LỜI CẢM ƠN

Em xin được bày tỏ lòng biết ơn sâu sắc tới giáo viên, THs. Hồ Thị Hương Thơm, người đã trực tiếp hướng dẫn, tận tình chỉ bảo em trong suốt quá trình làm đồ án tốt nghiệp.

Em xin chân thành cảm ơn tất cả các thầy cô giáo 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 hoàn thành tốt quá trình tốt nghiệp.

Cuối cùng em xin cảm ơn gia đình đã tạo điều kiện giúp đỡ em trong suốt quá trình làm tốt nghiệp. Và em xin cảm ơn tất cả các bạn đã góp ý, trao đổi hỗ trợ cho em trong suốt thời gian vừa qua.

Em xin chân thành cảm ơn!

Hải Phòng, ngày 17 tháng 7 năm 2011

Sinh viên

Hoàng Thị Thu Dung

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

DANH MỤC CÁC CHỮ VIẾT TẮT

Từ viết tắt	Ý nghĩa	Diễn giải
MBNS	Multiple Base Notational System.	Hệ thống đa ký hiệu cơ sở.
DES	Data Encryption Standard.	Tiêu chuẩn Mã hóa Dữ liệu.
RSA	R.Rivest, A.Shamir và L.Adleman.	Viết tắt từ tên 3 nhà toán học đã phát minh ra hệ mã RSA.
BMP	Bitmap.	Ảnh không nén Bitmap.
JPG	Joint Photographic Group.	Ảnh nén JPG.
PNG	Portable Network Graphics.	Ảnh PNG.
GIF	Graphics Interchange Format.	Định dạng trao đổi hình ảnh.
SPNR	Peak signal-to-noise ratio.	Tỉ số tín hiệu cực đại trên nhiễu.
MSE	Mean squared error.	Lỗi bình phương.
HVS	Human vision system.	Hệ thống cảm nhận con người.
PVD	Pixel Value Differencing.	Phương pháp vi phân điểm ảnh.

LỜI NÓI ĐẦU

Sự ra đời và phát triển một cách bùng nổ của mạng internet như ngày nay, là điều kiện để tất cả mọi người đều có thể truy cập vào mạng internet và tìm kiếm thông tin một cách dễ dàng thông qua các nhà cung cấp dịch vụ.

Do đó, mạng internet 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…v.v. Và chính trong môi trường mở và tiện nghi như thế đã xuất hiện những vấn nạn, tiêu cực đang rất cần đến các giải pháp hữu hiệu cho vấn đề an toàn thông tin như nạn ăn cắp bản quyền, nạn xuyên tạc thông tin, truy nhập thông tin trái phép…v.v.

Một trong những giải pháp hữu hiệu để giải quyết các vấn nạn, tiêu cực đó là công nghệ giấu tin (datahiding), với công nghệ này chúng ta có thể truyền tin trên các phương tiện đại chúng mà không sợ bị phát hiện. Như bạn có thể giấu một bài thơ tình vào một bức ảnh mà không làm thay đổi bức ảnh (đối với cảm nhận của con người). Cùng với sự phát triển của máy tính, công nghệ giấu tin ngày càng trở lên tinh vi hơn. Chính vì vậy, trong đồ án này tìm hiểu một trong số kỹ thuật của công nghệ giấu tin đó là kỹ thuật giấu tin trong ảnh dựa trên MBNS.

MBNS là hệ thống các ước số cơ sở. Kỹ thuật giấu tin sử dụng MBNS sẽ chia thông điệp ra làm nhiều phân đoạn, và giấu vào các đoạn dữ liệu ảnh dựa vào việc chia cơ sở cho chính các đoạn thông điệp được một hệ thống các bội số của nó. Chỉnh hóa để có thế giấu tin không ảnh hưởng đến cảm nhận của hệ thống mắt người.

Bố cục đồ án được trình bày trong 4 chương, có phần kết luận, phần tài liệu tham khảo, trong đó:

Chương 1: Tổng quan về giấu tin trong ảnh.

Chương 2: Một số khái niệm.

Chương 3: Kỹ thuật giấu tin dựa trên hệ thống MBNS.

Chương 4: Cài đặt và thử nghiệm.

CHƯƠNG 1: TỔNG QUAN GIẤU TIN TRONG ẢNH

1.1. Tổng quan giấu tin

1.1.1. Sơ lược về lịch sử giấu tin

Các câu chuyện kể về kỹ thuật giấu thông tin được truyền qua nhiều thế hệ. Có lẽ những ghi chép sớm nhất về kỹ thuật giấu thông tin (thông tin được hiểu theo nghĩa nguyên thủy của nó) thuộc về sử gia Hy-Lạp Herodotus. Khi bạo chúa Hy-Lạp Histiaeus bị vua Darius bắt giữ ở Susa vào thế kỷ thứ năm trước công nguyên, ông ta đã gửi một thông báo bí mật cho con rể của mình là Aristagoras ở Miletus. Histiaeus đã cạo trọc đầu của một nô lệ tin cậy và xăm một thông báo trên da đầu của người nô lệ ấy. Khi tóc của người nô lệ này mọc đủ dài người nô lệ được gửi tới Miletus.

Một câu chuyện khác về thời Hy-Lạp cổ đại cũng do Herodotus ghi lại. Môi trường để ghi văn bản chính là các viên thuốc được bọc trong sáp ong. Demeratus, một người Hy-Lạp, cần thông báo cho Sparta rằng Xerxes định xâm chiếm Hy-Lạp. Để tránh bị phát hiện, anh ta đã bóc lớp sáp ra khỏi các viên thuốc và khắc thông báo lên bề mặt các viên thuốc này, sau đó bọc lại các viên thuốc bằng một lớp sáp mới. Những viên thuốc được để ngỏ và lọt qua mọi sự kiểm tra một cách dễ dàng.

Mực không màu là phương tiện hữu hiệu cho bảo mật thông tin trong một thời gian dài. Người Romans cổ đã biết sử dụng những chất sẵn có như nước quả, nước tiểu và sữa để viết các thông báo bí mật giữa những hàng văn tự thông thường. Khi bị hơ nóng, những thứ mực không nhìn thấy này trở nên sẫm màu và có thể đọc dễ dàng.

Ý tưởng về che giấu thông tin đã có từ hàng nghìn năm về trước nhưng kỹ 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 hàng loạt công trình nghiên cứu giá trị. Cuộc cách mạng số hoá 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 kỹ thuật thay thế, sửa đổi tinh vi, cộng với sự lưu thông phân phối trên mạng của các dữ liệu đa phương tiện đã sinh ra nhiều 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.

1.1.2. Phương pháp giấu tin

Trong một quá trình phát triển lâu dài, nhiều phương pháp bảo vệ thông tin đã được đưa ra và được ứng dụng rất phổ biến cho đến tận ngày nay như những hệ mã phức tạp DES, RSA, NAPSACK... Thông tin ban đầu sẽ được mã hoá thành các ký hiệu vô nghĩa, sau đó sẽ được lấy lại thông qua việc giải mã nhờ khoá của hệ mã. Một phương pháp khác đã và đang được nghiên cứu và ứng dụng rất mạnh mẽ ở nhiều nước trên thế giới đó là phương pháp giấu tin.

Giấu thông tin là một kĩ thuật nhúng thông tin vào trong một nguồn đa phương tiện gọi là các phương tiện chứa mà không gây ra sự nhận biết về sự tồn tại của thông tin giấu trong phương tiện chứa.

Phương pháp giấu tin là phương pháp mới và phức tạp, nó đang được xem như một công nghệ chìa khoá cho vấn đề bảo vệ bản quyền, nhận thực thông tin và điều khiển truy cập… ứng dụng trong an toàn và bảo mật thông tin.

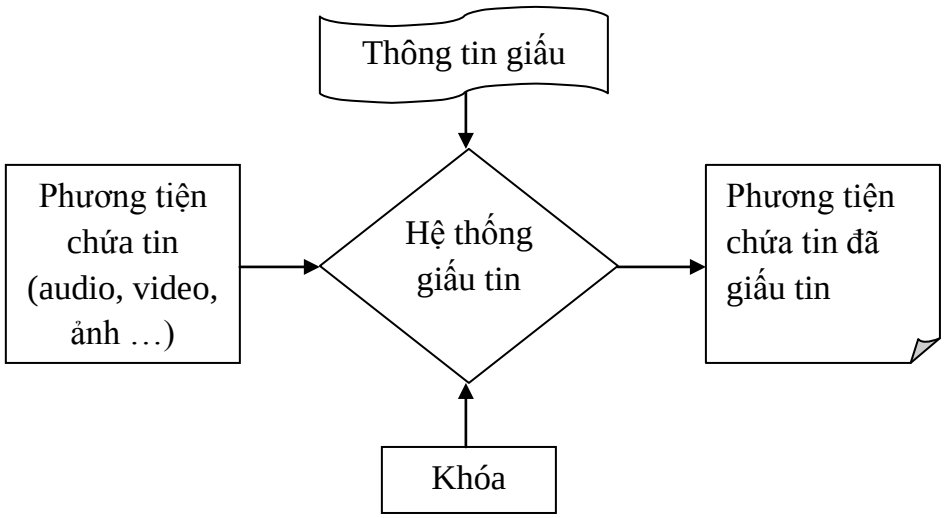
Phương pháp giấu tin là làm cho người ta khó có thể biết được có thông tin giấu bên trong đó do tính chất ẩn của thông tin được giấu.

Sự khác biệt chủ yếu giữa mã hoá thông tin và giấu thông tin là phương pháp mã hoá làm cho các thông tin hiện rõ là nó có được mã hoá hay không còn đối với phương pháp giấu thông tin thì người ta sẽ khó biết được là có thông tin giấu bên trong do tính chất ẩn của thông tin được giấu. Một khi những thông tin mã hoá bị phát hiện thì những tên tin tặc sẽ tìm mọi cách để triệt phá. Và cuộc chạy đua giữa những người bảo vệ thông tin và bọn tin tặc vẫn chưa kết thúc tuyệt đối về bên nào. Trong hoàn cảnh đó thì giấu thông tin trở thành một phương pháp hữu hiệu để che giấu thông tin mà các hacker không thể phát hiện ra.

