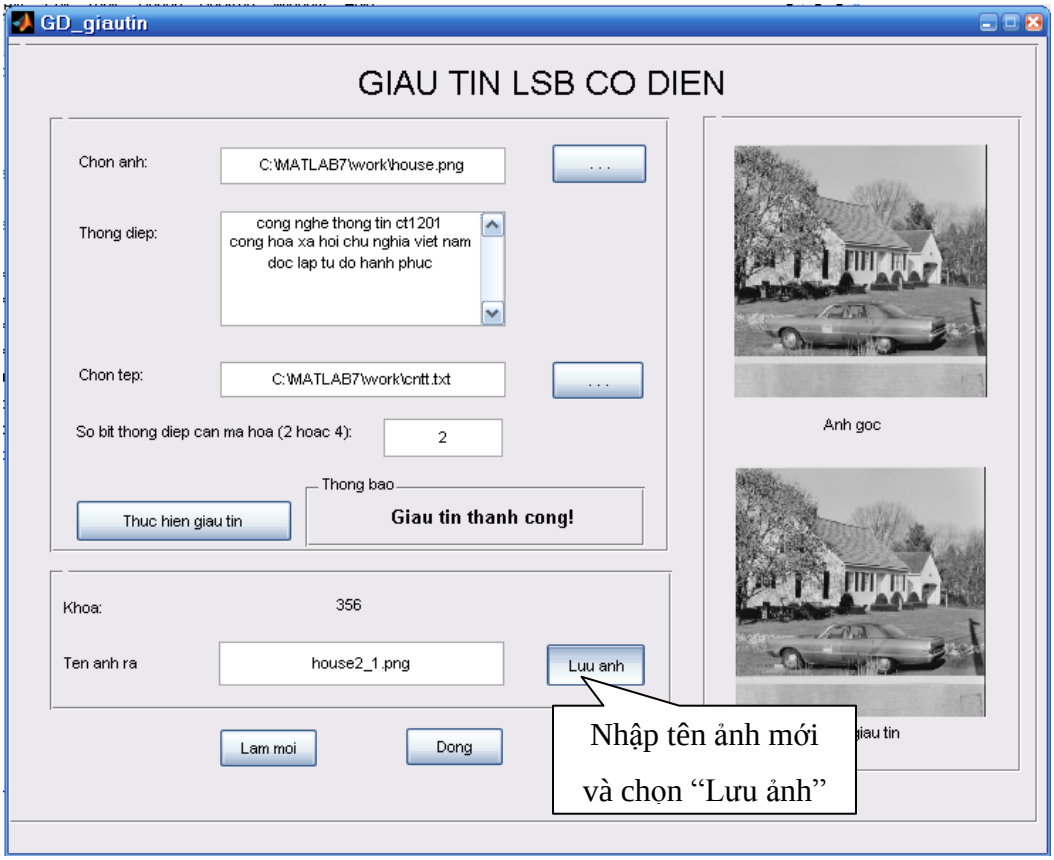
➢ Trước khi giấu tin: yêu cầu nhập những thông tin cần thiết

- Chọn ảnh gốc cấp xám từ tệp ảnh có sẵn.
- Chọn văn bản muốn giấu tin (dạng text).
- Nhập số bit thông điệp cần mã hóa (ở đây có 2 trường hợp 2 hoặc 4 bit).

+ Nếu chọn 2 bit: mỗi lần thực hiện giấu sẽ lấy 2 bit của thông điệp ghép với 6 bit ảnh.

+ Nếu chọn 4 bit: mỗi lần thực hiện giấu sẽ lấy 4 bit của thông điệp ghép với 4 bit ảnh.

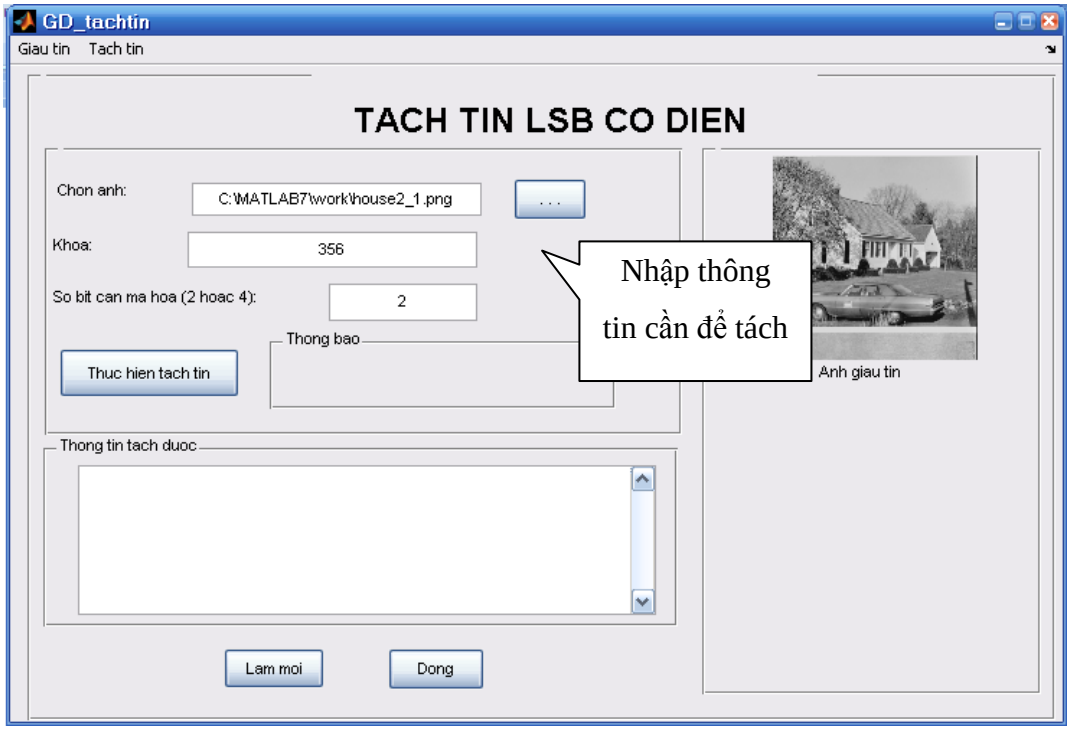
➢ Sau đó chọn "*Thực hiện giấu tin*" để chương trình tiến hành giấu tin.



