

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



ISO 9001 : 2008

BÁO CÁO KHOA HỌC

NGÀNH CÔNG NGHỆ THÔNG TIN

KỸ THUẬT PHÁT HIỆN THÔNG TIN ẨN GIẤU TRONG ẢNH JPEG2000

Chủ nhiệm đề tài: Phạm Thị Quỳnh
Thành viên: Phạm Thị Thu Trang

Giáo viên hướng dẫn: ThS. Hồ Thị Hoàng Thơm

HẢI PHÒNG 08-2009

BÁO CÁO KHOA HỌC

Đề tài: Kỹ thuật giấu thông tin trong ảnh JPEG2000

Chủ nhiệm đề tài : *Phạm Thị Quỳnh* **Lớp CT901**

Thành viên : *Phạm Thị Thu Trang* **Lớp CT901**

Giáo viên hướng dẫn: *Ths. Hồ Thị Hương Thơm*

MỤC LỤC

LỜI CẢM ƠN	0
LỜI MỞ ĐẦU	0
CHƯƠNG 1. TỔNG QUAN KỸ THUẬT GIẤU TIN	2
1.1. Định nghĩa giấu tin.....	2
1.2. Mục đích của giấu tin.....	2
1.3 Mô hình kỹ thuật giấu thông tin cơ bản	2
1.4. Môi trường giấu tin	3
a) Giấu tin trong ảnh.....	3
b) Giấu tin trong audio	4
c) Giấu tin trong video	4
d) Giấu thông tin trong văn bản dạng text	4
1.5. Phân loại giấu tin theo cách thức tác động lên các phương tiện.....	4
1.6. Phân loại giấu tin theo các mục đích sử dụng.....	4
CHƯƠNG 2. CHUẨN NÉN ẢNH TĨNH DỰA TRÊN BIẾN ĐỔI WAVELET– JPEG2000	6
2.1. Khái niệm nén ảnh.	6
2.2. Sự ra đời của JPEG2000	6
2.3. Các tính năng của JPEG2000.....	6
2.4. Các bước thực hiện nén ảnh theo chuẩn JPEG2000	7
2.4.1. Xử lý trước khi biến đổi.....	7
2.4.2. Biến đổi liên thành phần	7
2.4.3. Biến đổi riêng thành phần (biến đổi Wavelet).....	8
2.4.4. Lượng tử hóa – Giải lượng tử hóa.....	8
2.4.5. Mã hóa và kết hợp dòng dữ liệu sau mã hóa.....	9
2.4.6. Phương pháp mã hóa SPIHT.....	9
2.4.7. Phương pháp mã hóa EZW	11
2.4.8. So sánh chuẩn JPEG2000 với JPEG và các chuẩn nén ảnh tĩnh khác	12
CHƯƠNG 3. PHƯƠNG PHÁP GIẤU THỦY VÂN DỰA VÀO CẶP TẦN SỐ GIỮA DWT	16
3.1. Giới thiệu.....	16
3.2. Thủy vân trong miền DWT	17
3.2.1. Sự tương quan giữa các hệ số của các dải giữa dưới sự biến đổi cặp xám.....	18

3.2.2. Thuật toán nhúng và tách thủy vân (thuật toán 1) [1].....	20
a. Kỹ thuật nhúng thủy vân	20
b. Kỹ thuật tách thủy vân	21
3.2.3. Thuật toán nhúng và tách thủy vân cải tiến (thuật toán 2).....	23
a. Kỹ thuật nhúng thủy vân:	23
b. Kỹ thuật tách thủy vân:	23
CHƯƠNG 4. VẤN ĐỀ PHÁT HIỆN ẢNH CÓ GIẤU TIN TRÊN MIỀN TẦN SỐ GIỮA DWT	25
4.1. Tổng quan về kỹ thuật phát hiện tin ẩn giấu trong ảnh (Steganalysis)....	25
4.2. Với kỹ thuật giấu 1	26
4.3. Với kỹ thuật giấu 2.....	26
CHƯƠNG 5. CÀI ĐẶT THỬ NGHIỆM.....	27
5.1. Môi trường cài đặt.....	27
5.2. Thử nghiệm	28
KẾT LUẬN	36
TÀI LIỆU THAM KHẢO	37

LỜI CẢM ƠN

Chúng em xin chân thành cảm ơn hội đồng khoa Công Nghệ Thông Tin, hội đồng khoa học trường Đại Học Dân Lập Hải Phòng đã tạo điều kiện để chúng em thực hiện tốt đề tài nghiên cứu khoa học.

Chúng em xin chân thành cảm ơn cô giáo: Ths. Hồ Thị Hương Thơm – giảng viên khoa công nghệ thông tin trường ĐHDL Hải Phòng, đã tận tình hướng dẫn và chỉ đạo chúng em trong suốt thời gian nghiên cứu đề tài.

Cuối cùng, chúng mình xin cảm ơn tất cả các bạn đồng môn đã động viên, góp ý và trao đổi hỗ trợ cho chúng mình trong suốt thời gian nghiên cứu vừa qua.

Vì thời gian nghiên cứu chỉ có hạn, trình độ hiểu biết của bản thân chúng em còn nhiều hạn chế. Cho nên trong đề tài không tránh khỏi những thiếu sót, chúng em rất mong được sự góp ý quý báu của tất cả các thầy cô giáo cũng như các bạn để đề tài của chúng em được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

Hải Phòng, ngày 14 tháng 8 năm 2009

Nhóm thực hiện

**Phạm Thị Quỳnh
Phạm Thị Thu Trang**

LỜI MỞ ĐẦU

Môi trường mạng Internet phát triển rộng rãi cùng với sự hỗ trợ của các phương tiện đa truyền thông đã đem lại nhiều thuận lợi và cơ hội cho con người trên mọi lĩnh vực của đời sống xã hội, trong giao lưu, hợp tác, kinh doanh, ... Nhưng đồng thời nó cũng như đặt ra nhiều thách thức trong việc đảm bảo tính an toàn cho các thông tin được truyền giao qua các phương tiện truyền thông như: nguy cơ sử dụng trái phép, xuyên tạc bất hợp pháp thông tin lưu chuyển trên mạng. Việc sử dụng một cách bình đẳng, an toàn các dữ liệu đa phương tiện cũng như cung cấp một cách kịp thời tới nhiều người dùng cuối và các thiết bị cuối cũng là một vấn đề quan trọng.

Hơn nữa, sự phát triển mạnh của các phương tiện kỹ thuật số đã làm cho việc lưu trữ, sửa đổi và sao chép dữ liệu ngày càng đơn giản, từ đó việc bảo vệ bản quyền và chống xâm phạm trái phép các dữ liệu đa phương tiện (âm thanh, hình ảnh, tài liệu) cũng gặp nhiều khó khăn. Một công nghệ mới được ra đời đã phần nào giải quyết được các khó khăn trên là giấu thông tin trong các nguồn đa phương tiện như các nguồn âm thanh, hình ảnh, ảnh tĩnh. Mục tiêu của giấu thông tin là làm cho thông tin trở nên vô hình, từ đó khiến ta không thể thấy được đối tượng.

Trong những năm gần đây, giấu thông tin trong ảnh là một bộ phận chiếm tỷ lệ lớn nhất trong các chương trình ứng dụng, các phần mềm, hệ thống giấu tin trong đa phương tiện bởi lượng thông tin được trao đổi bằng ảnh là rất lớn. Nó đóng vai trò rất 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 của tác giả... Thông tin sẽ được giấu cùng với dữ liệu ảnh nhưng chất lượng ảnh ít thay đổi và không ai biết được đằng sau nó mang những thông tin có ý nghĩa. Ngày nay, khi ảnh số đã được sử dụng rất phổ biến thì giấu thông tin trong ảnh đã đem lại nhiều những ứng dụng to lớn trên hầu hết các lĩnh vực trong đời sống xã hội.

Giấu thông tin là một kỹ thuật còn tương đối mới và đang phát triển rất nhanh thu hút được sự quan tâm của cả giới khoa học và giới công nghiệp nhưng

cũng còn rất nhiều thách thức. Bản báo cáo này trình bày về một kỹ thuật giấu thông tin trong ảnh JPEG2000.

Nội dung của đề tài được trình bày trong 5 chương:

Chương 1: Tổng quan về kỹ thuật giấu tin trong ảnh

Chương 2: Chuẩn nén ảnh tĩnh dựa trên biến đổi WAVELET-JPEG2000

Chương 3: Phương pháp giấu thủy vân dựa vào cặp tần số giữa DWT

Chương 4: Vấn đề phát hiện ảnh có giấu tin trên miền tần số giữa DWT

Chương 5: Cài đặt thử nghiệm

CHƯƠNG 1. TỔNG QUAN KỸ THUẬT GIẤU TIN

1.1. Định nghĩa giấu tin

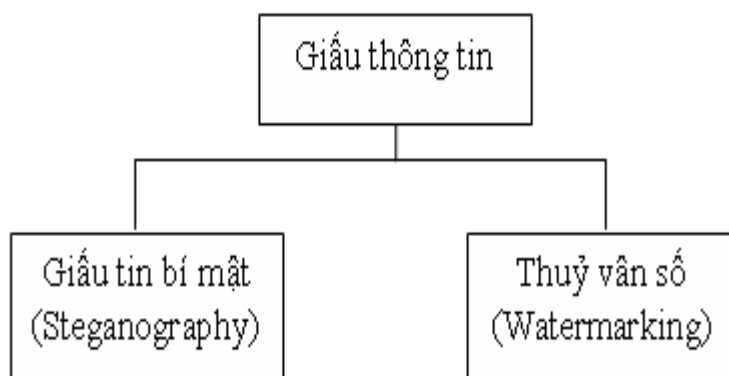
Giấu tin là một kỹ thuật giấu hoặc nhúng một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác (giấu tin nhiều khi không phải là hành động giấu cụ thể mà chỉ mang ý nghĩa quy ước).

1.2. Mục đích của giấu tin

Có 2 mục đích của giấu thông tin:

- Bảo mật cho những dữ liệu được giấu.
- Bảo đảm an toàn (bảo vệ bản quyền) cho chính các đối tượng chứa dữ liệu giấu trong đó.

Có thể thấy 2 mục đích này hoàn toàn trái ngược nhau và dần phát triển thành 2 lĩnh vực với những yêu cầu và tính chất khác nhau.



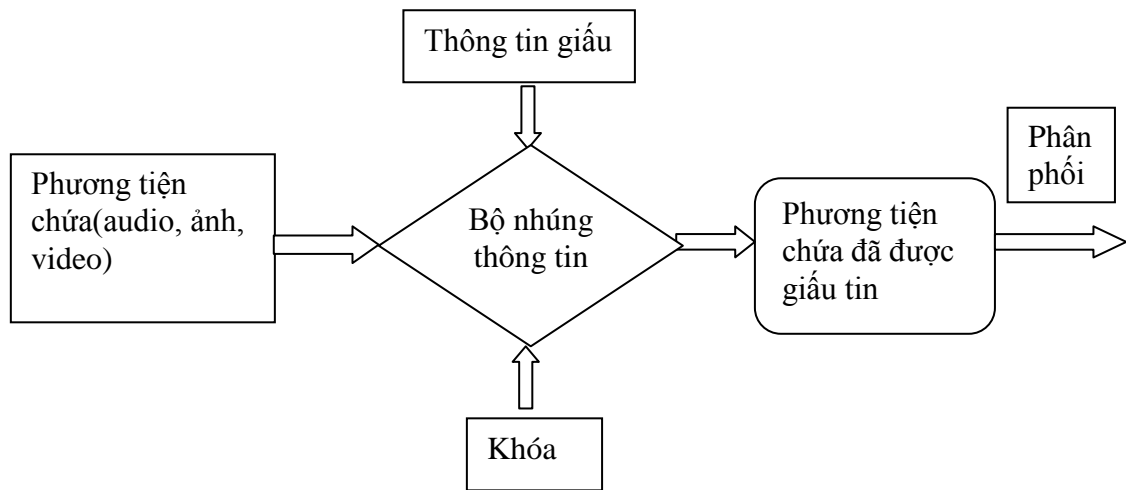
Hình 1.1. Hai lĩnh vực chính của kỹ thuật giấu thông tin.