1.1.3. Mô hình kỹ thuật giấu tin cơ bản

Quá trình giấu thông tin vào môi trường chứa tin xem Hình 1.1 và quá trình tách lấy thông tin xem Hình 1.2 là hai quá trình trái ngược nhau.

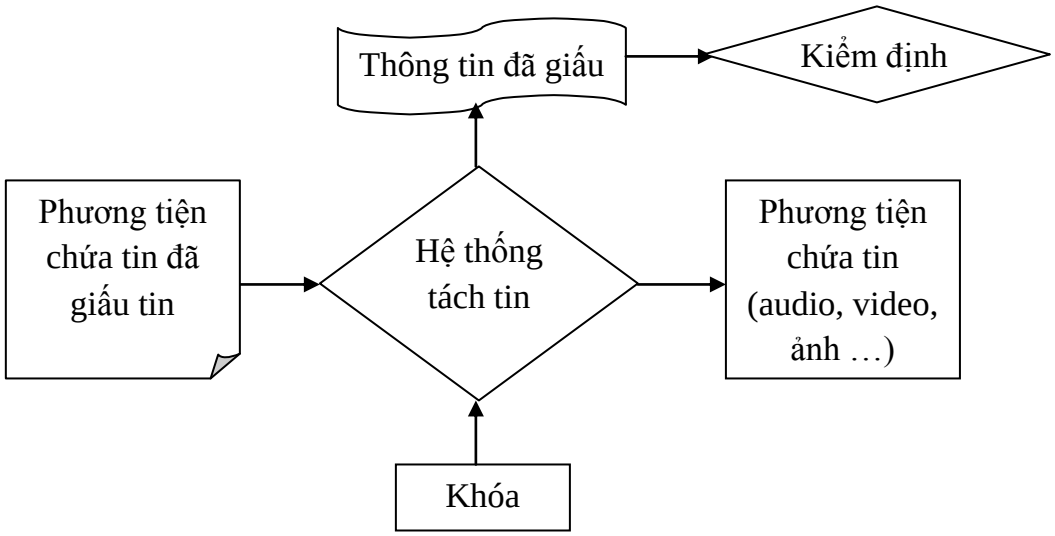
1.1.3.1. Quá trình giấu thông tin



Hình 1.1 Sơ đồ chung cho quá trình giấu tin.

- 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 tin: các file ảnh, text, audio… là môi trường để giấu tin.
- Hệ thống giấu tin: là những chương trình thực hiện việc giấu tin.
- Khóa: là khoá mật tham gia vào quá trình giấu tin, tăng tính bảo mật.
- Đầu ra: là các phương tiện chứa đã có tin giấu trong đó.

1.1.3.2. Quá trình tách thông tin



Hình 1.2 Sơ đồ chung cho quá trình tách tin.

Quá trình tách tin được thực hiện trái ngược với quá trình giấu tin. Sau khi nhận được phương tiện chứa tin đã giấu tin, nó sẽ được đưa vào các chương trình tách tin trong hệ thống tách tin để lấy thông tin đã giấu. Quá trình tách tin cũng sử dụng khóa để khôi phục thông tin đã giấu và phương tiện chứa tin ban đầu. Sau khi lấy được thông tin đã giấu, thông tin đó sẽ được mang đi kiểm định so với thông tin ban đầu.

1.2. Giấu tin trong ảnh

1.2.1. Tổng quan

Hiện nay giấu tin trong ảnh 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 tin trong ảnh cũng đóng vai trò hết sức quan trọng trong hầu hết các ứng dụng bảo vệ an toàn thông tin như: nhận thực thông tin, xác định xuyên tạc thông tin, bảo vệ bản quyền tác giả, điều khiển truy cập…. 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.

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. Ngày nay khi ảnh số được sử dụng rất phổ biến thì giấu thông tin trong ảnh là một công nghệ đem lại rất nhiều tác dụng quan trọng trên nhiều lĩnh vực trong đời sống xã hội. Ví dụ như đối với các nước phát triển, chữ kí tay đã được số hóa và lưu trữ sử dụng như là hồ sơ cá nhân của các dịch vụ ngân hàng và tài chính, nó được dùng để nhận thực trong các thẻ tín dụng của người tiêu dùng.

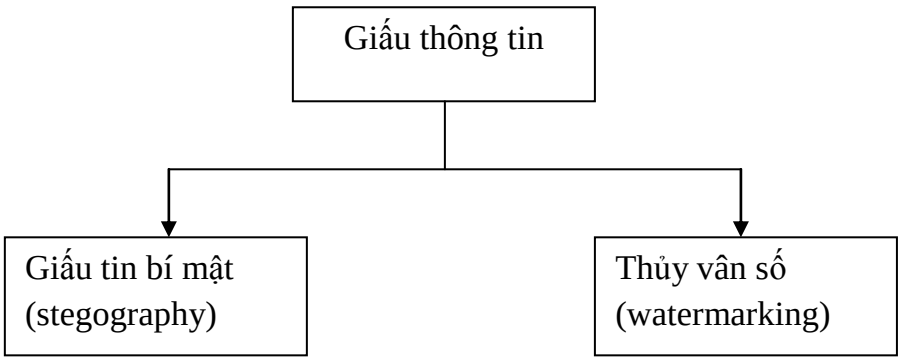
Thêm vào đó, lại có rất nhiều loại thông tin quan trọng cần được bảo mật như những thông tin về an ninh, thông tin về bảo hiểm hay các thông tin về tài chính, các thông tin này được số hóa và lưu trữ trong hệ thống máy tính hay trên mạng. Chúng rất dễ bị lấy cắp và bị thay đổi bởi các phần mềm chuyên dụng. Việc nhận thực cũng như phát hiện thông tin xuyên tạc đó trở nên vô cùng quan trọng và cấp thiết.

Và một đặc điểm của giấu thông tin trong ảnh đó là thông tin được giấu trong ảnh một cách vô hình, nó như 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 đặc biệt đối với ảnh màu hay ảnh xám.

1.2.2. Phân loại giấu tin trong ảnh

Giấu tin trong ảnh có hai khía cạnh: Một là bảo mật cho dữ liệu đem giấu (embedded data), thông tin mật được giấu kỹ trong một đối tượng khác sao cho người khác không phát hiện được (stegography) [2].

Hai là bảo mật chính đối tượng được dùng để giấu dữ liệu vào (host data), như ứng dụng bảo vệ bản quyền, phát hiện xuyên tạc thông tin (watermarking).



Hình 1.3. Sơ đồ phân loại giấu tin trong ảnh.

Kỹ thuật giấu thông tin bí mật (Steganography) là một kỹ thuật nhúng thông tin vào trong một nguồn đa phương tiện gọi là các phương tiện chứa mà không gây ra sự nhận biết về sự tồn tại của thông tin giấu. Từ Steganography bắt nguồn từ Hi Lạp và được sử dụng cho tới ngày nay, nó có nghĩa là tài liệu được phủ (covered writing).

Kỹ thuật thủy vân số (watermarking) là ứng dụng cơ bản nhất của kỹ thuật giấu tin trong ảnh. Một thông tin nào đó sẽ được nhúng vào trong một ảnh, giả sử hình ảnh 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.

1.2.3. Đặc trưng và tính chất

Giấu tin trong ảnh chiếm vị trí chủ yếu trong các kỹ thuật giấu tin, vì vậy mà các kỹ thuật giấu tin phần lớn cũng tập trung vào các kỹ thuật giấu tin trong ảnh. Các phương tiện chứa khác nhau sẽ có các kỹ thuật giấu khác nhau. Đối tượng ảnh là một đối tượng dữ liệu tĩnh có nghĩa là dữ liệu tri giác không biến đổi theo thời gian. Dữ liệu ảnh có nhiều định dạng, mỗi định dạng có những tính chất khác nhau nên các kỹ thuật giấu tin trong ảnh thường chú ý những đặc trưng và các tính chất cơ bản sau [1]:

– *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 phụ thuộc vào các loại ảnh khác nhau. Chẳng hạn đối với ảnh đen trắng, ảnh xám hay ảnh màu ta cũng có những kỹ thuật riêng cho từng loại ảnh có những đặc trưng khác nhau.

– *Kỹ thuật giấu tin lợi dụng tính chất hệ thống thị giác của con người:* Giấu tin trong ảnh ít nhiều cũng gây ra những thay đổi trên dữ liệu ảnh gốc. 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 ra được sự thay đổi đó vì có như thế thì mới đảm bảo được độ an toàn cho thông tin giấu. Rất nhiều các kỹ thuật đã lợi dụng các tính chất của hệ thống thị giác để giấu tin chẳng hạn như mắt người cảm nhận về sự biến đổi về độ chói kém hơn sự biến đổi về màu hay cảm nhận của mắt về màu xanh da trời kém nhất trong ba màu cơ bản.

– *Giấu thông tin trong ảnh tác động lên dữ liệu ảnh nhưng không thay đổi kích thước ảnh:* Các thuật toán thực hiện công 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 khó có thể bị phát hiện dễ dàng so với ảnh gốc.

Yêu cầu này dường như khá đơn giản đối với ảnh màu hoặc ảnh xám bởi mỗi điểm ảnh được biểu diễn bởi nhiều bit, nhiều giá trị và khi ta thay đổi một giá trị nhỏ nào đó thì chất lượng ảnh thay đổi không đáng kể, thông tin giấu khó bị phát hiện, nhưng đối với ảnh đen trắng mỗi điểm ảnh chỉ là đen hoặc trắng, và nếu ta biến đổi một bit từ trắng thành đen và ngược lại mà không khéo thì sẽ rất dễ bị phát hiện.