Hình 3.5. Kết quả thu được sau khi thực hiện giấu tin

- Sau khi thực hiện giấu tin thành công, đầu ra sẽ bao gồm:
  - Thông báo "*Giấu tin thành công!*".
  - Khóa.
  - Ảnh đã giấu tin.
  - Nhập tên ảnh mới đã mang tin vào mục "*Tên ảnh ra"* (tên ảnh có phần mở rộng).
  - Sau đó chọn "*Lưu ảnh"* để lưu lại.
- Nếu thực hiện giấu không thành công thì có thể do những vấn đề sau:
  - Nhập thiếu dữ liệu đầu vào như: Tên ảnh vào, thông điệp cần giấu, số bit cần mã hóa thông điệp. Khi đó chương trình sẽ thông báo để người sử dụng có thể khắc phục.

➢ Quy trình tách tin:

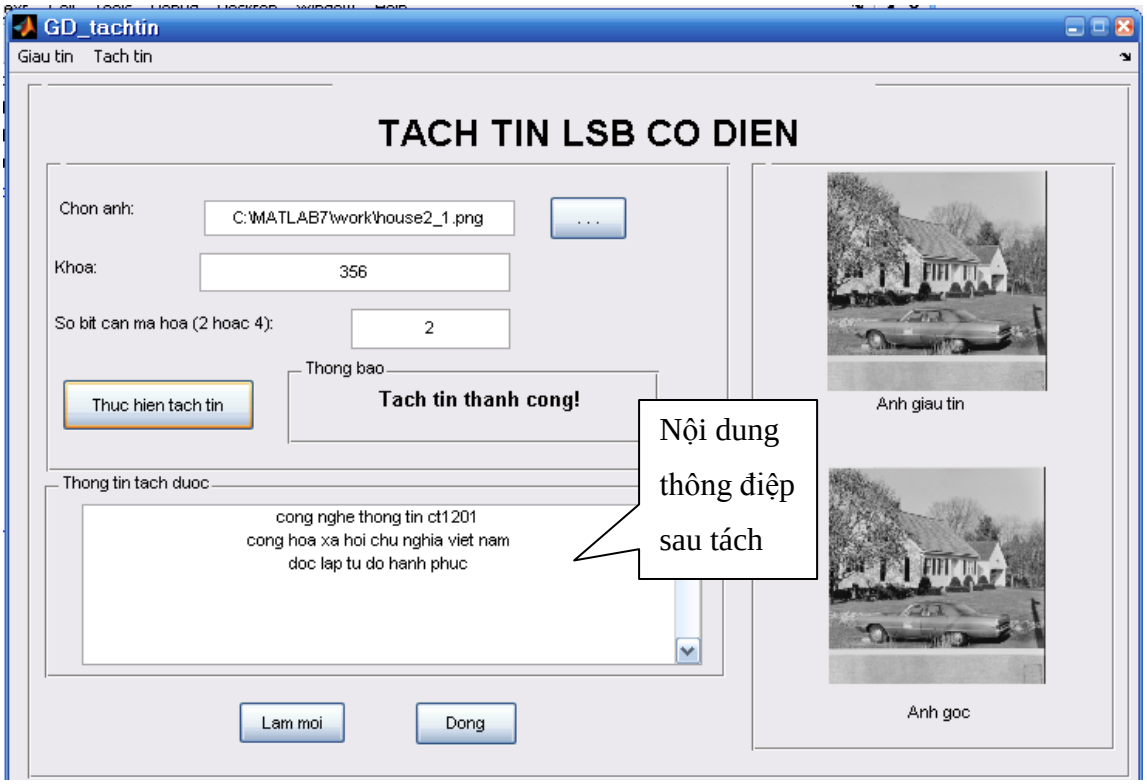


Hình 3.6. Nhập thông tin trước khi tách

➢ Trước khi thực hiện tách ảnh đã mang tin để lấy được thông điệp bí mật yêu cầu nhập những dữ liệu sau:

- Chọn ảnh đã mang tin cần tách từ vị trí đã lưu trước đó.
- Nhập khóa thu được từ kết quả đầu ra trong quá trình giấu.
- Nhập số bit cần mã hóa thu được từ kết quả đầu ra trong quá trình giấu.

