

**LỜI CẢM ƠN**

*Trước hết em xin bày tỏ lòng biết ơn sâu sắc nhất tới cô giáo hướng dẫn Tiến sĩ Hồ Thị Hương Thơm đã tận tình giúp đỡ, hướng dẫn em rất nhiều trong suốt quá trình tìm hiểu nghiên cứu và hoàn thành báo cáo tốt nghiệp. Cùng với đó em cũng xin gửi lời cảm ơn đến thầy phản biện Thạc sĩ Nguyễn Trịnh Đông đã góp ý, sửa chữa và hoàn thiện để bài báo cáo của em hoàn thành tốt hơn.*

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

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

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

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

*Em xin chân thành cảm ơn!*

*Hải phòng, ngày... tháng...năm 2013*

*Sinh viên thực hiện*

## MỤC LỤC

<b>LỜI CẢM ƠN .....</b>	<b>1</b>
<b>MỤC LỤC .....</b>	<b>2</b>
<b>DANH MỤC CÁC TỪ VIẾT TẮT .....</b>	<b>4</b>
<b>LỜI MỞ ĐẦU .....</b>	<b>5</b>
<b>CHƯƠNG 1: TỔNG QUAN VỀ GIẤU TIN.....</b>	<b>6</b>
<b>1.1. Giới thiệu chung về giấu thông tin .....</b>	<b>6</b>
<i>1.1.1. Lịch sử giấu tin .....</i>	<i>6</i>
<i>1.1.2. Phương pháp giấu tin .....</i>	<i>7</i>
<i>1.1.3. Mô hình giấu thông tin cơ bản .....</i>	<i>9</i>
<b>1.2. Môi trường giấu tin.....</b>	<b>10</b>
<i>1.2.1. Giấu tin trong ảnh .....</i>	<i>10</i>
<i>1.2.2. Giấu tin trong audio .....</i>	<i>11</i>
<i>1.2.3. Giấu thông tin trong video .....</i>	<i>11</i>
<i>1.2.4. Giấu thông tin trong văn bản dạng text .....</i>	<i>12</i>
<b>1.3. Phân loại kỹ thuật giấu tin .....</b>	<b>12</b>
<b>1.4. Các đặc trưng và ứng dụng của phương pháp giấu tin trong ảnh số .....</b>	<b>14</b>
<i>1.4.1. Các đặc trưng cơ bản .....</i>	<i>14</i>
<i>1.4.2. Các ứng dụng của kỹ thuật giấu tin .....</i>	<i>15</i>
<b>1.5. Ảnh BITMAP và phương pháp đánh giá chất lượng ảnh sau khi giấu tin bằng PSNR.....</b>	<b>16</b>
<i>1.5.1. Ảnh BITMAP .....</i>	<i>16</i>
<i>1.5.2. Phương pháp đánh giá chất lượng ảnh sau khi giấu tin bằng PSNR ....</i>	<i>18</i>
<b>CHƯƠNG 2: KỸ THUẬT GIẤU TIN THUẬN NGHỊCH TRÊN MIỀN BIẾN ĐỔI SÓNG NHỎ (WAVELET) CHO ẢNH CHẤT LƯỢNG CAO .....</b>	<b>20</b>
<b>2.1. Khái niệm về giấu tin thuận nghịch .....</b>	<b>20</b>
<b>2.2. Kỹ thuật giấu tin thuận nghịch trên miền biến đổi wavelet .....</b>	<b>21</b>

---

2.2.1. Khái niệm miền biến đổi sóng nhỏ.....	21
2.2.2. Kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao.....	25
<b>CHƯƠNG 3: CÀI ĐẶT VÀ THỬ NGHIỆM.....</b>	<b>32</b>
<b>3.1. Môi trường cài đặt .....</b>	<b>32</b>
<b>3.2. Giao diện chương trình .....</b>	<b>33</b>
3.2.1. <i>Giao diện chương trình chính .....</i>	33
3.2.2. <i>Giao diện chức năng giấu tin .....</i>	33
3.2.3. <i>Giao diện chức năng tách tin .....</i>	37
3.2.4. <i>Giao diện chức năng đánh giá PSNR.....</i>	42
<b>3.3. Kết quả thực nghiệm và nhận xét.....</b>	<b>44</b>
3.3.1. <i>Kết quả thực nghiệm.....</i>	44
3.3.2. <i>Nhận xét.....</i>	53
<b>KẾT LUẬN .....</b>	<b>55</b>
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>56</b>

**DANH MỤC CÁC TỪ VIẾT TẮT**

<b>HVS</b>	<b>Human Vision System</b>
<b>HAS</b>	<b>Human Auditory System</b>
<b>BMP</b>	<b>BitMap</b>
<b>PSNR</b>	<b>Peak Signal To Noise Ratio</b>
<b>MSE</b>	<b>Mean Squared Error</b>
<b>DE</b>	<b>Difference Expansion</b>
<b>NSAS</b>	<b>Kỹ thuật giấu thuận nghịch NSAS</b>
<b>DIH</b>	<b>Difference Image Histogram</b>
<b>HKC</b>	<b>Kỹ thuật giấu tin của ba tác giả J. Hwang, J. Kim và J</b>
<b>MBNS</b>	<b>Multiple - Base Notational System</b>
<b>RCM</b>	<b>Kỹ thuật giấu thuận nghịch RCM</b>
<b>RL</b>	<b>Kỹ thuật giấu thuận nghịch RL</b>
<b>LSB</b>	<b>Least Significant Bit</b>
<b>RVH</b>	<b>Reversible Vertical Horizontal Technique</b>
<b>STFT</b>	<b>Short Time Fourier Transform</b>
<b>DWT</b>	<b>Discrete Wavelet Transform</b>
<b>IDWT</b>	<b>Inverse Discrete Wavelet Transformation</b>
<b>LL</b>	<b>Horizontally and vertically lowpass</b>
<b>LH</b>	<b>Horizontally lowpass and vertically highpass</b>
<b>HL</b>	<b>Horizontally highpass and vertically lowpass</b>
<b>HH</b>	<b>Horizontally and vertically highpass</b>

## LỜI MỞ ĐẦU

Giấu tin trong dữ liệu đa phương tiện một công nghệ mới trong bảo mật thông tin. Đây là một phương pháp mới và phức tạp, nó đang được xem như một công nghệ chìa khóa cho vấn đề bảo vệ bản quyền và điều khiển truy cập... ứng dụng trong bảo mật thông tin.

Cuộc cách mạng thông tin kỹ thuật số đã đem lại những thay đổi sâu sắc trong xã hội và trong cuộc sống của chúng ta. Những thuận lợi mà thông tin kỹ thuật số mang lại cũng sinh ra những thách thức và cơ hội mới cho quá trình đổi mới. 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 thương thức các dữ liệu đa phương tiện. 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 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.. 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. Do đó trong đề án này tìm hiểu phương pháp giấu tin trong ảnh. Nội dung gồm 3 chương chính sau:

➤ Chương 1. Tổng quan về giấu tin trong ảnh: Giới thiệu về một số định nghĩa giấu thông tin, môi trường giấu tin, sơ lược về mô hình giấu tin cơ bản. Tìm hiểu về ảnh bitmap, phương pháp đánh giá chất lượng ảnh sau khi giấu thông tin.

➤ Chương 2. Trình bày kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao: Thuật toán, sơ đồ thuật toán, ví dụ minh họa của hai quá trình giấu tin và tách tin.

➤ Chương 3. Cài đặt và thử nghiệm: Đưa ra môi trường cài đặt, giới thiệu giao diện chương trình và chạy thử nghiệm trên một số ảnh kèm theo đó là đưa ra nhận xét cho thử nghiệm.

➤ Kết luận và danh mục tài liệu tham khảo.

## CHƯƠNG 1: TỔNG QUAN VỀ GIẤU TIN

### 1.1. Giới thiệu chung về giấu thông tin

#### 1.1.1. 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 sẫm có như nước quả, nước tiểu và sữa để viết các thông báo bí mật giữa những hàng văn tự thông thường. Khi bị hơi 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

#### 1.1.2.1. Sơ lược về phương pháp giấu tin

Giấu thông tin là một kỹ thuật nhúng dữ liệu vào một nguồn đa phương tiện gọi là môi trường, ví dụ như file âm thanh, ảnh động, ảnh tĩnh . . . Mục đích của che giấu thông tin là làm cho dữ liệu trở lên không thể nghe thấy hay nhìn thấy. Điều đó có nghĩa là đối phương không nhận thấy sự tồn tại của dữ liệu đã được nhúng dù có lắng nghe hay cố gắng nhìn thật cẩn thận vào môi trường có giấu dữ liệu.

Mỗi kỹ thuật giấu tin gồm :

- Thuật toán giấu tin
- Bộ giải mã thông tin

Thuật toán giấu tin được dùng để giấu thông tin vào một phương tiện mang bằng cách sử dụng một khóa bí mật được dùng chung bởi người mã và người giải mã, việc giải mã thông tin chỉ có thể thực hiện được khi có khóa. Bộ giải mã trên phương tiện mang đã chứa dữ liệu và trả lại thông điệp ẩn trong nó.

Ví dụ 1: Thông điệp cần gửi đã được mã hóa và giấu vào trong ảnh.



Hình 1.1. Ảnh đã được giấu thông tin

Ví dụ 2: Thông điệp được giấu trong 1 đoạn văn bản.

Bản tin: Đến gặp trại trưởng ở nhà

Nhà anh ở tận cuối làng

Thờ ông thờ bà kính tôn

Đề cho anh ấy hướng dẫn

Dự cuộc họp mặt vui chơi

Lễ mừng ngày tết thiếu nhi.

Chìa khóa: Tập hợp các đội trưởng nghe lệnh.

Cách giải: Khi đó ta lấy tất cả các chữ đầu của mỗi hàng ghép lại thành 1 thông tin mật: “Đến nhà thờ để dự lễ”.

#### *1.1.2.2. Những đối tượng chính trong phương pháp giấu tin*

**Thông tin mật:** Là thông tin nhúng vào trong đối tượng chứa và là thông tin cần được bảo vệ.

**Đối tượng chứa:** Được sử dụng để chứa thông điệp mật.

**Đối tượng đã nhúng:** Là đối tượng sau khi nhúng thông tin mật. Ví dụ nếu đối tượng chứa là ảnh thì đối tượng đã nhúng là Stego-Image.

**Khóa mật:** Là khóa tham gia vào quá trình nhúng cũng như tách, tùy từng phương pháp khóa mật sẽ tham gia những cách khác nhau.

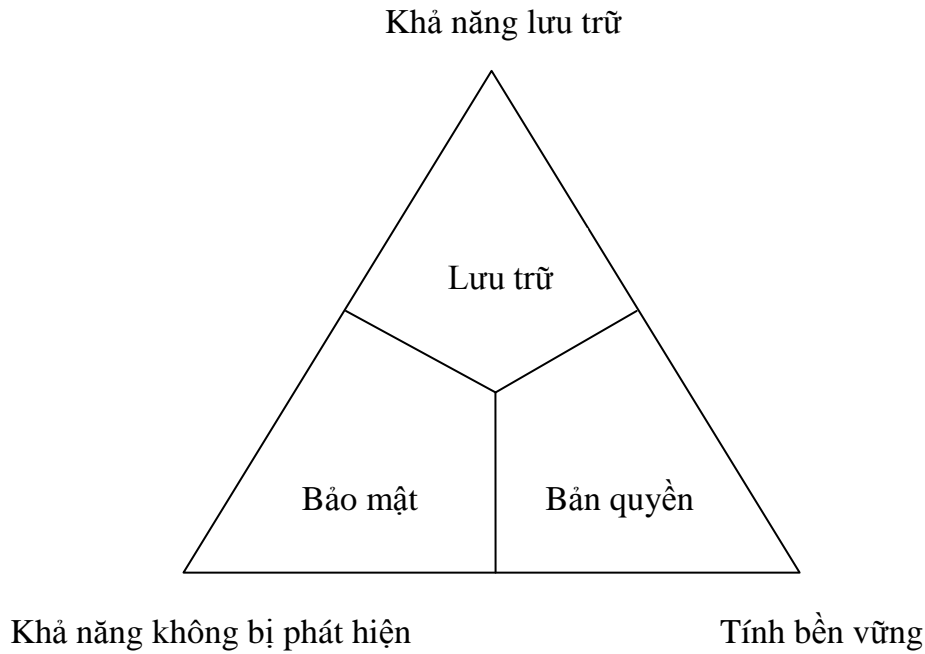
#### *1.1.2.3. Các yêu cầu trong phương pháp giấu tin*

**Tính bền vững:** Thể hiện khả năng ít bị thay đổi từ những tác động bên ngoài như thay đổi định dạng, nội dung. Hiện nay chưa có phương pháp nào thỏa mãn tính bền vững tuyệt đối. Với từng ứng dụng cụ thể thì yêu cầu này cũng thể hiện khác nhau.

**Khả năng bị phát hiện:** Thể hiện ở việc khó xác định đối tượng có giấu tin hay không. Hầu hết các phương pháp giấu tin đều dựa trên đặc điểm của hai hệ tri giác của con người là thị giác và thính giác để khai thác. khả năng này còn gọi là khả năng giả dạng.

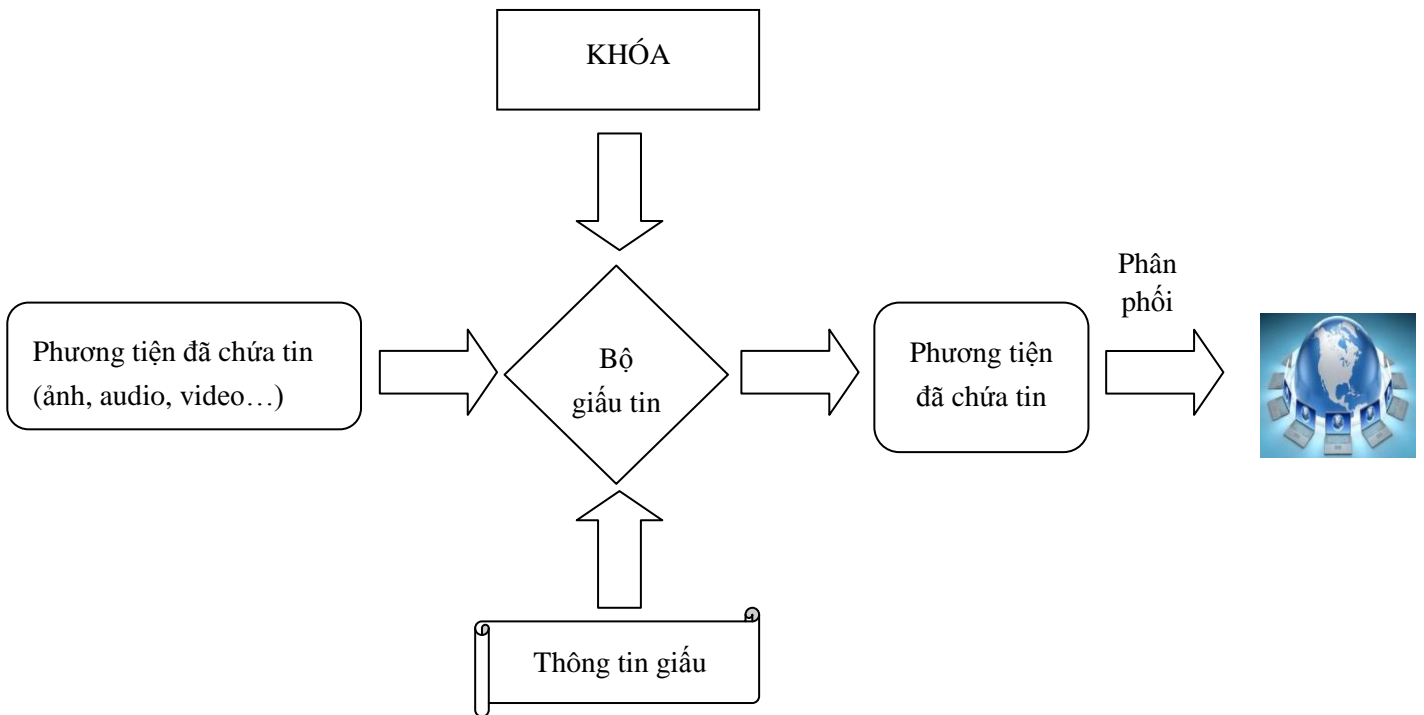
**Khả năng lưu trữ:** Thể hiện ở lượng thông tin của thông điệp có thể nhúng vào trong đối tượng. Do tính bảo mật nên khả năng lưu trữ bị hạn chế đi rất nhiều. Vậy nên muốn giấu một thông tin có kích thước lớn ta thường chia nhỏ ra nhiều phần và thực hiện nhúng từng phần.