Do đó, yêu cầu đối với các thuật toán giấu thông tin trong ảnh màu hay ảnh xám và giấu thông tin trong ảnh đen trắng là khác nhau. Trong khi đối với ảnh màu thì các thuật toán chú trọng vào việc làm sao giấu được càng nhiều thông tin càng tốt thì các thuật toán áp dụng cho ảnh đen trắng lại tập trung vào việc làm thế nào để thông tin giấu khó bị phát hiện nhất.

– *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 sẽ 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 thực 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. Đa số các kỹ thuật giấu tin mật thì thường không cần ảnh gốc để giải mã. Thông tin được giấu trong ảnh sẽ được mang cùng với dữ liệu ảnh, khi giải mã chỉ cần ảnh đã mang thông tin giấu mà không cần dùng đến ảnh gốc để so sánh đối chiếu.

1.2.4. Các yêu cầu đối với giấu tin trong ảnh

Mục đích của giấu tin cho ảnh là bảo vệ bản quyền cho chủ sỡ hữu 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. Nếu tính ẩn của tin không được đảm bảo thì không những nó làm ảnh hưởng tới chất lượng của ảnh mà còn dễ dàng tạo điều kiện cho các hình thức tấn công nhằm loại bỏ tin ra khỏi ảnh. Với ảnh được đánh dấu một cách lý tưởng, ảnh có bản quyền và ảnh gốc sẽ không thể phân biệt được bằng mắt thường. Như vậy giá trị của bức ảnh sẽ không bị thay đổi và việc giấu tin như vậy sẽ là rào cản lớn cho những kẻ phá hoại trong việc cố ý xoá hoặc sửa đổi các thông tin về bản quyền ảnh.

Trên thực tế, khi chèn tin vào ảnh thì ảnh kết quả và ảnh gốc sẽ có những sai khác, để không thể nhận ra được những thay đổi về nội dung dữ liệu này, người ta thường khai thác các đặc điểm về khả năng cảm thụ của mắt người.

Tính bền của giấu tin liên quan đến việc tách tin từ ảnh có bản quyền, một ảnh sau khi được đánh dấu có thể được đem ra xử lý để phục vụ cho các mục đích khác nhau như nén ảnh, biến đổi hình học, lọc ảnh cải thiện ảnh, các biến đổi cố tình để xoá đánh dấu tin ra khỏi ảnh,…v.v. Vấn đề được đặt ra liệu sau khi ảnh bị xử lý ta còn có thể tách được lượng tin ra khỏi ảnh không? Và tách được thì chất lượng của tin có đảm bảo tin cậy không?

CHƯƠNG 2: MỘT SỐ KHÁI NIỆM CƠ BẢN

2.1. Độ lệch chuẩn (Standard Deviation)

Phương pháp tính độ lệch chuẩn từ một dãy n giá trị cho trước x_1, x_2,... x_n theo [4]:

1. Tìm giá trị trung bình của dãy số đã cho $(x_1+x_2+...+x_n)/n$.
2. Với mỗi x trong dãy số đã cho, tính độ lệch của nó so với giá trị trung bình.
3. Tính bình phương của các giá trị thu được ở bước 2.
4. Tìm giá trị trung bình của các bình phương độ lệch tìm được ở bước 3. Các giá trị này được biết đến như là phương sai σ^2.
5. Tính căn bậc hai của phương sai ta được kết quả cần tìm.

Công thức thể hiện phương pháp tính trên:

$$\bar{x} = \frac{x_1+x_2+\cdots+x_N}{N} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{2.1}$$

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2} \tag{2.2}$$

Độ lệch chuẩn là một giá trị thể hiện mức độ hội tụ hay sức phân tán của một tập dữ liệu. Nếu một tập dữ liệu có độ lệch chuẩn nhỏ điều đó chứng tỏ các phần tử dữ liệu nhìn trên phương diện tổng quát có sự tương đồng cao, ngược lại thì dữ liệu có vùng phân tán lớn, rải rác trong không gian giá trị của chúng.

2.2. Hệ thống MBNS

MBNS là một hệ thống các ước số cơ sở, mà được sử dụng để ẩn đi một thông tin mật. Nó được biết đến như hệ thập phân là vị trí thuận tiện trong cuộc sống hàng ngày và hệ thống nhị phân trong hoạt động của máy tính. Căn cứ vào các hệ thống này, hệ 10 và 2 tương ứng là không đổi trong suốt. Nói cách khác, thông tin mật được chuyển đổi thành một loạt các cơ sở sai phân tương ứng với hệ số của chúng. Điều này được giải thích như sau [3]:

Giả sử một số nguyên *x* được thể hiện trong hệ thống các ước số cơ sở được biểu diễn như công thức (2.3):

$$x = (d_{n-1}d_{n-2}\dots d_2 d_1 d_0)_{b_{n-1}b_{n-2}\dots b_2 b_1 b_0} \tag{2.3}$$

$$0 \le d_i < b_i \ (i = 0, 1, \dots, n-1)$$

Trong đó $b_0, b_1, b_2, \dots, b_{n-2}$ và b_{n-1} là các cơ sở sai phân tương ứng, tương ứng với các hệ số $d_0, d_1, d_2, \dots, d_{n-2}$ và d_{n-1}.

Giá trị thập phân của *x* được tính theo công thức (2.4).

$$x = d_0 + \sum_{i=1}^{n-1} (d_i . \prod_{j=0}^{i-1} b_j) \quad (2.4)$$

Trong đó:

- Π là phép nhân.
- Σ là phép tính tổng.

Nếu giá trị thập phân của *x* và các cơ sở $b_0, b_1, b_2, \dots, b_{n-2}$ và b_{n-1} được đưa ra, ta có thể chuyển đổi *x* vào hệ thống các ước số cơ sở theo công thức (2.5) và (2.6).

$$d_0 = x \; mod \; b_0 \quad (2.5)$$

$$d_k = \text{mod} \left\{ \frac{1}{\prod_{j=0}^{k-1} b_j} \left[x - d_0 - \sum_{i=1}^{k-1} \left(d_i \cdot \Pi_{j=0}^{i-1} b_j \right) \right], b_k \right\}, \; k \geq 1. \quad (2.6)$$

Theo công thức (2.5) và công thức (2.6), $d_0, d_1, d_2, \dots, d_{n-2}$ và d_{n-1} có thể thu được liên tiếp. Ví dụ, $49 = (1301)_{3532}$ và $158 = (3142)_{6254}$.

Ví dụ:

- Cho số nguyên *x* = 49 , n = 4 và $b_0 = 2, b_1 = 3, b_2 = 5, b_3 = 3$.
- Theo công thức (2.5) thì $d_0 = 49 \bmod 2 = 1$;
- Theo công thức (2.6) thì:

$d_1 = ((x - d_0) / b_0) \bmod b_1$
$= ((49 - 1) / 2) \bmod 3 = 24 \bmod 3 = 0$;

$d_2 = ((x - d_0 - (d_1 \times b_0)) / (b_0 \times b_1)) \bmod b_2$
$= ((49 - 1 - (0 \times 2)) / (2 \times 3)) \bmod 5 = 8 \bmod 5 = 3$;

$d_3 = ((x - d_0 - (d_1 \times b_0 + d_2 \times b_0 \times b_1)) / (b_0 \times b_1 \times b_2)) \bmod b_3$
$= ((49 - 1 - (0 \times 2 + 3 \times 2 \times 3)) / 2 \times 3 \times 5) \bmod 3 = 1 \bmod 3 = 1$;

- Thử lại bằng cách tính theo công thức (2.4) thì,

$x = d_0 + d_1 \times b_0 + d_2 \times b_0 \times b_1 + d_3 \times b_0 \times b_1 \times b_2$
$= 1 + 0 \times 2 + 3 \times 2 \times 3 + 1 \times 2 \times 3 \times 5$
$= 1 + 0 + 18 + 30 = 49$

Với một chuỗi các bit trong tay, đầu tiên có thể giải thích nó như là một số nguyên dương bằng cách sử dụng (2.4), và sau đó lại thể hiện nó trong một hệ thống các ước số cơ sở bằng cách sử dụng (2.5) và (2.6) với một bộ cơ sở nhất định.

2.3. Cấu trúc ảnh bitmap.

Có một vài định dạng phổ biến cho tệp ảnh kĩ thuật số bao gồm BMP, JPG, PNG…trong đồ án này đã nghiên cứu được với tệp ảnh BMP vì tệp ảnh này đơn giản, có lợi thế về tính chất vì tính chất của BMP là được tiêu chuẩn hóa cao và tính lan rộng mạnh. Trong đồ họa máy tính BMP còn được biết đến với tên Windows bitmap, là một định tập tin hình ảnh phổ biến. Các tập tin đồ họa lưu dưới dạng BMP thường có đuôi là .BMP hoặc .DIB.

2.3.1. Các thuộc tính tiêu biểu của một tập tin ảnh BMP

Các thuộc tính tiêu biểu của một tập tin ảnh BMP nói chung là [2][6]:

– 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), cho bởi điểm ảnh (pixel).

– Chiều rộng của ảnh (width), cho bởi điểm ảnh.

2.3.2. Cấu trúc của tệp ảnh BMP

Tệp ảnh bitmap là tệp nhị phân, được phân chia thành 4 phần. Bao gồm FileHeader, ImageHeader, ColorTable, và cuối cùng là Pixel Data.

❖ *FileHeader:(14 byte)*

FileHeader lưu trữ thông tin tổng hợp về tệp tin BMP có các chức năng chính:

+ Xác định đây có phải là tệp tin BMP hay không (2 byte đầu tiên).
+ Độ lớn của tệp ảnh (4 byte tiếp theo).
+ Xác đinh vị trí của dữ liệu ảnh.

Bảng 2.1 Chi tiết khối byte tiêu đề của tệp tin BMP.

Tên trường	Kích thước (byte)	Miêu tả
Type	2	Là 2 kí tự ‘B’ và ‘M’.
Size	4	Kích thước của file.
Reserved 1	2	Không được sử dụng, phải có giá trị là 0.
Reserved 2	2	
OffBits	4	Vị trí bắt đầu phần The Pixel Data.