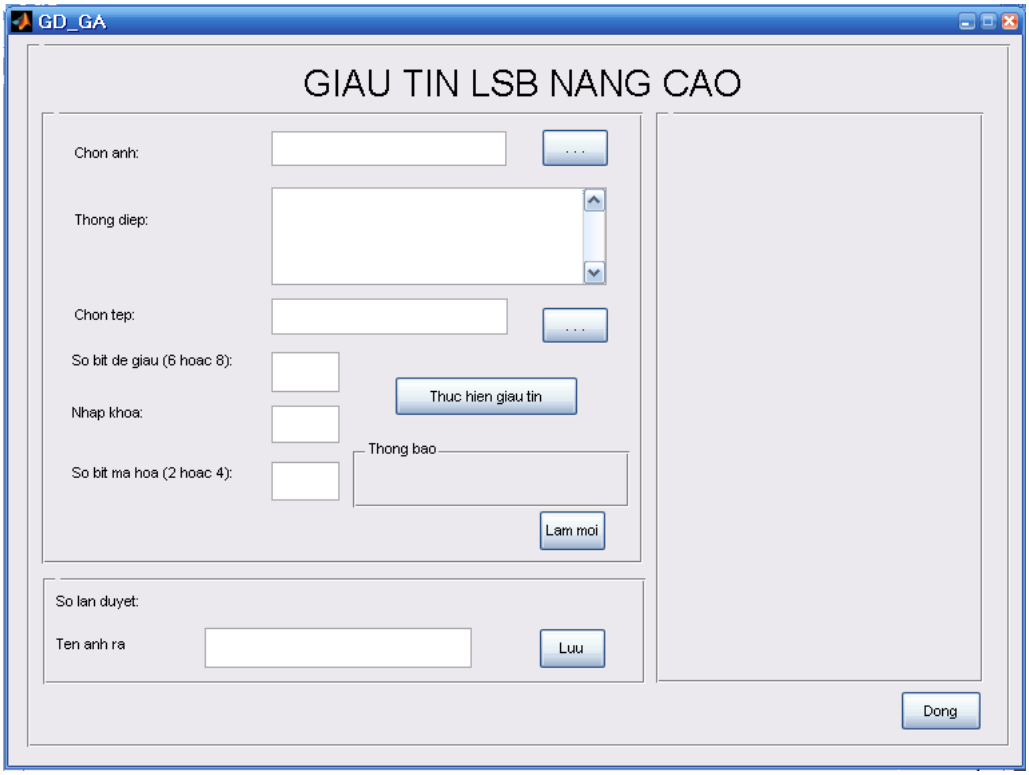
➢ Chọn "*Thực hiện tách tin"* để tiến hành tách tin khỏi ảnh.



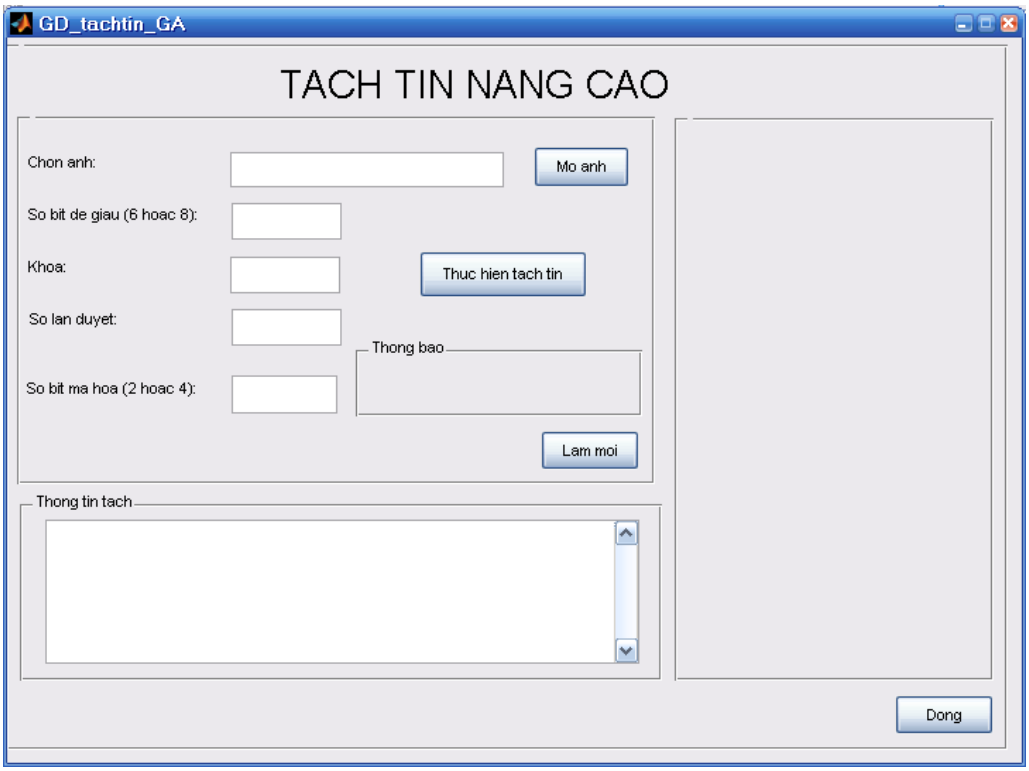
Hình 3.7. Kết quả thu được sau khi tách tin

- Sau khi thực hiện tách tin thành công, đầu ra của chương trình sẽ bao gồm:
  - Nội dung thông điệp bí mật trước khi giấu vào ảnh.
  - Ảnh sau khi đã tách thông điệp bí mật.
- Nếu tách tin không thành công thì có thể do những lỗi sau:
  - Do chọn sai ảnh đã mang tin.
  - Do nhập sai khóa.
  - Do nhập sai số bit cần mã hóa.

Khi đó phải kiểm tra lại những lý do trên để thu được kết quả đúng.