Hình 1.2. Các yêu cầu trong phương pháp giấu tin

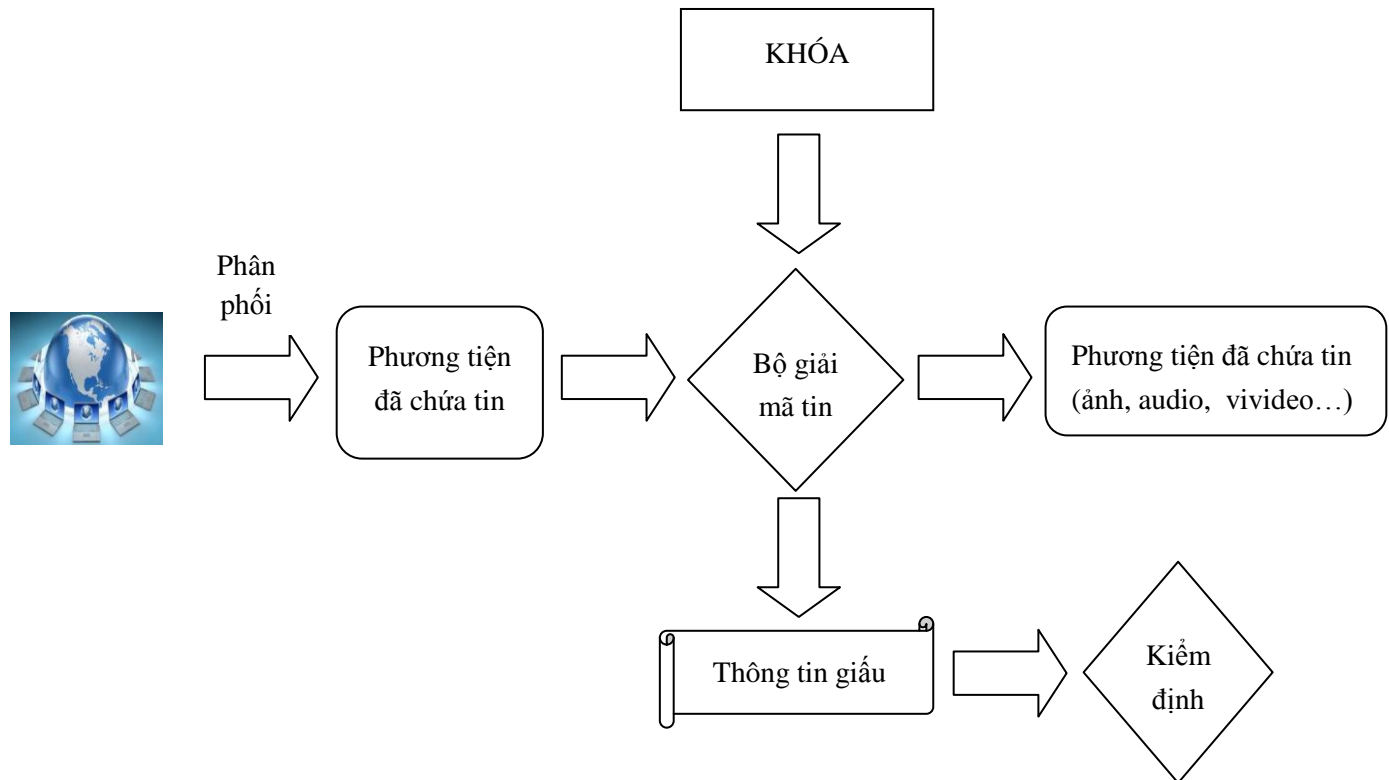
**1.1.3. Mô hình giấu thông tin cơ bản**



Hình 1.3. Lược đồ chung cho giấu thông tin

Hình 1.3 biểu diễn mô hình giấu tin cơ bản. Trong đó, phương tiện chứa tin có thể bao gồm: văn bản, ảnh, audio, video... Thông tin cần giấu tùy theo mục đích của người sử dụng. Thông tin được giấu vào trong phương tiện chứa tin nhờ một bộ nhúng.

Bộ nhúng là những chương trình thực hiện theo những thuật toán để giấu tin và được thực hiện với một khóa bí mật giống như trong một số hệ mật mã. Đầu ra của quá trình nhúng tin là phương tiện chứa đã được giấu tin. Các phương tiện chứa này có thể được phân phối trên mạng.



Hình 1.4. Lược đồ chung cho quá trình giải mã

Hình 1.4 mô tả quá trình giải mã thông tin đã được giấu trước đó. Đầu vào là phương tiện có chứa tin giấu, qua một bộ giải mã tin (tương ứng với bộ nhúng tin) cùng với khóa sẽ được thực hiện việc giải mã thông tin. Đầu ra của quá trình là phương tiện chứa tin và thông tin mật đã giấu trước đó. Trong trường hợp cần thiết, thông tin lấy ra có thể được xử lý, kiểm định và so sánh với thông tin đã giấu ban đầu.

Tóm lại, giấu thông tin vừa là khoa học vừa là nghệ thuật. Mục đích của giấu tin mật là che giấu những thông tin bên trong những thông tin khác mà không làm ảnh hưởng đáng kể đến thông tin này và bằng một cách thức nào đó sao cho người không có thẩm quyền không thể phát hiện hoặc không thể phá hủy chúng.

## 1.2. Môi trường giấu tin

### 1.2.1. Giấu tin trong ảnh

Ngày nay khi khoa học kỹ thuật phát triển, ảnh số đã được sử dụng rất phổ biến thì giấu tin trong ảnh đem lại những ứng dụng quan trọng trên các lĩnh vực trong đời

sống xã hội. Ví dụ như ở 1 số nước phát triển chữ kí tay đã được số hóa và lưu trữ sử dụng như hồ sơ cá nhân cho các dịch vụ ngân hàng tài chính.

Một đặc điểm quan trọng của giấu tin trong ảnh là thông tin được giấu một cách vô hình, nó như một cách truyền thông tin mật cho nhau mà người khác không thể biết được bởi sau khi giấu thông tin chất lượng ảnh không thay đổi với cả ảnh màu hay ảnh xám.

### ***1.2.2. Giấu tin trong audio***

Giấu thông tin trong audio mang những đặc điểm riêng khác với giấu thông tin trong các đối tượng đa phương tiện khác. Một trong những yêu cầu cơ bản của giấu tin là đảm bảo tính chất ẩn của thông tin được giấu đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu gốc. Kỹ thuật giấu thông tin trong ảnh phụ thuộc vào hệ thống thị giác của con người - HVS còn kỹ thuật giấu thông tin trong audio lại phụ thuộc vào hệ thống thính giác - HAS. Đây được coi là một vấn đề khó khăn vì hệ thống thính giác của con người nghe được các tín hiệu ở các dải tần rộng và công suất lớn nên đã gây khó dễ đối với các phương pháp giấu tin trong audio. Nhưng thật may là HAS lại kém trong việc phát hiện sự khác biệt các dải tần và công suất điều này có nghĩa là các âm thanh to, cao tần có thể che giấu được các âm thanh nhỏ thấp một cách dễ dàng. Các mô hình phân tích tâm lí đã chỉ ra điểm yếu trên và thông tin này sẽ giúp ích cho việc chọn các audio thích hợp cho việc giấu tin.

Vấn đề khó khăn thứ hai đối với giấu thông tin trong audio là kênh truyền tin. Kênh truyền hay băng thông chậm sẽ ảnh hưởng đến chất lượng thông tin sau khi giấu. Giấu thông tin trong audio đòi hỏi yêu cầu rất cao về tính đồng bộ và tính an toàn của thông tin. Các phương pháp giấu thông tin trong audio đều lợi dụng điểm yếu trong hệ thống thính giác của con người.

### ***1.2.3. Giấu thông tin trong video***

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

Nhiều nhà nghiên cứu đã dùng những hàm cosin riêng và các hệ số truyền sóng riêng để giấu tin. Trong các thuật toán khởi nguồn thì thường các kỹ thuật cho phép giấu các ảnh vào trong video nhưng thời gian gần đây các kỹ thuật cho phép giấu cả âm thanh và hình ảnh vào video. Như phương pháp của Swanson đã sử dụng phương

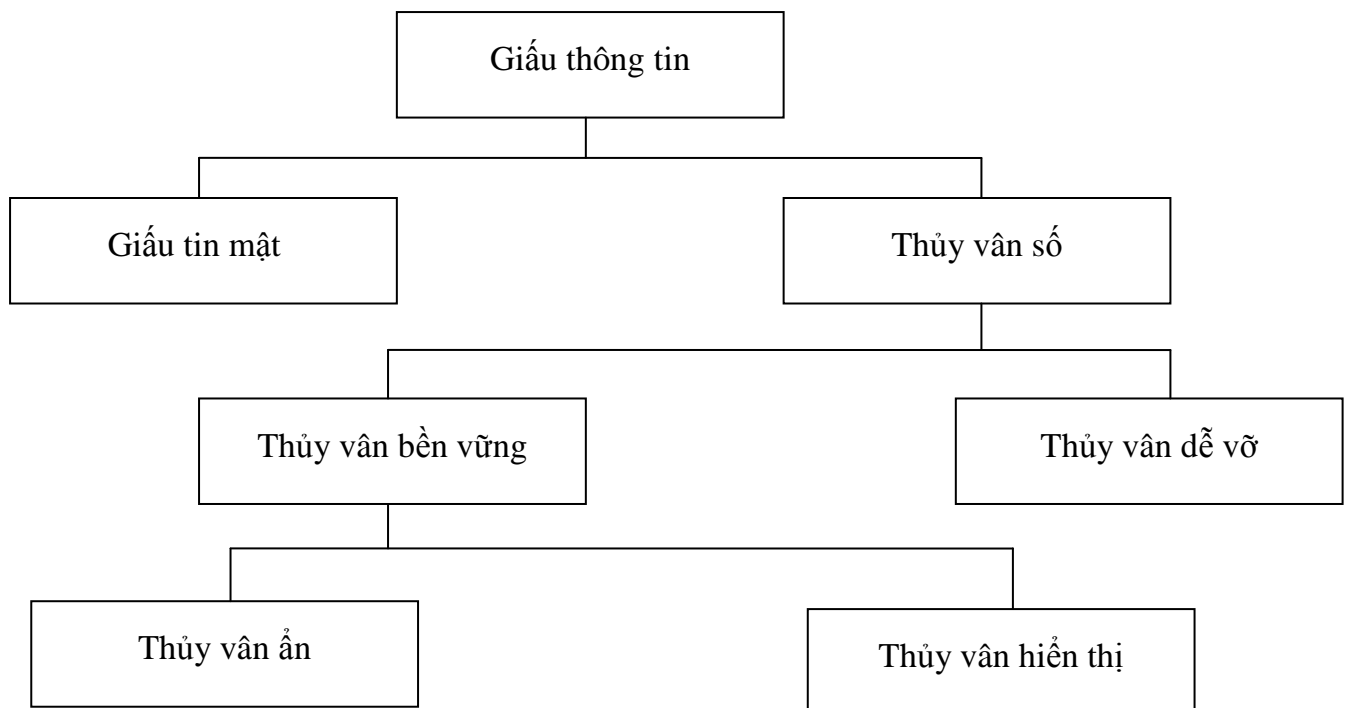
pháp giấu theo khối, phương pháp này đã giấu được hai bit vào khối 8\*8. Hay gần đây nhất là phương pháp của Mukherjee là kỹ thuật giấu audio vào video sử dụng cấu trúc lưới đa chiều...

#### 1.2.4. Giấu thông tin trong văn bản dạng text

Giấu thông tin vào các văn bản dạng text khó thực hiện hơn do có ít các thông tin dư thừa, để làm được điều này người ta phải khéo léo khai thác các dư thừa tự nhiên của ngôn ngữ. Một cách khác là tận dụng các định dạng văn bản (mã hóa thông tin và khoảng cách giữa các từ khóa hay các dòng văn bản). Từ nội dung của thông điệp cần truyền đi, người ta cũng có thể sử dụng văn phạm phi ngữ cảnh để tạo nên các văn bản “phương tiện chứa” rồi truyền đi.

#### 1.3. Phân loại kỹ thuật giấu tin

Có nhiều cách để phân loại các kỹ thuật giấu thông tin trong ảnh số, dựa trên lĩnh vực áp dụng các kỹ thuật người ta chia kỹ thuật giấu tin trong ảnh thành hai loại: thủy vân số và giấu tin mật.



Hình 1.5. Sơ đồ phân loại kỹ thuật giấu tin

**Giấu tin mật:** Là kỹ thuật dùng một ảnh môi trường để lưu trữ và chuyển giao các dữ liệu quan trọng với kích thước tương đối lớn một cách an toàn. Mục đích của ảnh giấu tin là làm cho dữ liệu trở nên không quan sát được đối với thị giác của con người.

**Thủy vân số:** Là kỹ thuật nhúng một biểu tượng hay còn gọi là thủy vân vào trong ảnh môi trường để xác định quyền sở hữu ảnh môi trường. Kích thước của biểu tượng thường nhỏ (từ vài bit đến vài nghìn bit). Kỹ thuật này cho phép đảm bảo nguyên vẹn biểu tượng khi ảnh môi trường bị biến đổi bởi các phép thao tác như lọc, nén mất dữ liệu, hay các biến đổi hình học... Tuy nhiên, việc đảm bảo nguyên vẹn biểu tượng không kể đến khi có sự tấn công dựa trên việc hiểu rõ thuật toán và có bộ giải mã trong tay.

**Thủy vân bền vững:** thường được ứng dụng trong các ứng dụng bảo vệ bản quyền. Thủy vân được nhúng trong sản phẩm như một hình thức dán tem bản quyền. Trong trường hợp này, 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 bền vững có hai loại:

- ✓ **Thủy vân ẩn:** cũng giống như giấu tin, bằng mắt thường không thể nhìn thấy thủy vân.
- ✓ **Thủy vân hiển thị:** là loại thủy vân được hiện ngay trên sản phẩm và người dùng có thể nhìn thấy được.

**Thủy vân dễ vỡ:** là kỹ thuật nhúng thủy vân vào trong ảnh sao cho khi phân bố sản phẩm trong môi trường mở nếu có bất cứ một phép biến đổi nào làm thay đổi đối tượng sản phẩm gốc thì thủy vân đã được giấu trong đối tượng sẽ không còn nguyên vẹn như trước khi giấu nữa (dễ vỡ).

Bảng 1.1. So sánh Giấu tin mật và Thủy vân số

	<b>Giấu tin mật</b>	<b>Thủy vân số</b>
<b>Mục đích</b>	-) Che giấu sự hiện hữu của thông điệp. -) Thông tin che giấu độc lập với vỏ bọc.	-) Thêm vào thông tin bản quyền. -) Che giấu thông tin gắn với đối tượng vỏ bọc.
<b>Yêu cầu</b>	-) Không phát hiện được thông điệp bị che giấu. -) Dung lượng tin được giấu.	-) Tiêu chuẩn bền vững.
<b>Tấn công thành công</b>	-) Thông tin mật đã được che giấu bị phát hiện.	-) Thủy vân bị phá vỡ.

## 1.4. Các đặc trưng và ứng dụng của phương pháp giấu tin trong ảnh số

### 1.4.1. Các đặc trưng cơ bản

Giấu tin trong ảnh chiếm vị trí chủ yếu trong các kỹ thuật giấu tin. Vì vậy phần lớn các kỹ thuật giấu tin cũng tập trung vào kỹ thuật giấu tin trong ảnh. 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 tới các đặc trưng sau:

**Phương tiện có chứa dữ liệu tri giác tĩnh:** Dữ liệu gốc ở đây là dữ liệu tĩnh, dù đã giấu 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 ảnh...

**Kỹ thuật giấu phụ thuộc ảnh:** Kỹ thuật giấu tin phụ thuộc vào từng loại ảnh khác nhau. Ví dụ như 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 sự thay đổi trên dữ liệu 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 thay đổi trên ảnh phải là rất nhỏ sao cho bằng mắt thường khó và có thể là không thể nào nhận ra như thế mới đảm bảo được độ an toàn cho thông tin giấu.

**Giấu tin trong ảnh nhưng không làm thay đổi kích thước ảnh:** Các thuật toán thực hiện công việc giấu tin sẽ được thực hiện trên dữ liệu của ảnh. Dữ liệu ảnh bao gồm phần header, bảng màu (nếu có) và dữ liệu. Do vậy kích thước ảnh trước và sau khi giấu tin là ko thay đổi.

**Đảm bảo chất lượng sau khi giấu tin:** Đây là một yêu cầu quan trọng với giấu tin trong ảnh. Sau khi giấu tin ảnh phải đảm bảo không bị biến đổi để có thể bị phát hiện dễ dàng so với ảnh gốc. Yêu cầu này khá đơn giản với ảnh màu hoặc ảnh xám vì mỗi điểm ảnh được biểu diễn bằng nhiều bit, nhiều giá trị nên ta có thay đổi một giá trị nào đó cũng không ảnh hưởng nhiều đến chất lượng ảnh, nhưng với ảnh đen trắng mỗi điểm ảnh chỉ có thể là đen hoặc trắng thì khi biến đổi rất dễ bị phát hiện. Vậy nên trong ảnh màu thì thuật toán trú trọng để số lượng thông tin giấu càng nhiều càng tốt còn ảnh đen trắng là làm thế nào để khó phát hiện nhất.

**Thông tin trong ảnh sẽ biến đổi nếu có bất kì biến đổi nào trên ảnh:** vì giấu tin trong ảnh dựa trên việc điều chỉnh giá trị của các bit theo một quy tắc nào đó để sau khi giải mã theo các giá trị đó tìm ra thông tin giấu. Do đó, nếu một phép biến đổi nào đó làm thay đổi giá trị của các bit thì sẽ làm cho thông tin bị sai lệch. Nhờ đó mà giấu tin trong ảnh có tác dụng phát hiện xuyên tạc thông tin.

**Vai trò của ảnh gốc khi giải tin:** Đa số các kỹ thuật giấu tin mật 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.

#### *1.4.2. Các ứng dụng của kỹ thuật giấu tin*

**Bảo vệ bản quyền tác giả:** Đây là ứng dụng cơ bản nhất của kỹ thuật thủy vân số. Một thông tin mang ý nghĩa quyền sở hữu tác giả gọi là thủy vân sẽ được nhúng vào trong các sản phẩm, thủy vân đó chỉ một mình chủ sở hữu hợp pháp các sản phẩm đó có và được dùng làm minh chứng cho bản quyền sản phẩm. Yêu cầu kỹ thuật đối với ứng dụng này là thủy vân phải tồn tại bền vững cùng sản phẩm, muốn bỏ thủy vân này không được phép của người chủ sở hữu thì chỉ có cách phá hủy sản phẩm.

**Xác thực thông tin hay phát hiện giả mạo:** Một tập các thông tin sẽ được giấu trong phương tiện chứa sau đó sử dụng để nhận biết xem dữ liệu trên phương tiện chứa sau đó được sử dụng để nhận biết xem dữ liệu trên phương tiện gốc đó có bị thay đổi hay không. Các thủy vân nên được ẩn để tránh sự tò mò của kẻ thù và hơn thế nữa là làm khó việc làm giả các thủy vân hợp lệ hay xuyên tạc thông tin nguồn. Yêu cầu chung đối với ứng dụng này là khả năng giấu tin cao và thủy vân bền vững.

**Giấu vân tay hay dán nhãn:** Thủy vân trong những ứng dụng này được sử dụng để nhận diện người gửi hay người nhận của một thông tin nào đó. Với ứng dụng này thì yêu cầu là đảm bảo độ an toàn cao cho các thủy vân tránh sự mất mát thông tin trong khi phân phối.