Kỹ thuật giấu thông tin bí mật (Steganography): với mục đích đảm bảo tính an toàn và bảo mật thông tin tập trung vào các kỹ thuật giấu tin để có thể giấu được nhiều thông tin nhất. Thông tin mật được giấu kỹ trong một đối tượng khác sao cho người khác không phát hiện được.

Kỹ thuật giấu thông tin theo kiểu đánh dấu (watermarking) có mục đích là để bảo vệ bản quyền của đối tượng chứa thông tin thì lại tập trung đảm bảo một số các yêu cầu như đảm bảo tính bền vững... đây là ứng dụng cơ bản nhất của kỹ thuật thủy vân số.

1.3 Mô hình kỹ thuật giấu thông tin cơ bản

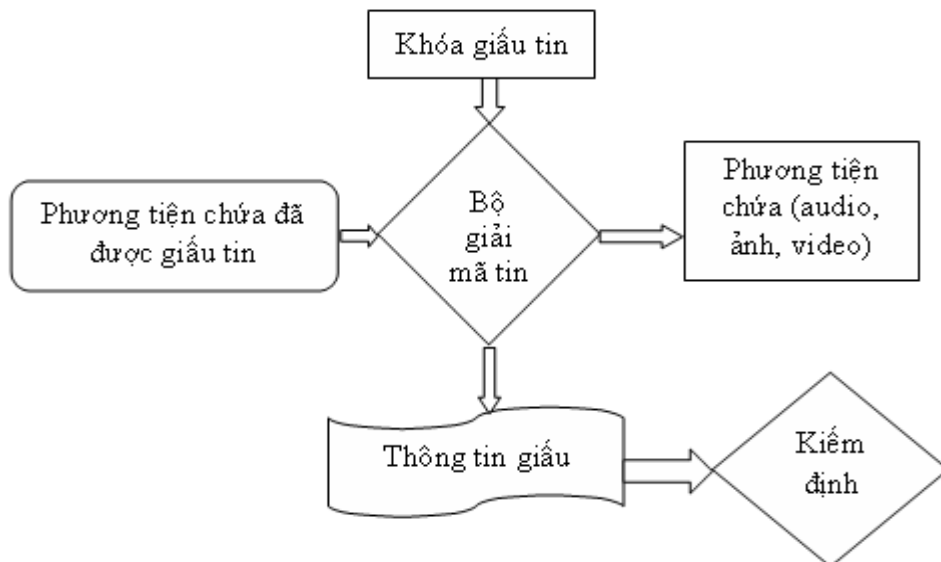
Giấu thông tin vào phương tiện chứa và tách lấy thông tin là 2 quá trình trái ngược nhau và có thể mô tả qua sơ đồ khối của hệ thống như sau:



Hình 1.2. Lược đồ chung cho quá trình giấu tin

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

Hình vẽ sau chỉ ra các công việc giải mã thông tin đã giấu.



Hình 1.3. Lược đồ chung cho quá trình giải mã

1.4. Môi trường giấu tin

a) Giấu tin trong ảnh

Giấu tin trong ảnh hiện đang rất được quan tâm. Nó 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... Thông tin sẽ được giấu cùng với dữ liệu ảnh nhưng chất lượng ảnh ít thay đổi và không ai

biết được đằng sau ảnh đó mang những thông tin có ý nghĩa. Ngày này, khi ảnh số đã được sử dụng rất phổ biến thì giấu thông tin trong ảnh đã đem lại nhiều những ứng dụng quan trọng trên các lĩnh vực trong đời sống xã hội.

b) Giấu tin trong audio

Khác với kỹ thuật giấu thông tin trong ảnh: phụ thuộc vào hệ thống thị giác của con người – HSV (Human Vision System), kỹ thuật giấu thông tin trong audio lại phụ thuộc vào hệ thống thính giác HAS (Human Auditory System). Bởi vì tai con người rất kém trong việc phát hiện sự khác biệt giữa các giải tần và công suất, có nghĩa là các âm thanh to, cao tần có thể che giấu đi được các âm thanh nhỏ, thấp một cách dễ dàng.

c) Giấu 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 thức thông tin, bản quyền tác giả...

Một phương pháp giấu tin trong video được đưa ra bởi Cox là phương pháp phân bố đều. Ý tưởng cơ bản của phương pháp là phân phối tin giấu dàn trải theo tần số của dữ liệu gốc.

d) Giấu thông tin trong văn bản dạng text

Giấu thông tin trong văn bản dạng text thì khó thực hiện hơn do có ít thông tin dư thừa, để làm được điều này người ta phải biết khéo léo khai thác các dư thừa tự nhiên của ngôn ngữ. Một cách khác là tận dụng các định dạng văn bản (mã hoá thông tin vào khoảng cách giữa các từ hay các dòng văn bản).

1.5. Phân loại giấu tin theo cách thức tác động lên các phương tiện

Phương pháp chèn dữ liệu: Phương pháp này tìm các vị trí trong file để bị bỏ qua và chèn dữ liệu cần giấu vào đó, cách giấu này không làm ảnh hưởng gì tới sự thể hiện các file dữ liệu ví dụ như được giấu sau các ký tự EOF.

Phương pháp tạo các phương tiện chứa: Từ các thông điệp cần chuyển sẽ tạo ra các phương tiện chứa để phục vụ cho việc truyền thông tin đó, từ phía người nhận dựa trên các phương tiện chứa này sẽ tái tạo lại các thông điệp.

1.6. Phân loại giấu tin theo các mục đích sử dụng

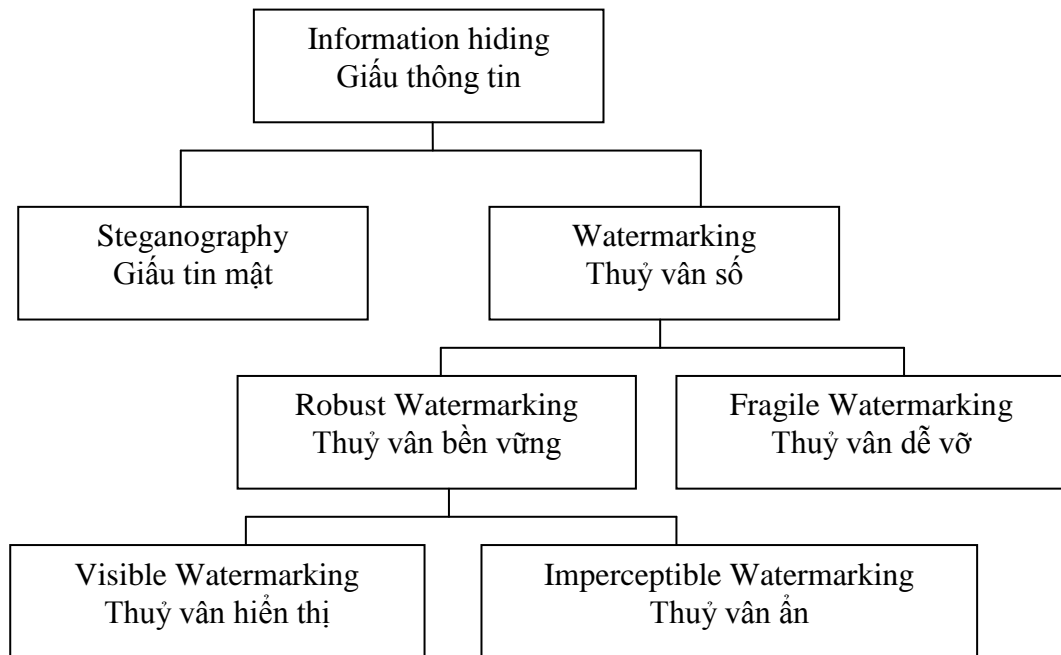
➤ Giấu thông tin bí mật: đây là ứng dụng phổ biến nhất từ trước đến nay, đối với giấu thông tin bí mật người ta quan tâm chủ yếu tới các mục tiêu:

- + Độ an toàn của giấu tin - khả năng không bị phát hiện của giấu tin.
- + Lượng thông tin tối đa có thể giấu trong một phương tiện chứa cụ thể mà vẫn có thể đảm bảo an toàn.

+ Độ bí mật của thông tin trong trường hợp giấu tin bị phát hiện.

- Giấu thông tin thuỷ vân: do yêu cầu bảo vệ bản quyền, xác thực... nên việc giấu tin thuỷ vân có yêu cầu khác với giấu tin bí mật. Yêu cầu đầu tiên là các dấu hiệu thuỷ vân đủ bền vững trước các tấn công vô hình hay cố ý gỡ bỏ nó. Thêm vào đó các dấu hiệu thuỷ vân phải có ảnh hưởng tối thiểu (về mặt cảm nhận) đối với các phương tiện chứa. Như vậy các thông tin cần giấu càng nhỏ càng tốt.

Như vậy tùy theo các mục đích khác nhau thuỷ vân cũng có các yêu cầu khác nhau.

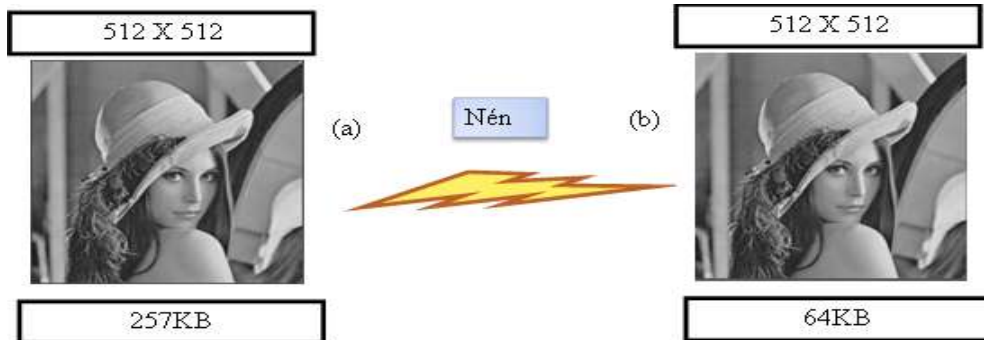


Hình 1.4. Phân loại các kỹ thuật giấu tin

CHƯƠNG 2. CHUẨN NÉN ẢNH TĨNH DỰA TRÊN BIẾN ĐỔI WAVELET– JPEG2000

2.1. Khái niệm nén ảnh.

- Nén là quá trình làm giảm thông tin dư thừa trong dữ liệu gốc.



Hình 2.1. ảnh ban đầu(a) và ảnh sau khi nén(b)

- Như vậy, nén ảnh có thể giảm nhỏ kích thước ảnh, giảm thời gian truyền và làm giảm chi phí xử lý ảnh trong khi chất lượng ảnh là tốt hơn.

2.2. Sự ra đời của JPEG2000

- Để việc nén ảnh có hiệu quả hơn, tháng 12/1999 một bản phác thảo tiêu chuẩn nén hình ảnh theo công nghệ mới JPEG2000 thay thế cho chuẩn nén ảnh tĩnh JPEG.

- Tháng 8/2000, bản phác thảo về tiêu chuẩn JPEG2000 đã được lưu hành trong giới chuyên gia hình ảnh.

- 12/2000 và được ISO hợp thức hóa năm nay để cho phép ứng dụng vào các hệ xử lý, phân phối.

- JPEG-2000 sử dụng kỹ thuật mã hóa dạng sóng rời rạc (DWT – Discrete Wavelet Transform) dùng mã số học.