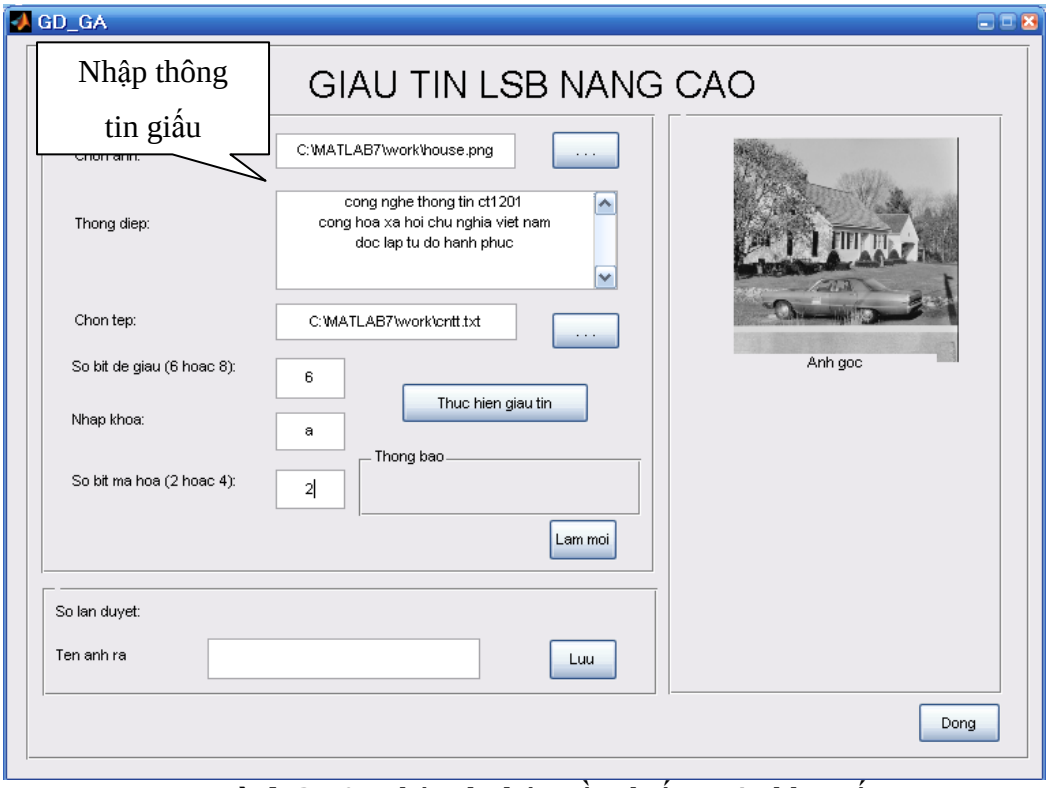


Hình 3.8. Giao diện giấu tin LSB nâng cao



Hình 3.9. Giao diện tách tin LSB nâng cao

➢ Quy trình giấu tin:



Hình 3.10. Nhập dữ liệu cần thiết trước khi giấu

➢ Trước khi tiến hành giấu tin yêu cầu nhập những thông tin sau:

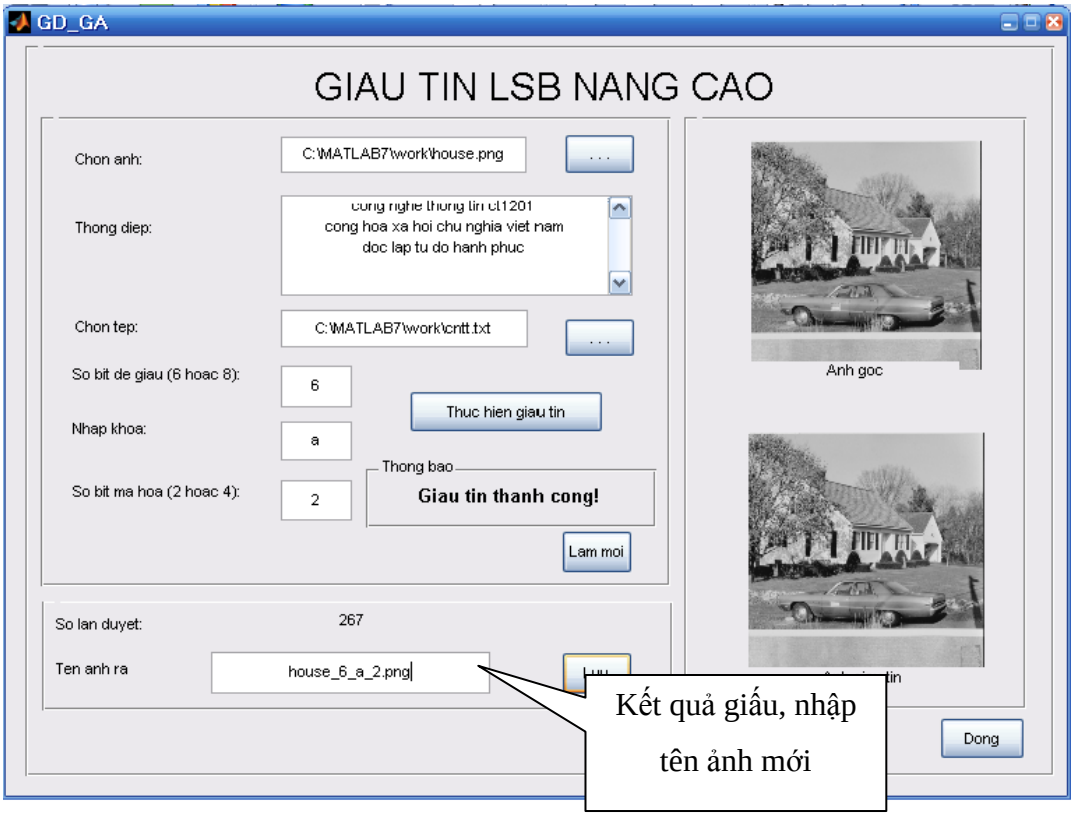
- Chọn ảnh gốc cấp xám trong tập ảnh có sẵn.
- Chọn thông điệp cần giấu tin (có dạng text).
- Nhập số bit để giấu (6 hoặc 8 bit thông điệp).

+ Nếu chọn 8 bit: mỗi kí tự của thông điệp sẽ được chuyển về dạng nhị phân 8 bit.

+ Nếu chọn 6 bit: mỗi kí tự của thông điệp sẽ được quy đổi về một chuỗi 6 bit do người lập trình định nghĩa.