❖ *ImageHeader: (40 byte)*

Chức năng chính: Đưa ra thông tin chi tiết về ảnh và định dạng dữ liệu như:

+ Chiều rộng và chiều cao của ảnh.
+ Bao nhiêu bit được sử dụng cho 1 pixel.
+ Dữ liệu ảnh có được nén hay không.

Bảng 2.2 Chi tiết khối byte thông tin tệp tin BMP.

Tên trường	Kích thước (byte)	Miêu tả
Size	4	Kích thước phần Header, phải nhỏ hơn 40.
Width	4	Chiều rộng file theo Pixel.
Height	4	Chiều cao file theo Pixel.
Planes	2	Phải là 1.
BitCount	2	Số bit trên 1 Pixel : 1, 2, 4, 8, 16, 24, hoặc 32.
Compression	4	Kiểu nén (0 = Không được nén).
SizeImage	4	Kích thước ảnh, phải là 0 đối với ảnh không được nén.
XPelsPerMeter	4	Ưu tiên độ phân giải pixels/ meter.
YPelsPerMeter	4	Ưu tiên độ phân giải pixels/ meter.
ClrUsed	4	Số màu Map được sử dụng thực sự.
ClrImportant	4	Số màu có ý nghĩa.

❖ *Bảng màu (ColorTables)*

Tiếp theo là Palette màu của BMP, gồm nhiều bộ có kích thước 4 byte xếp liền nhau theo cấu trúc Blue-Green-Red và một Byte dành riêng cho Itensity. Kích thước của vùng Palette màu bằng 4 × số màu của ảnh. Byte 15-16 của Info là 24 hoặc 32 thì không có vùng Palette, vì Palette màu của màn hình có cấu tạo theo thứ tự Red-Green-Blue nên khi đọc Palette màu của ảnh BMP ta phải chuyển đổi lại cho phù hợp. Số màu của ảnh được biết dựa trên số bit cho 1 pixel cụ thể là:

– Nếu là ảnh 24 bit, thì ColorTable không được biểu diễn.

– Nếu là ảnh 8 bit thì ColorTable chứa 256 "entry" với mỗi "entry" chứa 4 byte của dữ liệu. 3 byte đầu tiên là giá trị cường độ màu Blue, Green, Red. Byte cuối cùng không được sử dụng và phải bằng zero.

❖ *Dữ liệu điểm ảnh (The Pixel Data)*

– *The Pixel Data* lưu trữ từng pixel của hình ảnh thực tế.

– Với ảnh 8 bit, mỗi pixel được biểu diễn bởi 1 byte đơn của dữ liệu.

– Với ảnh 24 bit, mỗi pixel được biểu diễn bởi 3 byte tuần tự của dữ liệu.

2.4. Ảnh xám

Đơn vị tế bào của ảnh số là pixel. Tùy theo mỗi định dạng là ảnh màu hay ảnh xám mà từng pixel có thông số khác nhau. Đối với ảnh màu từng pixel sẽ mang thông tin của ba màu cơ bản tạo ra bảng màu khả kiến là :

- Đỏ (R)
- Xanh lá (G)
- Xanh biển (B)

[Thomas 1892].

Trong mỗi pixel của ảnh màu, ba màu cơ bản R, G và B được bố trí sát nhau và có cường độ sáng khác nhau. Thông thường, mỗi màu cơ bản được biểu diễn bằng tám bit tương ứng 256 mức độ màu khác nhau. Như vậy mỗi pixel chúng ta sẽ có: 2^8x3=2^24 màu (khoảng 16.78 triệu màu).

Đối với ảnh xám, thông thường mỗi pixel mang thông tin của 256 mức xám (tương ứng với 8-bit), như vậy ảnh xám hoàn toàn có thể tái hiện đầy đủ cấu trúc của một ảnh màu tương ứng thông qua tám mặt phẳng bit theo độ xám.

Trong hầu hết quá trình xử lý ảnh, chúng ta chủ yếu chỉ quan tâm đến cấu trúc của ảnh và bỏ qua ảnh hưởng của yếu tố màu sắc. Do đó bước chuyển từ ảnh màu thành ảnh xám là một công đoạn phổ biến trong các quá trình xử lý ảnh vì nó làm tăng tốc độ xử lý là giảm mức độ phức tạp của các thuật toán trên ảnh.

CHƯƠNG 3: KỸ THUẬT GIẤU TIN MBNS

3.1. Giới thiệu

Kỹ thuật giấu tin MBNS được đề xuất bởi hai tác giả Xingpeng Zhang and Shuozhong Wang năm 2005[3], là kỹ thuật sử dụng độ nhạy thị lực của con người để che giấu một số lượng lớn các bit bí mật vào ảnh gốc. Trong kỹ thuật này, dữ liệu bị nhúng được chuyển đổi thành một loạt các ký hiệu trong một hệ thống các ước số cơ sở. Các cơ sở cụ thể sử dụng được xác định bởi mức độ biến đổi địa phương của cường độ điểm ảnh trong ảnh gốc để cho điểm ảnh ở khu vực bận có khả năng mang nhiều dữ liệu ẩn hơn.

Trong kỹ thuật này, một thông tin mật được nhúng vào trong ảnh gốc bằng cách thay đổi giá trị phần tử ảnh gốc đó theo một thứ tự nào đó, thứ tự đó chính là khóa. Một quy tắc chung là càng có nhiều hơn các biến thể của các giá trị phần tử ảnh trong vùng lân cận của một điểm ảnh, càng có nhiều các điểm ảnh được sửa đổi, cho phép một sự thay đổi lớn hơn.

Về mặt khai thác, người nhận có thể tìm lại được tất cả những cơ sở sai phân tương ứng với hệ số của chúng từ ảnh giấu tin. Ở bên nhận, ảnh gốc là không cần thiết để khôi phục thông tin đã nhúng.

Một khóa bí mật, cái được chia sẻ bởi người ẩn thông tin mật và người nhận, xác định một đường dẫn cụ thể của giả ngẫu nhiên đi qua các điểm ảnh. Điều này đạt được bằng cách thực hiện theo các bước sau:

- *Bước 1*: Giả sử S_0 là một tập hợp gồm các điểm ảnh trong hàng trên nhất và các cột trái nhất, và S_1 là một tập hợp các điểm ảnh còn lại. Giả sử H là một chuỗi các điểm ảnh, bước đầu rỗng.
- *Bước 2*: Chọn một điểm ảnh $p(i,j)$ từ S_1 đó đáp ứng các điều kiện, $p(i-1, j)$, $p(i-1, j-1)$ và $p(i, j-1) \in S_0$, và thêm nó vào cuối của H. Nếu có nhiều hơn một điểm ảnh đáp ứng điều kiện, phần tử được nối vào H được quyết định theo khóa. Cập nhật S_0 và S_1 bằng cách thêm $p(i, j)$ vào S_0 và loại bỏ $p(i,j)$ từ S_1 , tức là, $S_0 \leftarrow S_0 + \{p(i, j)\}$ và $S_1 \leftarrow S_1 - \{p(i, j)\}$.
- *Bước 3*: Lặp đi lặp lại Bước 2 cho đến khi S_1 trở nên trống rỗng.

Vì vậy, chuỗi cuối cùng H có tất cả các điểm ảnh $p(i,j)$ ($2 \le i \le M$, $2 \le j \le N$) được sửa đổi, trong đó M và N là số hàng và số cột của ảnh gốc, và các thông tin mật sẽ được nhúng vào tất cả các điểm ảnh, ngoại trừ các hàng hàng đầu nhất và các cột trái nhất sau một con đường chỉ định bởi H suy ra khoá. Tức là, phần tử đầu tiên ở H

là $p(2,2)$ và phần tử cuối cùng là $p(M, N)$. Bất kỳ điểm ảnh nào trong ảnh gốc chỉ có thể được xử lý sau khi các điểm láng giềng trái, đầu và trái nhất đã được xử lý trước đó. Một ví dụ đơn giản như việc đi bộ qua các điểm ảnh trong một ảnh gốc lưu trữ có kích thước 4 × 8 được thể hiện trong Hình 3.1. Trình tự của chuỗi H trong trường hợp này là {p(2,2) p(2,3) p(3,2)p(2,4) p(3,3)… p(4,8)}.

	1	2	4	6	7	11	16
	3	5	9	12	15	18	19
	8	10	13	14	17	20	21

Hình 3.1. Một ví dụ của điểm ảnh để chèn dữ liệu.

3.2. Quá trình giấu tin

3.2.1. Ý tưởng

- Đầu vào: ảnh xám 8-bit màu, tham số Δ, khóa bí mật và thông tin mật.
- Đầu ra: ảnh giấu tin.

3.2.2. Các bước thực hiện.

Bước 1: Giá trị điểm ảnh trong ảnh gốc và giấu tin được biểu hiện tương ứng là *p(i, j)* và *p'(i. j)*. Giá trị điểm ảnh ở hàng trên nhất và cột trái nhất của ảnh gốc không được sử dụng cho dữ liệu nhúng. Nói cách khác,

$$p'(i,j) = p(i,j), \quad i = 1 \; or \; j = 1 \tag{3.1}$$

Bước 2: Chia dòng bit của thông tin mật thành các phân đoạn, mỗi bộ bao gồm l bit (ví dụ: $l = 8$ tức là mỗi phân đoạn của thông điệp bí mật sẽ có độ dài 8 bit).

Bước 3:

- Chuyển đổi mỗi đoạn nhị phân thành một số nguyên dương *x*.
- Thiết lập giá trị ban đầu của một tham số $u = 1$, được sử dụng để xác định tổng số các cơ sở cần thiết cho các đoạn bí mật tương ứng này trong hệ thống các ước số cơ sở.

Bước 4:

- Tính độ lệch chuẩn σ(i, j) của ba giá trị *p'(i – 1, j), p'(i – 1, j – 1)* và *p'(i, j – 1)* theo công thức (2.2).

