

LỜI CẢM ƠN

Trước hết em xin được bày tỏ lòng kính trọng và biết ơn sâu sắc tới cô giáo, ThS. Hồ Thị Hương Thom – giảng viên khoa công nghệ thông tin trường ĐHDL Hải Phòng, đã tận tình hướng dẫn và tạo mọi điều kiện thuận lợi để em hoàn thành báo cáo đồ án tốt nghiệp của mình.

Em xin chân thành cảm ơn tất cả các thầy cô giáo trong khoa Công nghệ thông tin - Trường ĐHDL Hải Phòng đã nhiệt tình giảng dạy và cung cấp những kiến thức quý báu để em có thể hoàn thành tốt đợt thực tập tốt nghiệp này.

Xin cảm ơn tất cả các bạn đã đồng viên, góp ý và trao đổi hỗ trợ cho em trong suốt thời gian vừa qua.

Cuối cùng em xin bày tỏ lòng biết ơn sâu sắc tới những người thân trong gia đình đã dành cho em sự quan tâm hết mực và động viên em.

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

Em xin chân thành cảm ơn!

Hải Phòng, ngày 1 tháng 7 năm 2009

Sinh viên

Phạm Thị Quỳnh

MỤC LỤC

LỜI MỞ ĐẦU	1
CHƯƠNG I. TỔNG QUAN KỸ THUẬT THỦY VÂN SỐ	2
1. 1. Khái niệm.....	2
1. 2. Phân loại thủy vân số.....	2
1.3. Ứng dụng thủy vân số.....	3
1.3.1. Bảo vệ quyền tác giả	3
1.3.2. Lấy dấu vân tay	4
1.3.3. Chống sao chép	4
CHƯƠNG II. KỸ THUẬT NÉN ẢNH JPEG2000	5
2.1. Khái niệm nén ảnh.	5
2.2. Sự ra đời của JPEG2000	5
2.3. Các tính năng của JPEG2000	5
2.4. Các bước thực hiện nén ảnh theo chuẩn JPEG2000.....	6
2.4.1. Xử lí trước khi biến đổi.....	6
2.4.2. Biến đổi liên thành phần.....	6
2.4.3. Biến đổi riêng thành phần (biến đổi Wavelet)	7
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.....	8
2.4.6. Phương pháp mã hóa SPIHT.....	9
2.4.7. Phương pháp mã hóa EZW	10
2.4.8. So sánh chuẩn JPEG2000 với JPEG và các chuẩn nén ảnh tĩnh khác.....	12
CHƯƠNG III. KỸ THUẬT GIẤU THỦY VÂN.....	16
3.1. Thủy vân số trong DWT	16
3.2. Sự tương quan giữa các hệ số các dải giữa với sự biến đổi cấp xám.	17
3.3. Thuật toán nhúng và tách thủy vân.....	19
3.3.1. Ý tưởng.....	19
3.3.2. Kỹ thuật nhúng thủy vân	19
3.3.3. Kỹ thuật tách thủy vân	20
CHƯƠNG IV. KỸ THUẬT PHÁT HIỆN ẢNH CÓ GIẤU TIN.....	21

4.1. Tổng quan kỹ thuật phát hiện tin ẩn giấu (Steganalysis)	21
4.2. Kỹ thuật phát hiện bằng thống kê χ^2	22
4.3. Kỹ thuật phát hiện giấu tin trên miền WAVELET.....	24
4.3.1. Ý tưởng.....	24
4.3.2. Sự khác biệt về mức năng lượng(energy difference)-Cơ sở sự phát hiện.	24
4.3.3. Phân tích histogram.....	25
4.3.4. Phân tích quang phổ và sự khác biệt về mức năng lượng.....	27
4.3.5. Sự lựa chọn các bộ lọc wavelet.....	27
4.3.6. Ước lượng ngưỡng tối ưu.....	27
CHƯƠNG V. KẾT QUẢ THỰC NGHIỆM	29
5.1. Môi trường cài đặt	29
5.2. Kết quả thử nghiệm	29
5.3. Đánh giá thuật toán.....	31
KẾT LUẬN	32
TÀI LIỆU THAM KHẢO	33