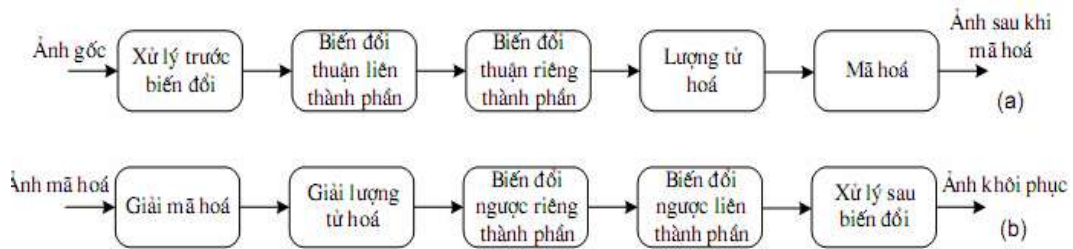
2.3. Các tính năng của JPEG2000

JPEG2000 nhiều chức năng đặc biệt hơn mọi chuẩn nén ảnh tĩnh khác như JPEG hay GIF. Dưới đây là các chức năng ưu việt của JPEG2000 so với các chuẩn nén ảnh tĩnh khác :

- ✓ Cho chất lượng ảnh tốt nhất khi áp dụng nén ảnh tĩnh có tổn thất.
- ✓ Sử dụng được với truyền dẫn và hiển thị lũy tiến về chất lượng, độ phân giải, các thành phần màu và có tính định vị không gian.
- ✓ Sử dụng cùng một cơ chế nén ảnh cho cả hai dạng thức nén.
- ✓ Truy nhập và giải nén tại mọi thời điểm trong khi nhận dữ liệu.

- ✓ Giải nén từng vùng trong ảnh mà không cần giải nén toàn bộ ảnh.
- ✓ Có khả năng mã hóa với tỷ lệ nén theo từng vùng khác nhau.
- ✓ Nén một lần nhưng có thể giải nén với nhiều cấp chất lượng tùy theo yêu cầu của người sử dụng.

2.4. Các bước thực hiện nén ảnh theo chuẩn JPEG2000



Hình 2.2. Trình tự mã hóa và giải mã JPEG2000

2.4.1. Xử lý trước khi biến đổi

Do sử dụng biến đổi Wavelet, JPEG2000 cần có dữ liệu ảnh đầu vào ở dạng đối xứng qua 0. Xử lý trước biến đổi chính là giai đoạn đảm bảo dữ liệu đưa vào nén ảnh có dạng trên. Ở phía giải mã, giai đoạn xử lý sau biến đổi sẽ trả lại giá trị gốc ban đầu cho dữ liệu ảnh.

2.4.2. Biến đổi liên thành phần

Giai đoạn này sẽ loại bỏ tính tương quan giữa các thành phần của ảnh. JPEG2000 sử dụng hai loại biến đổi liên thành phần là biến đổi thuận nghịch (Reversible Color Transform - RCT) và biến đổi màu không thuận nghịch (Irreversible Color Transform - ICT) trong đó biến đổi thuận nghịch làm việc với các giá trị nguyên, còn biến đổi không thuận nghịch làm việc với các giá trị thực. ICT và RCT chuyển dữ liệu ảnh từ không gian màu RGB sang YCrCb. RCT được áp dụng cho nén có tổn thất. Việc áp dụng các biến đổi màu trước khi nén ảnh không nằm ngoài mục đích làm tăng hiệu quả nén. Các thành phần Cr, Cb có ảnh hưởng rất ít tới sự cảm nhận hình ảnh của mắt trong khi thành phần độ chói Y có ảnh hưởng rất lớn tới ảnh. Chúng ta có thể thấy rõ điều này trên hình 2.3.

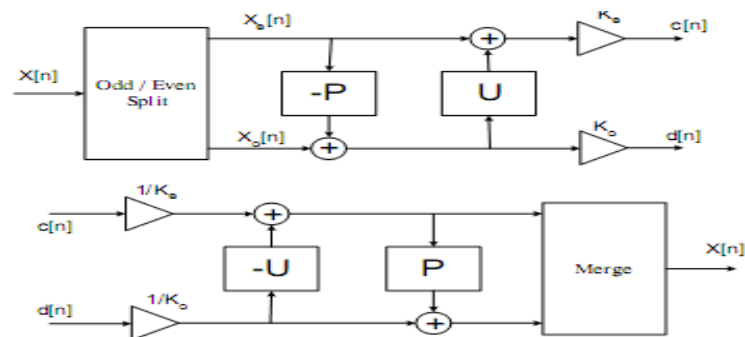


Hình 2.3. Minh họa ảnh với RGB và YcrCb

2.4.3. Biến đổi riêng thành phần (biến đổi Wavelet)

Biến đổi riêng thành phần được áp dụng trong JPEG2000 chính là biến đổi Wavelet. Để đảm bảo tính toàn vẹn thông tin cũng phải áp dụng các phép biến đổi thuận nghịch hoặc không thuận nghịch. Do phép biến đổi Wavelet không phải là một phép biến đổi trực giao như biến đổi DCT mà là một phép biến đổi băng con nên các thành phần sẽ được phân chia thành các băng tần số khác nhau và mỗi băng sẽ được mã hóa riêng rẽ. JPEG2000 áp dụng biến đổi Wavelet nguyên thuận nghịch 5/3 (IWT) và biến đổi thực không thuận nghịch Daubechies 9/7. Việc tính toán biến đổi trong JPEG2000 này sẽ được thực hiện theo phương pháp Lifting.

Sơ đồ của phương pháp Lifting ID áp dụng trong JPEG2000 trên hình 2.4. Việc tính toán biến đổi Wavelet ID 2D suy ra từ biến đổi Wavelet ID theo các phương pháp phân giải ảnh tùy chọn. Trong JPEG2000 có 3 phương pháp giải ảnh nhưng phương pháp được sử dụng nhiều nhất là *phương pháp kim tự tháp*.



Hình 2.4. Phương pháp Lifting 1D dùng tính toán biến đổi Wavelet

Do biến đổi Wavelet 5/3 là biến đổi thuận nghịch nên có thể áp dụng cho nén ảnh theo cả 2 phương pháp, có tổn thất và không tổn thất trong khi biến đổi 9/7 chỉ áp dụng cho nén ảnh theo phương pháp có tổn thất thông tin.

2.4.4. Lượng tử hóa – Giải lượng tử hóa

Các hệ số của phép biến đổi sẽ được tiến hành lượng tử hóa. Quá trình lượng tử hóa cho phép đạt tỉ lệ nén cao hơn bằng cách thể hiện các giá trị biến đổi với độ chính xác tương ứng cần thiết với các mức chi tiết của ảnh cần nén. Các hệ số biến đổi sẽ được lượng tử hóa theo phép lượng tử hóa vô hướng. Các hàm lượng tử hóa khác nhau sẽ được áp dụng cho các băng con khác nhau và được thực hiện theo biểu thức :

$$\left[V(x, y) = \left[\frac{|U(x, y)|}{\Delta} \right] \text{sgn} U(x, y) \right]$$

Với Δ là bước lượng tử, $U(x, y)$ là giá trị băng con đầu vào; $V(x, y)$ là giá trị sau lượng tử hóa. Trong dạng biến đổi nguyên, đặt bước lượng tử bằng 1. Với dạng biến đổi thực thì bước lượng tử sẽ được chọn tương ứng cho từng băng con riêng rẽ. Bước lượng tử của mỗi băng do đó phải có ở trong dòng bit truyền đi để phía thu có thể giải lượng tử cho ảnh.

Công thức giải lượng tử hóa là :

$$U(x, y) = [V(x, y) + r \text{sgn} V(x, y)]$$

Với r là một tham số xác định dấu và làm tròn, các giá trị $U(x, y)$; $V(x, y)$ tương ứng là các giá trị khôi phục và giá trị lượng tử hóa nhận được. JPEG2000 không cho trước r tuy nhiên thường chọn $r = 1/2$.

2.4.5. Mã hóa và kết hợp dòng dữ liệu sau mã hóa

JPEG2000 theo khuyến nghị của ủy ban JPEG quốc tế có thể sử dụng nhiều phương pháp mã hóa khác nhau cũng như nhiều cách biến đổi Wavelet khác nhau để có thể thu được chất lượng ảnh tương ứng với ứng dụng cần xử lý. Điều này giúp cho JPEG2000 mềm dẻo hơn nhiều so với JPEG. Việc áp dụng các phương pháp mã hóa khác nhau cũng được mở rộng sang lĩnh vực nén ảnh động bằng biến đổi Wavelet. Trong thực tế các phương pháp mã hóa ảnh được áp dụng khi nén ảnh bằng biến đổi Wavelet cũng như JPEG2000 thì có phương pháp được coi là cơ sở và được áp dụng nhiều nhất: phương pháp SPIHT và phương pháp EZW. Hiện nay JPEG2000 vẫn được áp dụng mã hóa bằng 2 phương pháp này và một phương pháp phát triển từ 2 phương pháp này là phương pháp mã hóa mặt phẳng bit. Vì thế ở đây chúng ta sẽ xem xét hai phương pháp này. Việc kết hợp dòng dữ liệu sau mã hóa của JPEG2000 thực chất là để thực hiện các tính năng đặc biệt của JPEG2000 như tính năng ROI v.v.

2.4.6. Phương pháp mã hóa SPIHT

Có thể thấy rằng dù áp dụng biến đổi Wavelet nào hay cùng với nó là một phép phân giải ảnh nào thì trong các băng con có số thứ tự thấp cũng là những thành phần tần số cao (mang thông tin chi tiết của ảnh) trong khi những băng con có số thứ tự cao hơn thì sẽ chứa những thành phần tần số thấp (mang thông tin chính về ảnh). Điều đó nghĩa là các hệ số chi tiết sẽ giảm dần từ băng con mức thấp (HH_1 chẳng hạn) (ứng với thành phần tần số cao) xuống băng con mức

cao (ứng với thành phần tần số thấp) và có tính tương tự về không gian giữa các băng con

Ví dụ như một đường biên của hình vẽ trong ảnh sẽ tồn tại ở cùng một vị trí trên các băng con đó (tương ứng với mức độ phân giải của băng con ấy).

Điều này đã dẫn tới sự ra đời của phương pháp SPIHT (Set partitioning in hierarchical trees – phương pháp mã hóa phân cấp theo phân vùng). Phương pháp SPIHT được thiết kế tối ưu cho truyền dẫn lũy tiến. Điều này có nghĩa là tại mọi thời điểm trong quá trình giải nén ảnh theo phương pháp mã hóa này thì chất lượng ảnh hiển thị tại thời điểm ấy là tốt nhất có thể đạt được với một số lượng bit đưa vào giải mã tính cho tới thời điểm ấy. Ngoài ra, phương pháp này sử dụng kỹ thuật embedded coding; điều đó có nghĩa là một ảnh sau nén với kích cỡ (lưu trữ) lớn (tỷ lệ nén thấp) sẽ chứa chính dữ liệu sau nén của ảnh có kích cỡ (lưu trữ) nhỏ (tỷ lệ nén cao). Bộ mã hóa chỉ cần nén một lần nhưng có thể giải nén ra nhiều mức chất lượng khác nhau.