**Kiểm soát sao chép:** Các thủy vân trong trường hợp này được sử dụng để kiểm soát sao chép đối với các thông tin. Các thiết bị phát hiện ra thủy vân thường được gắn sẵn vào trong các hệ thống đọc/ghi. Các ứng dụng loại này cũng yêu cầu thủy vân phải được đảm bảo an toàn và cũng sử dụng phương pháp phát hiện thủy vân đã giấu mà không cần thông tin gốc.

**Giấu tin mật:** Các thông tin giấu được trong trường hợp này càng nhiều càng tốt, việc giải mã để nhận được thông tin cũng không cần phương tiện chứa ban đầu.



Các yêu cầu mạnh về chống tấn công của kẻ thù không cần thiết lắm thay vào đó là thông tin giấu phải đảm bảo tính không thể phát hiện.

## 1.5. Ảnh BITMAP và phương pháp đánh giá chất lượng ảnh sau khi giấu tin bằng PSNR

### 1.5.1. Ảnh BITMAP

Số bit trên mỗi điểm ảnh thường được ký hiệu là  $n$ . Một ảnh bitmap  $n$ -bit có  $2^n$  màu. giá trị càng lớn thì ảnh càng có nhiều màu, và càng rõ nét hơn. Giá trị tiêu biểu của ảnh là 1 (ảnh đen trắng), 4 (ảnh 16 màu), 6 (ảnh 256 màu), 16 (ảnh 65536 màu), và 24 (ảnh 16 triệu màu). Ảnh bitmap 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 (pixel).

Ảnh bitmap gồm 4 phần :

- Bitmap Header (14 byte) : giúp nhận dạng ảnh bitmap.
- Bitmap Information (40 byte) : lưu một số thông tin chi tiết giúp hiển thị ảnh.
- Color Palette (4\*x byte), x là số màu của ảnh: định nghĩa các màu sẽ được sử dụng trong ảnh.
- Bitmap Data : lưu dữ liệu ảnh.

Các cấu trúc cụ thể của ảnh Bitmap.

### *Bitmap Header*

Bảng 1.2. Bảng Bitmap header

Byte thứ	Ý nghĩa	Giá trị
1-2	Nhận dạng file	'BM' hay 19778
3-6	Kích thước file	Kiểu long trong Turbo C
7-10	Dự trữ	Thường mang giá trị 0
11-14	Byte bắt đầu vùng dữ liệu	Offset của byte bắt đầu vùng dữ liệu
15-18	Số byte cho vùng info	4 byte
19-22	Chiều rộng ảnh BMP	Tính bằng pixel



23-26	Chiều cao ảnh BMP	Tính bằng pixel
27-28	Số Planes màu	Cố định là 1
29-30	Số bit cho một pixel	Có thể là 1,4,8,16,24 tùy theo loại ảnh
31-34	Kiểu nén dữ liệu	0: Không nén 1: Nén run-length 8 bit/pixel 2: Nén run-length 4 bit/pixel
35-38	Kích thước ảnh	Tính bằng byte
39-42	Độ phân giải ngang	Tính bằng pixel/metter
43-46	Độ phân giải dọc	Tính bằng pixel/metter
47-50	Số màu sử dụng trong ảnh	
51-54	Số màu được sử dụng khi hiển thị ảnh	

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

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

Thành phần Bit Count của cấu trúc Bitmap Header cho biết số bit dành cho mỗi điểm ảnh và số lượng màu lớn nhất của ảnh. Bit Count có thể nhận các giá trị sau:

**1:** Bitmap là ảnh đen trắng, mỗi bit biểu diễn một điểm ảnh. Nếu bit mang giá trị 0 thì điểm ảnh là điểm đen, bit mang giá trị 1 điểm ảnh là điểm ảnh trắng.

**4:** Bitmap là ảnh 16 màu, mỗi điểm ảnh được biểu diễn bởi 4 bit.

**8:** Bitmap là ảnh 256 màu, mỗi điểm ảnh được biểu diễn bởi 1 byte.

**16:** Bitmap là ảnh high color, mỗi dãy 2 byte liên tiếp trong bitmap biểu diễn cường độ tương đối của màu đỏ, xanh lá cây, xanh lơ của một điểm ảnh.

**24:** Bitmap là ảnh true color (224 màu), mỗi dãy 3 byte liên tiếp trong bitmap biểu diễn cường độ tương đối của màu đỏ, xanh lá cây, xanh lơ (RGB) của một điểm ảnh.

Thành phần Color Used của cấu trúc Bitmap Header xác định số lượng màu của bảng màu thực sự được sử dụng để hiển thị bitmap. Nếu thành phần này được đặt là 0, bitmap sử dụng số màu lớn nhất tương ứng với giá trị của Bit Count.

### 1.5.2. Phương pháp đánh giá chất lượng ảnh sau khi giấu tin bằng PSNR

Cụm từ **tỉ số tín hiệu cực đại trên nhiễu** thường được viết tắt là **PSNR**, là một thuật ngữ dùng để tính tỉ lệ giữa giá trị năng lượng tối đa của một tín hiệu và năng lượng nhiễu ảnh hưởng đến độ chính xác của thông tin. Bởi vì có rất nhiều tín hiệu có phạm vi biến đổi rộng, nên PSNR thường được biểu diễn bởi đơn vị logarithm decibel.

PSNR được sử dụng để đo chất lượng tín hiệu khôi phục của các thuật toán nén có mất mát dữ liệu (ví dụ: dùng trong nén ảnh). Tín hiệu trong trường hợp này là dữ liệu gốc, và nhiễu là các lỗi xuất hiện khi nén. Khi so sánh các thuật toán nén thường dựa vào sự cảm nhận gần chính xác của con người đối với dữ liệu được khôi phục, chính vì thế trong một số trường hợp dữ liệu được khôi phục của thuật toán này dường như có chất lượng tốt hơn những cái khác, mặc dù nó có giá trị PSNR thấp hơn (thông thường PSNR càng cao thì chất lượng dữ liệu được khôi phục càng tốt). Vì vậy khi so sánh kết quả của 2 thuật toán cần phải dựa trên codecs giống nhau và nội dung của dữ liệu cũng phải giống nhau.

Cách đơn giản nhất là định nghĩa thông qua **MSE** được dùng cho ảnh 2 chiều có kích thước  $m \times n$  trong đó I và K là ảnh gốc và ảnh được khôi phục tương ứng.

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

PSNR được định nghĩa bởi:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10} (MAX_I^2 / MSE) \\ &= 20 \cdot \log_{10} (MAX_I / \sqrt{MSE}) \end{aligned}$$

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

Giá trị thông thường của PSNR trong ảnh và nén video nằm từ 30 đến 50 dB, giá trị càng cao thì càng tốt. Giá trị có thể chấp nhận được khi truyền tín hiệu không dây có tổn thất khoảng từ 20 dB đến 25 dB.

## CHƯƠNG 2: KỸ THUẬT GIẤU TIN THUẬN NGHỊCH TRÊN MIỀN BIẾN ĐỔI SỐNG NHỎ (WAVELET) CHO ẢNH CHẤT LƯỢNG CAO

### 2.1. Khái niệm về giấu tin thuận nghịch

Giấu tin 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 kỹ thuật giấu tin trong ảnh điện hình:*

Thời gian gần đây do đặc thù của một số lĩnh vực: y học, quân sự, nghiên cứu năng lượng hoặc hệ thống thông tin vệ tinh, ... đòi hỏi yêu cầu sau khi tách thông tin chúng ta có thể khôi phục lại ảnh gốc ban đầu. Vì vậy kỹ thuật giấu tin thuận nghịch ra đời.

Năm 1999, Honsinger và các cộng sự đề xuất kỹ thuật giấu thuận nghịch đầu tiên, mở ra một hướng mới trong lĩnh vực giấu tin. Tiếp đó một loạt các kỹ thuật giấu tin thuận nghịch khác được công bố.

Kỹ thuật mở rộng sai phân DE do Tian đưa ra (2002), đây là kỹ giấu tin dựa trên mở rộng hệ số sai phân của điểm ảnh, dữ liệu ảnh được tính sai phân theo biểu thức  $D_i = I_i - I_{i+1}$ , trong đó  $I_i$  là giá trị pixel ảnh, thông tin được giấu trên LSB của các hệ số sai phân sau khi được mở rộng. Sau đó tác giả đề xuất tiếp phương pháp mở rộng trên các hệ số wavelet để giấu tin.

Đến năm 2008, Shaowei Weng và các đồng nghiệp đưa ra kỹ thuật DE cải tiến bằng cách thêm vào hàm nén – giãn trong quá trình giấu tin sử dụng DE nhằm giảm nhiễu xảy ra (theo đánh giá bằng PSNR) của kỹ thuật giấu thuận nghịch DE.

Năm 2003, Ni và cộng sự đề xuất kỹ thuật giấu thuận nghịch dựa trên dịch chuyển biểu đồ tần suất gọi là NSAS. Tiếp đó một loạt các kỹ thuật giấu thuận nghịch dựa phương pháp này ra đời: kỹ thuật DIH (2004) (dịch chuyển biểu đồ tần suất hệ số sai phân), kỹ thuật HKC (cải tiến kỹ thuật giấu NSAS), kỹ thuật IWH (dựa trên dịch chuyển biểu đồ tần suất hệ số wavelet nguyên), kỹ thuật RL (2008) là kỹ thuật giấu thuận nghịch cho ảnh nhị phân dựa trên dịch chuyển tần suất của các loạt đen trong ảnh.

***Một số kỹ thuật giấu thuận nghịch khác không dựa trên biểu đồ tần suất:***

Kỹ thuật giấu MBN: dữ liệu cần giấu được chuyển đổi thành các hệ số nhỏ hơn theo phương pháp phân tích nhân tử thành đa thức, các điểm ảnh sẽ được điều chỉnh để lưu trữ các hệ số này.

Kỹ thuật giấu RCM: dựa trên hiệu chỉnh LSB của ảnh theo bản đồ màu tương phản.

Kỹ thuật giấu hai pha ngang dọc RVH: chuỗi thông tin giấu M được chia thành hai chuỗi con bằng nhau M1 và M2, sau đó được giấu lần lượt vào hai pha:

- Pha giấu ngang thực hiện giấu trên các cột lẻ của ma trận ảnh
- Pha giấu dọc thực hiện giấu trên các hàng chẵn của ma trận ảnh

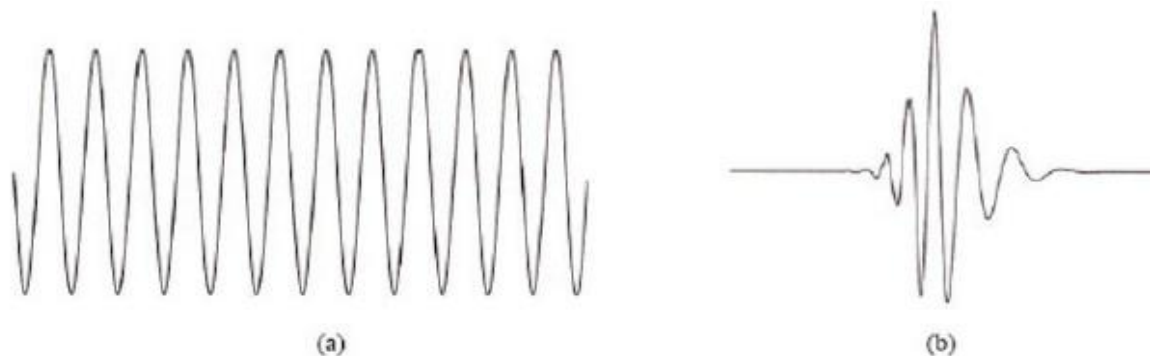
**2.2. Kỹ thuật giấu tin thuật nghịch trên miền biến đổi wavelet**

***2.2.1. Khái niệm miền biến đổi sóng nhỏ***

***2.2.1.1. Giới thiệu về sóng nhỏ***

Biến đổi tín hiệu không làm thay đổi nội dung thông tin của tín hiệu. Biến đổi sóng nhỏ cung cấp cách biểu diễn thời gian – tần số của tín hiệu. Biến đổi này tạo ra nhằm khắc phục những hạn chế của biến đổi Fourier thời gian ngắn và cũng được sử dụng để phân tích tín hiệu động. Trong khi đó STFT cho độ phân dải không đổi ở tất cả các tần số. Biến đổi sóng nhỏ sử dụng kỹ thuật đa độ phân dải bằng cách với mỗi tần số khác nhau nó phân tích với một độ phân giải khác nhau.

Mỗi sóng là một hàm dao động của thời gian hoặc không gian và tuần hoàn. Ngược lại, sóng nhỏ là sóng cục bộ, chúng có năng lượng tập trung ở thời gian hoặc không gian và thích hợp để phân tích tín hiệu tạm thời. Trong khi biến đổi fourier và STFT sử dụng sóng để phân tích tín hiệu thì biến đổi sóng nhỏ sử dụng sóng nhỏ của năng lượng hữu hạn.



Hình 2.1. Sự khác nhau giữa sóng (a) và sóng nhỏ (b)

Trong phân tích sóng nhỏ, tín hiệu được phân tích nhiều lần với hàm sóng nhỏ và sự biến đổi được tính toán với mỗi phần được tạo ra. Với tần số cao, biến đổi sóng nhỏ cho độ phân dải rất tốt về thời gian và độ phân dải không tốt về tần số. Với tần số thấp, biến đổi sóng nhỏ cho độ phân dải tốt về tần số và độ phân dải không tốt về thời gian.

2.2.1.2. Lý thuyết biến đổi sóng nhỏ rời rạc cho thủy văn ảnh (DWT)

DWT là chủ đề rất lớn. Ở đây chỉ tập trung vào những vấn đề của DWT mà có liên quan đến vấn đề ta đang quan tâm là thủy văn.

Hai vấn đề chung của tất cả các thuật toán biến đổi sang miền tần số là biến đổi thuận và biến đổi ngược.

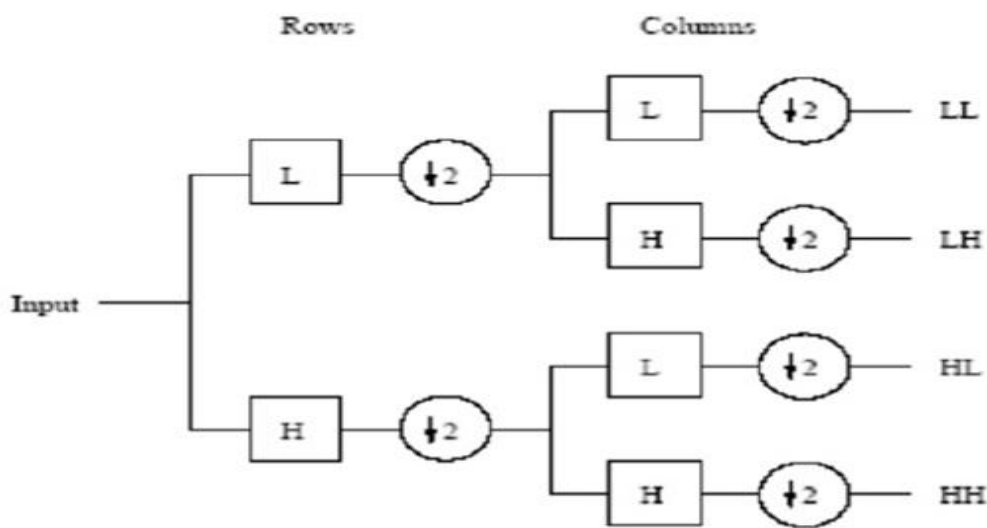
DWT sử dụng để biến đổi dữ liệu mẫu thành hệ số sóng nhỏ.

IDWT dùng để biến đổi ngược hệ số sóng nhỏ thành dữ liệu mẫu gốc. Ở đây ta thảo luận về ảnh có kích thước NxN.

**- Xử lý phân tách**

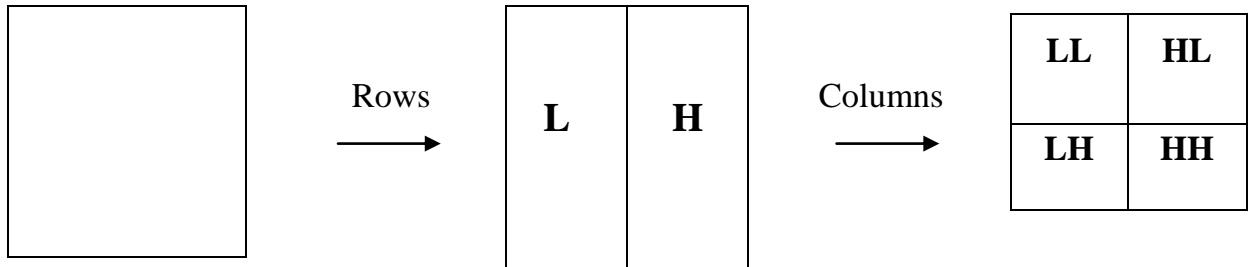
Xử lý phân tách được thể hiện trên hình 2.2. Ảnh được lọc thông cao và thông thấp giữa các dòng. Kết quả lọc của mỗi lần được lấy mẫu hai lần theo thông cao và thông thấp.

Hai tín hiệu con này tương ứng với thành phần tần số cao và thành phần tần số thấp giữa các dòng. Mỗi tín hiệu con này một lần nữa được lọc thông cao và thông thấp, nhưng lần này là giữa các cột.



Hình 2.2. Bước phân tách của ảnh hai chiều.

Ở bước này dữ liệu gốc được phân thành 4 ảnh con, mỗi ảnh có kích thước  $N/2 \times N/2$  chứa thông tin về các thành phần tần số khác nhau.