- Nhập khóa: gồm 1 kí tự (bởi người lập trình đã quy ước).
- Nhập số bit mã hóa (2 hoặc 4 bit): Tương tự như giấu trên k-LSBs cổ điển.

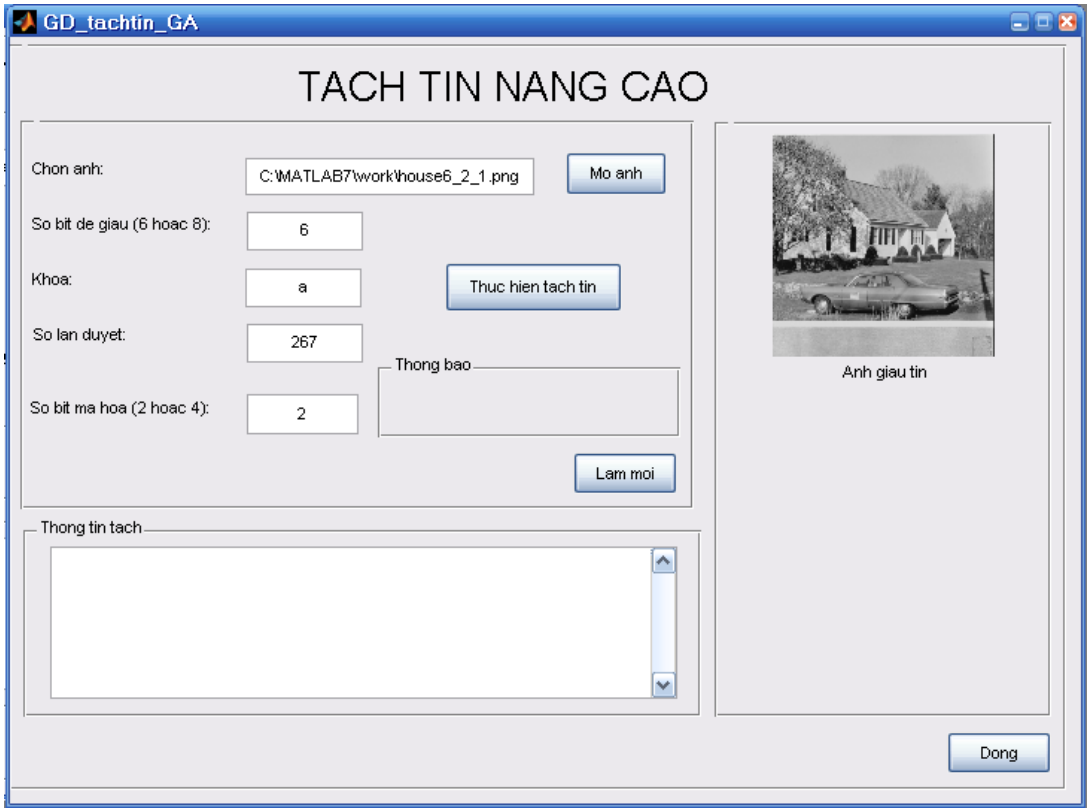
➢ Sau đó ấn "*Thực hiện giấu tin*".



Hình 3.11. Kết quả thu được sau khi thực hiện giấu tin

- Nếu thực hiện giấu thành công, đầu ra sẽ thu được:
  - Ảnh đã giấu tin rất giống ảnh gốc nếu nhìn bằng mắt thường.
  - Thông báo "*Giấu tin thành công!*".
  - Số lần duyệt.
- Nhập tên ảnh ra vào ô "*Tên ảnh ra*" (có phần mở rộng) và chọn "*Lưu ảnh*".
- Nếu thực hiện giấu không thành công có thể do những yếu tố sau:
  - Nhập thiếu hoặc sai thông tin cần thiết như: ảnh gốc để giấu tin, thông điệp bí mật để giấu tin, số bit mã hóa, số bit giấu, khóa. Khi đó chương trình sẽ thông báo lỗi để người sử dụng điều chỉnh.
  - Cài đặt thuật toán sai.

➢ Quy trình tách:



Hình 3.12. Nhập thông tin trước khi tách

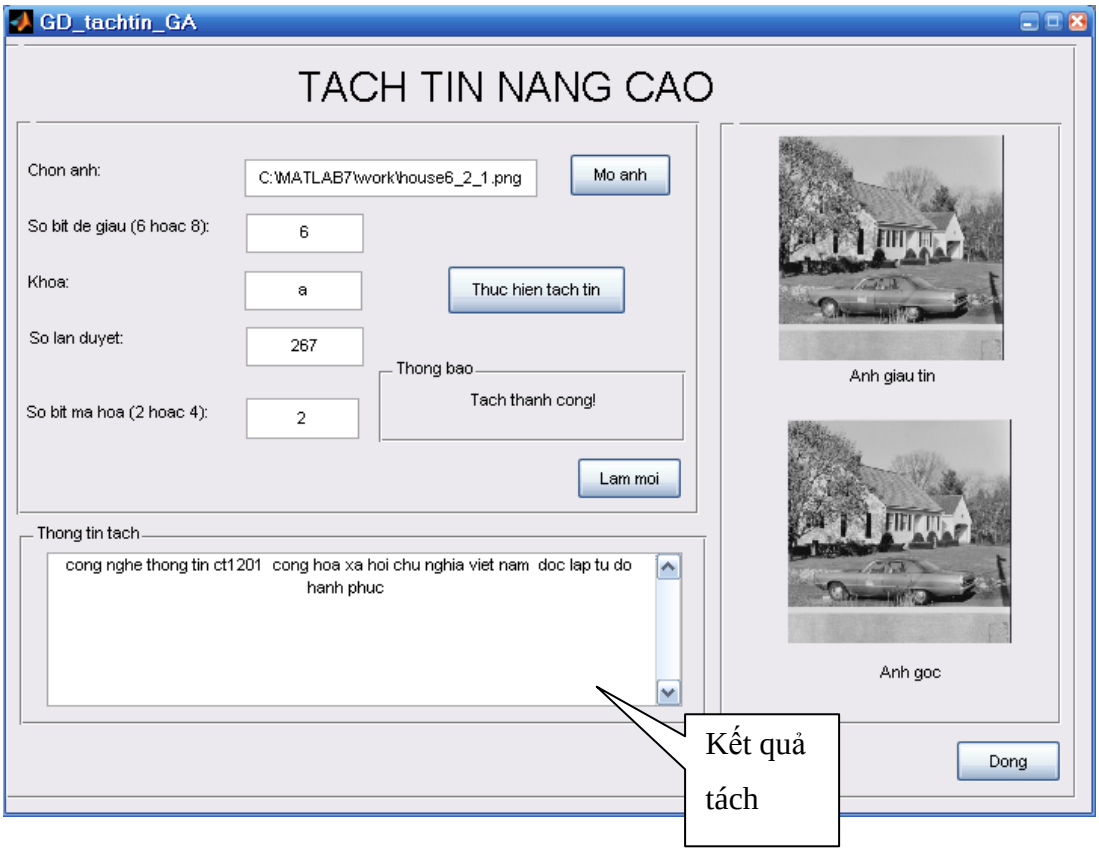
➢ Trước khi tách cần nhập những thông tin sau:

- Chọn ảnh đã mang tin.
- Nhập số bit để giấu tin (6 hoặc 8 bit).
- Nhập khóa: là khóa sử dụng khi giấu tin.
- Nhập số lần duyệt: là kết quả số lần duyệt có được khi giấu tin.
- Nhập số bit mã hóa.

+ Với trường hợp 8 bit để giấu có 2 sự lựa chọn là 2 hoặc 4 bit mã hóa.

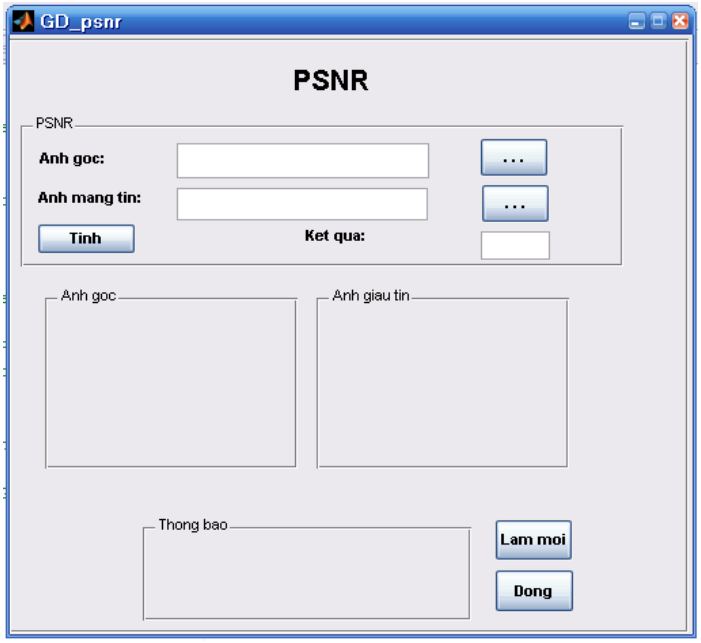
+ Với trường hợp 6 bit để giấu chỉ sự dụng 2 bit mã hóa.

➢ Chọn "*Thực hiện tách tin*" để tiến hành tách nội dung bí mật trong ảnh.

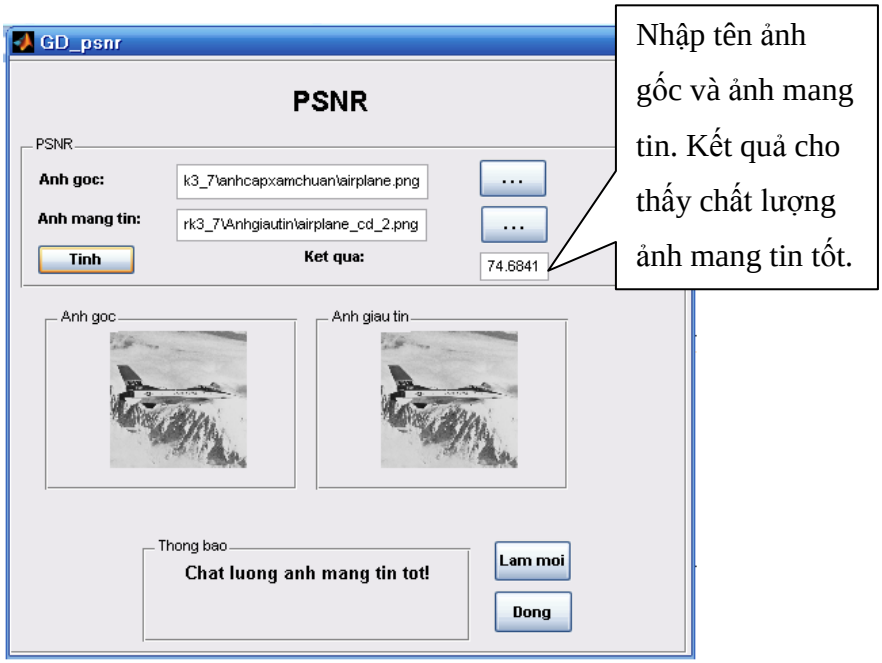


Hình 3.13. Kết quả thu được sau khi tách tin

- Nếu quá trình tách tin thành công sẽ thu được:
  - Ảnh sau khi tách tin.
  - Thông báo "*Tách thành công!*".
  - Ở bảng "*Thông tin tách*" sẽ đưa ra nội dung của thông điệp bí mật.
- Nếu tách không thành công thì có thể do những lý do sau:
  - Nhập thiếu hoặc sai các thông tin cần thiết như: ảnh đã mang tin, số bit để giấu, khóa, số lần duyệt, số bit mã hóa.
  - Cài đặt thuật toán sai.