Giả sử gọi các pixel trong một ảnh p cần mã hóa là $p_{i,j}$. Áp dụng một phép biến đổi Wavelet T nào đó cho các pixel trong ảnh để tạo ra các hệ số của phép biến đổi Wavelet là $c_{i,j}$. Các hệ số này tạo ra một ảnh biến đổi là C . Phép biến đổi này được viết dưới dạng toán tử như sau: $C=T(p)$. Trong phương pháp truyền dẫn lũy tiến với ảnh thì bộ mã hóa sẽ bắt đầu quá trình khôi phục (giải nén) ảnh bằng cách đặt các giá trị của ảnh khôi phục từ các hệ số biến đổi là c . Sử dụng các giá trị giải mã của các hệ số biến đổi để tạo ra một ảnh khôi phục (vẫn chưa áp dụng biến đổi ngược Wavelet) là \hat{c} và sau đó áp dụng biến đổi Wavelet để tạo ra ảnh cuối cùng là p_t

$$\text{với } p_t = T^{-1}(\hat{c}).$$

Nguyên tắc quan trọng của phương pháp truyền dẫn ảnh theo kiểu lũy tiến là phương pháp này luôn truyền đi các giá trị mang thông tin quan trọng hơn của ảnh đi trước. Sở dĩ làm như vậy là do các thông tin đó chính là các thông tin sẽ làm giảm thiểu nhiều nhất độ méo dạng của ảnh. Đây chính là lý do tại sao phương pháp SPIHT luôn truyền đi các hệ số lớn trước và cũng là một nguyên tắc quan trọng của phương pháp này. Một nguyên tắc nữa là các bit có trọng số lớn bao giờ cũng mang thông tin quan trọng nhất trong dữ liệu nhị phân. Phương pháp SPIHT sử dụng cả 2 nguyên tắc này, nó sắp xếp các hệ số biến đổi và

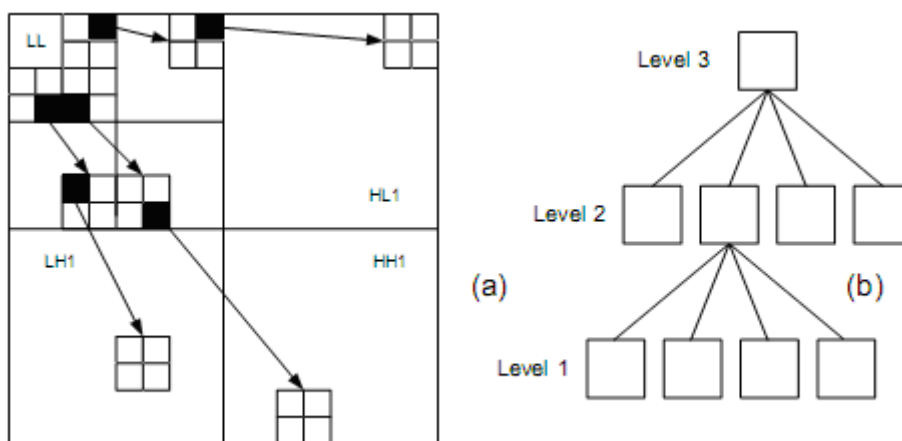
truyền đi các bit có trọng số lớn nhất. Quá trình giải mã có thể dừng lại ở bất kỳ một bước nào ứng với giá trị ảnh cần mã hóa yêu cầu.

Đây chính là cách mà phương pháp mã hóa SPIHT làm tồn thất thông tin.

2.4.7. Phương pháp mã hóa EZW

Phương pháp mã hóa EZW (Embedded Zerotree Wavelet Encoder) cũng dựa trên cơ sở phép mã hóa lũy tiến (progressive coding) giống như phương pháp SPIHT. Phương pháp này chủ yếu dựa trên khái niệm về cây zero. Về cơ bản, thuật toán này dựa trên hai nguyên tắc như đã trình bày ở phần phương pháp mã hóa SPIHT. Sau đây là các khái niệm cơ bản của thuật toán:

Cây tứ phân: Sau khi áp dụng biến đổi Wavelet ứng với các mức phân giải khác nhau chúng ta có thể biểu diễn các hệ số biến đổi dưới dạng một cây. Ta thấy rằng với cây biểu diễn này là do quá trình biến đổi Wavelet ở các tỉ lệ khác nhau. Ta gọi đây là các cây tứ phân (quatree). Sơ đồ cây tứ phân được minh họa ở hình 2.5.



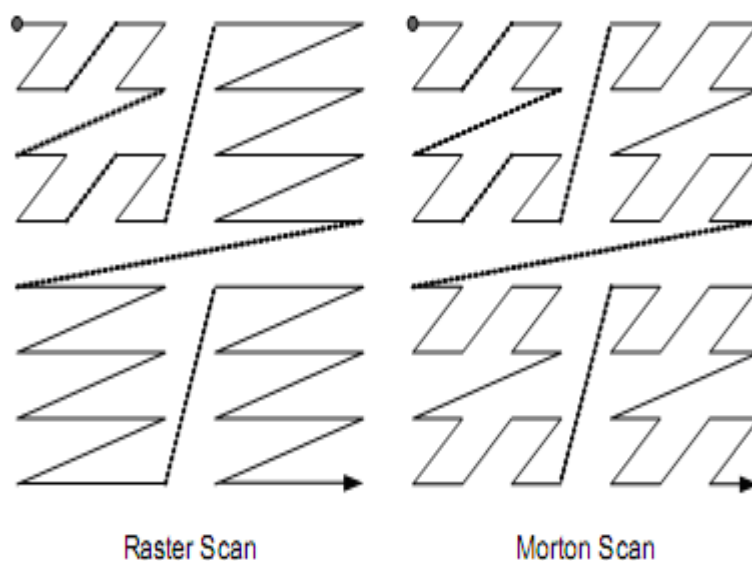
Hình 2.5. Minh họa cây tứ phân (a) và sự phân mức (b)

Cây zero (zero tree): Cây zero là một cây tứ phân, trong đó tất cả các nút của nó đều nhỏ hơn nút gốc. Một cây như vậy khi mã hóa sẽ được mã hóa bằng một đối tượng duy nhất và khi giải mã thì chúng ta cho tất cả các giá trị bằng không. Ngoài ra để có thể mã hóa được các hệ số Wavelet trong trường hợp này, giá trị của nút gốc phải nhỏ hơn giá trị ngưỡng đang được xem xét ứng với hệ số Wavelet đó.

Nguyên lý hoạt động của thuật toán: Thuật toán sẽ mã hóa các hệ số theo thứ tự giảm dần. Chúng ta sẽ dùng một giá trị gọi là ngưỡng và sử dụng ngưỡng này để tiến hành mã hóa các hệ số biến đổi. Các hệ số được mã hóa theo thứ tự

từ vùng tần số thấp đến vùng tần số cao. Và chỉ những hệ số có giá trị tuyệt đối lớn hơn hoặc bằng ngưỡng thì mới được mã hóa. Tiếp theo giảm ngưỡng và tiếp tục làm như vậy cho tới khi ngưỡng đạt tới giá trị nhỏ hơn giá trị của hệ số nhỏ nhất. Cách giảm giá trị ngưỡng ở đây thực hiện tương đối đặc biệt, giá trị của ngưỡng giảm xuống một nửa so với trước đó. Bộ giải mã phải biết các mức ngưỡng này thì mới có thể giải mã ảnh thành công. Nhưng khi ta đi từ nút cha đến nút con trong cây tứ phân thì nó vẫn có 3 nút con. Vậy ta phải đi theo nhánh có nút con nào trước. Nói một cách đầy đủ hơn ta di chuyển từ hệ số này đến hệ số khác theo thứ tự như thế nào. Có nhiều cách di chuyển khác nhau, tuy nhiên hai cách di chuyển trên hình 2.6 được sử dụng nhiều nhất.

Việc sắp xếp này còn phải được quy ước thống nhất giữa quá trình mã hóa và quá trình giải mã để việc giải mã ảnh được thành công.

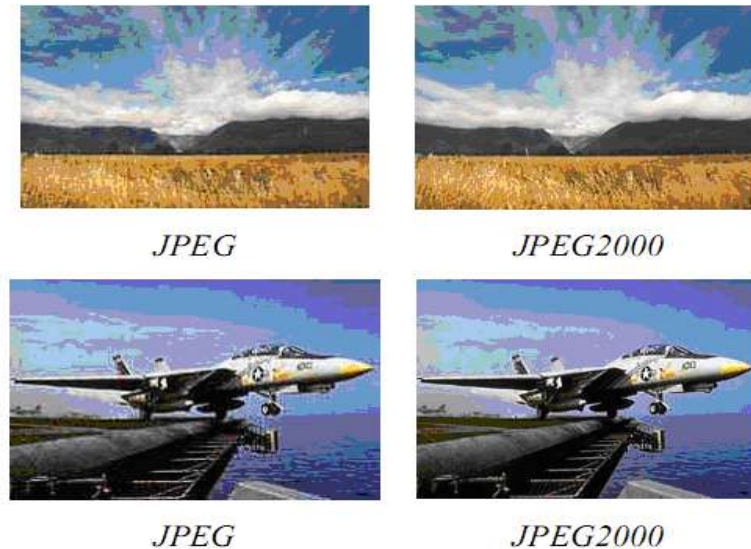


Hình 2.6. Hai cách sắp xếp thứ tự các hệ số biến đổi.

2.4.8. So sánh chuẩn JPEG2000 với JPEG và các chuẩn nén ảnh tĩnh khác

Một tính năng quan trọng và là ưu điểm rõ nét nhất của JPEG2000 so với JPEG cũng như các chuẩn nén ảnh khác như MPEG 4 VTC hay JPEG – LS v.v... là JPEG2000 đưa ra cả 2 kỹ thuật nén có tổn thất và không tổn thất theo cùng một cơ chế mã hóa nghĩa là JPEG2000 thực hiện tất cả các dạng thức của JPEG chỉ bằng một cơ chế mã hóa duy nhất. Nếu xét về sự tồn tại của 2 kỹ thuật này thì JPEG cũng có khả năng nén ảnh có tổn thất và không tổn thất thông tin. Tuy nhiên với JPEG thì cơ chế mã hóa với hai dạng này là khác nhau và rất khó để sử dụng cả hai dạng này cùng lúc cho cùng một ứng dụng. Do đó, có thể thấy

rằng JPEG có tính mềm dẻo hơn bất kì chuẩn nén ảnh tĩnh nào trước đây. Hơn thế, những thống kê về thực tế cho thấy với cùng một tỉ lệ nén và một loại ảnh thì ảnh được nén bởi JPEG2000 luôn có chất lượng tốt hơn so với JPEG. Chúng ta xem xét hai ảnh trên hình 2.7 để thấy rõ điều này, ảnh bên trái được nén theo JPEG còn ảnh bên phải được nén theo JPEG2000.



Hình 2.7. So sánh JPEG và JPEG2000

Tính năng ưu việt thứ 2 của JPEG2000 so với JPEG chính là trong dạng thức nén có tổn thất thông tin, JPEG2000 có thể đưa ra tỉ lệ nén cao hơn nhiều so với JPEG. Các phần mềm nén ảnh JPEG hiện nay (kể cả Photoshop) cũng chỉ thiết kế để có thể nén được tới tỉ lệ 41:1 nhưng với JPEG2000 thì tỉ lệ nén có thể lên tới 200:1. Theo công thức tính PSNR trong đơn vị dB, chúng ta có: (b là số bit dùng biểu diễn 1 pixel trong ảnh gốc)

$$PSNR(dB) = -20 \log \left(\frac{RMSE}{2^b - 1} \right)$$

Với 2 ảnh ở hình 2.7, sự so sánh về tham số PSNR cho trên bảng 2.1. Để có thể so sánh dễ dàng hơn, ta xét ảnh được nén với các tỉ lệ khác nhau (đo lường bởi hệ số bit/pixel hay bpp), Tất cả các số liệu trên bảng đều cho thấy JPEG2000 nén ảnh tốt hơn là JPEG: hơn thế hệ số PSNR mà chúng ta xét trong bảng được đo trong hệ đơn vị logarit.

Bit per pixel	0.125	0.50	2.00
Ảnh 1 theo <i>JPEG</i>	24.42	31.17	35.15
Ảnh 1 theo <i>JPEG2000</i>	28.12	32.95	37.35
Ảnh 2 theo <i>JPEG</i>	22.6	28.92	35.99
Ảnh 2 theo <i>JPEG2000</i>	24.85	31.13	38.80

Bảng 2.1. So sánh JPEG và JPEG2000

Tính năng ưu việt thứ 3 của JPEG2000 so với JPEG là chuẩn nén ảnh này có thể hiển thị được các ảnh với độ phân giải và kích thước khác nhau từ cùng một ảnh nén. Với JPEG thì điều này là không thể thực hiện. Sở dĩ có điều này là do JPEG2000 sử dụng kỹ thuật phân giải ảnh và mã hóa đính kèm mà chúng ta đã nói tới ở phần mã hóa ảnh theo JPEG2000. Tính năng này là một lợi thế đặc biệt quan trọng của JPEG2000, trong khi JPEG cũng như các chuẩn nén ảnh tĩnh trước đây phải nén nhiều lần để thu được chất lượng với từng lần nén khác nhau thì với JPEG2000 ta chỉ cần nén một lần còn chất lượng ảnh thì sẽ được quyết định tùy theo người sử dụng trong quá trình giải nén ảnh theo JPEG2000. Một tính năng ưu việt nữa của JPEG2000 là tính năng mã hóa ảnh quan trọng theo vùng (ROI – Region of Interest) mà chúng ta đã đề cập trong phần mã hóa ảnh theo JPEG2000. Chất lượng của toàn bộ ảnh cũng được thấy rõ trên hình 2.8:



Hình 2.8. Minh họa tính năng ROI

Như chúng ta thấy trên hình 2.8, chất lượng của vùng ảnh được lựa chọn tăng cao hơn khi vùng đó được áp dụng phương pháp nén ảnh ROI.