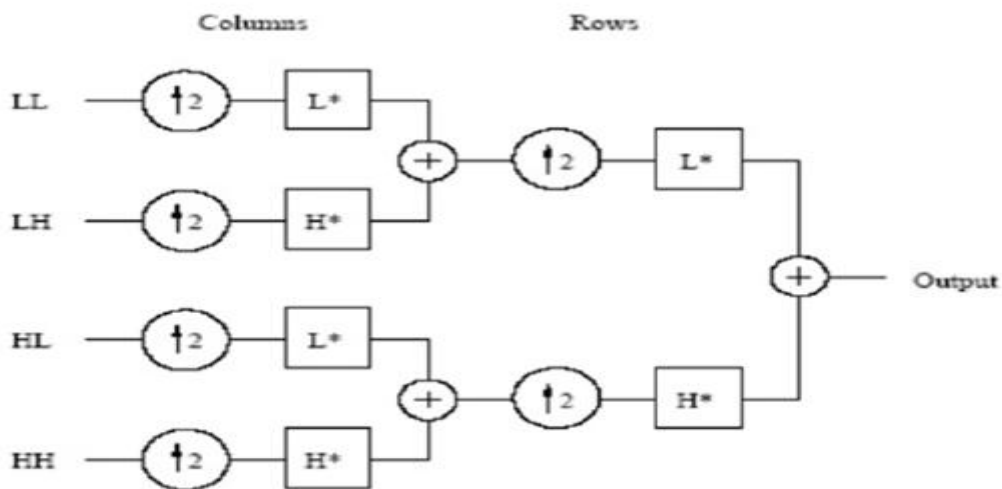


Hình 2.3. Bước phân tách DWT

LL là kết quả lọc thông thấp cả dòng và cột, chứa thành phần miêu tả thô về ảnh. Do đó LL còn được gọi là xấp xỉ của ảnh. HH là kết quả lọc thông cao theo cả hàng và cột và nó chứa thành phần tần số cao của tín hiệu tương tự. HL và LH là kết quả của lọc thông thấp một chiều và lọc thông cao ở chiều còn lại. LH chứa thông tin chi tiết theo chiều đứng, tương ứng với cung ngang. HL biểu diễn thông tin chi tiết theo chiều ngang từ cung đứng. Tất cả 3 thành phần con: HL, LH, HH được gọi là nhánh con chi tiết vì nó bổ sung chi tiết tần số cao cho ảnh xấp xỉ.

**- Xử lý ghép**

Xử lý ngược thể hiện trên hình 2.4. Thông tin từ 4 ảnh con được lấy mẫu và lọc ngược giữa các cột. Kết quả thu được một lần nữa được lấy mẫu và lọc ngược với bộ lọc ngược. Kết quả cuối cùng thu được chính là ảnh gốc. Ở đây không có sự mất mát thông tin trong quá trình phân tách cũng như quá trình ghép để thu được ảnh gốc.



Hình 2.4. Bước ghép 4 thành phần ảnh con

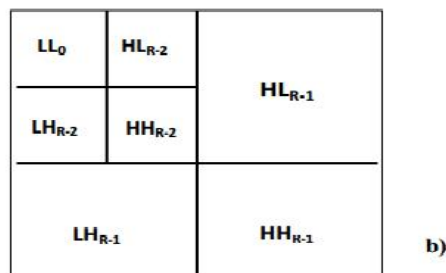
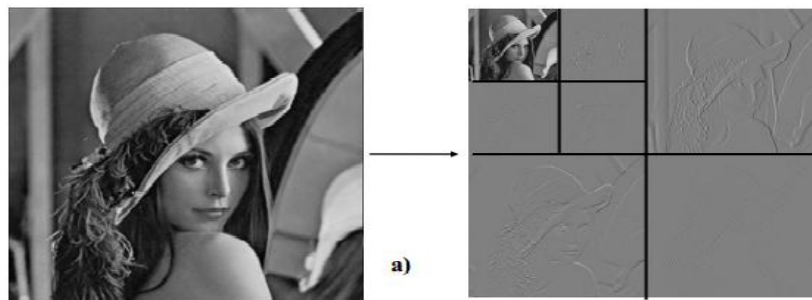
Với DWT có thể phân tách ảnh nhiều lần. Có thể tiếp tục phân tách cho đến khi tín hiệu được phân tách toàn bộ hoặc để người dùng tự động ngắt quá trình phân tách một cách thủ công. Với các ứng dụng nén và thủy vân, thông thường quá trình phân tách không thực hiện quá 5 lần.

Hầu hết sử dụng hai cách phân tách sau:

- Phân tách kiểu hình chóp
- Phân tách kiểu đóng gói

Phép biến đổi tần số wavelet rời rạc sẽ phân tách ảnh ra thành nhiều dải tần số gọi là các subband. Mỗi mức wavelet sẽ được tác động hai lần: một lần duyệt theo chiều ngang và một lần duyệt theo chiều dọc (thứ tự này không quan trọng bởi bản chất đối xứng) và do đó ta thu được bốn dải :

- 1) Horizontally and vertically lowpass (LL)
- 2) Horizontally lowpass and vertically highpass (LH)
- 3) Horizontally highpass and vertically lowpass (HL)
- 4) Horizontally and vertically highpass (HH)



Hình 2.5. a) Biến đổi wavelet, b) Cấu trúc dải

Chúng ta sẽ cùng xem xét tín hiệu ảnh đầu vào (hoặc tín hiệu tile - component đối với ảnh lớn). Giả sử với sự phân tách wavelet mức  $R-1$  tương ứng với mức phân giải thứ  $R$ , đánh số từ 0 tới  $R-1$  thì 0 tương ứng với mức phân giải kém nhất (coarsest resolution) và  $R-1$  tương ứng với mức phân giải tốt nhất (finest resolution). Mỗi một



dải trong một lần phân tách sẽ được xác định bởi hướng (orientation) của chính nó (ví dụ LL, LH, HL, HH) và mức phân giải tương ứng của nó (ví dụ  $0, 1, \dots, R-1$ ). Tại mỗi mức phân giải (ngoại trừ mức thấp nhất), dải LL là dải sẽ bị phân tách nhỏ hơn. Giả dụ, dải  $LL_{R-1}$  là dải sẽ bị phân tách thành các dải  $LL_{R-2}$ ,  $HL_{R-2}$ ,  $LH_{R-2}$  và  $HH_{R-2}$ . Sau đó, tại mức tiếp theo dải  $LL_{R-2}$  sẽ bị phân tách và cứ như vậy. Quá trình này sẽ lặp đi lặp lại cho tới khi ta thu được dải  $LL_0$  và kết quả hiển thị trong hình 2.5. Nếu không thực hiện biến đổi ( $R=0$ ) thì chỉ có duy nhất dải  $LL_0$ .

### 2.2.1.3. Họ sóng nhỏ

Có một số hàm cơ sở được dùng làm họ sóng nhỏ cho biến đổi sóng nhỏ. Vì họ sóng nhỏ tạo ra tất cả các hàm sóng nhỏ, nó xác định đặc trưng của biến đổi sóng nhỏ sau khi thực hiện. Do đó, chi tiết của ứng dụng cụ thể nên được xem xét kỹ để xác định ra họ sóng nhỏ nên sử dụng sao cho quá trình biến đổi sóng nhỏ sẽ hiệu quả cho ứng dụng tương ứng.

Hàm Haar là một trong những hàm đơn giản và lâu đời nhất. Do đó bất kỳ thảo luận nào về sóng nhỏ đều bắt đầu với hàm Haar. Hàm Daubechies là hàm phổ biến nhất. Nó thể hiện cơ sở của xử lý tín hiệu sóng nhỏ và thường dùng cho các ứng dụng lớn. Hai hàm Haar và Daubechies còn được gọi là sóng Maxflat vì đáp ứng xung của chúng có độ dẹt nhất ở tần số 0 và  $\pi$ . Đây là đặc trưng mà nhiều ứng dụng mong muốn đạt được. Hàm Haar, Daubechies, Symlets và Coiflets đều được hỗ trợ sóng nhỏ trực giao. Sóng này cùng với sóng nhỏ Meyer có khả năng xây dựng lại cấu trúc một cách hoàn hảo. Sóng Meyer, Morlet và Mexican Hat là các sóng có hình dạng đối xứng.

## 2.2.2. Kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao

### 2.2.2.1. Ý tưởng của kỹ thuật

Đây là kỹ thuật giấu tin thuận nghịch cho miền biến đổi sóng nhỏ dựa trên biến đổi hệ số wavelet. Ban đầu, miền không gian ảnh số được biến đổi sang miền tần số wavelet nguyên (the integer wavelet transform - IWT) được bốn băng tần LL (Low - Low), LH (Low - High), HL (High - Low), HH (High - High). Sau đó, thông tin mật sẽ được nhúng vào các băng tần LH, HL, HH sử dụng thay đổi hệ số wavelet.

Kỹ thuật giấu tin thuận nghịch miền biến đổi sóng nhỏ dựa trên hệ số wavelet là nghiên cứu của nhóm tác giả người Đài Loan: Ching-Yu Yang, Chih-Hung Lin, Wu-Chih Hu đề xuất năm 2008. Các tác giả nhúng một đoạn thông tin vào trong miền tần số dựa trên việc điều chỉnh hệ số wavelet. Đầu tiên, một hình ảnh đầu vào được tách ra thành các miền biến đổi wavelet. Tiếp theo, các bit dữ liệu được nhúng vào các



khối có băng cao tần của miền biến đổi Wavelet: LH, HL, HH. Khi nhúng vào, các hệ số Wavelet nằm trong khoảng  $(\beta, 2\beta)$  và  $(-2\beta, -\beta)$  sẽ được dán nhãn và cấm cờ, các hệ số này sẽ được giấu tin. Cuối cùng các bit thông tin được chuyển sang hệ nhị phân rồi giấu vào các hệ số của khối thuộc khoảng  $(\beta, 2\beta)$  và  $(-2\beta, -\beta)$ . Với  $\beta$  là thông số kiểm soát (khóa).

2.2.2.2. Thuật toán giấu tin

❖ Đầu vào:

- Ảnh sử dụng để giấu tin.
- Thông tin cần giấu.

❖ Đầu ra:

- Ảnh đã giấu tin.

**Các bước thực hiện:**

**Bước 1:** Đặt  $C_j = \{c_{jk}\}_{k=0}^{n^2-1}$  là khối thứ  $j$  kích thước  $n \times n$  lấy từ LH (hoặc HL,LL) băng con của miền biến đổi IWT (của ảnh đầu vào). Gọi  $C_{jp} = \{c_p | \beta \leq c_p < 2\beta\}$  và  $C_{jm} = \{c_m | -2\beta \leq c_m < -\beta\}$  là hai tập hợp con của  $C_j$  với  $\beta$  ở đây là một tham số điều khiển.

**Bước 2:** Chọn một khối  $C_j$  chưa được xử lý.

**Bước 3:** Nếu  $|C_{jp}| \neq \emptyset$  thì sau đó lấy  $C_{jp}$  trừ đi  $\beta$  và đánh dấu một lá cờ để sửa đổi hệ số.

**Bước 4:** Nếu  $|C_{jm}| \neq \emptyset$  thì sau đó cộng lấy  $C_{jm}$  cộng đi  $\beta$  và đánh dấu một lá cờ để sửa đổi hệ số.

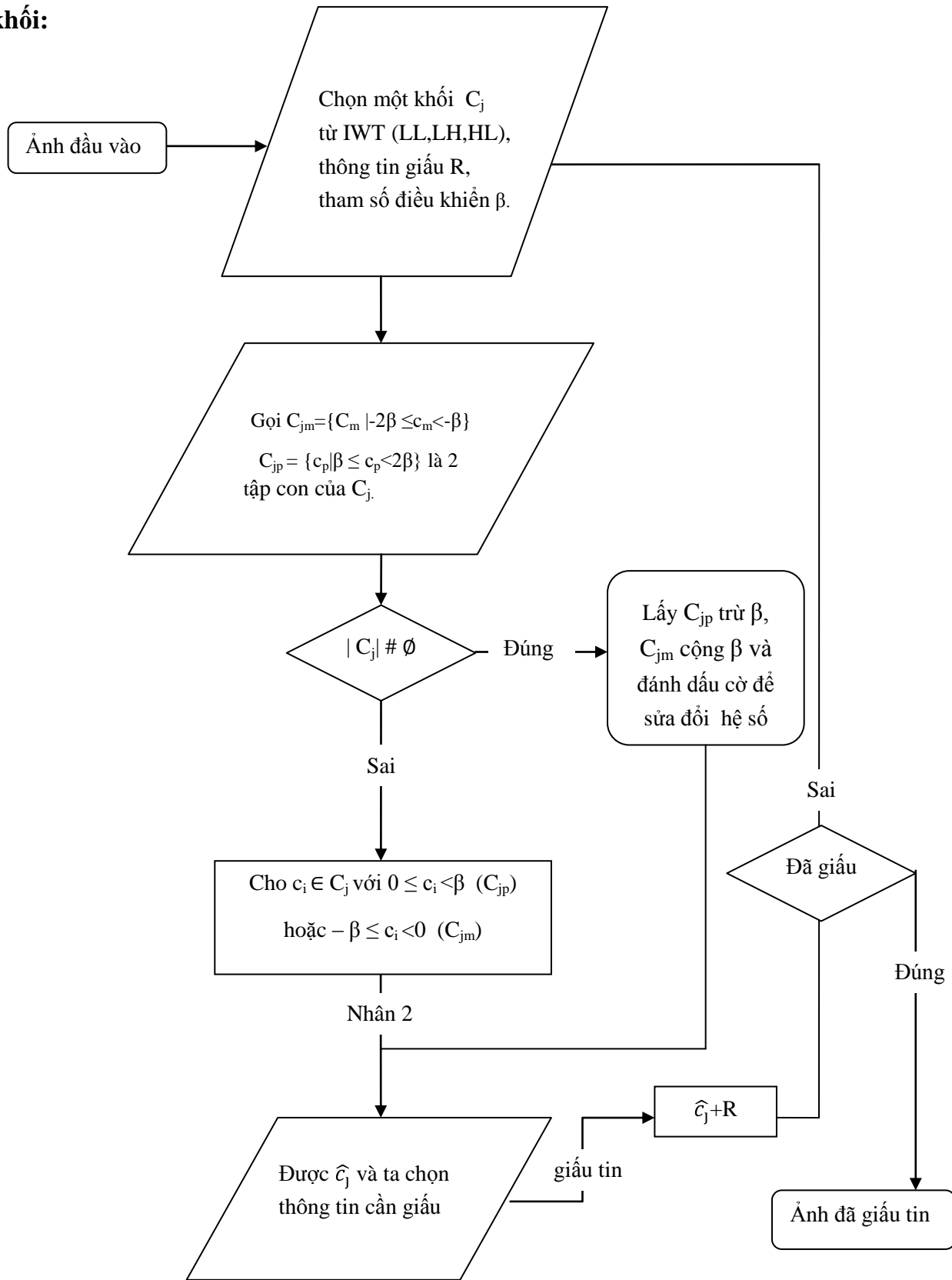
**Bước 5:** Giấu từng bit thông tin  $R$  bằng cách chọn các hệ số  $c_i \in C_j$  với  $0 \leq c_i < \beta$  (hoặc  $-\beta \leq c_i < 0$ ) nhân  $c_i$  với 2 để có được  $\hat{c}_i$ , và thêm một thông tin cần giấu  $R$  vào  $\hat{c}_i$  theo biểu thức  $(\hat{c}_i + R)$ .

**Bước 6:** Lặp lại từ bước 1 cho đến khi giấu hết các bit thông tin. Giảm đồ cho việc điều chỉnh hệ số giá trị cho trên hai bước được minh họa trong hình. 2.6.



Hình 2.6. Giảm đồ của việc điều chỉnh hệ số. (a) cho các hệ số âm và (b) cho các hệ số dương

Sơ đồ khối:



Hình 2.7. Sơ đồ khối thuật toán giấu tin.

**Ví dụ minh họa.**

❖ **Đầu vào:**

- Một khối IWT = [7 -3 -5 -2; -1 4 3 7; -6 0 -1 6; -2 0 -3 0].
- Với các thông số khóa :  $\beta = 3$
- Dãy dữ liệu bit cần giấu R: 110110

❖ **Đầu ra:**

- Ta được khối đã giấu tin.

Cho  $C_j$ :

7	-3	-5	-2
-1	4	3	7
-6	0	-1	6
-2	0	-3	0

$C_{jp}$ ,  $C_{jm}$  và cờ:

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

FLAG

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

$C_{jp}$

7	-3	-5	-2
-1	4	3	7
-6	0	-1	6
-2	0	-3	0

$C_{jm}$

7	-3	-5	-2
-1	4	3	7
-6	0	-1	6
-2	0	-3	0

Nhân  $c_j$  với 2 để được  $\hat{c}_j$  :

$C_{jp}$

7	-3	-5	-2
-1	8	6	7
-6	0	-1	6
-2	0	-3	0

$C_{jm}$

7	-6	-10	-2
-1	4	3	7
-12	0	-1	6
-2	0	-6	0

Giấu chuỗi 110110:

7	-3	-5	-2
-1	9	7	7
-6	0	-1	6
-2	0	-3	0

7	-6	-9	-2
-1	4	3	7
-11	0	-1	6
-2	0	-6	0

Hệ số Wavelet ảnh đã giấu tin:

7	-6	-9	-2
-1	9	7	7
-11	0	-1	6
-2	0	-6	0

### 2.2.2.3. Thuật toán tách tin

#### ❖ Đầu vào:

- Ảnh có giấu tin.
- Thông số kiểm soát  $\beta$  và cờ.

#### ❖ Đầu ra:

- Thông tin được giấu trong ảnh.
- Ảnh gốc.

#### Các bước thực hiện:

**Bước 1:** Nhập một  $D_j$  là khối  $j$  thứ  $m$  bất kì của kích thước  $n \times n$  được lấy từ các băng con LL, (HL), LH của miền biến đổi IWT.