LỜI MỞ ĐẦU

Kỹ thuật giấu tin và phát hiện thông tin hiện này là một lĩnh vực rất mới được tập trung nghiên cứu 10 năm trở lại đây. Ở Việt Nam có rất nhiều các trung tâm nghiên cứu như Viện công nghệ thông tin – Viện khoa học Việt Nam, trường Đại học Công nghệ - Đại Học Quốc Gia, trường Đại học bách khoa thành phố Hồ Chí Minh, tổng cục I, tổng cục V, bộ công an... Các đơn vị này chủ yếu tập trung vào kỹ thuật giấu tin còn vấn đề phát hiện chưa có nhiều kết quả công bố.

Các thành tựu đạt được trong lĩnh vực nghiên cứu này đã bắt đầu được áp dụng hiệu quả cho mục đích bảo vệ bản quyền, chống sao chép, phân tán trái phép các sản phẩm trong môi trường số hoá và nhiều mục đích khác. Nhiều phương pháp giấu thông tin khác nhau đã được đề xuất, mỗi phương pháp có những ưu điểm, nhược điểm riêng và thích hợp cho một nhóm ứng dụng nào đó.

Báo cáo này nghiên cứu phương pháp phát hiện thông tin ẩn giấu trong ảnh JPEG2000 gồm các nội dung sau:

Chương I. Tổng quan kỹ thuật thủy văn số.

Chương II. Kỹ thuật nén ảnh JPEG 2000.

Chương III. Kỹ thuật giấu thủy văn.

Chương IV. Kỹ thuật phát hiện ảnh có giấu tin.

Chương V. Kết quả thử nghiệm.

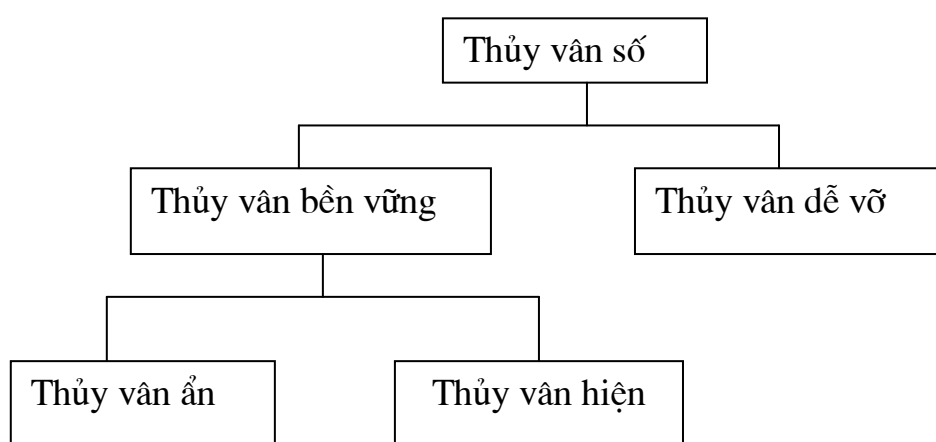
CHƯƠNG I. TỔNG QUAN KỸ THUẬT THỦY VÂN SỐ

1. 1. Khái niệm

- Kỹ thuật thủy vân số (watermarking) là một triển vọng công nghệ có thể giúp chúng ta giải quyết các vấn đề liên quan đến các ứng dụng như bảo hộ quyền tác giả và nội dung xác thực

1. 2. Phân loại thủy vân số

- Mô hình phân loại kỹ thuật thủy vân số:



Hình 1.1. Sơ đồ phân loại kỹ thuật thủy vân số

- 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 lại được phân thành hai loại:

+ Thủy vân ẩn: cũng giống như giấu tin, bằng mắt thường không thể nhìn thấy thủy vân.