JPEG2000 còn có một khả năng đặc biệt ưu việt hơn JPEG, đó chính là khả năng vượt trội trong khôi phục lỗi. Đó là khi một ảnh được truyền trên mạng viễn thông thì thông tin có thể bị nhiễu, với các chuẩn nén ảnh như JPEG thì nhiễu này sẽ được thu vào và hiển thị, tuy nhiên với JPEG2000, do đặc trưng của phép mã hóa có thể chống lỗi, JPEG2000 có thể giảm thiểu các lỗi này với mức hầu như không có.

	<i>JPEG2000</i>	<i>JPEG - LS</i>	<i>JPEG</i>	<i>MPEG -4 VTC</i>	<i>PNG</i>
Khả năng nén ảnh không tổn thất	+++	++++	+	-	+++
Khả năng nén ảnh có tổn thất	+++++	+	+++	++++	-
Khả năng lũy tiến trong khôi phục ảnh	+++++	-	++	+++	+
Kỹ thuật mã hoá theo vùng <i>ROI</i>	+++	-	-	+	-
Khả năng tương tác với các vật thể có hình dạng bất kỳ	-	-	-	++	-
Khả năng truy nhập ngẫu nhiên dòng bit của ảnh nén	++	-	-	-	-
Tính đơn giản	++	+++++	+++++	+	+++
Khả năng khôi phục lỗi	+++	++	++	+++	+
Khả năng thay đổi tỷ lệ nén	+++	-	-	+	-
Tính mềm dẻo (khả năng nén nhiều loại ảnh khác nhau)	+++	+++	++	++	+++

Bảng 2.2. So sánh tính năng của JPEG2000 với các chuẩn nén ảnh tĩnh khác.

CHƯƠNG 3. PHƯƠNG PHÁP GIẤU THỦY VÂN DỰA VÀO CẶP TẦN SỐ GIỮA DWT

3.1. Giới thiệu

Khác so với các phương pháp thủy vân cũ, ở phương pháp này, thủy vân sẽ được nhúng vào các hệ số tần số giữa bằng cách lượng tử hóa cặp hệ số tần số giữa, chính là các dải LH và HL trong các hệ số DWT.

Một kỹ thuật thủy vân tốt cần đạt những yêu cầu sau:

- An toàn (security): thủy vân đã nhúng vào chỉ có thể được truy nhập vào bởi các tổ chức có quyền. Mặc dù thuật toán thủy vân đều được công bố rộng rãi cho mọi người, nhưng những người này nếu không có khóa bí mật sẽ không thể truy nhập vào thủy vân trong ảnh đã được bảo vệ.
- Tính vô hình (Impertibility): người xem khó có thể nhìn thấy được thủy vân trong ảnh. Điều đó có nghĩa là sau quá trình nhúng thủy vân, chất lượng của ảnh không bị suy giảm.

Trong những năm gần đây, có rất nhiều nghiên cứu về kỹ thuật thủy vân. Trong đó, kỹ thuật thủy vân mờ rất được mọi người chú ý. Nó có điểm thuận lợi thấy rõ là không cần ảnh gốc vẫn có thể lấy được thủy vân.

Nhìn chung các kỹ thuật thủy vân có thể chia làm 2 nhóm:

- Kỹ thuật vùng không gian: nhúng tin vào các bit ít quan trọng nhất – các bit thấp (LSB).
- Kỹ thuật thay đổi vùng: phương pháp này tốt hơn so với kỹ thuật vùng không gian. Hai phương pháp biến đổi: biến đổi cosin rời rạc (DCT) và biến đổi sóng rời rạc (DWT) là 2 phương pháp biến đổi quan trọng. Trong đó, phương pháp biến đổi DWT có ưu điểm hơn hẳn. Vì DCT được tính toán một cách độc lập trên các khối pixel nên một lỗi mã hóa sẽ gây ra sự không liên tục giữa các khối thu được. Đó là lí do tại sao JPEG2000 tránh dùng DCT thay vào đó nó chọn DWT. DWT sẽ thao tác trên toàn bộ ảnh. Nó có thể tách ảnh thành các dải tần số khác nhau mà vẫn giữ được các thông tin về không gian. Việc cân bằng giữa tính bền vững và tính vô hình có thể được thực hiện một cách hoàn chỉnh.

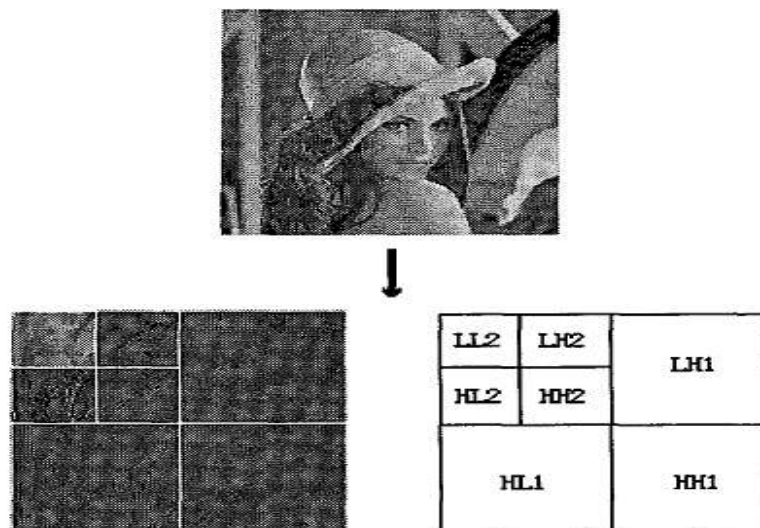
Các kỹ thuật trước đây chỉ bền vững trước các tấn công như blurring, sharpening và nén ảnh JPEG. Phương pháp giấu thủy vân dựa vào cặp tần số

giữa DWT sẽ cho thấy khả năng ấn tượng của nó trong việc không chỉ chống lại các tần công thông thường mà còn chống lại các loại biến đổi cấp xám. Các loại biến đổi cấp xám khác với các tần công khác ở chỗ chúng thường không gây ra sự suy giảm về mặt chất lượng ảnh. Đôi khi cân bằng histogram được sử dụng như một quá trình nâng cao chất lượng ảnh. Nhưng chúng thường gây ra những thay đổi trầm trọng về ảnh do đó chúng sẽ làm hỏng thủy vân được nhúng vào trong ảnh. Trong báo cáo này sẽ đề cập đến mối tương quan giữa các hệ số DWT với các tần công dạng này.

3.2. Thủy vân trong miền DWT

Việc tách wavelet có thể được thực hiện một cách dễ dàng bởi thuật toán kim tự tháp. Bằng cách kết hợp 2 bộ lọc low-pass và high-pass, ảnh sẽ được phân tích thành các dải: thấp-thấp (low-low LL), thấp-cao (low-high LH), cao-thấp (high- low HL) và cao-cao (high-high HH). Để thu được các hệ số wavelet nhỏ hơn thì dải LL sẽ được phân tách nhỏ hơn và thu được các mẫu con. Quá trình xử lý này được thực hiện lại vài lần tùy theo yêu cầu của người dùng. Hơn nữa, từ các hệ số DWT này, ta có thể xây dựng lại ảnh gốc. Quá trình xây dựng này được gọi là đảo ngược DWT (IDWT).

Nhìn chung, thủy vân được nhúng vào dải LL bền vững trước các tần công nhưng sẽ gây ra sự suy giảm về chất lượng ảnh. Ngược lại, sự thay đổi các hệ số wavelet cụ thể (dải HH), tin giấu dễ bị nhìn thấy và dễ bị tấn công thay đổi. Thông thường thủy vân số được nhúng vào dải tần số giữa HL hoặc LH bởi chúng cân đối giữa hai điều trên, nghĩa là vẫn đảm bảo tính bền vững và vô hình trước mắt người.



Hình 3.1. Hai lần phân tách wavelet

3.2.1. Sự tương quan giữa các hệ số của các dải giữa dưới sự biến đổi cấp xám

Các dải LH và HL được gọi là các dải ở giữa (middle bands) bởi vì chúng chứa thông tin chi tiết về một chiều và các thông tin suy ra được của các chiều khác. Bằng thực nghiệm người ta đã chứng minh mối quan hệ giữa các hệ số của dải giữa với sự biến đổi cấp xám dựa vào cơ sở trực giao harr.

Hai ảnh cấp xám baboon (256 x 256) và lena (512 x 512) trong hình 3.2 thể hiện sự khác nhau sau khi cân bằng mức xám. PSNR (peak to signal to noise ratio) thể hiện tỉ số tín hiệu nhiễu giữa hai ảnh. PSNR được định nghĩa:

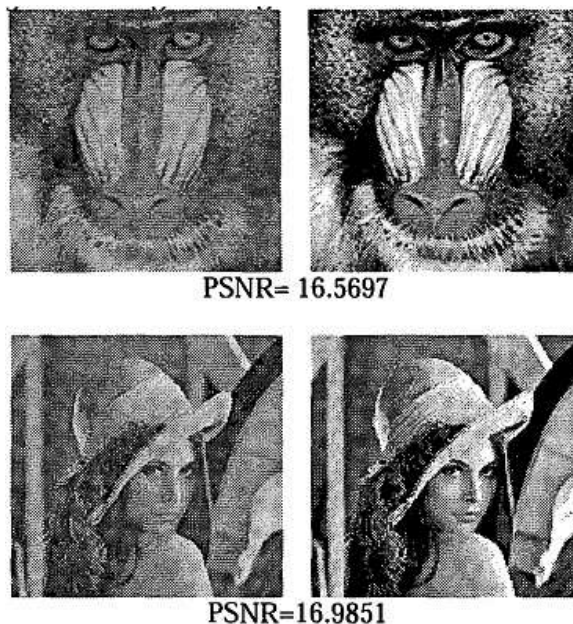
Với MSE (mean square error) là sai số bình phương trung bình giữa ảnh gốc (I) và ảnh đã biến đổi (K):

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

Thì PSNR được tính như sau:

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

MAX là giá trị lớn nhất có thể của pixel trong ảnh. Nếu ảnh đa cấp xám thì MAX=255.