– Tính *b(i, j)* theo công thức (3.2).

$$b(\mathrm{i},\mathrm{j}) = \min\left(\left\lceil\frac{\sigma(\mathrm{i},\mathrm{j})}{\Delta}\right\rceil, 16\right) \tag{3.2}$$

Trong đó Δ là một hằng số và $\lceil\bullet\rceil$ có các số nguyên gần nhất về phía vô cùng. Các cơ sở *b(i, j)* tỷ lệ với $\sigma(i,j)$ trừ khi cơ sở được cắt bớt tới 16.

Bước 5 : Nếu *b(i, j)* ≤ 1, bỏ qua điểm ảnh này và quay trở lại Bước 4.

Ngược lại, tính toán hệ số tương ứng trong hệ thống các ước số cơ sở (3.3).

$$d(i,j) = \mathrm{mod}[x, b(i,j)]. \tag{3.3}$$

Bước 6: Tính p'_1 theo công thức (3.4) và p'_2 theo công thức (3.5):

$$p'_1 = \left\lfloor\frac{p(i,j) - d(i,j)}{b(i,j)}\right\rfloor \cdot b(i,j) + d(i,j) \tag{3.4}$$

và

$$p'_2 = \left\lfloor\frac{p(i,j) - d(i,j)}{b(i,j)} + 1\right\rfloor \cdot b(i,j) + d(i,j) \tag{3.5}$$

Trong đó toán tử $\lfloor\bullet\rfloor$ có các số nguyên gần nhất đối với âm vô cực. Giá trị của điểm ảnh trong ảnh giấu tin đơn giản là chọn giữa p'_1 và p'_2.

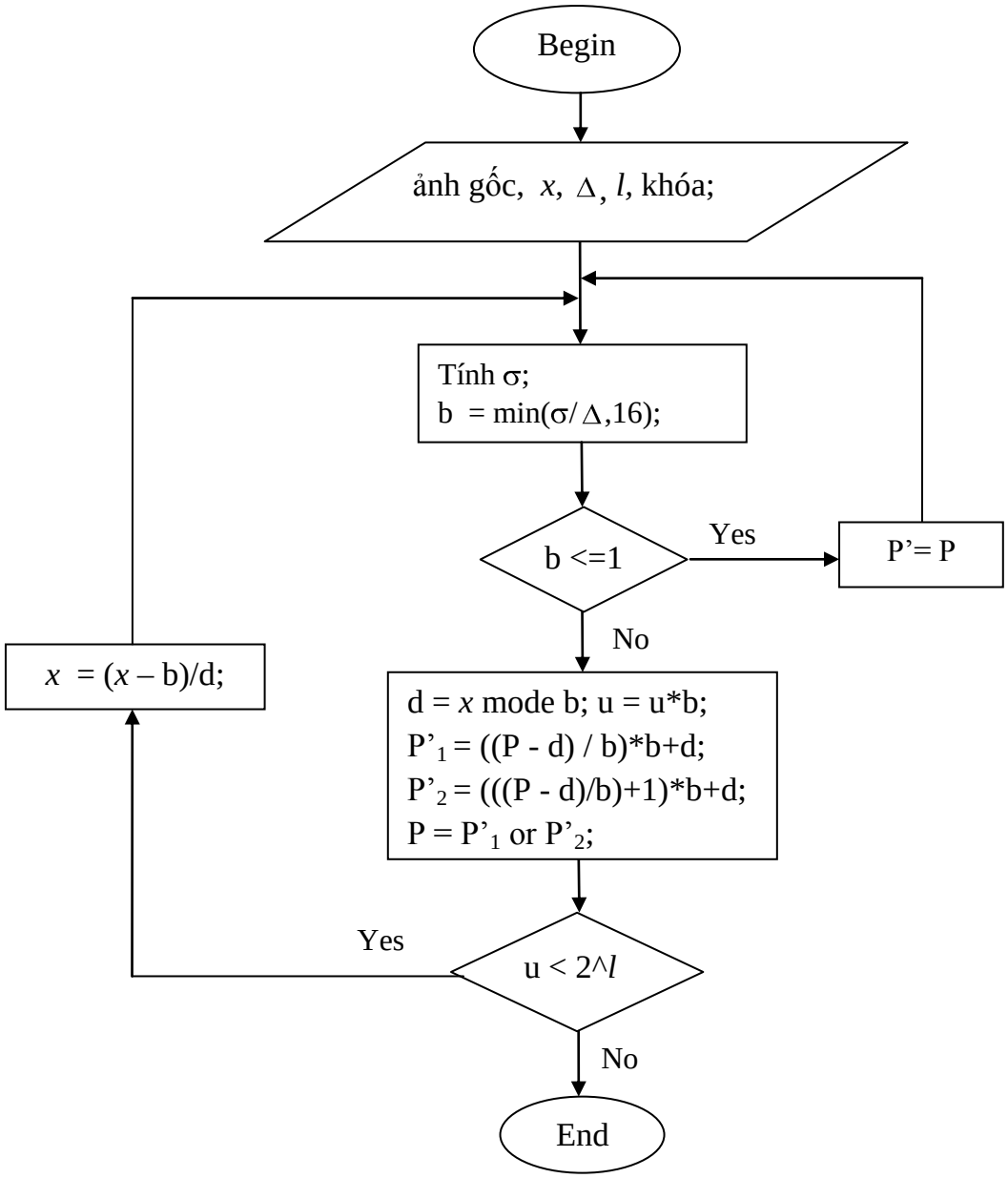
Bước 7: Cập nhật các tham số *u*:

$$u \leftarrow u \cdot b(i,j). \tag{3.6}$$

Nếu u < 2^l , có nghĩa là phân khúc bí mật chưa được biểu diễn hoàn toàn, vào bước 4 sau khi cập nhật giá trị của *x:*

$$x \leftarrow \frac{x - d(i,j)}{b(i,j)}. \tag{3.7}$$

Ngược lại, thực hiện lại bước 3 để nhúng một đoạn nhị phân, cho đến khi tất cả các phân đoạn của dòng bit bí mật được nhúng. Bằng cách này, mỗi phân đoạn nhị phân được nhúng vào một số điểm ảnh trong ảnh gốc.



Hình 3.2. Lưu đồ thuật toán giấu tin

3.3. Quá trình tách tin

3.3.1. Ý tưởng

Quá trình tách tin sử dụng đầu ra của quá trình giấu tin làm đầu vào, cùng với khóa bí mật và tham số Δ để phục hồi thông tin mật đã nhúng.

- Đầu vào: ảnh giấu tin, khóa bí mật, tham số Δ.
- Đầu ra: thông tin mật.

3.3.2. Các bước thực hiện

Bước 1:

- Tính độ lệch chuẩn σ.
- Tính lần lượt *b(i, j)* từ ảnh giấu tin sử dụng công thức (3.2).

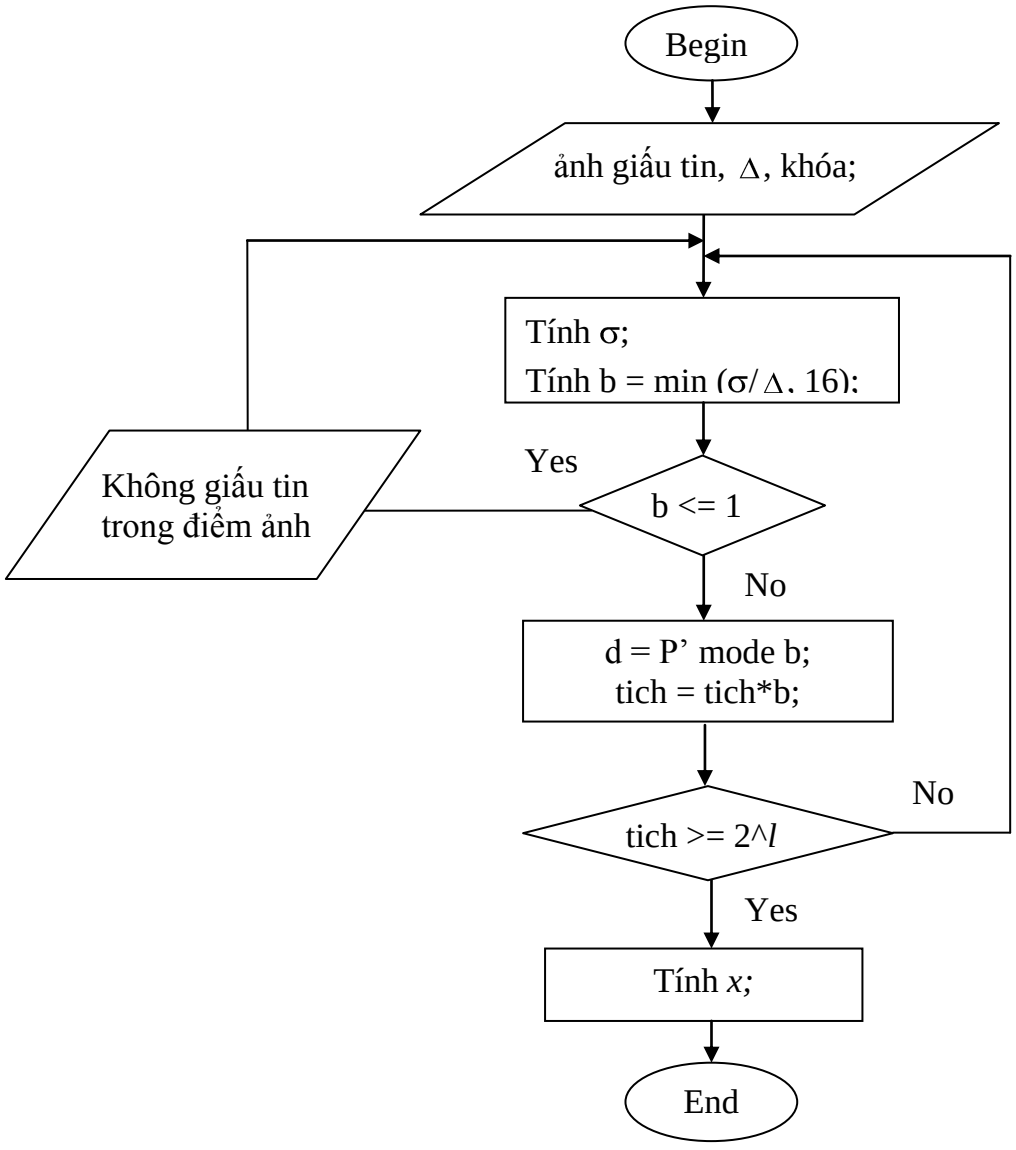
Bước 2:

- Nếu *b(i, j)* > 1.
  - Tính *d(i, j)* theo (3.8).

$$d(i,j) = mod[p'(i,j), b(i,j)] \quad (3.8)$$

  - Tính tích của các cơ sở *b(i, j)* vừa tìm được.
- Ngược lại thực hiện bước 1.