**Bước 2:** Cho  $\hat{D}_j = \{\hat{d}_j \mid -2\beta \leq \hat{d}_j < 2\beta\}$  với  $\hat{D}_j \subseteq D_j$ .

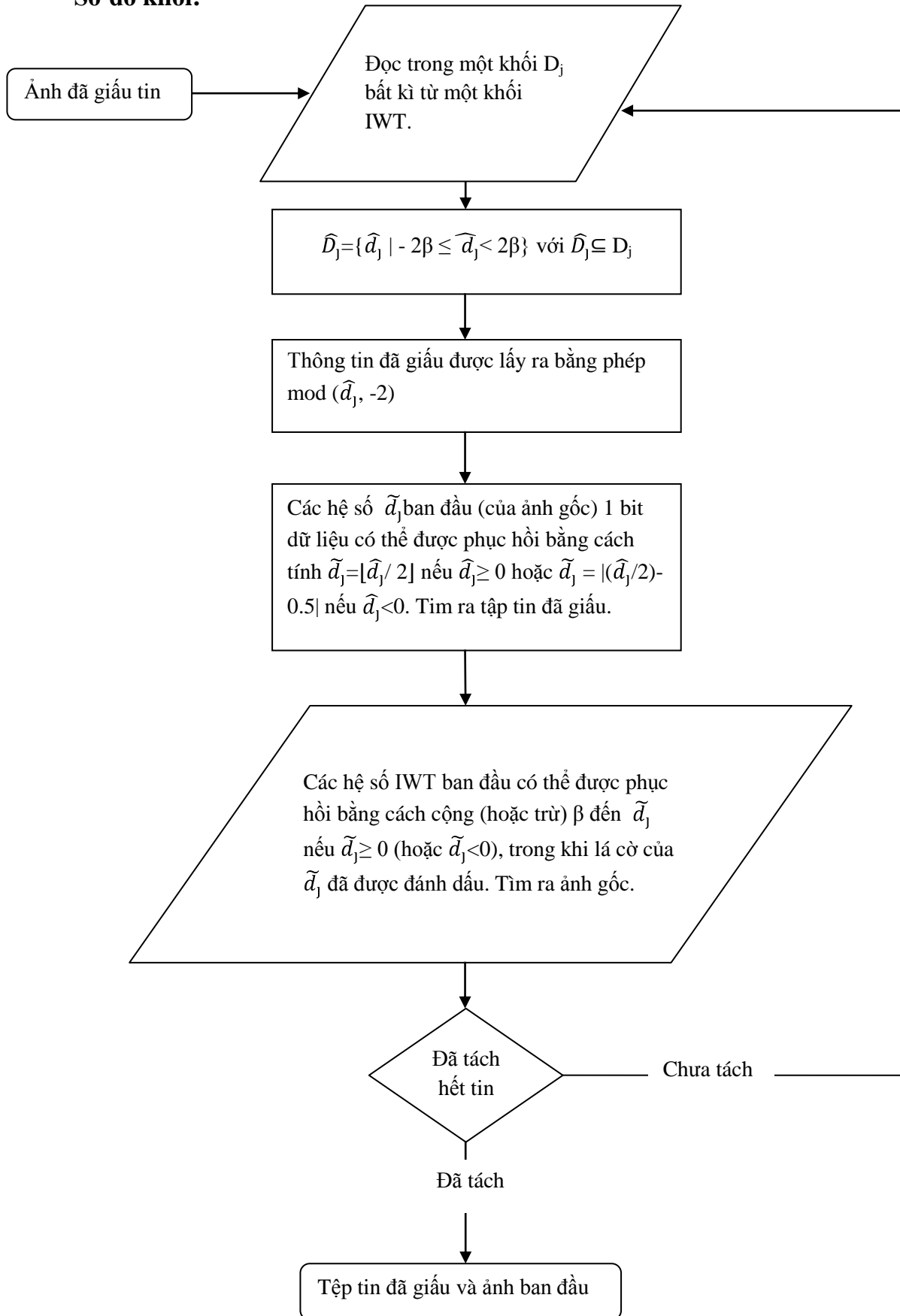
**Bước 3:** Thông tin đã giấu được lấy ra bằng phép mod  $(\hat{d}_j, -2)$ .

**Bước 4:** Các hệ số IWT  $\tilde{d}_j$  ban đầu (của ảnh gốc) một bit dữ liệu có thể được phục hồi bằng cách thực hiện hay  $\tilde{d}_j = \lfloor \hat{d}_j / 2 \rfloor$  nếu  $\hat{d}_j \geq 0$  hoặc  $\tilde{d}_j = \lceil (\hat{d}_j / 2) - 0.5 \rceil$  nếu  $\hat{d}_j < 0$ .

**Bước 5:** Các hệ số IWT ban đầu có thể được phục hồi bằng cách cộng (hoặc trừ)  $\beta$  đến  $\tilde{d}_j$  nếu  $\tilde{d}_j \geq 0$  (hoặc  $\tilde{d}_j < 0$ ), trong khi lá cờ của  $\tilde{d}_j$  đã được đánh dấu.

**Bước 6:** Lặp lại từ bước 1 cho đến khi tất cả các bit dữ liệu được trích ra.

Sơ đồ khối:



Hình 2.8. Sơ đồ khối thuật toán tách tin

**Ví dụ minh họa.**

❖ **Đầu vào :**

- Một khối đã giấu tin [7 -6 -9 -2;-1 9 7 7;-11 0 -1 6;-2 0 -6 0].
- Với các thông số khóa :  $\beta = 3$  và cờ.

❖ **Đầu ra :**

- Ta tìm được khối ban đầu và dữ liệu giấu.

Cho  $D_j$  :

7	-6	-9	-2
-1	9	7	7
-11	0	-1	6
-2	0	-6	0

$C_{jp}$ ,  $C_{jm}$  và cờ để tìm chuỗi đã giấu :

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

FLAG

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

$C_{jp}$

7	-3	-5	-2
-1	9	7	7
-6	0	-1	6
-2	0	-3	0

$C_{jm}$

7	-6	-9	-2
-1	4	3	7
-11	0	-1	6
-2	0	-6	0

Chuỗi đã giấu 110110, khôi phục ảnh gốc :

$C_{jp}$

7	-3	-5	-2
-1	4	3	7
-6	0	-1	6
-2	0	-3	0

$C_{jm}$

7	-3	-5	-2
-1	4	3	7
-6	0	-1	6
-2	0	-3	0

7	-3	-5	-2
-1	4	3	7
-6	0	-1	6
-2	0	-3	0

Hệ số wavelet ban đầu

## CHƯƠNG 3: CÀI ĐẶT VÀ THỬ NGHIỆM

### 3.1. Môi trường cài đặt

- Ngôn ngữ cài đặt: Ngôn ngữ lập trình Matlab phiên bản 7.7
- Môi trường soạn thảo: Matlab phiên bản 7.7
- Môi trường chạy chương trình: Môi trường giao diện Matlab phiên bản 7.7
- Cấu hình tối thiểu để cài đặt Matlab:
  - + Intel hoặc AMD x86 processor supporting SSE2
  - + Windows XP SP2 x64, SP3, 7, 8 ...
  - + Dung lượng ổ cứng từ 16 GB tới 32GB, bộ nhớ RAM tối thiểu 1GB

Ở chương 3 chúng ta sẽ cài đặt và thử nghiệm chương trình với 1 bài toán giấu tin trong ảnh cấp xám 8 bit như sau:

#### **Đầu vào:**

- Ảnh cấp xám 8 bit C có kích thước  $m \times n$ .
- Chuỗi thông điệp cần giấu.

#### **Đầu ra:**

- Ảnh cấp xám 8 bit S đã được giấu tin.

#### **Chức năng giấu tin:**

- Giấu tin dựa trên bày kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao.

- Giấu vào chuỗi kí tự: do người dùng nhập vào từ bàn phím.
- Giấu vào tệp văn bản: Chọn một tệp văn bản định dạng \*.txt để giấu vào ảnh.

#### **Chức năng tách tin:**

- Tách tin trên bằng kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao đã được giấu từ trước.

- Tách chuỗi thông điệp đã giấu và lưu lại dưới dạng tập \*.txt.

### 3.2. Giao diện chương trình

#### 3.2.1. Giao diện chương trình chính



Hình 3.1. Giao diện chương trình chính

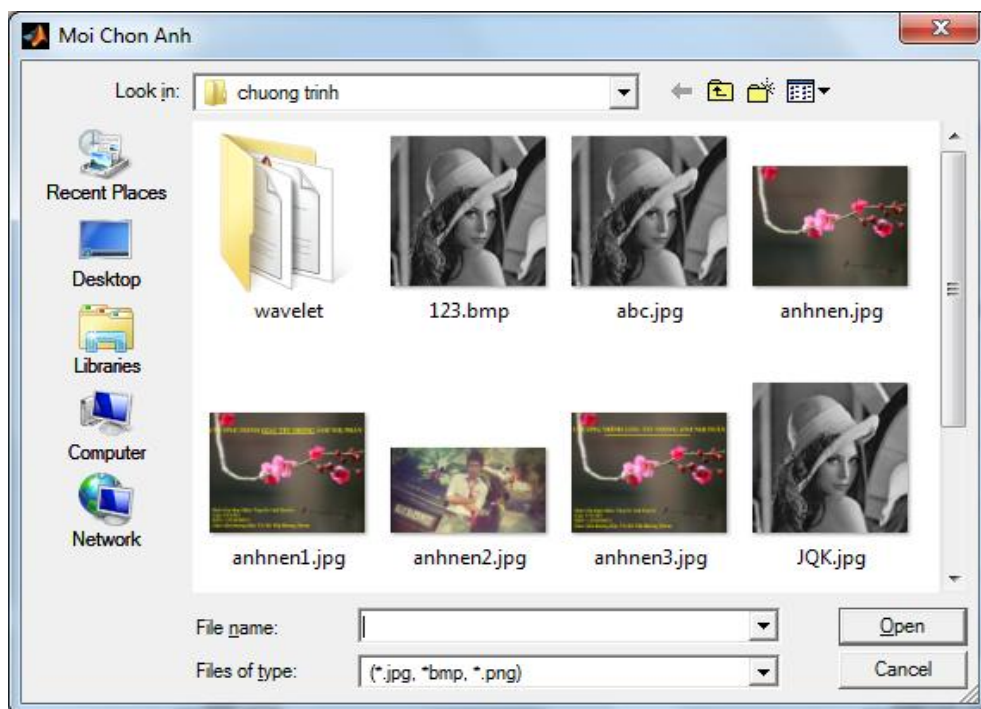
#### 3.2.2. Giao diện chức năng giấu tin



Hình 3.2. Giao diện chức năng giấu tin

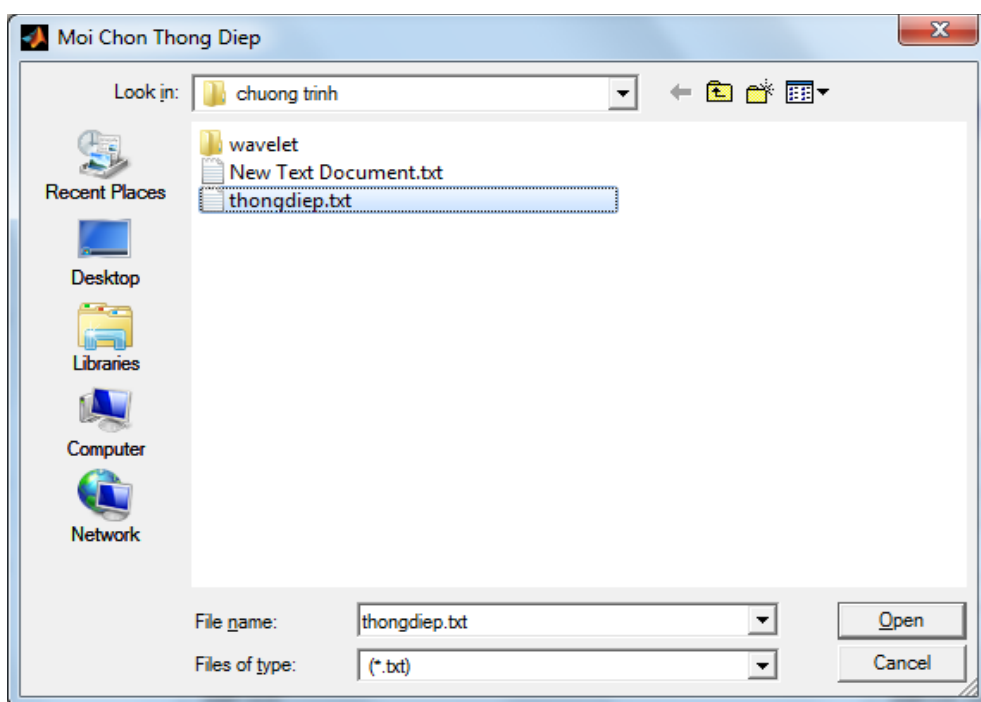


Từ giao diện chính của chương trình chúng ta chọn ảnh cần giấu tin bằng cách nhấn vào nút “CHON ANH”. Khi đó chương trình sẽ mở ra hộp thoại duyệt ảnh.



Hình 3.3. Hộp thoại chọn ảnh cấp xám 8 bit cần giấu tin

Chúng ta sẽ chọn ảnh cấp xám 8 bit bất kì để thực hiện giấu tin vào ảnh đó. Sau khi chọn ảnh xong, ta nhập thông điệp vào từ bàn phím hoặc từ 1 file \*.txt bất kì bằng cách kích vào nút “CHON THÔNG DIỆP” để giấu tin.



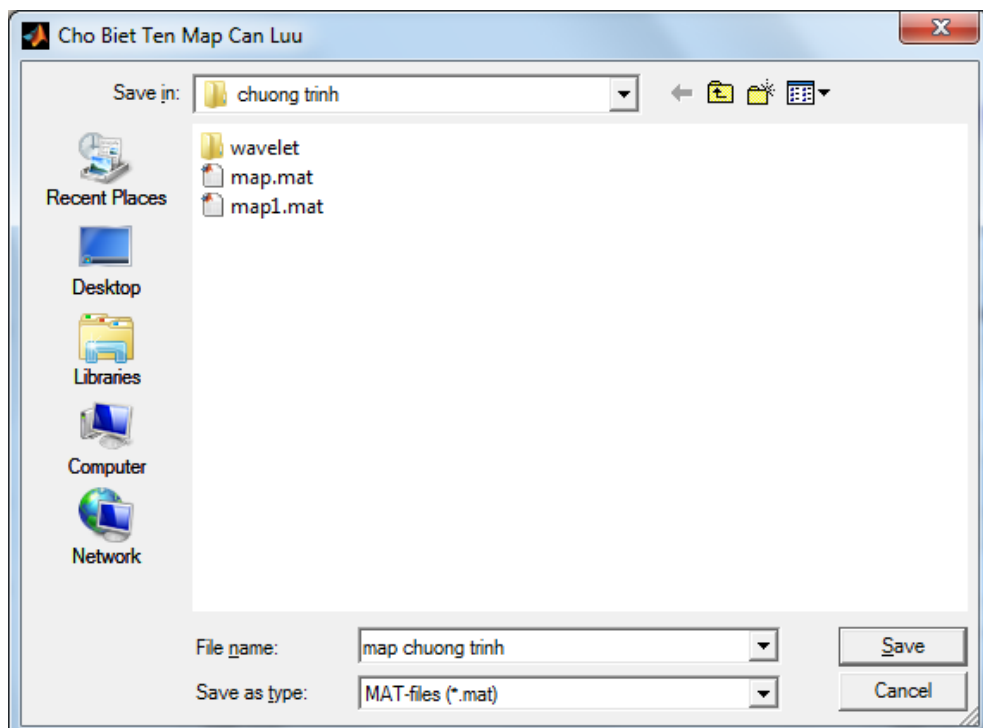
Hình 3.4. Hộp thoại chọn thông điệp cần giấu

Chọn 1 khóa điều khiển Beta bất kì để thực hiện giấu tin.



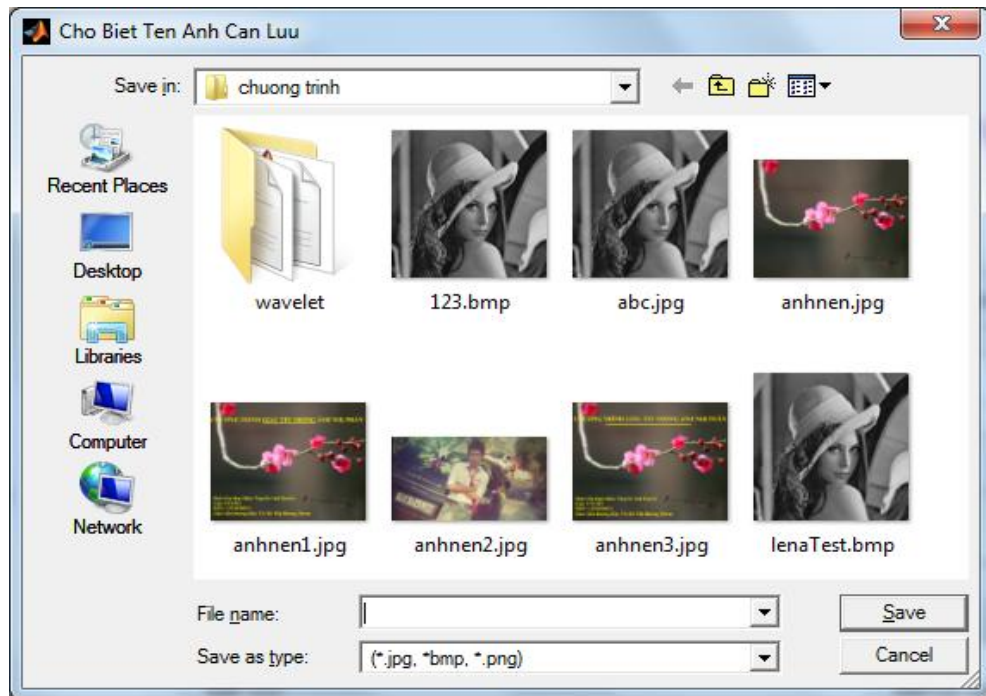
Hình 3.5. Nhập Beta bất kì vào trong chương trình

Chúng ta cần chọn nơi sẽ lưu bản đồ định vị Map sau khi đã giấu tin vào bằng cách chọn “LUU MAP” từ giao diện.



Hình 3.6. Hộp thoại cho biết Map định vị sau khi đã giấu tin

Chúng ta cần chọn nơi sẽ lưu ảnh kết quả sau khi đã giấu tin vào bằng cách chọn “LUU ANH” từ giao diện.