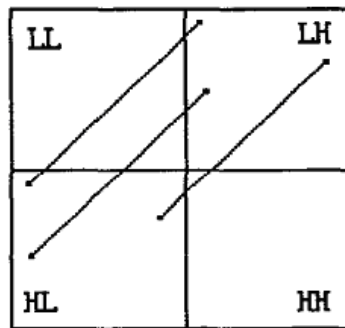
Hình 3.2. Cân bằng mức xám

Ảnh đã được phân tách 2 lần và chọn các dải LH2 và HL2 để kiểm tra độ tương quan giữa các hệ số trước và sau khi biến đổi. Sự tương quan correlation được định nghĩa như sau:

$$Correlation(x, y) = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2} \sqrt{\sum (y - \bar{y})^2}}$$

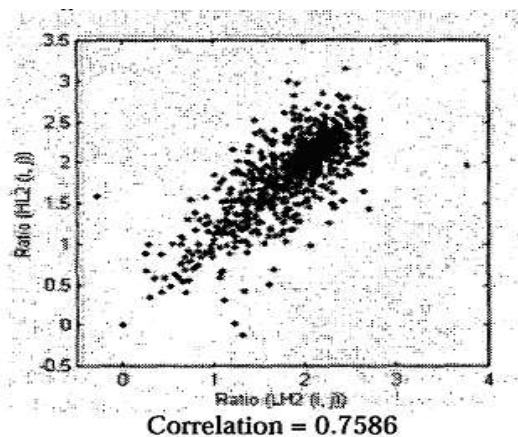
Thông thường trong các dải HL và LH, một vài hệ số có giá trị lớn sẽ được tăng cường về giá trị. Chúng được gọi là các hệ số quan trọng (significant coefficients). Các hệ số này phù hợp để nhúng thủy vân bởi chúng bền vững trước các tấn công thông thường vào ảnh. Và ở đây họ sử dụng nó để làm cơ sở đo mối tương quan. Một cặp hai dải tần số giữa chính là một cặp hệ số nằm trên cùng một vị trí trong dải HL và LH được thể hiện trong hình 3.3. Họ dùng tỉ lệ giữa các giá trị trước và sau tấn công để chứng tỏ sự thay đổi của hệ số. Điều đó có nghĩa là, tại vị trí (i,j):

$$Ratio(LH(i, j)) = \frac{ABS(LH(i, j))_{afterattacks}}{ABS(LH(i, j))_{beforeattacks}}$$



Hình 3.3 Cặp dải tần số giữa

Chúng ta có thể tính toán tỉ lệ giữa $Ratio(LH2(i,j))$ và $Ratio(HL2(i,j))$ của $\frac{1}{4}$ trong số các hệ số của ảnh Baboon sau khi cân bằng histogram. Các hệ số này đại diện cho các hệ số quan trọng trong ảnh 3.4.

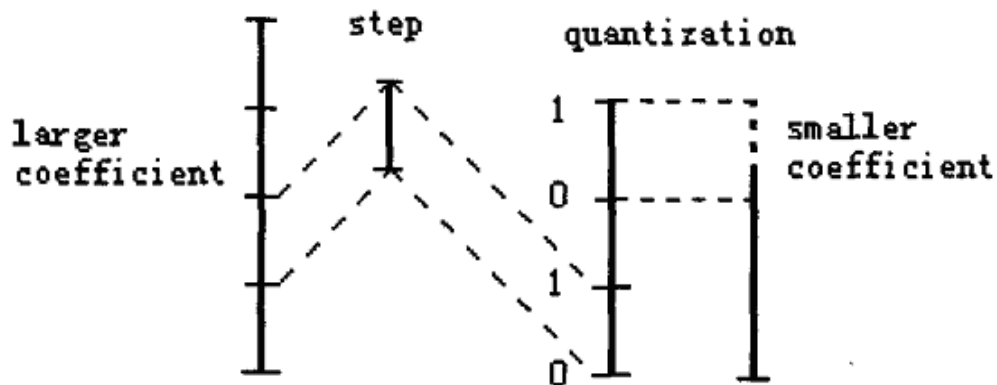


Hình 3.4. Mối quan hệ cặp dải trung gian LH2 và HL2 sau khi cân bằng Histogram

Dưới các tần công khác, sự thay đổi của cặp tần số giữa cũng thể hiện mối tương quan nhiều hơn hoặc ít hơn. Ví dụ như khi thực hiện làm mờ ảnh, giá trị trung bình $\text{Ratio}(\text{LH2}(i,j))$ bằng 0,8368 và giá trị trung bình $\text{Ratio}(\text{HL2}(i,j))$ bằng 0,8461. Dưới tần công làm nét ảnh (sharpen attack), giá trị trung bình $\text{Ratio}(\text{LH2}(i,j))$ của nửa lớn nhất của tất cả các hệ số là 1.2621; giá trị trung bình $\text{Ratio}(\text{HL2}(i,j)) = 0,8461$.

3.2.2. Thuật toán nhúng và tách thủy vân (thuật toán 1) [1]

Ý tưởng: sử dụng một hệ số trong cặp tần số giữa để lượng tử hóa hệ số còn lại. Bước lượng tử hóa là phần cố định của hệ số lớn hơn. Lựa chọn hệ số nhỏ hơn để thực hiện lượng tử hóa (hình 3.5). 1/3 các giá trị lớn nhất của tất cả các hệ số được lựa chọn là các hệ số quan trọng để thực hiện việc lượng tử hóa này. Đối với các hệ số nhỏ sử dụng một bước Step duy nhất để lượng tử hóa.



Hình 3.5. Lượng tử hóa cặp tần số dải trung gian

a. Kỹ thuật nhúng thủy vân

- Bước 1: thủy vân là 1 ảnh nhị phân. Ảnh gốc được tách thành 2 mức. Nhúng thủy vân vào các dải LH2 và HL2. Giả sử kích thước của LH2 là $m \times n$ và của thủy vân là $r \times l$. Thủy vân được nhúng ít nhất là $\lceil m \times n / r \times l \rceil$ lần.
- Bước 2: ngưỡng T của các hệ số nhỏ đặt bằng tầm quan trọng của hệ số lớn nhất trong 1/3 các giá trị lớn nhất của tất cả các hệ số trong dải LH2 và HL2. S (step) là khoảng cách cố định và D là số chia cố định. Thủy vân được nhúng vào dải LH2 và HL2 cho đến khi tất cả các hệ số đều được lượng tử hóa. Mỗi vị trí (i,j) được lượng tử hóa theo 1 bit thủy vân. Nếu bit này =1, hệ số được làm tròn đến con số lẻ gần nhất, nếu không nó được làm tròn đến con số chẵn gần nhất như trong hình 3.5 thể hiện.

For tất cả hệ số có trong dải LH2 và HL2

If $ABS(HL2(i,j)) < T$ and $ABS(LH2(i,j)) < T$

Lượng tử hóa LH2(i,j) và (HL2(i,j)) bằng khoảng cách cố định S;

Else

Maxcoef=Max(ABS(HL2(i,j)), ABS(LH2(i,j)));

If Maxcoef=ABS(LH2(i,j))

Lượng tử hóa HL2(i,j) bằng Maxcoef/D;

Else

Lượng tử hóa LH2(i,j) bằng Maxcoef/D;

End if

End if

End for

- Sau đó thực hiện IDWT 2 chiều để lập thành ảnh thủy vân.

b. Kỹ thuật tách thủy vân

Ảnh được phân tách thành 2 mức. Khi thủy vân được thêm vào ảnh gốc một cách dư thừa, các hệ số của tần số giữa sẽ chia thành các phần., mỗi phần sẽ có số các hệ số bằng với số bit của thủy vân. Gọi B(i,j) là các bit lấy ra được tại các vị trí (i,j)

For tất cả hệ số trong dải LH2 và HL2

If $ABS(HL2(i,j)) < T$ and $ABS(LH2(i,j)) < T$

$B(i,j) = (LH2(i,j)/S \bmod 2 + \text{và } HL2(i,j)/S \bmod 2) / 2;$

Else

Maxcoef=Max(ABS(HL2(i,j)), ABS(LH2(i,j)));

Step = Maxcoef / D;

If Maxcoef=ABS(LH2(i,j))

$B(i,j) = HL2(i,j) / \text{Step} \bmod 2;$

Else

$B(i,j) = LH2(i,j) / \text{Step} \bmod 2;$

End if

End if

End for

Một số vấn đề xảy ra khi thực nghiệm kỹ thuật này:

Ý tưởng của thuật toán trên là sau khi giấu các bit thông điệp làm cho các hệ số lượng tử trở thành lẻ nếu bit cần thủy vân có giá trị 1 và thành

chặn nếu bit cần thuỷ vân có giá trị 0. Khoá dùng để tách thuỷ vân chính là các hệ số lượng tử chặn lẻ. Nếu biết được bí mật này có thể dễ dàng tách thuỷ vân được nhúng trong ảnh.

Khi thực nghiệm kỹ thuật này nhóm tác giả thấy rằng nó chỉ phù hợp với kỹ thuật nhúng thuỷ vân trên miền biến đổi DWT sau đó nó sử dụng biến đổi IDWT2 để lập ảnh thuỷ vân. Không thích hợp với kỹ thuật nhúng thuỷ vân trên miền tần số DWT đã lượng tử hoá của quá trình nén ảnh JPEG2000, vì khi tách thuỷ vân trong quá trình giải nén ảnh JPEG2000, thuỷ vân được tách không đúng với thuỷ vân ban đầu đem nhúng trong ảnh. Điều này được giải thích như sau: do các hệ số DWT lượng tử trong quá trình giải nén ảnh bị thay đổi, các hệ số DWT được khôi phục là các hệ số thực, khi làm tròn các hệ số DWT thành số nguyên sẽ cho một số hệ số DWT có giá trị trùng với giá trị của quá trình nén ảnh một số không trùng với hệ số DWT ban đầu, vì vậy chỉ với một vài thay đổi nhỏ hệ số chặn thành hệ số lẻ có thể dẫn đến mất mát thông tin của thuỷ vân.

Ví dụ: ta có chuỗi bit sau cần thuỷ vân trong ảnh `Img01.pgm`

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

Ta thực hiện nén ảnh JPEG2000 cho ảnh `Img01.pgm` được miền DWT đã bị lượng tử trước khi giấu tin:

-4.548036 -4.017501 -4.724448 -5.2533717 -1.3734832 -0.09918876 -5.709606
 -5.921742 -0.5623639 -0.68907404 -5.535633 -5.9311047 -0.039984897
 -5.8014956 -0.05264521 -1.1272874 -0.36676776 -0.020146813 -1.7391355
 -0.5642951 ...

Giá trị các hệ số DWT sau khi giấu tin

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

Giá trị của các hệ số DWT cần khôi phục thuỷ vân

-6 -6 -6 -6 0 0 -6 -6 0 0 -6 -6 0
 -6 0 0 0 0 0 0 0

Từ hai vấn đề trên nhóm tác giả cải tiến thuật toán trên và nâng cao tính bảo mật của thông điệp được thuỷ vân theo thuật toán dưới đây.

3.2.3. Thuật toán nhúng và tách thuỷ vân cải tiến (thuật toán 2)

Ý tưởng: Thuỷ vân trước khi đem nhúng là một chuỗi nhị phân sẽ được mã hoá bằng một khoá KEY, sau đó được nhúng vào miền tần số giữa HL2 và LH2 của các hệ số DWT đã bị lượng tử hoá dựa vào một ngưỡng Mark (Mark được chọn thuộc miền giá trị của các hệ số DWT trên miền HL2 và LH2 sau khi đã bị lượng tử bởi quá trình nén JPEG2000). Nếu chọn giá trị nhỏ hơn các hệ số DWT đã lượng tử sẽ bị mất trong quá trình nén ảnh JPEG2000, điều đó sẽ dẫn đến mất thuỷ vân nhúng trong ảnh.

a. Kỹ thuật nhúng thuỷ vân:

- Bước 1: Cắn thuỷ vân 1 văn bản vào trong miền biến đổi DWT của ảnh JPEG2000, văn bản được chuyển thành dãy nhị phân. Sau đó thuỷ vân thực hiện mã hoá với một khoá KEY (là một chuỗi nhị phân có độ dài bằng kích thước của chuỗi nhị phân thuỷ vân) bằng phép toán XOR ta được một chuỗi nhị phân mới B.

Ảnh gốc được tách thành 2 mức. Nhúng thuỷ vân vào các dải LH2 và HL2. Giả sử kích thước của LH2 là $m \times n$ và của thuỷ vân là l .

- Bước 2: Chọn Mark thuộc miền giá trị của các hệ số DWT trên miền HL2 và LH2 sau khi đã bị lượng tử. Đặt mark vào phần tử đầu tiên (hoặc vị trí cuối cùng) trong mảng hệ số DWT. Thuỷ vân được nhúng vào dải LH2 và HL2 cho đến khi nhúng hết các bit thuỷ vân. Các bit thuỷ vân được nhúng vào hệ số DWT như sau: nếu bit thuỷ vân =1, hệ số được đặt bằng mark, nếu không nó được giữ nguyên.
- Thực hiện tiếp quá trình nén ảnh JPEG2000 ta được ảnh j2k đã chứa thông điệp

b. Kỹ thuật tách thuỷ vân:

Giải nén ảnh j2k ta nhận các hệ số lượng tử DWT đã bị lượng tử, sử dụng các hệ số miền tần số giữa HL2 và LH2 để tách thuỷ vân. Lấy giá trị mark tại phần tử đầu tiên (hoặc vị trí nào đó theo quá trình gấu quy định) trong mảng hệ số DWT của miền tần số giữa HL2 và LH2.