Bước 3: Nếu tích < 2^l quay lại bước1. Ngược lại áp dụng công thức (2.4) để tính *x*.



Hình 3.3. Lưu đồ thuật toán tách tin

CHƯƠNG 4: CÀI ĐẶT THỬ NGHIỆM CHƯƠNG TRÌNH

4.1. Môi trường thử nghiệm

4.1.1. Giới thiệu môi trường thử nghiệm

Hệ điều hành được dùng để thử nghiệm là: Window XP, bộ vi xử lý Intel(R) Pentium(R) D CPU 3.00GHz, Ram 1Gb, ổ cứng 60Gb.

Ngôn ngữ sử dụng để cài đặt kỹ thuật là ngôn ngữ Matlab. Matlab là một phần mềm toán học của hãng Mathworks để tính toán trên các số và có tính trực quan rất cao. Matlap đã qua nhiều phiên bản, chương trình cài đặt này được cài đặt bằng phiên bản Matlab7.7.0.471 (R2008b).

Matlap có thể làm việc với nhiều kiểu dữ liệu khác nhau như: ma trận, chuỗi ký tự, các bài toán về giải tích số, xử lý tín hiệu số, xử lý đồ họa….Matlab có đến hàng ngàn lệnh và hàm tiện ích. Ngoài các hàm cài đặt sẵn trong chính ngôn ngữ, matlab còn có các lệnh và hàm ứng dụng chuyên biệt trong các toolbox.

Matlab còn có giao diện đồ họa rất đẹp mắt và dễ sử dụng. Có thể tính toán và tạo nên các hình ảnh đồ họa 2, 3 chiều cho trình ứng dụng của mình.

4.1.2. Tập dữ liệu thử nghiệm

Tập dữ liệu thử nghiệm bao gồm 10 ảnh chuẩn kích thước 512×512 [6] xem Hình 4.1 và 20 ảnh bất kỳ được chụp từ điện thoại di động, máy ảnh kỹ thuật số và được convert thành ảnh xám 8 bit bởi phần mềm Adobe Photoshop CS với nhiều kích cỡ khác nhau xem Hình 4.2.

Hình 4.1. 10 ảnh chuẩn.

Hình 4.2. 20 ảnh bất kỳ.

4.1.3. Tiêu chuẩn đánh giá chất lượng mã hóa ảnh (PSNR)

Để đánh giá chất lượng của bức ảnh ở đầu ra của bộ mã hóa, người ta thưởng sử dụng hai tham số: Sai số bình phương trung bình – MSE và tỉ số tín hiệu trên nhiễu đỉnh – PSNR [5]. MSE thường được gọi là phương sai lượng tử.

Cho hai hình ảnh P và P’ có kích thước $m \times n$, PSNR được tính theo công thức(4.1) và công thức(4.2) :

$$\text{PSNR} = 10 \log_{10} \frac{Max^2}{MSE} db \tag{4.1}$$

$$\text{MSE} = \left(\frac{1}{m*n}\right) \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(P(i,j) - P'(i,j)\right)^2 \tag{4.2}$$

Trong đó, MAX là giá trị tối đa điểm ảnh của hình ảnh. Khi các điểm ảnh được biểu diễn bằng cách sử dụng 8 bit / màu, Max = 255.

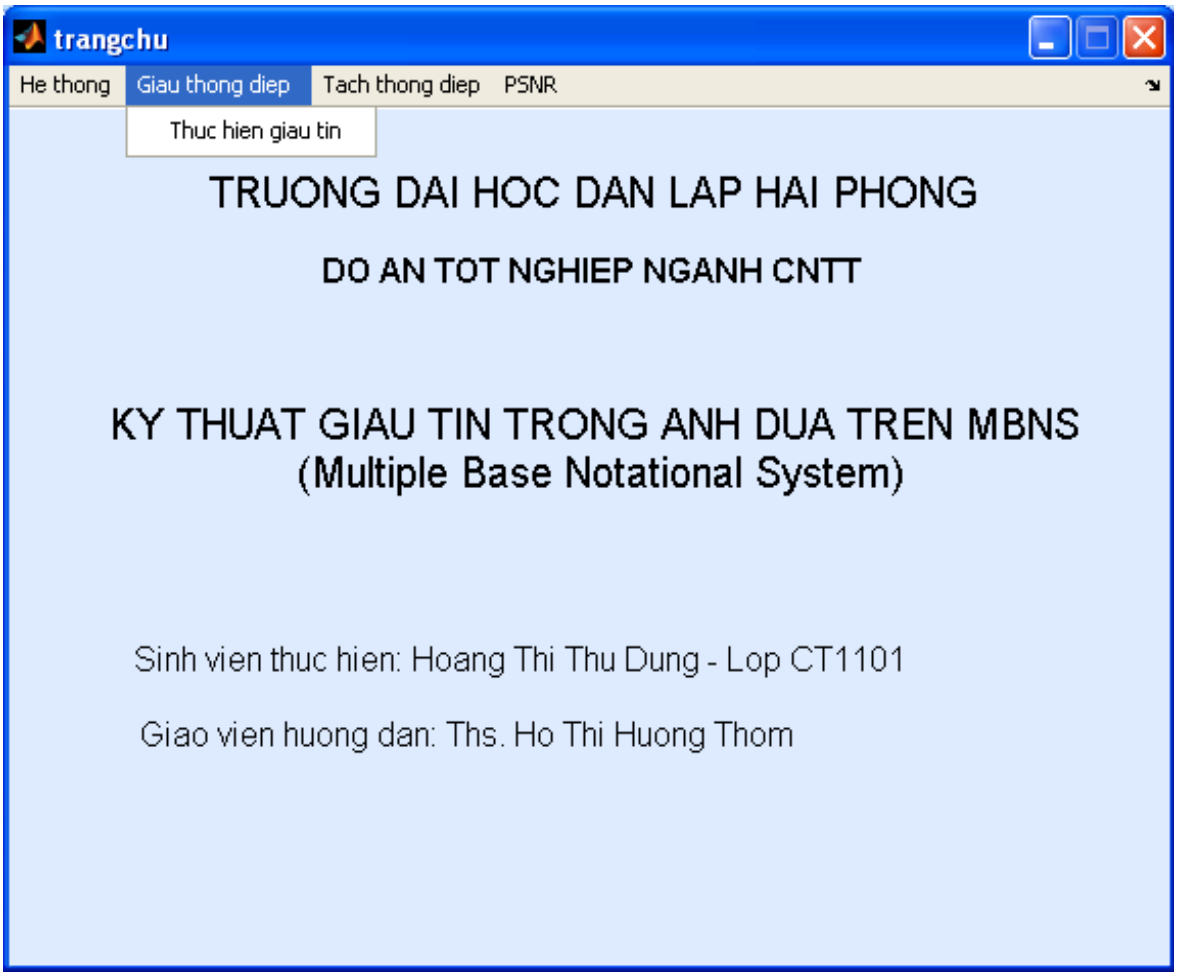
Khi hai hình ảnh giống hệt nhau, các MSE sẽ là số không. Đối với các giá trị này là không xác định PSNR.

4.1.4. Một số giao diện chương trình

4.1.4.1. Giao diện chính của chương trình

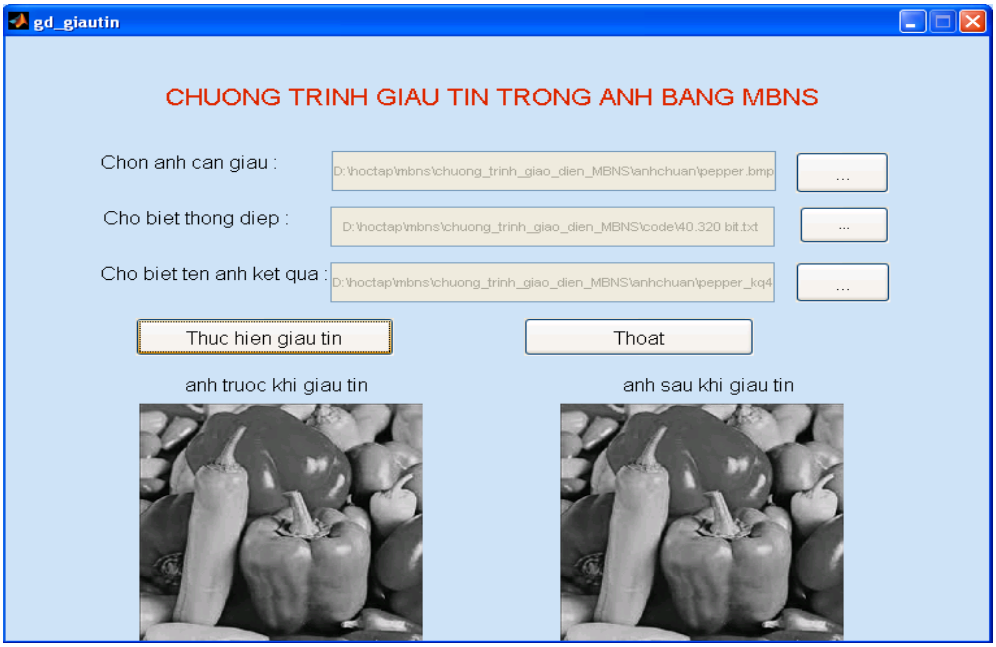
Bao gồm các chức năng:

+ Hệ thống: chức năng thoát để thoát khỏi chương trình.
+ Giấu thông điệp: Chức năng thực hiện giấu tin giấu thông tin mật vào ảnh.
+ Tách thông điệp: Chức năng thực hiện tách tin tách thông tin mật giấu trong ảnh.
+ PSNR: Đánh giá PSNR.