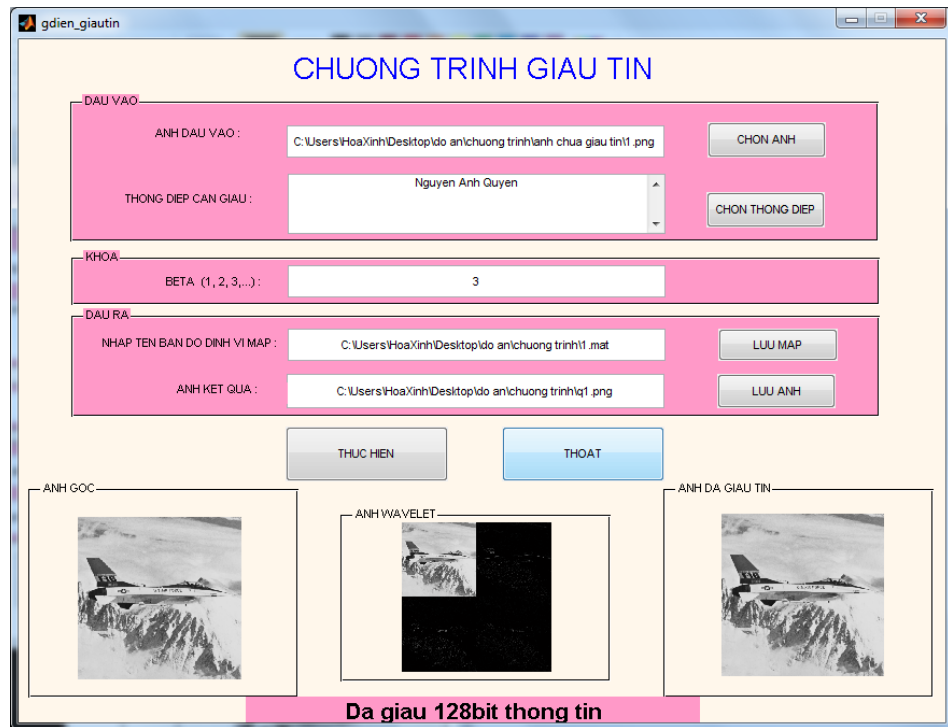
Hình 3.7. Hộp thoại cho biết tên ảnh sau khi đã giấu tin

Sau khi đã lựa chọn xong đầu vào và đầu ra cho chương trình, chúng ta chọn nút “THUC HIEN”. Chương trình sẽ thực hiện và đưa ra kết quả ảnh đã giấu tin và độ dài thông điệp ngay trên giao diện của chương trình.



Hình 3.8. Giao diện sau khi giäu tin

Sau khi hoàn thành mọi việc kích nút “THOAT” để thoát khỏi chương trình giấu tin.



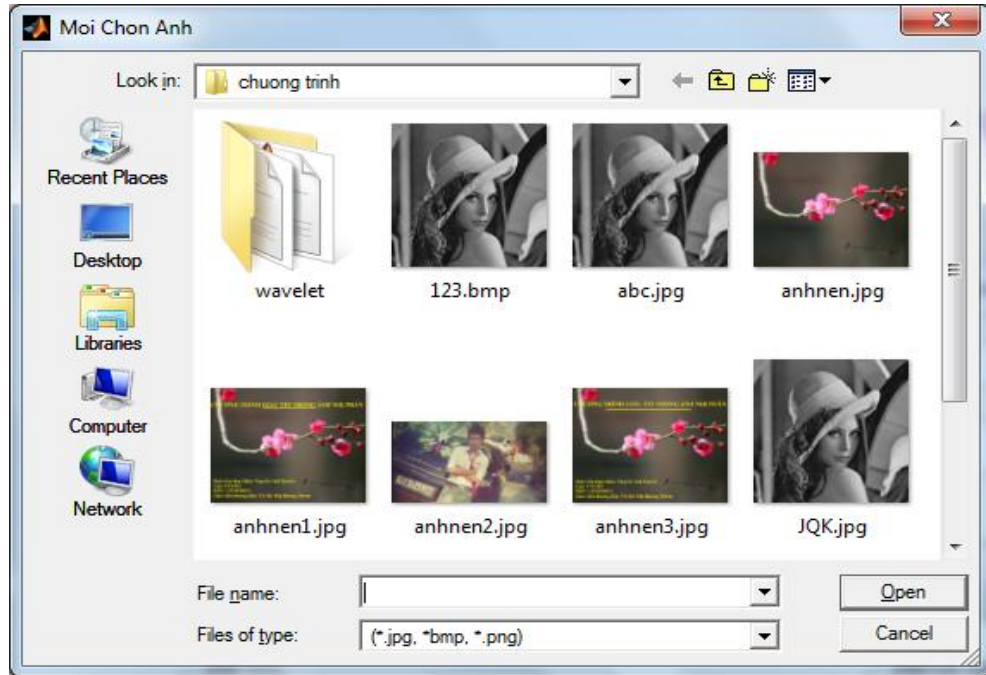
Hình 3.9. Giao diện kết thúc chương trình giấu tin

### 3.2.3. Giao diện chức năng tách tin



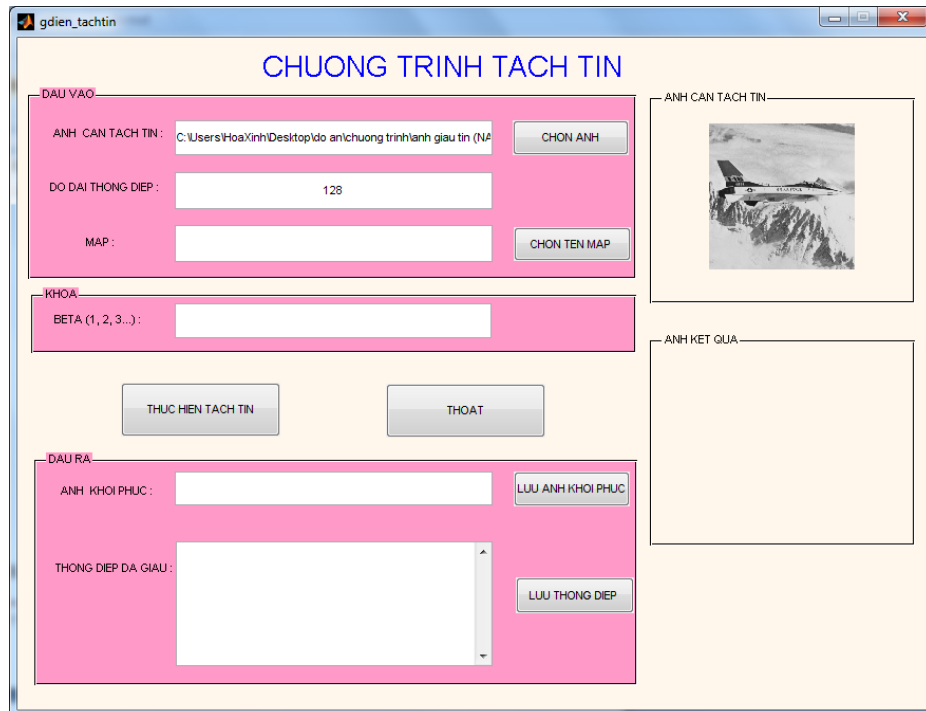
Hình 3.10. Giao diện chức năng tách tin

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



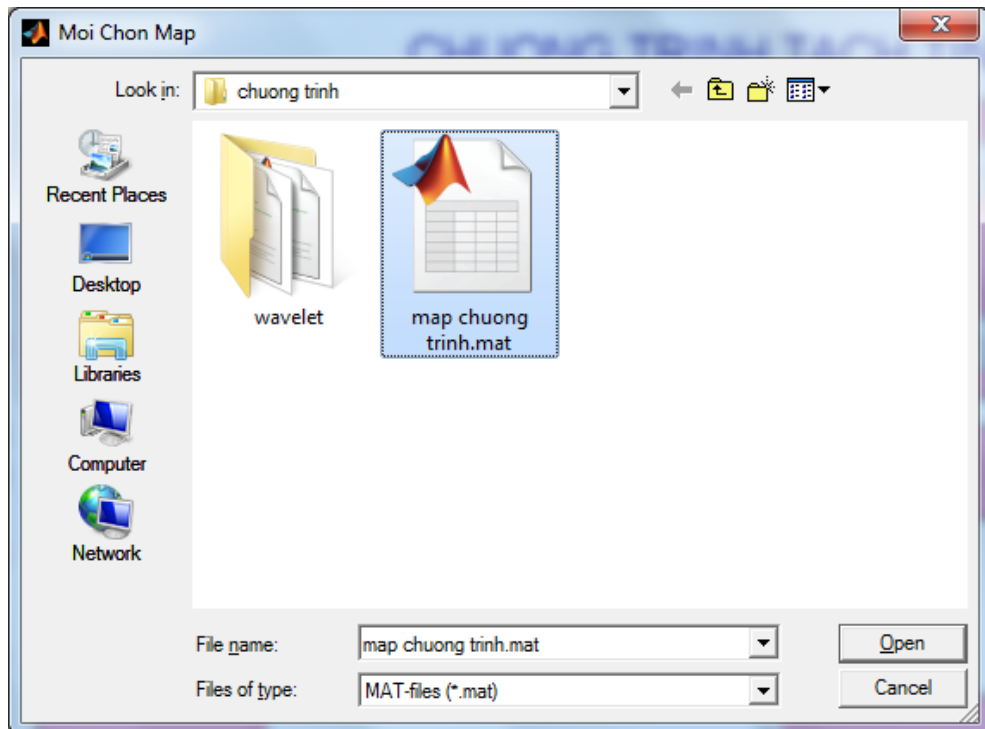
Hình 3.11. Hộp thoại chọn ảnh cấp xám 8 bit cần tách tin

Chúng ta sẽ chọn ảnh cấp xám 8 bit đã giấu tin ở trên để thực hiện tách tin trong ảnh đó. Sau khi chọn ảnh cần tách xong ta sẽ nhập từ bàn phím độ dài thông điệp đã hiện ở bên giấu tin .

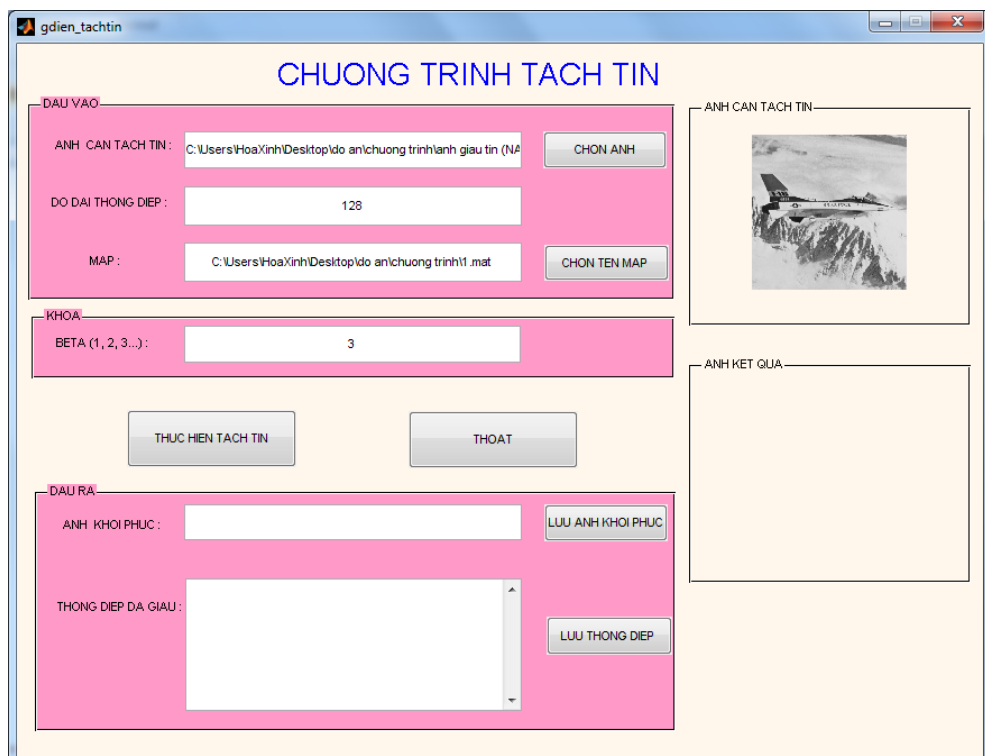


Hình 3.12. Giao diện chức năng nhập độ dài thông điệp giấu tin từ bàn phím

Chúng ta cần chọn bản đồ định vị Map khi giấu tin đã lưu vào bằng cách nhấn nút “CHON TEN MAP” từ giao diện.



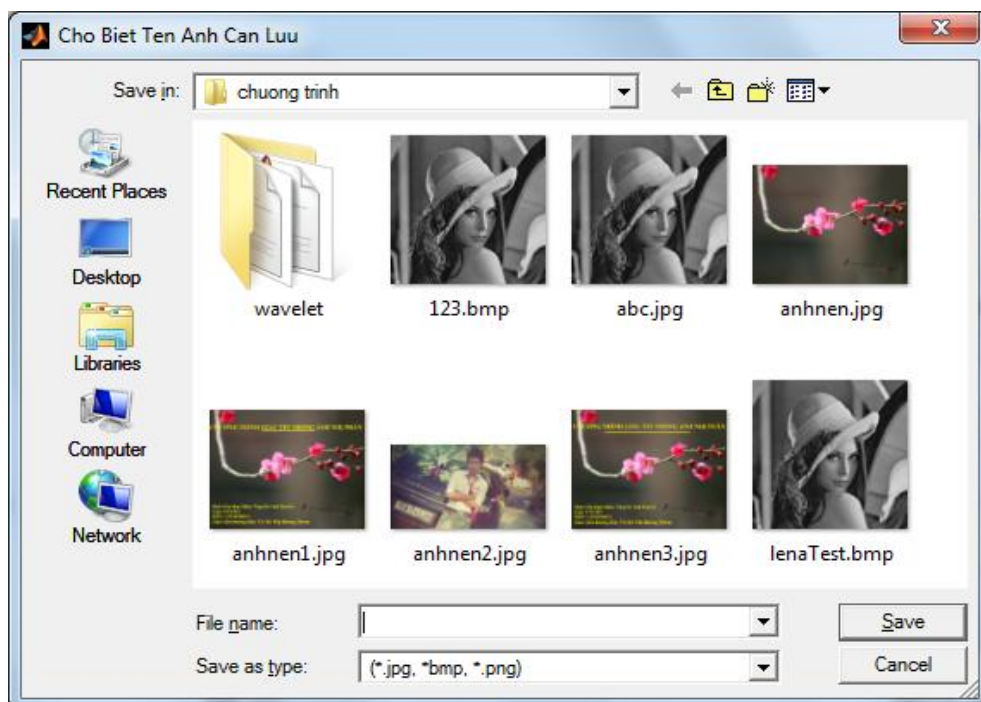
Hình 3.13. Hộp thoại cho biết Map định vị sau khi đã giấu tin  
Chọn khóa điều khiển Beta như bên giấu tin để thực hiện tách tin.



Hình 3.14. Nhập Beta ban đầu vào trong chương trình

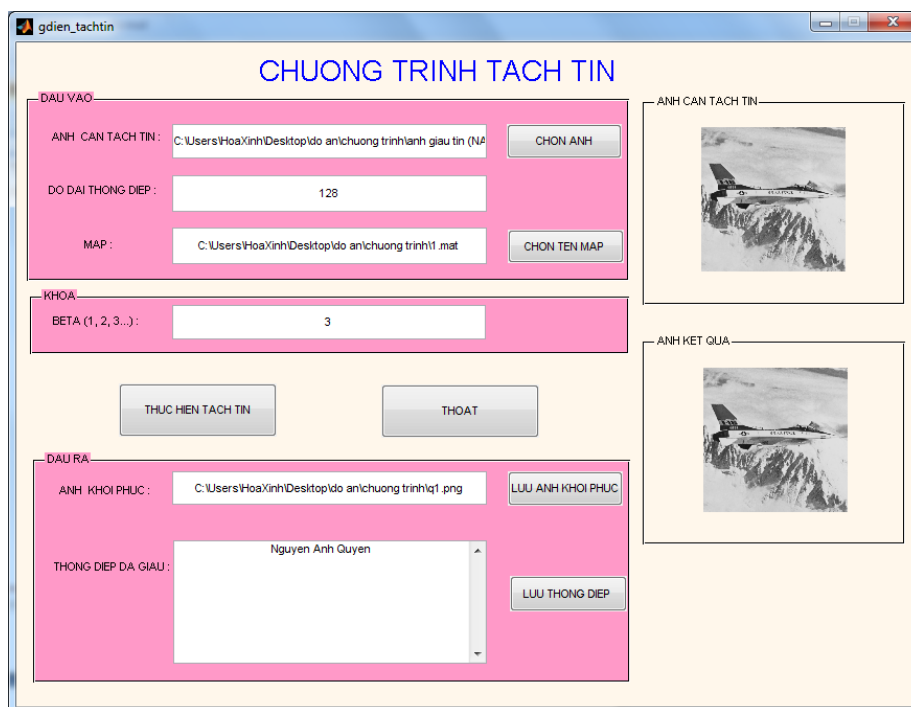


Chúng ta cần chọn nơi sẽ lưu ảnh kết quả sau khi đã tách tin vào bằng cách chọn “LUU ANH KHOI PHUC” từ giao diện.



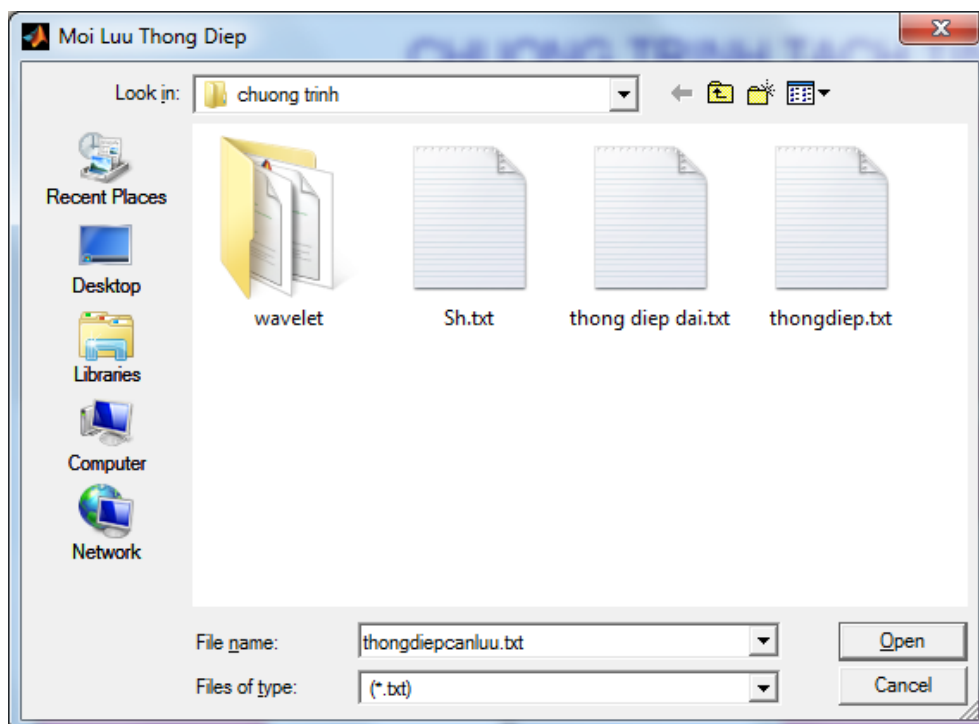
Hình 3.15. Hộp thoại cho biết tên ảnh sau khi đã tách tin

Sau khi đã lựa chọn xong đầu vào và đầu ra cho chương trình, chúng ta chọn nút “THUC HIEN TACH TIN”. Chương trình sẽ thực hiện và đưa ra kết quả ảnh đã tách tin và thông điệp ngay trên giao diện của chương trình.