Gọi $B(i,j)$ là các bit lấy ra được tại các vị trí (i,j) . Nếu hệ số bằng mark thì $B(i,j) = 1$. Nếu hệ số không bằng mark thì $B(i,j) = 0$. Sau đó chuỗi B được thực hiện phép toán XOR với key để khôi phục lại chuỗi nhị phân ban đầu \Rightarrow chuyển ngược lại văn bản đã nhúng.

Ví dụ: ta có chuỗi bit sau cần thuỷ vân trong ảnh `Img01.pgm`

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

Ta thực hiện nén ảnh JPEG2000 cho ảnh `Img01.pgm` được miền DWT đã bị lượng tử trước khi giấu tin:

1.4519639 1.9824992 1.2755519 0.7466281 -1.3734832 -0.09918876
 0.29039386 0.07825812 -0.5623639 -0.68907404 0.4643671 0.06889546 -
 0.039984897 0.19850446 -0.05264521 -1.1272874 -0.36676776 -0.020146813 -
 1.7391355 -0.5642951...

Giá trị của mark= 3.0

GIA TRI CAC HE SO DWT SAU KHI GIAU TIN

Gia tri cua mark 3.0

GIA TRI CAC HE SO DWT SAU KHI GIAU TIN

1.4519639 **3.0** 1.2755519 **3.0** -1.3734832 -0.09918876 0.29039386 **3.0** -
 0.5623639 -0.68907404 0.4643671 **3.0 3.0 3.0** -0.05264521 **3.0** -0.36676776 -
 0.020146813 -1.7391355 **3.0**...

Khôi phục thông điệp đã thuỷ vân trong ảnh

Giá trị của Mark=3.0043945 (đã bị thay đổi trong quá trình giải nén). Các hệ số DWT có giá trị bằng 3.0 đều bị thay đổi 3.0043945.

Giá trị của các hệ số DWT cần khôi phục thuỷ vân

0.0 **3.0043945** 0.0 **3.0043945** 0.0 0.0 0.0 **3.0043945** 0.0 0.0 0.0 **3.0043945**
3.0043945 3.0043945 0.0 **3.0043945** 0.0 0.0 0.0 **3.0043945**...

Các bit được khôi phục:

0 1 0 1 0 0 0 1 0 0 0 1 1 1 0 1 0 0 0 1 ...

CHƯƠNG 4. VẤN ĐỀ PHÁT HIỆN ẢNH CÓ GIẤU TIN TRÊN MIỀN TẦN SỐ GIỮA DWT

4.1. Tổng quan về kỹ thuật phát hiện tin ẩn giấu trong ảnh (Steganalysis)

Steganalysis là kỹ thuật phát hiện sự tồn tại của thông tin ẩn giấu trong multimedia. Giống như thám mã, mục đích của Steganalysis là phát hiện ra thông tin ẩn và phá vỡ tính bí mật của vật mang tin ẩn.

Phân tích tin ẩn giấu thường dựa vào các yếu tố sau:

- Phân tích dựa vào các đối tượng đã mang tin.
- Phân tích bằng so sánh đặc trưng: So sánh vật mang tin chưa được giấu tin với vật mang tin đã được giấu tin, đưa ra sự khác biệt giữa chúng.
- Phân tích dựa vào thông điệp cần giấu để dò tìm.
- Phân tích dựa vào các thuật toán giấu tin và các đối tượng giấu đã biết: Kiểu phân tích này phải quyết định các đặc trưng của đối tượng giấu tin, chỉ ra công cụ giấu tin (thuật toán) đã sử dụng.
- Phân tích dựa vào thuật toán giấu tin, đối tượng gốc và đối tượng sau khi giấu tin.

Các phương pháp phân tích có thể phân thành 3 nhóm:

- Phân tích trực quan: Thường dựa vào quan sát hoặc dùng biểu đồ histogram giữa ảnh gốc và ảnh chưa giấu tin để phát hiện ra sự khác biệt giữa hai ảnh căn cứ đưa ra vấn đề nghi vấn. Với phương pháp phân tích này thường khó phát hiện với ảnh có độ nhiễu cao và kích cỡ lớn.

- Phân tích theo dạng ảnh: Phương pháp này thường dựa vào các dạng ảnh bitmap hay là ảnh nén để đoán nhận kỹ thuật giấu hay sử dụng như các ảnh bitmap thường hay sử dụng giấu trên miền LSB, ảnh nén thường sử dụng kỹ thuật giấu trên các hệ số biến đổi như DCT, DWT, DFT. Phương pháp này rất rộng.

- Phân tích theo thống kê: Đây là phương pháp sử dụng các lý thuyết thống kê và thống kê toán sau khi đã xác định được nghi vấn đặc trưng. Phương pháp này thường đưa ra độ tin cậy cao hơn và đặc biệt là cho các ảnh dữ liệu lớn.

Trong phần tiếp theo sẽ trình bày một số vấn đề về phát hiện ảnh có giấu tin trên miền biến đổi DWT đã đưa ra trong chương 3.

4.2. Với kỹ thuật giấu 1

Kỹ thuật này giấu chỉ cần biến đổi miền dữ liệu ảnh với hệ số DWT làm tròn thành chẵn và lẻ. Do chưa cài đặt được kỹ thuật này trên ảnh JPEG2000 lên chưa thể đưa ra được vấn đề và phương pháp phát hiện cụ thể.

4.3. Với kỹ thuật giấu 2

Kỹ thuật này giấu thông điệp trên miền DWT tần số cao HL và LH trong quá trình nén ảnh JPEG2000. Có thể áp dụng cho kỹ thuật đánh dấu bản quyền, nhận thực thông tin. Vấn đề phát hiện thông điệp giấu trong kỹ thuật này tương đối khó khăn vì:

- Thứ nhất các hệ số DWT là các hệ số thực lên không thể dùng thống kê khi-bình phương (POV) để phát hiện.

- Thứ hai ảnh này có PSNR trung bình là 40.53528 dB (theo thực nghiệm) lên có tính vô hình rất cao.

- Thứ ba người tấn công phải biết hệ số Mark dùng để đánh dấu thông điệp nhúng vào. Giá trị Mark nằm trong miền giá trị thuộc 1/3 các hệ số DWT lớn nhất của tất cả các hệ số DWT, do đó người tấn công sẽ phải thử ...

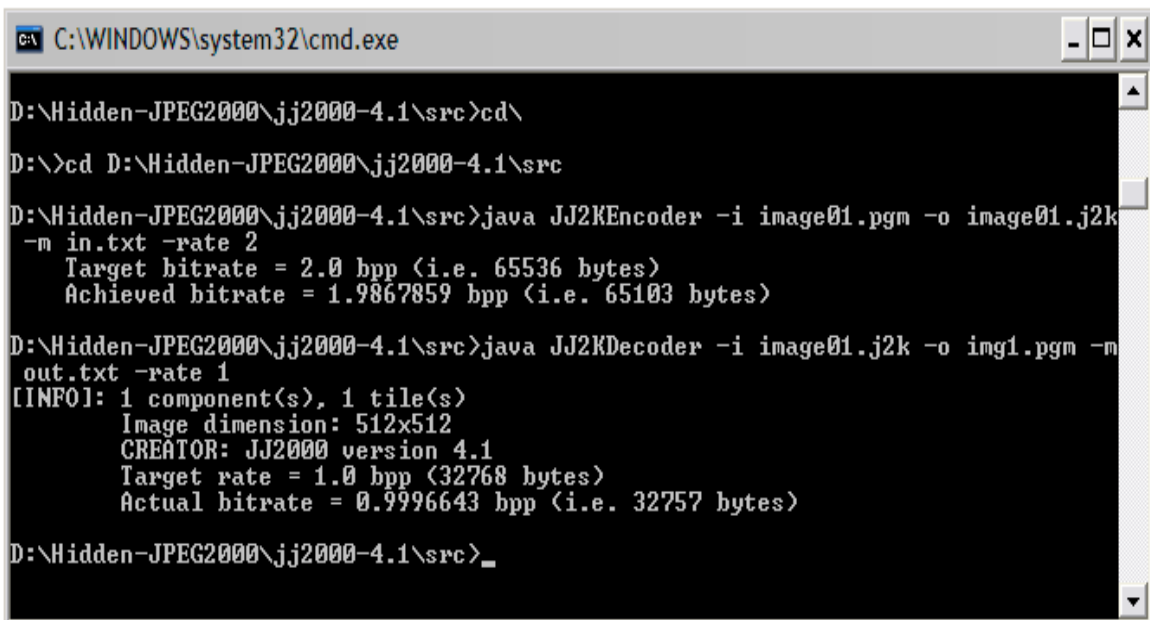
- Thứ tư trong trường hợp người tấn công biết hệ số Mark và tách được thông điệp người tấn công cần phải biết khoá KEY để khôi phục đúng nguyên gốc của thông điệp ban đầu. Nếu thông điệp đem giấu có độ dài n bit thì khoá KEY có độ dài tương tự do đó người tấn công phải thử 2^n lần để tìm đúng khoá KEY mã hoá thông điệp giấu.

Ví dụ: thông điệp đem giấu là một văn bản "Cong hoa xa hoi" văn bản này có 16 ký tự (cả cách trống) chuyển sang nhị phân có độ dài là 128 bit và sẽ cần dùng một khoá KEY là một chuỗi bit nhị phân (được sinh theo kỹ thuật sinh số giả ngẫu nhiên) có kích thước bằng 128. Khi đó người tấn công phải duyệt $2^{128} = 3.4028236692093846346337460743177e+38$ lần để dò tìm khoá KEY.

CHƯƠNG 5. CÀI ĐẶT THỬ NGHIỆM

5.1. Môi trường cài đặt

- Ngôn ngữ cài đặt: Java là một ngôn ngữ lập trình có hiệu quả cao, cấu trúc độc lập nên các ứng dụng của nó chỉ cần viết sao cho chạy được trên máy ảo Java là có thể cài đặt và chạy tốt trên mọi hệ thống.
- Môi trường soạn thảo: Jcreator 4.5.
- Môi trường chạy chương trình: môi trường dòng lệnh của DOS.
- Dưới đây là giao diện chính của chương trình:



```
C:\WINDOWS\system32\cmd.exe
D:\Hidden-JPEG2000\jj2000-4.1\src>cd\
D:\>cd D:\Hidden-JPEG2000\jj2000-4.1\src
D:\Hidden-JPEG2000\jj2000-4.1\src>java JJ2KEncoder -i image01.pgm -o image01.j2k
-m in.txt -rate 2
Target bitrate = 2.0 bpp (i.e. 65536 bytes)
Achieved bitrate = 1.9867859 bpp (i.e. 65103 bytes)
D:\Hidden-JPEG2000\jj2000-4.1\src>java JJ2KDecoder -i image01.j2k -o img1.pgm -m
out.txt -rate 1
[INFO]: 1 component(s), 1 tile(s)
Image dimension: 512x512
CREATOR: JJ2000 version 4.1
Target rate = 1.0 bpp (32768 bytes)
Actual bitrate = 0.9996643 bpp (i.e. 32757 bytes)
D:\Hidden-JPEG2000\jj2000-4.1\src>_
```

Hình 5.1. Giao diện chương trình

Giải thích dòng lệnh giấu thông tin:

java JJ2KEncoder -i image01.pgm -o anhgiautin.j2k -m in.txt -rate 2

- Đối số JJ2KEncoder: là tên file chạy khởi đầu của chương trình thực hiện giấu - encoder.
- Đối số -i: cho biết ảnh đầu vào (input).
- Đối số image01.pgm: tên file ảnh đầu vào.
- Đối số -o: cho biết ảnh đầu ra (output).
- Đối số anhgiautin.j2k: tên file ảnh đầu ra.
- Đối số -m: cho biết thông điệp cần giấu (message).
- Đối số in.txt: tên file chứa thông điệp cần giấu.