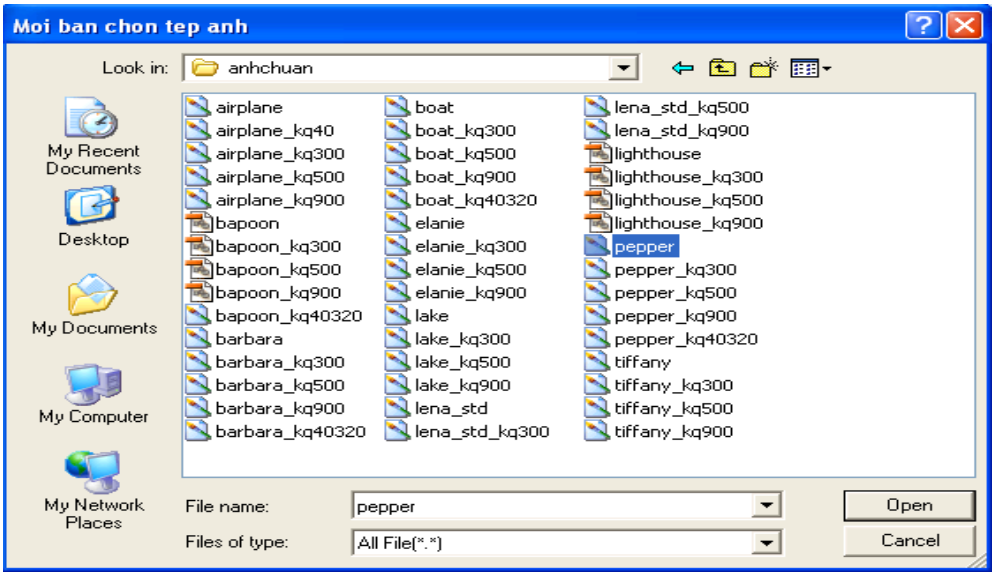


Hình 4.3. Giao diện chính của chương trình

4.1.4.2. Giao diện quá trình giấu tin



Hình 4.4. Giao diện quá trình giấu tin



Hình 4.5. Chọn ảnh

Ô nhập dữ liệu:

- Chọn ảnh cần giấu: click vào [...] để chọn ảnh.
- Cho biết thông điệp: click vào [...] nhập thông điệp cần giấu.
- Cho biết tên ảnh kết quả: click vào [...] để lưu ảnh kết quả.

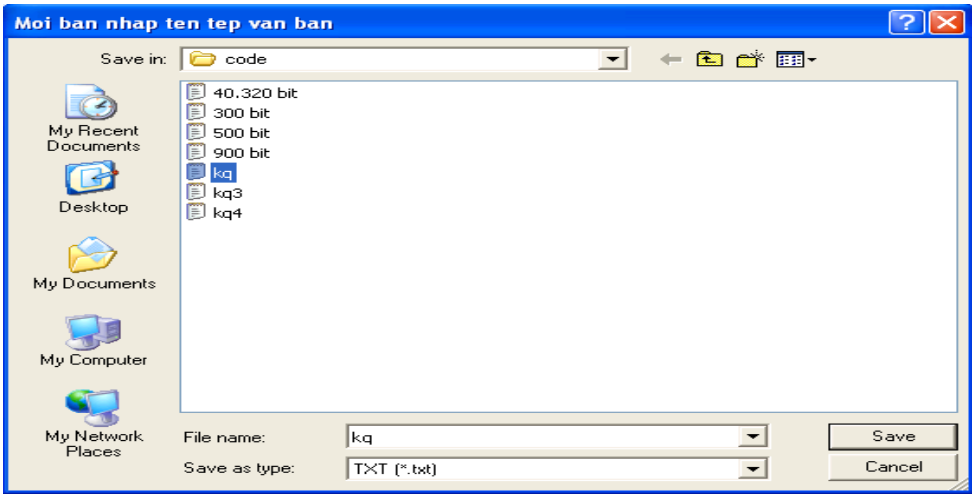
Nút bấm:

- Thực hiện giấu tin: nút thực hiện quá trình giấu thông tin mật.
- Thoát: thoát khỏi giao diện giấu tin.

Khi click vào [...] thứ nhất ta có thể chọn ảnh cần giấu tin, thao tác này xem Hình 4.5. Lần lượt click vào các nút bấm thứ hai và thứ ba để chọn tệp thông tin cần giấu và nơi lưu ảnh kết quả. Sau đó click vào nút bấm thực hiện giấu tin, quá trình giấu tin sẽ được thực hiện và cho kết quả như Hình 4.4.

4.1.4.3. Giao diện quá trình tách tin

Hình 4.6. Giao diện quá trình tách tin



Hình 4.7. Chọn tệp lưu thông tin đã giấu.

Ô nhập dữ liệu:

- Chọn ảnh cần tách tin: click vào [...] để chọn ảnh có giấu tin.

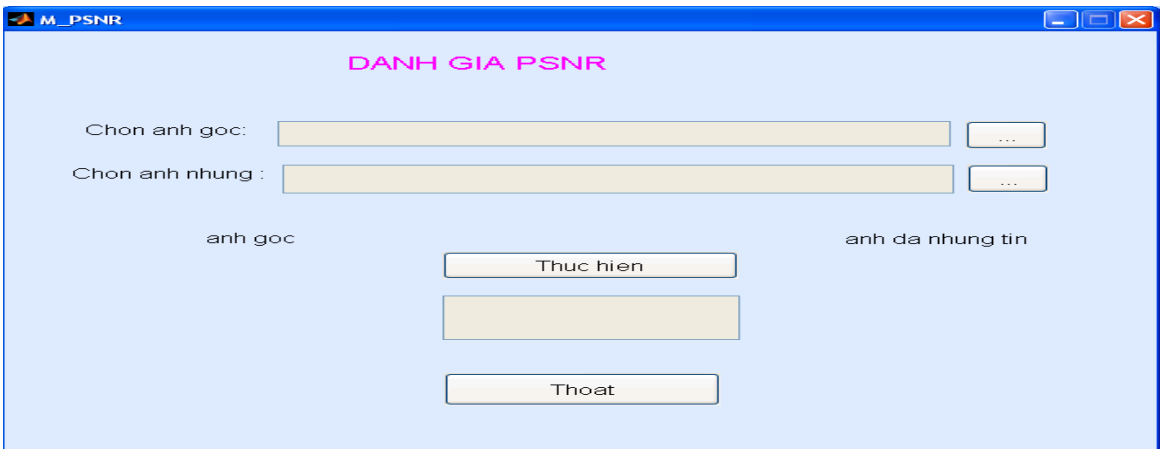
– Chọn tệp cần lưu: click vào [...] để chọn tệp lưu thông tin mật đã giấu.

Nút bấm:

– Thực hiện tách tin: nút thực hiện quá trình tách thông tin mật.
– Thoát: thoát khỏi giao diện tách tin.

Quá trình tách tin sẽ thực hiện ngược lại với quá trình giấu tin. Đầu vào của quá trình tách tin sẽ là ảnh giấu tin, để chọn ảnh click vào [...] để chọn ảnh cần tách thông tin mật, ảnh sẽ được hiện lên trong giao diện để ta biết rằng đã chọn đúng ảnh hay chưa. Tiếp đó sẽ chọn tệp để lưu thông tin mật đó, xem Hình 4.7. Cuối cùng bấm nút thực hiện tách tin, quá trình tách tin sẽ được thực hiện xem Hình 4.6.

4.1.4.4. Giao diện tính PSNR



Hình 4.8-a. trước khi tính PSNR.

Hình 4.8-b. Sau khi tính PSNR

Ô nhập dữ liệu:

- Chọn ảnh gốc: click vào  bên cạnh để chọn ảnh gốc.
- Chọn ảnh nhúng: click vào  bên cạnh để chọn ảnh giấu tin.

Nút bấm:

- Thực hiện tách tin: nút thực hiện quá trình tách thông tin mật.
- Thoát: thoát khỏi giao diện tách tin.

Khi kích chọn ảnh gốc, ảnh gốc sẽ xuất hiện, sau đó kích chọn ảnh nhúng thì ảnh giấu tin sẽ xuất hiện. Việc này sẽ giúp ích cho quá trình thực hiện tính đó là không chọn nhầm ảnh. Tiếp theo sẽ kích chọn nút bấm "thực hiện", kết quả PSNR tính được sẽ xuất hiện như hình 4.8-b.

4.2. Các modul cài đặt

4.2.1. Chức năng: Giấu thông tin vào ảnh.

Các tham số đầu vào:

- tenanh: tên của ảnh sẽ giấu tin lên.
- Hằng số Δ và khóa.
- tt: nội dung thông điệp giấu vào.

Tham số đầu ra:

- tenanh_kq: tên ảnh kết quả sau khi giấu tin.