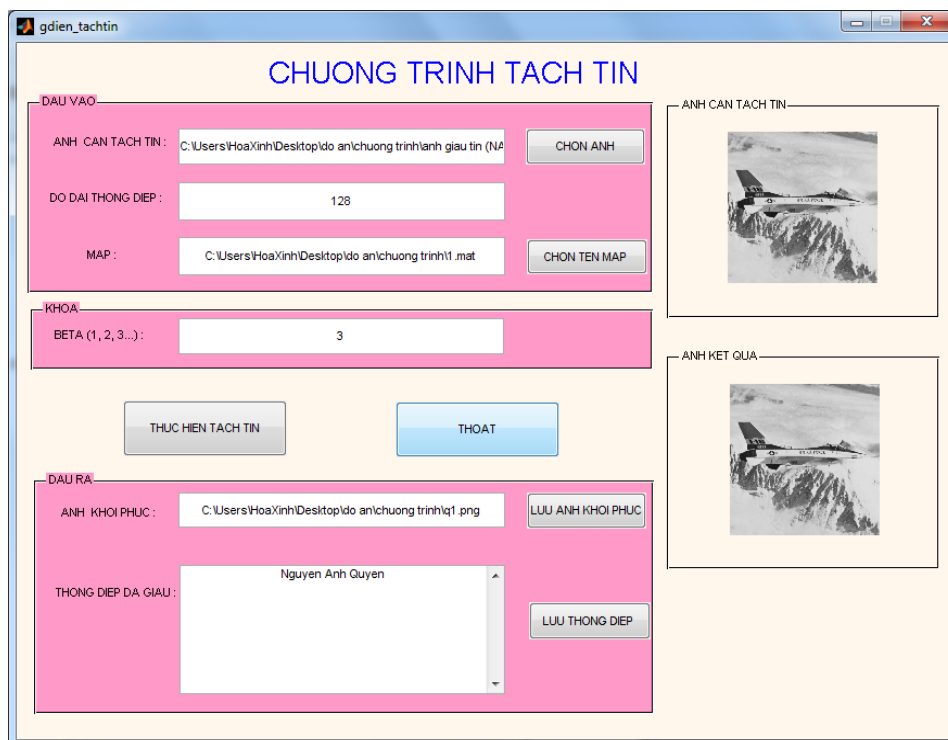
Hình 3.16. Giao diện sau khi giấu tin

Lưu lại thông điệp đã tách bằng cách ấn nút “LUU THÔNG ĐIỆP” trên giao diện.



Hình 3.17. Hộp thoại cho biết tên thông điệp sau khi đã tách tin

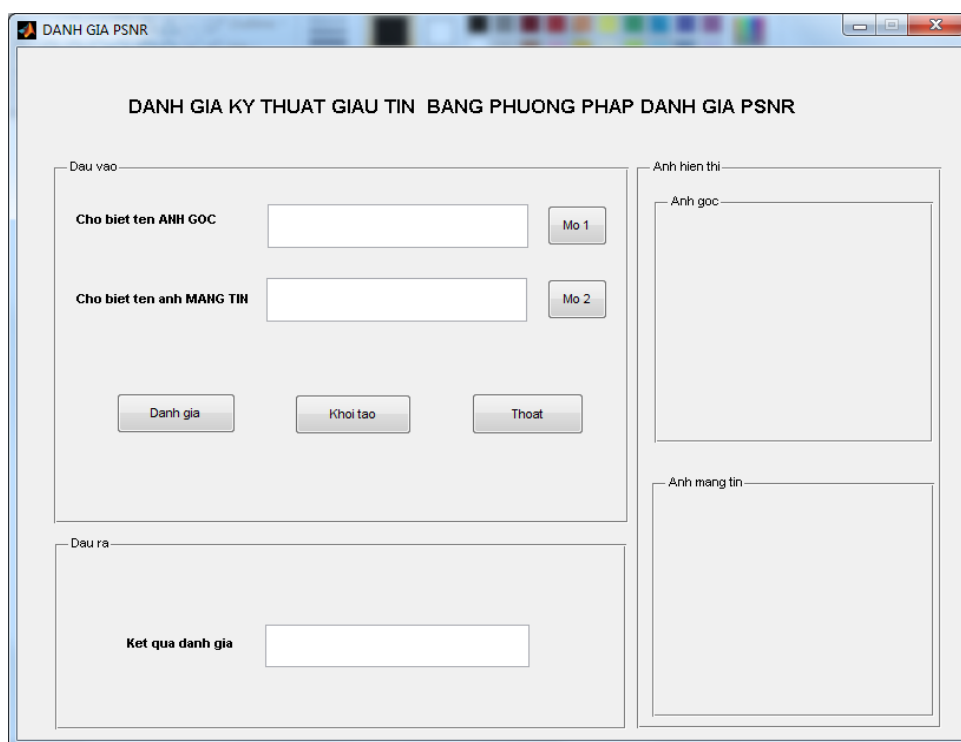
Sau khi hoàn thành mọi việc kích nút “THOAT” để thoát khỏi chương trình giấu tin.



Hình 3.18. Giao diện kết thúc chương trình tách tin

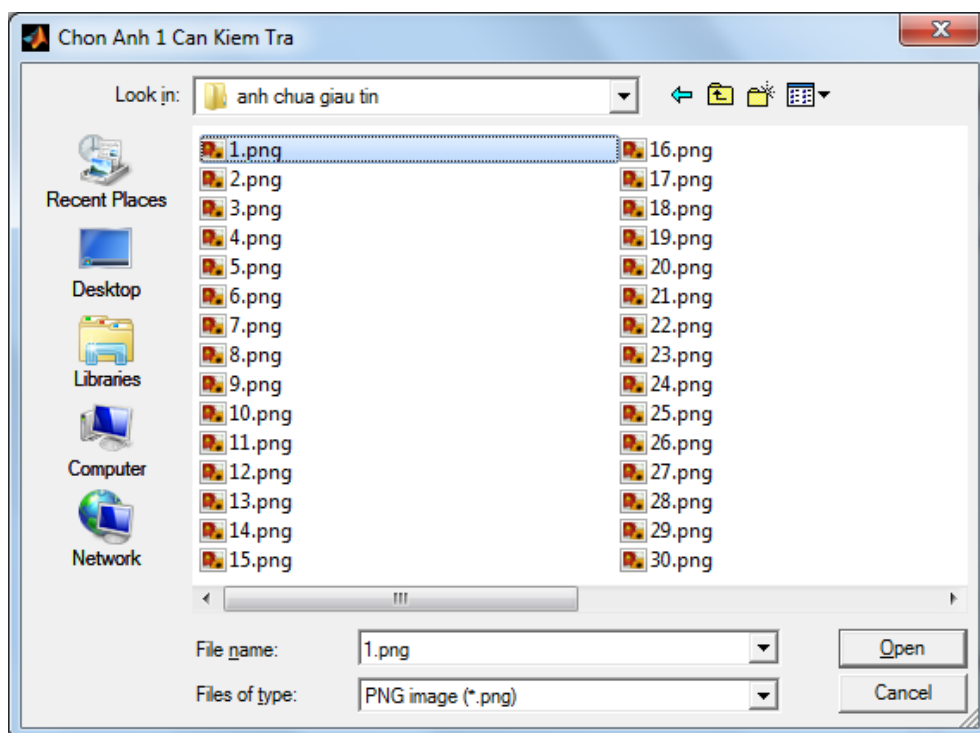


### 3.2.4. Giao diện chức năng đánh giá PSNR



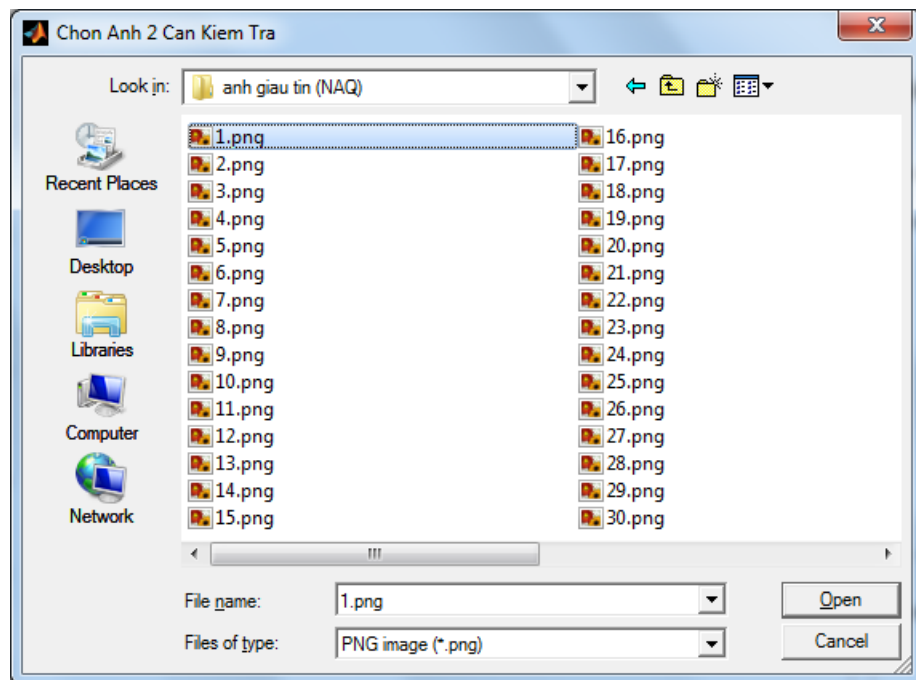
Hình 3.19. Giao diện chức năng giấu tin

Từ giao diện chính của chương trình chúng ta chọn ảnh cần kiểm tra bằng cách nhấn vào nút “MO 1”. Khi đó chương trình sẽ mở ra hộp thoại duyệt ảnh.



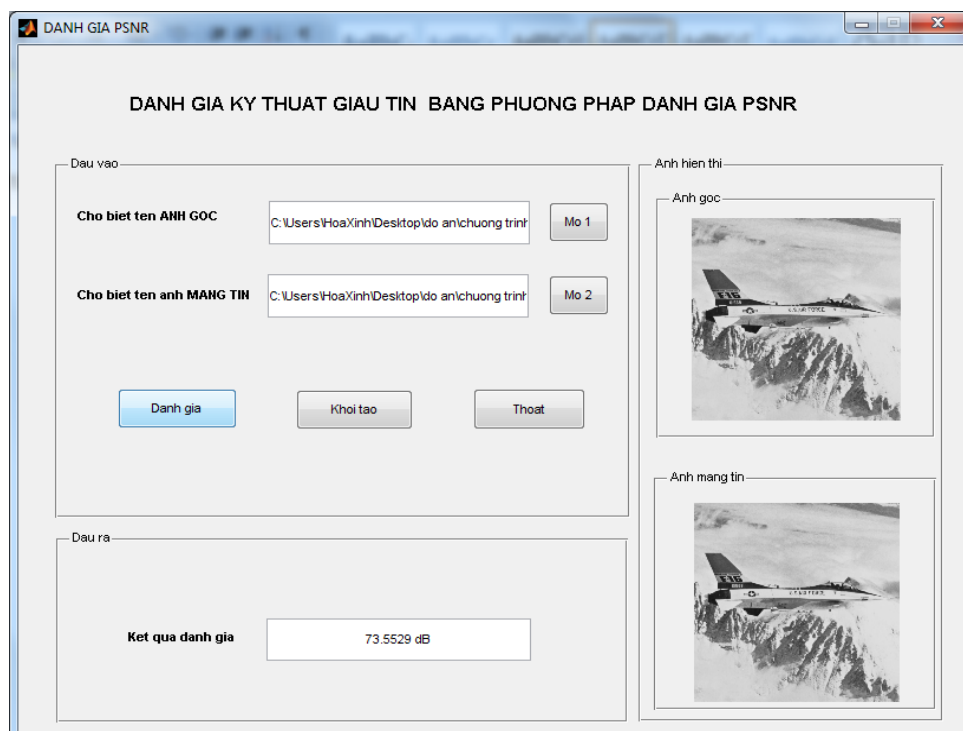
Hình 3.20. Hộp thoại chọn ảnh nhị phân cần kiểm tra

Từ giao diện chính của chương trình chúng ta chọn ảnh cần kiểm tra bằng cách nhấn vào nút “MO 2”. Khi đó chương trình sẽ mở ra hộp thoại duyệt ảnh.



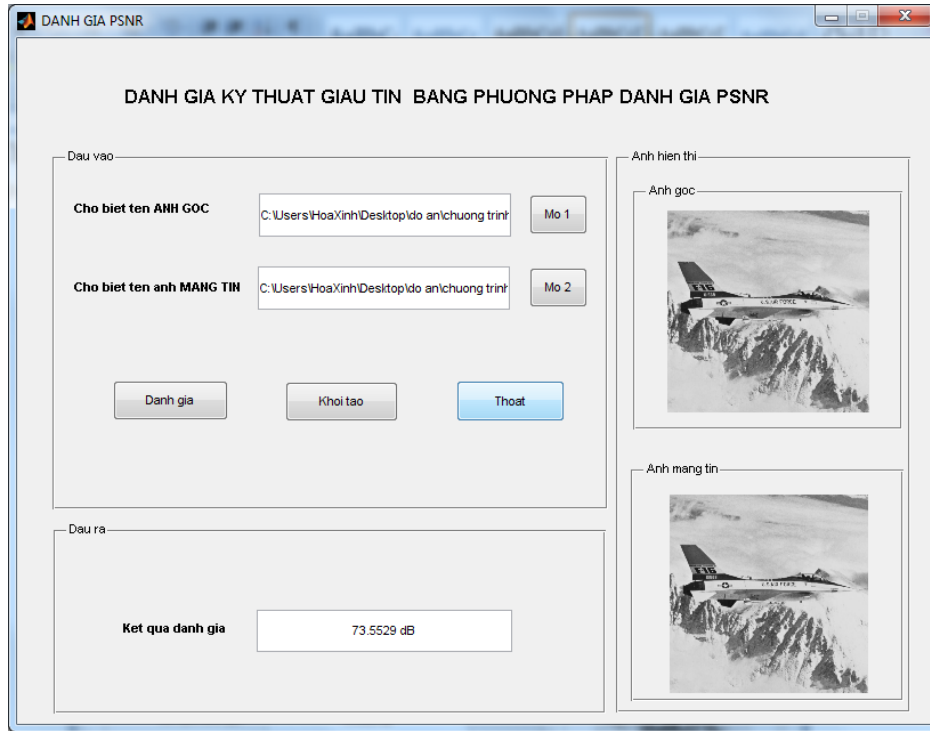
Hình 3.21. Hộp thoại chọn ảnh nhị phân cần kiểm tra

Từ giao diện chính của chương trình chúng ta nhấn vào nút “DANH GIA”. Khi đó chương trình sẽ cho ra kết quả đánh giá ngay trên giao diện trưng trình.



Hình 3.22. Giao diện đánh giá PSNR

Thoát khỏi chương trình đánh giá PSNR bằng cách nhấn vào nút “THOAT” trên giao diện chương trình.



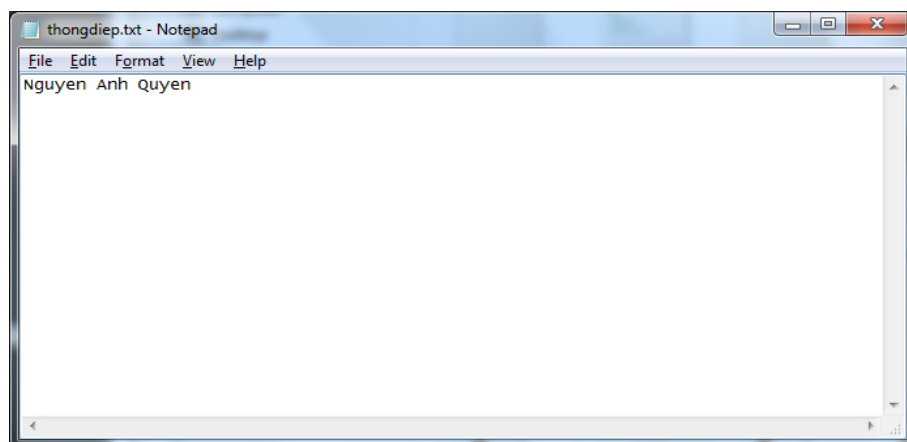
Hình 3.23. Giao diện thoát chương trình đánh giá PSNR

### 3.3. Kết quả thực nghiệm và nhận xét

#### 3.3.1. Kết quả thực nghiệm

Thực nghiệm này sẽ đưa ra khả năng giấu tin khi sử dụng bày kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao với ảnh cấp xám 8 bit.