- Đối số rate: cho biết là thực hiện giấu hay tách lấy thông điệp. Với 1 là thực hiện giấu.

Giải thích dòng lệnh tách thông tin:

java JJ2KDecoder -i anhgiautin.j2k -o anhkhoiphuc.pgm -m out.txt -rate 1


- Đối số JJ2KDecoder: là tên file chạy khởi đầu của chương trình thực hiện tách lấy thông điệp - decoder.
- Đối số -i: cho biết ảnh đầu vào (input).
- Đối số anhgiautin.j2k: tên file ảnh đầu vào.
- Đối số -o: cho biết ảnh đầu ra (output).
- Đối số anhkhoiphuc.pgm: tên file ảnh đầu ra.
- Đối số -m: cho biết thông điệp tách lấy ra được (message).
- Đối số out.txt: tên file chứa thông điệp cần lấy.
- Đối số rate: cho biết là thực hiện giấu hay tách lấy thông điệp. Với 2 là thực hiện tách.

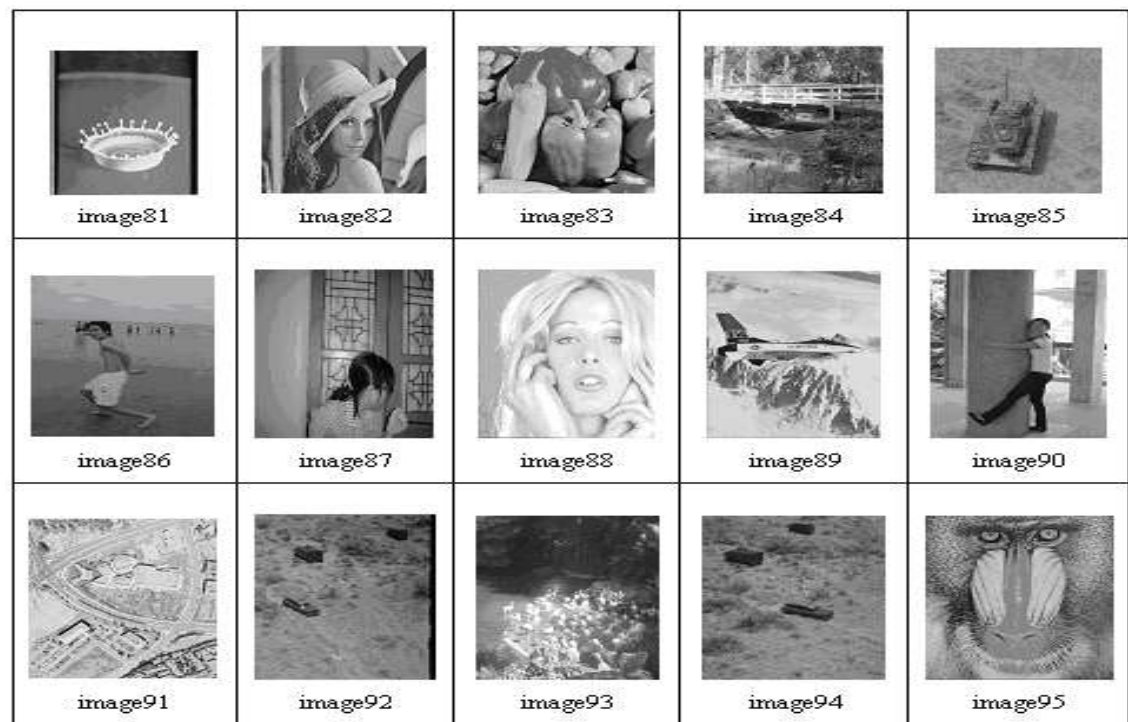
5.2. Thử nghiệm

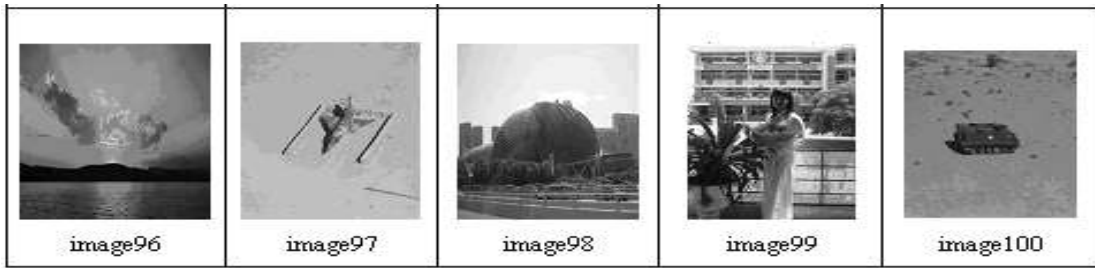
Dưới đây là một tập cơ sở dữ liệu ảnh gồm 100 ảnh đã được chuyển đổi sang định dạng PGM. Các ảnh được đặt tên từ image01 đến image100.



 image06	 image07	 image08	 image09	 image10
 image11	 image12	 image13	 image14	 image15
 image16	 image17	 image18	 image19	 Image20
 image21	 image22	 image23	 im age24	 image25
 image26	 image27	 image28	 image29	 image30

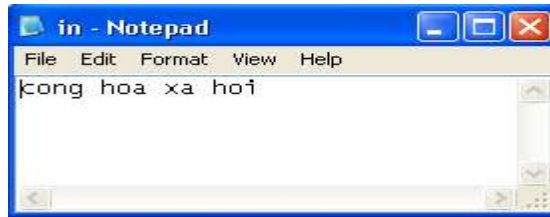
				
image31	image32	image33	image34	image35
				
image36	image37	image38	image39	image40
				
image41	image42	image43	image44	image45
				
image46	image47	image48	image49	image50
				
image51	image52	image53	image54	image55





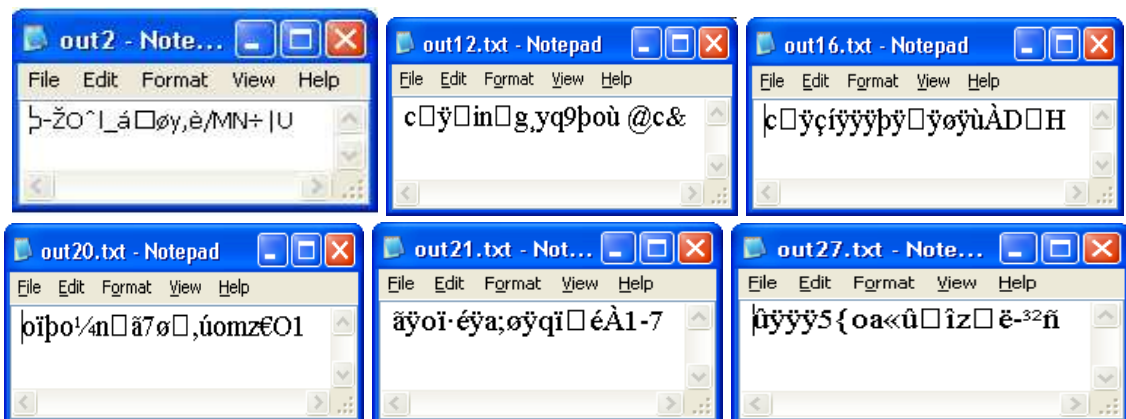
Bảng 5.1. Tập ảnh thử nghiệm

Sử dụng phương pháp thủy văn cải tiến để thực hiện giấu thông điệp (trong hình 5.2) vào tập cơ sở dữ liệu ảnh trên với $mark=3.0$, ta thu được kết quả PSNR trung bình trên 100 ảnh sau khi giấu tin là $PSNR_{TB}=40.53528$ (lớn hơn mức quy định là 40 dB, với $PSNR \geq 40dB$ thì mắt người không thể phân biệt được sự khác biệt giữa 2 ảnh [5])



Hình 5.2 Thông điệp giấu

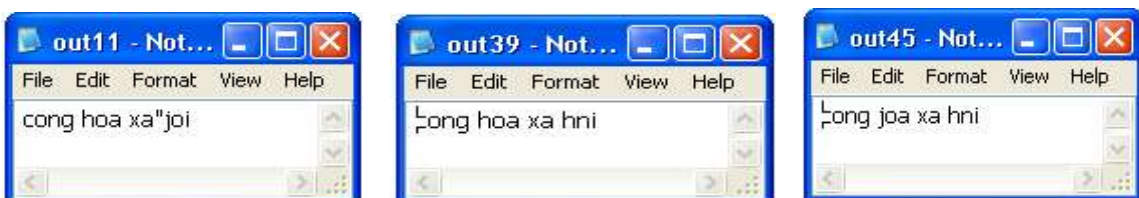
Sau khi giấu thông điệp thực hiện tách thông điệp đã giấu trên 100 ảnh nhóm tác giả thấy rằng có đến 27 ảnh (27%) ảnh bị tách sai thông điệp gồm các ảnh sau: image02, image11, image12, image16, image20, image21, image27, image30, image32, image34, image37, image40, image43, image44, image47, image49, image50, image53, image56, image57, image58, image77, image80, image84, image85, image91, image95. Thông điệp sau khi khôi phục của các ảnh này như sau:





Hình 5.3. Kết quả các thông điệp bị tách sai

Có ba ảnh bị tách sai một số ký tự của bản thông điệp là ảnh: image11 (3 ký tự), image39 (1 ký tự), image45 (2 ký tự). Thông điệp sau khi khôi phục của các ảnh này như hình 5.4



Vì vậy kỹ thuật này rất phù hợp đối với nhận thực bản quyền và chống xuyên tạc, mọi hình thức thanh đổi nào cũng có thể dẫn đến vỡ thuy vân trong ảnh.

KẾT LUẬN

Báo cáo đã trình bày những khái niệm tổng quan về giấu tin, cho thấy được tầm quan trọng của giấu tin trong đời sống hiện nay.

Trong thời gian nghiên cứu 4 tháng, nhóm nghiên cứu đã đạt được các kết quả sau:

- Nắm rõ được khái niệm tổng quan về kỹ thuật giấu tin trong ảnh
- Kỹ thuật nén ảnh JPEG2000
- Kỹ thuật giấu tin trên miền biến đổi rời rạc wavelet cặp tần số giữa
- Đề xuất kỹ thuật giấu cải tiến trên miền tần số Wavelet của miền tần số cao (HL, LH) dựa trên kỹ thuật giấu đã công bố đối trên các hệ số DWT đã được lượng tử hoá cho ảnh JPEG2000.
- Cài đặt, thử nghiệm và đánh giá kết quả.

Vì thời gian nghiên cứu có hạn nên chưa xây dựng được giao diện chương trình thân thiện với người dùng, giao diện chương trình còn thực hiện trên cửa sổ dòng lệnh.

Hướng nghiên cứu tiếp theo sẽ nghiên cứu tiếp một số kỹ thuật giấu tin khác như: QIM, MFP...và hoàn thiện cài đặt đóng gói thành một phần mềm chuyên dụng.

TÀI LIỆU THAM KHẢO

- [1]. Nguyễn Xuân Huy và Trần Quốc Dũng, “*Giáo trình giấu tin và thủy vân ảnh*”, Thông tin tư liệu, ĐHKHTN, 2003
- [2]. Quan Yuan, Hongxun Yao, Wen Gao, Sanghyun Joo, “*Blind watermarking method based on DWT middle frequency pair*”, Multimedia and Expo, 2002. ICME '02. Proceedings, 2002 IEEE International Conference on paper 473- 476 vol.2, 2002.
- [3]. Website: <http://www.JPEG.org/JPEG2000.html>.
- [4]. <http://jpeg2000.epfl.ch>
- [5]. Đỗ Ngọc Anh, NÉN ẢNH SỬ DỤNG BIẾN ĐỔI WAVELET VÀ ỨNG DỤNG TRONG CÁC DỊCH VỤ DỮ LIỆU ĐA PHƯƠNG TIỆN DI ĐỘNG, Luận văn cao học ĐTVT 2004 – 2006, Đại học Bách khoa Hà Nội.