Hình 3.14.Giao diện PSNR

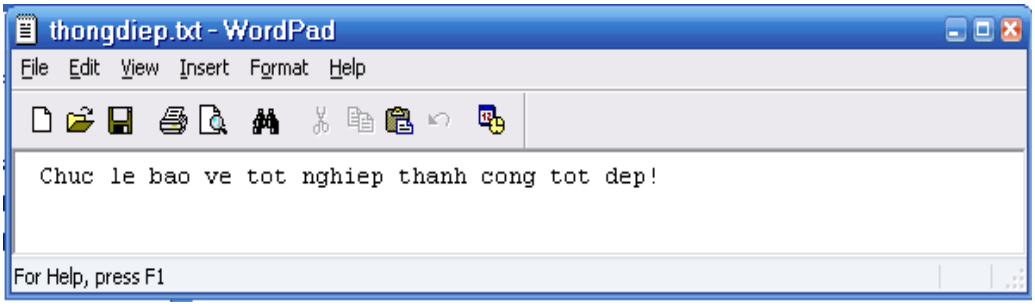


Hình 3.15. Đánh giá chất lượng ảnh sau khi giấu tin PSNR

- Các bước đo độ PSNR:
  - Chọn ảnh gốc và ảnh đó sau khi đã được giấu tin.
  - Chọn "*Tính*" để đo độ PSNR.
- Sau khi thực hiện đo:
  - Thu được kết quả ở mục "*Kết quả*".
  - Thông báo về đánh giá hiển thị ở "*Thông báo*".

3. 2. Thử nghiệm và nhận xét

3. 2. 1. Thử nghiệm



Hình 3.16. Thông điệp bí mật dùng để giấu tin (47 byte)

Tập ảnh A gồm 9 ảnh cấp xám chuẩn chưa giấu tin kích thước 512x512.

Hình 3.17. Tập ảnh A

Tập ảnh thử nghiệm B gồm 25 ảnh chưa giấu tin ngẫu nhiên được lấy từ mạng dùng để giấu tin.

Hình 3.18. Tập ảnh B

Bảng 3.1. Bảng kết quả đo PSNR trên tập ảnh A

STT	Ảnh gốc	K	LSB cổ điển	LSB nâng cao không quy đổi	LSB nâng cao có quy đổi
1	lena.png	2	75. 3601	75. 3982	76. 7704
		4	63. 8249	63. 9478	-
2	house.png	2	74. 7747	74. 7656	76. 1669
		4	66. 4553	65. 8376	-
3	beer.png	2	74. 1255	74. 5142	76. 5133
		4	67. 3805	67. 2032	-
4	baboon.png	2	75. 4903	75. 3104	75. 9574
		4	64. 8282	64. 5307	-
5	airplane.png	2	74. 6841	74. 569	75. 9937
		4	65. 6745	65. 5315	-
6	elaine.png	2	75. 6962	75. 0044	76. 5955
		4	63. 155	62. 9037	-
7	pepper.png	2	73. 9394	73. 4306	75. 5201
		4	64. 0563	63. 7178	-
8	sailboat.png	2	75. 1489	75. 3079	76. 1688
		4	64. 9278	64. 5978	-
9	tiffany.png	2	75. 7075	75. 5952	76. 3502
		4	63. 3235	63. 2442	-

Bảng 3.2. Bảng kết quả đo PSNR trên tập ảnh B

STT	Ảnh gốc	K	LSB cổ điển	LSB nâng cao không quy đổi	LSB nâng cao có quy đổi
1	h1.jpg	2	59. 8047	59. 8377	59. 951
		4	59. 3734	59. 3834	-
2	h2.jpg	2	64. 3247	64. 3247	64. 3247
		4	62. 7646	62. 8568	-
3	h3.jpg	2	64. 3412	64. 3412	64. 3412
		4	63. 0897	63. 5623	-
4	h4.jpg	2	81. 725	81. 8305	81. 8305
		4	76. 7855	77. 7805	-
5	h5.jpg	2	66. 5774	66. 5774	66. 5774
		4	64. 1865	64. 1938	-
6	h6.jpg	2	59. 6326	59. 6326	59. 6773
		4	58. 2885	58. 277	-
7	h7.jpg	2	64. 8836	64. 867	64. 9095
		4	63. 6549	64. 056	-
8	h8.jpg	2	66. 5807	66. 5807	66. 7737
		4	63. 809	63. 813	-
9	h9.jpg	2	56. 4276	56. 4219	56. 4617
		4	55. 8699	55. 9668	-
10	h10.jpg	2	51. 0443	51. 0501	51. 0348
		4	50. 9743	50. 9926	-
11	h11.jpg	2	63. 9759	63. 9905	63. 9905
		4	63. 3443	63. 6026	-
12	h12.jpg	2	57. 558	57. 5813	57. 5669
		4	57. 1083	57. 1731	-
13	h13.jpg	2	73. 5526	73. 5526	73. 6166
		4	68. 827	69. 5832	-
14	h14.jpg	2	62. 9828	62. 9828	62. 9828
		4	62. 7936	62. 8181	-
15	h15.jpg	2	44. 4263	44. 4264	44. 4261