4.2.2. Chức năng: Tách thông tin.

Tham số đầu vào:

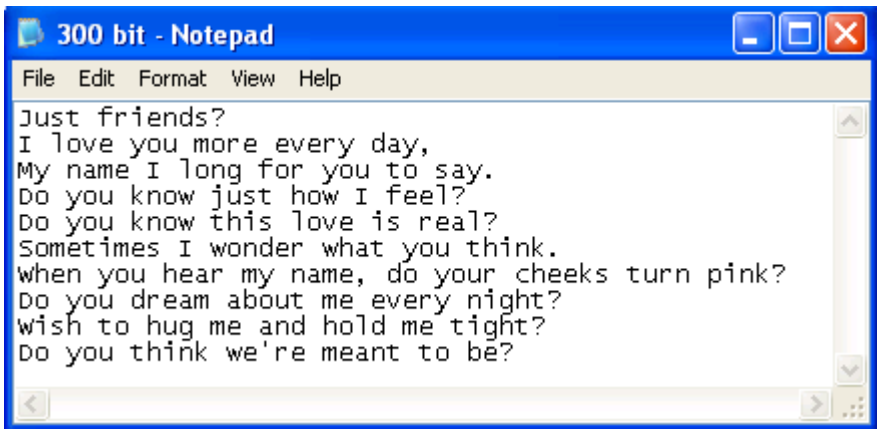
- tenanh: tên ảnh giau tin.
- Hằng số Δ và khóa.

Tham số đầu ra:

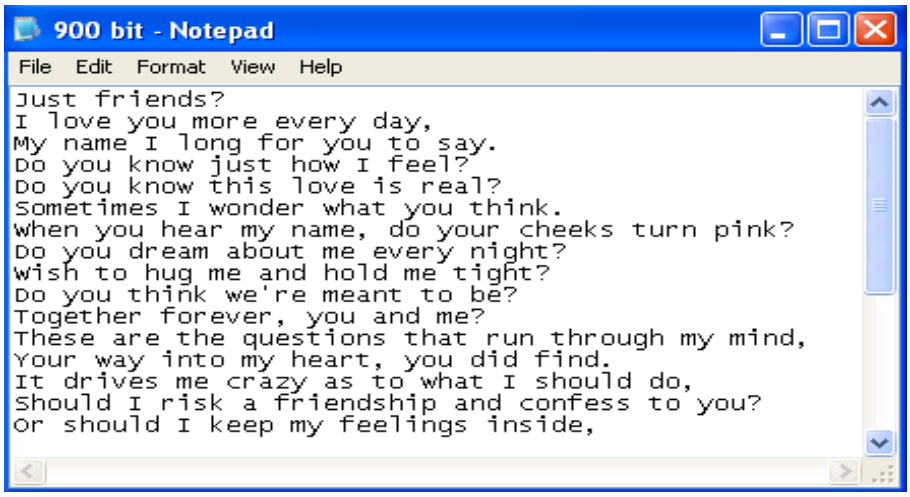
- tt: thông tin tách được từ ảnh đầu vào.

4.3. Thực nghiệm và đánh giá

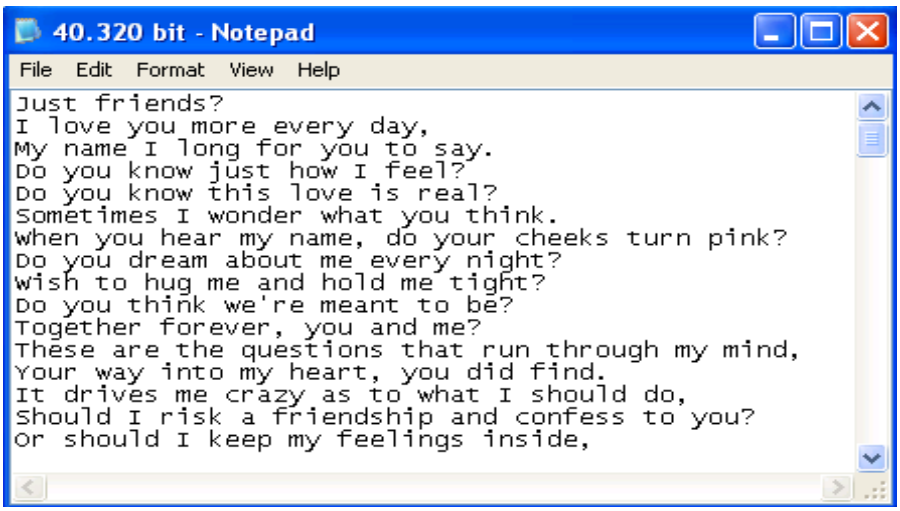
4.3.1. Thông điệp giấu



Hình 4.9. Thông điệp (nội dung 300 bit).



Hình 4.10. Thông điệp (nội dung 900 bit).



Hình 4.11. Thông điệp (nội dung 40.320 bit).

4.3.2. Giấu trên 10 ảnh chuẩn

Bảng 4.1. Kết quả thực nghiệm trên 10 ảnh chuẩn.

Số bit **Ảnh gốc**	**PSNR**		
	300	**900**	**40320**
Airplane	60.3614	56.4616	50.5363
bapoon	55.648	50.6087	43.6339
Barbara	57.2132	52.5983	46.3698
Boat	61.3687	56.2471	48.7056
Elanie	62.943	57.7939	50.3309
Happy	67.8139	63.7371	45.3164
Lena_std	63.7277	58.8445	50.9274
Lighthouse	61.0055	55.8497	48.1742
Pepper	57.5798	52.746	46.8319
Tiffany	65.5156	58.7521	49.1016
Trung bình	**61.31768**	**56.3639**	**47.9928**

Tập ảnh kết quả:

Hình 4.12. Tập ảnh chuẩn trước và sau khi giấu.

4.3.3. Giấu trên 20 ảnh bất kỳ

Bảng 4.2. Kết quả thực nghiệm 20 ảnh bất kỳ.

Số bit **Ảnh gốc**	**PSNR**		
	300	**900**	**40320**
01.png	53.7407	49.125	41.6319
02.png	60.6232	54.3189	40.307
03.bmp	55.1708	50.1816	43.1424
04.bmp	55.3854	51.1616	44.0812
05.bmp	51.2125	49.5213	41.0394
06.bmp	49.4411	44.6118	37.7963
07.bmp	62.2417	57.4447	49.4331
08.bmp	51.5485	46.6352	38.8222
09.bmp	48.6867	43.921	36.7959
10.bmp	55.1572	48.592	38.9122
11.bmp	50.1696	47.4947	42.7609
12.png	58.6543	53.0059	41.5758
13.bmp	57.742	54.7277	38.3548
14.bmp	50.7601	48.886	41.9198
15.png	54.328	46.4391	37.9486
16.bmp	58.55	53.6277	40.8378
17.bmp	51.8717	46.5806	39.6697
18.bmp	52.2064	45.2298	37.9341
19.bmp	49.4943	44.6083	38.6369
20.png	50.7048	46.7516	38.6479
Trung bình	**53.88445**	**49.14323**	**40.5124**

Hình 4.12. Tập ảnh trước và sau khi giấu.

Nhận xét: Thông qua các giá trị của Bảng 4.11 và Bảng 4.12, ta thấy kỹ thuật giấu được lượng thông tin lớn và quá trình xử lý nhanh, chất lượng hình ảnh sau khi giấu tin là tốt (PSNR >39).

Tập ảnh kết quả:

Hình 4.13. Tập ảnh bất kỳ trước và sau khi giấu tin.

KẾT LUẬN

Khóa luận đã thực hiện nhiệm vụ:

1. Trình bày tổng quan kỹ thuật giấu tin trong ảnh, cấu trúc ảnh bitmap, nghiên cứu kỹ thuật giấu tin dựa trên MBNS.

2. Viết chương trình thử nghiệm kỹ thuật giấu tin dựa trên MBNS.

Đây là một kiến thức rất hữu ích và cần thiết để khai thác ngày một hiệu quả các thành tựu của tin học. Đó cũng là một lý do để em chọn đề tài này làm đồ án tốt nghiệp, mong muốn giới thiệu và phổ biến những kiến thức rất cơ bản đến người đọc.

Việc kết hợp giấu thông tin và công nghệ thông tin là một vấn đề mới đang được nghiên cứu và phát triển để phục vụ nhiều lĩnh vực khác nhau. Trên thế giới người ta đã nghiên cứu nhiều về vấn đề này.

Kỹ thuật giấu thông tin trong ảnh nói chung và giấu thông tin trong ảnh xám nói riêng là một hướng nghiên cứu chính của kỹ thuật giấu thông tin hiện nay và đã đạt nhiều kết quả khả quan.

Trong đề tài này em đã trình bày một số khái niệm liên quan đến việc che giấu thông tin nói chung và cụ thể là thuật toán giấu thông tin trong ảnh xám nói riêng.

Do còn nhiều hạn chế về thời gian nghiên cứu nên đề tài này không tránh khỏi những thiếu sót, vì vậy em rất mong nhận được sự đóng góp ý kiến của các thầy cô và các bạn để đồ án được hoàn thiện.

Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

Tài iệu tiếng việt.

[1] *Nghiên cứu kỹ thuật bảo vệ bản quyền các sản phẩm đồ họa vectơ – Ngô Thái Hà - Luận văn thạc sĩ. Khoa Công nghệ thông tin trường Đại Học Thái Nguyên.*

Website: http://www.scribd.com/doc/51470401/14/Giấu-tin-trong-ảnh-những-đặc-trưng-và-tính-chất.

[2] *Đỗ Lâm Hoàng, Luận văn tốt nghiệp, ngành Công nghệ thông tin,năm 2010.*

Tài liệu tiếng anh.

[3] *Xinpeng Zhang anh Shuozhong Wang, Steganography Using Multiple-Base Notational System and Human Visison Sensitivity, IEEE Singnal Processing Letters, Vol. 12, No. 1, Jan. 2005, pp.67-70.*

[4] *http://www.ieev.org/2009/11/standard-deviation-o-lech-chuan.html.*

[5] *http://en.wikipedia.org/wiki/peak_signal-to-noise_ratio.*

[6] *http://sipi.usc.edu/database/database.php*

[7] *http://vi.wikipedia.org/wiki/BMP.*