**Trường hợp 1.** Giấu ít thông điệp: chuỗi gồm 16 kí tự.



Hình 3.24. Chuỗi thông điệp cần giấu ít kí tự



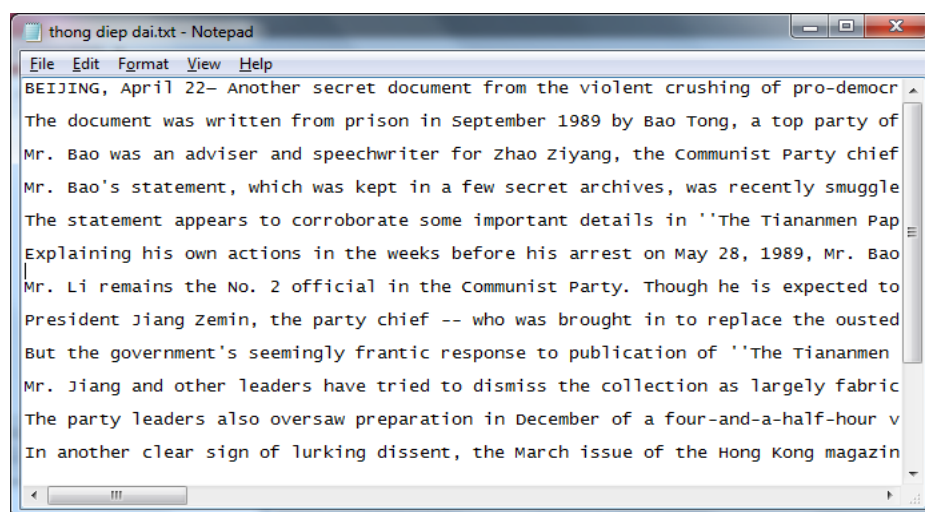
**Đánh giá PSNR đơn vị đo là dB:**

Bảng 3.1. Kết quả đánh giá PSNR trên ảnh cấp xám 8 bit của bày kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao.

<b>Tên ảnh (Kích cỡ ảnh)</b>	<b>Đánh giá PSNR (dB)</b>
1.png(512x512)	73.5529 dB
2.png(512x512)	74.8861 dB
3.png(512x512)	74.1703 dB
4.png(512x512)	75.1215 dB
5.png(512x512)	74.6129 dB
6.png(512x512)	74.7589 dB
7.png(512x512)	73.6622 dB
8.png(512x512)	73.7818 dB
9.png(512x512)	74.8499 dB
10.png(512 x768)	76.5918 dB
11.png(768x512)	76.0496 dB
12.png(512x768)	76.4578 dB
13.png(768x512)	77.0014 dB
14.png(768x512)	77.5838 dB
15.png(768x512)	77.5257 dB
16.png(768x512)	77.4119 dB
17.png(768x512)	76.5184 dB
18.png(768x512)	75.8554 dB
19.png(768x512)	77.3377 dB

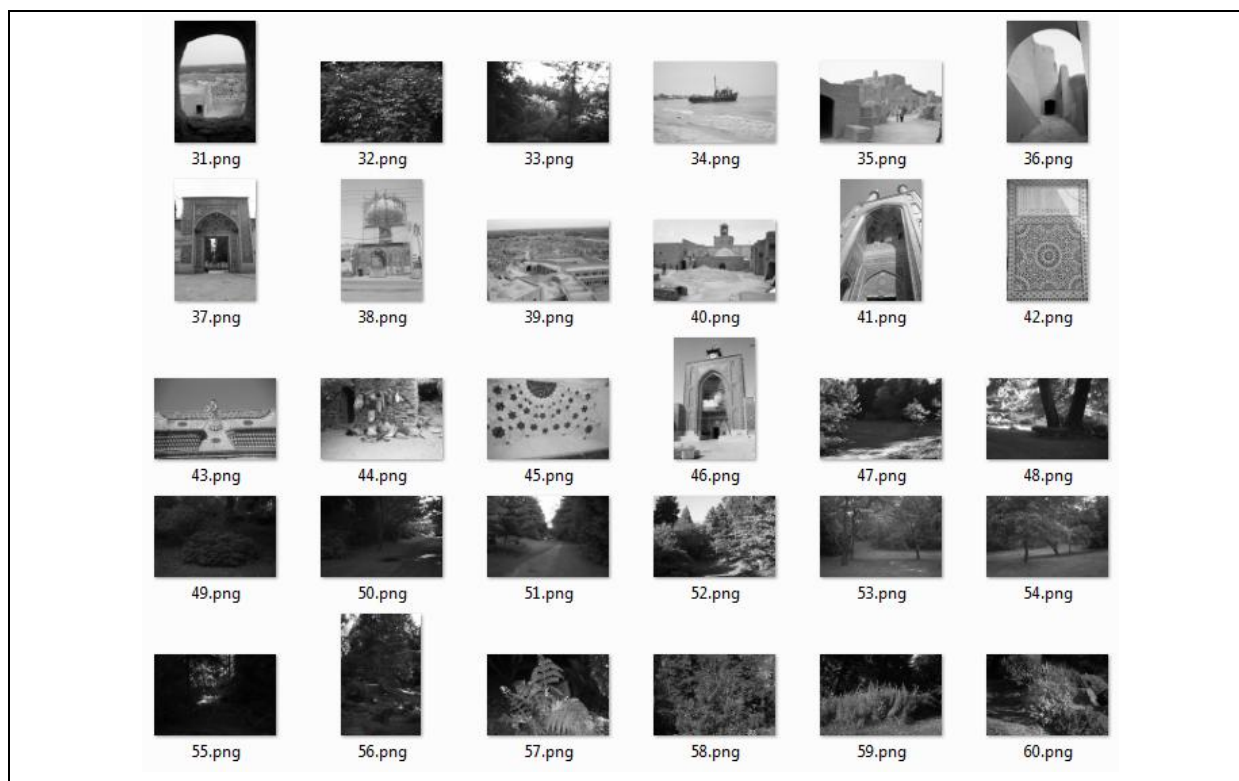
20.png(768x512)	77.2466 dB
21.png(512x768)	76.6735 dB
22.png(768x512)	75.2348 dB
23.png(768x512)	76.5184 dB
24.png(768x512)	75.797 dB
25.png(768x512)	76.4428 dB
26.png(768x512)	77.4495 dB
27.png(768x512)	75.2009 dB
28.png(768x512)	75.0067 dB
29.png(768x512)	76.4578 dB
30.png(768x512)	78.1002 dB
<b>Giá trị trung bình</b>	<b>75,93 dB</b>

**Trường hợp 2.** Giấu nhiều thông điệp: Chuỗi gồm 20000 ký tự.

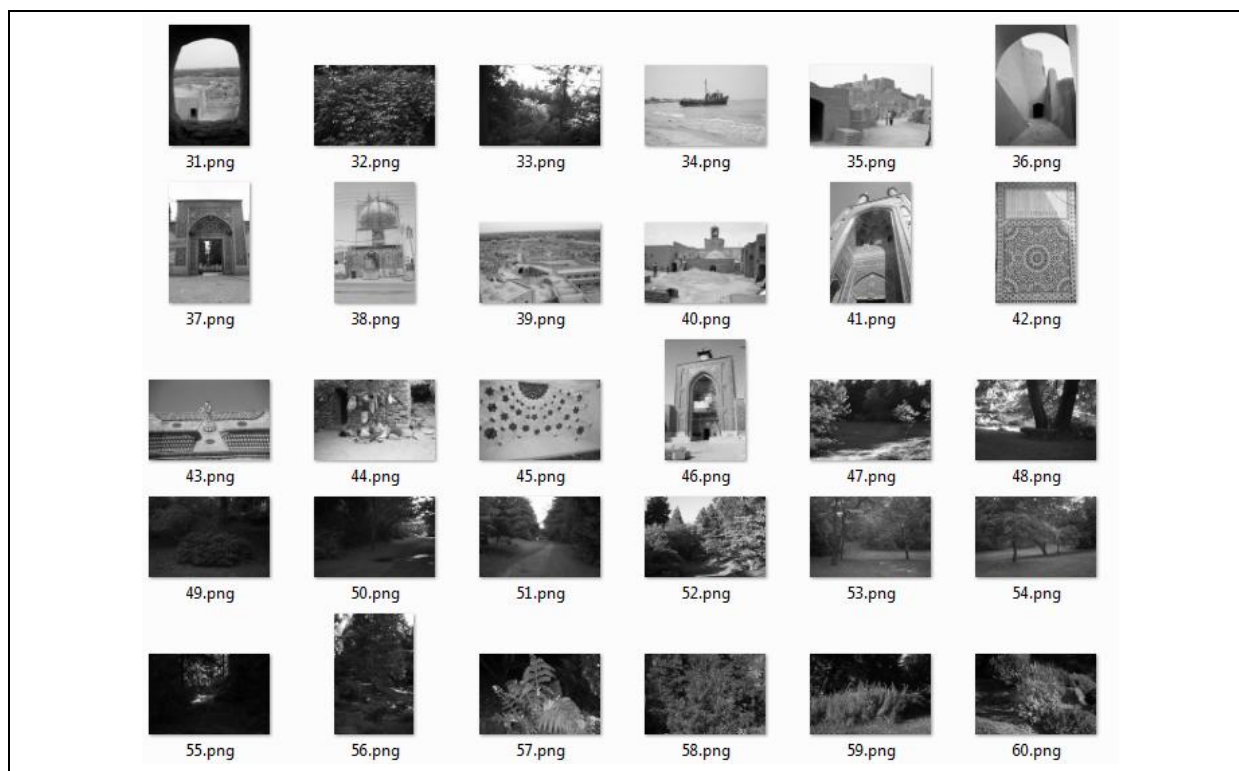


Hình 3.27. Chuỗi thông điệp 20000 ký tự cần giấu





Hình 3.28. Tập ảnh trước khi giấu tin



Hình 3.29. Tập ảnh sau khi giấu tin

**Đánh giá PSNR đơn vị đo là dB:**

Bảng 3.2. Kết quả đánh giá PSNR trên ảnh cấp xám 8 bit của bài kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao.

<b>Tên ảnh (Kích cỡ ảnh)</b>	<b>Đánh giá PSNR (dB)</b>
31.png(512x768)	56.6911 dB
32.png(768x504)	55.6859 dB
33.png(768x504)	57.25 dB
34.png(768x512)	56.3595 dB
35.png(768x512)	55.8712 dB
36.png(512x768)	55.7156 dB
37.png(512x768)	56.3634 dB
38.png(512x768)	55.9899 dB
39.png(768x512)	54.7333 dB
40.png(768x512)	56.4503 dB
41.png(512x768)	57.293 dB
42.png(512x768)	55.7568 dB
43.png(768x512)	57.4626 dB
44.png(768x512)	54.8569 dB
45.png(768x512)	54.3774 dB
46.png(512x768)	56.9927 dB
47.png(756x504)	57.3594 dB
48.png(756x504)	56.5533 dB
49.png(756x504)	55.3843 dB



50.png(756x504)	56.5958 dB
51.png(756x504)	55.7915 dB
52.png(756x504)	57.502 dB
53.png(756x504)	55.1358 dB
54.png(756x504)	55.0485 dB
55.png(756x504)	58.7043 dB
56.png(496x756)	55.6384 dB
57.png(756x504)	55.9076 dB
58.png(756x504)	57.1587 dB
59.png(756x504)	57.267 dB
60.png(756x504)	57.1851 dB
<b>Giá trị trung bình</b>	56.29 dB



**Đánh giá PSNR đơn vị đo là dB:**

Bảng 3.3. Kết quả đánh giá PSNR giữa ảnh gốc và ảnh gốc khôi phục được từ ảnh đã giấu tin (trong phần tách tin) của kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao.

<b>Tên ảnh (Kích cỡ ảnh)</b>	<b>Đánh giá PSNR (dB)</b>
1.png(512x512)	82.7244 dB
2.png(512x512)	82.2383 dB
3.png(512x512)	84.5469 dB
4.png(512x512)	83.3849 dB
5.png(512x512)	81.8012 dB
6.png(512x512)	84.0448 dB
7.png(512x512)	83.1286 dB
8.png(512x512)	85.0851 dB
9.png(512x512)	85.4142 dB
10.png(512 x768)	85.5038 dB
11.png(768x512)	95.0121 dB
12.png(512x768)	90.6529 dB
13.png(768x512)	85.948 dB
14.png(768x512)	85.1008 dB
15.png(768x512)	84.3458 dB
16.png(768x512)	85.269 dB
17.png(768x512)	86.5952 dB
18.png(768x512)	89.7635 dB
19.png(768x512)	84.9923 dB

20.png(768x512)	85.269 dB
21.png(512x768)	86.2238 dB
22.png(768x512)	89.7635 dB
23.png(768x512)	88.5141 dB
24.png(768x512)	88.7623 dB
25.png(768x512)	86.6735 dB
26.png(768x512)	84.5347 dB
27.png(768x512)	93.6632 dB
28.png(768x512)	92.9036 dB
29.png(768x512)	87.2647 dB
30.png(768x512)	85.269 dB
<b>Giá trị trung bình</b>	<b>86.48 dB</b>

### 3.3.2. Nhận xét

Với kết quả thử nghiệm thu được, dù chuỗi thông điệp nhỏ hay lớn quan sát bằng mắt thường đều không thể phân biệt được ảnh đã giấu tin hay chưa giấu tin, ở trường hợp giấu chuỗi thông điệp nhỏ giá trị PSNR trung bình đạt được rất là cao xấp xỉ 75,93 dB. Còn ở trường hợp giấu chuỗi thông điệp lớn giá trị PSNR trung bình ở mức độ cũng khá là cao xấp xỉ 56,29 dB. Có thể thấy phương pháp giấu tin trong ảnh này cho 1 kết quả và chất lượng hết sức cao. Nhưng sau khi đã có lượng thông tin được giấu vào trong ảnh gốc, nó sẽ để lại dù nhiều, dù ít. Những dấu vết khác với ảnh gốc ban đầu có thể thấy ở bảng 3.3 khi đánh giá PSNR giữa ảnh gốc và ảnh khôi phục chỉ nhận được 1 kết quả rất cao xấp xỉ 86,48 dB có những ảnh đạt kết quả đến 95 dB nhưng không 1 ảnh nào đạt 100 dB để giống y hệt ảnh gốc ban đầu.

Kết quả thử nghiệm trong bảng 3.1, 3.2 cho thấy khả năng giấu tin của mỗi ảnh khác nhau là khác nhau. Những ảnh có cùng kích cỡ khả năng giấu của những ảnh đó nằm trong 1 khoảng giá trị và xấp xỉ bằng nhau. Điều đó chứng tỏ khả năng giấu tin phụ thuộc vào giá trị điểm ảnh của ảnh. Một nguyên nhân nữa tác động lớn tới khả

năng giấu tin đó là việc lựa chọn khóa Beta. Vì giá trị điểm ảnh của mỗi ảnh là khác nhau, khả năng giấu của mỗi ảnh được tính liên quan tới Beta nên khi thay đổi Beta sẽ tạo nên khả năng giấu tin khác nhau.

Thời gian xử lý giấu tin phụ thuộc lớn vào dữ liệu đầu vào như kích thước ảnh gốc, thông điệp giấu lớn hay nhỏ. Độ an toàn của kỹ thuật cao, phụ thuộc vào giá trị của khóa Beta.

Qua thử nghiệm em nhận thấy kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao của ảnh có những ưu nhược điểm sau:

- Ưu điểm:

+ Khả năng bảo mật cao do khóa Beta và bản đồ Map do người nhận và người gửi biết với nhau. Phải đúng Beta và bản đồ Map mới có thể lấy được thông tin.

+ Độ nhiễu nhỏ, đạt chất lượng khá cao khi giấu lượng bit nhỏ và chấp nhận được khi giấu lượng bit lớn.

- Nhược điểm:

+ Phụ thuộc vào khóa Beta và bản đồ Map.

+ Không có bước tính toán khóa giấu tin Beta để tăng thêm độ an toàn cho dữ liệu.

+ Và sau khi đã có lượng thông tin được giấu vào trong ảnh gốc, nó sẽ để lại dù nhiều, dù ít những dấu vết khác với ảnh gốc ban đầu.

## KẾT LUẬN

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

Với bài kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao trên ảnh cấp xám 8 bit thì tính vô hình của thông tin sau khi giấu được đảm bảo, thông qua việc sử dụng một khoá Beta và một bản đồ Map trong quá trình giấu và tách thông tin. Về mặt lý thuyết thì sau khi đã có lượng thông tin được giấu vào trong ảnh gốc, nó sẽ để lại dấu nhiều, dù ít những dấu vết khác với ảnh gốc ban đầu. Dùng phương pháp đánh giá PSNR để đánh giá chất lượng ảnh trước và sau khi giấu tin kết quả đạt được là rất cao nếu giấu lượng bit nhỏ, và chấp nhận được nếu giấu lượng bit lớn. Như vậy bài kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao đã cho những kết quả hết sức tích cực. Tuy nhiên, giấu tin mật là vấn đề phức tạp, cộng với khả năng và kinh nghiệm còn hạn chế nên em còn gặp một số khó khăn trong việc tìm hiểu nghiên cứu các bài kỹ thuật giấu tin thuận nghịch trên miền biến đổi sóng nhỏ (wavelet) cho ảnh chất lượng cao trên ảnh cấp xám 8 bit.

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

Em xin chân thành cảm ơn!

**TÀI LIỆU THAM KHẢO**

- [1]. Nguyễn Xuân Huy, Trần Quốc Dũng, **Giáo trình giấu tin và thủy vân ảnh**, Trung tâm thông tin tư liệu, TTKHTN - CN 2003
- [2]. Nguyễn Xuân Huy, Trần Quốc Dũng, **Giáo trình giấu tin và thủy 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]. Ching-Yu Yanga Chih-Hung Linb and Wu-Chih Hu, **Reversible Data Hiding for High-Quality Images Based on Integer Wavelet Transform**, Journal of Information Hiding and Multimedia Signal Processing, Volume 3, Number 2, April 2012
- [5]. Dương Ưông Hiên – CT701, “**Nghiên cứu kỹ thuật giấu tin mật trên vùng biến đổi DWT**”, tiểu án tốt nghiệp ngành CNTT – 2008.
- [6]. Đỗ Trọng Phú – CT702, “**Nghiên cứu kỹ thuật giấu tin trên miền biến đổi DFT**”, tiểu án tốt nghiệp ngành CNTT – 2008.
- [7]. Hoàng Thị Huyền Trang – CT802, “**Nghiên cứu kỹ thuật phát hiện ảnh giấu tin trên miền biến đổi của ảnh**”, đồ án tốt nghiệp ngành CNTT – 2008.
- [8]. Trần Đại Dương, “**Kỹ thuật giấu tin thuận nghịch trong ảnh bằng hiệu chỉnh hệ số wavelet**”, đồ án tốt nghiệp ngành CNTT.