		4	44. 4001	44. 4034	-
16	h16.jpg	2	74. 1525	74. 1525	74. 1525
		4	66. 3101	67. 4175	-
17	h17.jpg	2	63. 6572	63. 6465	63. 7756
		4	63. 2805	63. 3375	-
18	h18.jpg	2	77. 6394	77. 6394	77. 6394
		4	69. 4375	69. 9947	-
19	h19.jpg	2	58. 483	58. 483	58. 483
		4	57. 5491	57. 6838	-
20	h20.jpg	2	69. 5551	69. 5551	69. 5551
		4	65. 5148	66. 9132	-
21	h21.jpg	2	66. 1036	66. 0476	66. 198
		4	64. 1178	63. 876	-
22	h22.jpg	2	79. 1286	79. 1286	79. 1286
		4	76. 7181	77. 2041	-
23	h23.jpg	2	72. 8774	72. 8563	72. 8774
		4	71. 4915	71. 9006	-
24	h24.jpg	2	62. 3506	62. 3647	62. 38
		4	62. 0216	61. 8795	-
25	h25.jpg	2	73. 2457	73. 2457	73. 2457
		4	72. 2931	72. 4276	-

3. 2. 2. Nhận xét

3. 2. 2. 1. Phương pháp thay thế k bit LSB cổ điển

- Dễ dàng cài đặt và thực hiện: Thuật toán đơn giản, giấu được lượng thông tin lớn và nhanh chóng. Tuy nhiên lại dễ bị tin tặc tấn công do tính đơn giản của thuật toán.

Bảng 3.3. Tính PSNR trung bình LSB cổ điển với các trường hợp của K

Tập ảnh \ K	2	4
A	74. 992	64. 847
B	65. 401	63. 360

- Trường hợp K=2 chất lượng ảnh sau khi giấu tốt hơn K=4, do chỉ thay thế 2 bit cuối của byte ảnh nên chất lượng ảnh ít bị thay đổi. Các phương pháp khác cũng vậy.

3. 2. 2. 2. Phương pháp thay thế k bit LSB nâng cao

Bảng 3.4. Tính PSNR trung bình LSB nâng cao với các trường hợp của K

Tập ảnh \ K	TH không quy đổi		TH có quy đổi
	2	4	2
A	74. 877	65. 405	76. 226
B	64. 613	63. 644	65. 436

- LSB nâng cao không quy đổi: Thuật toán tương đối phức tạp do có sự mã hóa thông điệp trước khi giấu vào ảnh, nên thời gian thực hiện thuật toán là lớn với những thông điệp có kích thước càng lớn. Tuy nhiên khó để bị tin tặc tấn công.
- LSB nâng cao có quy đổi: Tương tự như trên nhưng sử dụng một bảng quy đổi các chữ cái và chữ số nên số bit thông điệp đem nhúng vào ảnh giảm đáng kể, giúp cải thiện chất lượng ảnh. Tuy nhiên phương pháp này gây hạn chế do không nhận biết được các kí tự đặc biệt, chỉ áp dụng với văn bản gồm chữ cái và chữ số.

KẾT LUẬN

Hiện nay giấu thông tin trong ảnh là một bộ phận chiếm tỉ lệ lớn nhất trong các chương trình ứng dụng 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. Chính vì thế mà vấn đề này nhận được sự quan tâm rất lớn của các cá nhân, tổ chức, trường đại học và nhiều viện nghiên cứu trên thế giới. Trong đồ án này tìm hiểu về kỹ thuật giấu tin trên k bit LSB của ảnh.

Trong thời gian làm đồ án em đã nghiên cứu được những vấn đề sau:

- Nghiên cứu tổng quan kỹ thuật giấu tin trong ảnh.
- Nghiên cứu cấu trúc ảnh Bitmap.
- Tìm hiểu kỹ thuật giấu tin trên k bit LSB của ảnh.
- Cài đặt và thử nghiệm bằng Matlap 2007b.

Kỹ thuật giấu tin trên k bit LSB có thể triển khai tương tự cho ảnh màu, ảnh PNG, ảnh JPG… Việc cài đặt thuật toán không quá phức tạp, lại cho phép triển khai để giấu lượng thông tin khá lớn. Hơn nữa, kết quả đánh giá chất lượng ảnh sau khi giấu tin PSNR cho thấy kỹ thuật trên có độ tin cậy cao.

Vì thời gian nghiên cứu có hạn, trình độ hiểu biết của bản thân em còn nhiều hạn chế nên bài báo cáo của em không tránh khỏi những thiếu sót, em rất mong nhận được sự góp ý quý báu của tất cả các thầy cô giáo để báo cáo của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

[1]. USC-SIPI Image Database, Signal and Image Processing Institute, University of Southern California, http: //sipi. usc. edu/services/database/Database.html

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

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

[4]. Marghny Mohamed, Fadwa Al-Afari and Mohamed Bamatraf, Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation, International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011.

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

[6]. 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.

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

[8]. 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.

[9]. 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.

[10]. 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.

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

[12]. 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.

[13]. Mạc Như Hiển – CT901, “Nghiên cứu kỹ thuật giấu thông tin trong ảnh GIF”, đồ án tốt nghiệp ngành CNTT – 2009.

[14]. Phạm Thị Quỳnh – CT901, “NGHIÊN CỨU KỸ THUẬT PHÁT HIỆN THÔNG TIN ẨN GIẤU TRONG ẢNH JPEG 2000”, đồ án tốt nghiệp ngành CNTT – 2009.

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

[16]. 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.

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

[18]. 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.

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

[20]. 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.

[21]. 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.

[22]. Vũ Khắc Quyết – CT1001, “Nghiên cứu kỹ thuật giấu tin với dung lượng thông điệp lớn”, đồ án tốt nghiệp ngành CNTT – 2010.

[23]. 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.

[24]. Vũ Thị Ngọc – CT1101, “Nghiên cứu một giải pháp giấu văn bản trong ảnh”,

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

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

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

[28]. 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.

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

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

[31]. 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.