+ Thủy vân hiện: 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).

1.3. Ứng dụng thủy vân số

Kỹ thuật thủy vân được sử dụng trong nhiều ứng dụng. Sức chịu đựng được đề cập đến khả năng phát hiện thủy vân sau khi xử lý tín hiệu hoạt động phổ biến như nén mất mát, in ấn, quét và sự méo hình học (luân phiên, nhân rộng, dịch thuật vv...). Không phải tất cả các ứng dụng của thủy vân đòi hỏi sức chịu đựng để tất cả các tín hiệu có thể được xử lý. Tuy nhiên, mức độ chịu đựng của các thủy vân trong các ứng dụng là khác nhau. Ví dụ, việc áp dụng bảo vệ quyền tác giả đòi hỏi một thủy vân để chống lại sự sửa đổi, bổ sung trên word và do đó phải được mạnh mẽ. Mặt khác, việc áp dụng nội dung xác thực đòi hỏi một thủy vân để vô hiệu hóa ngay cả sự thay đổi nhỏ nhất trên word và do đó không được mạnh mẽ. Như vậy thủy vân được gọi là thủy vân dễ vỡ.

1.3.1. Bảo vệ quyền tác giả

Các vấn đề về bảo vệ quyền tác giả đã trở thành ngày càng quan trọng. Ứng dụng này của thủy vân đã đạt được rất nhiều về tầm quan trọng. Mục tiêu là để nhúng thông tin vào các mã nguồn có nghĩa là chủ sở hữu quyền tác giả. Do đó, thủy vân được sử dụng để giải quyết sự công bằng quyền sở hữu, và các ứng dụng này đòi hỏi mức độ chắc chắn rất cao. Ngoài ra các thủy vân phải không mập mờ và vẫn còn giải quyết sự công bằng quyền sở hữu nếu các bên khác nhúng thêm thủy vân vào. Các ứng dụng này ngày càng trở nên cần thiết hơn trên các trang web trên thế giới, nơi đang có hàng triệu hình ảnh hiện tại mà không có bất kỳ tài liệu tham khảo cho sự công bằng của các chủ sở hữu.



Hình 1.2. Ảnh Lena

Ví dụ: Việc kiểm tra hình ảnh phổ biến nhất (một bức ảnh của Lena Sjöoblom, hiển thị ở hình 1.2) trong nghiên cứu về xử lý hình ảnh hiện không tham khảo chủ sở hữu hợp pháp của nó. Lena của bức ảnh đầu tiên xuất hiện trong tạp chí Playboy. Những hình ảnh đã được cắt vào một mức độ như vậy mà chỉ có mặt và vai bên trái, vì nó và thậm chí cả bản quyền thông báo đã được gỡ bỏ. Hầu hết các nhà nghiên cứu đã sử dụng hình ảnh này đã không biết rằng họ đang vi phạm bản quyền của Playboy. Trong bất kỳ trường hợp nào, Playboy đã quyết định giám sát sự sử dụng phổ biến rộng rãi hình ảnh này.

1.3.2. Lấy dấu vân tay

Lấy dấu vân tay liên quan đến việc nhúng của một thủy vân khác vào mỗi bản sao phân tán. Ứng dụng này có một mục tiêu mang thông tin về pháp lý chứ không phải là người nhận các nguồn dữ liệu số, chủ yếu là để xác định phân phối duy nhất các bản sao dữ liệu. Điều này rất hữu ích để giám sát hoặc theo dõi quay lại bất hợp pháp sản xuất các bản sao của dữ liệu, mà có thể lưu thông, và rất giống với sê-ri số lượng sản phẩm phần mềm. Thủy vân trong ứng dụng lấy dấu vân tay cũng đòi hỏi phải có tiêu chuẩn cao về độ chắc chắn chống lại việc xử lý dữ liệu cũng như những tấn công ác hiểm.

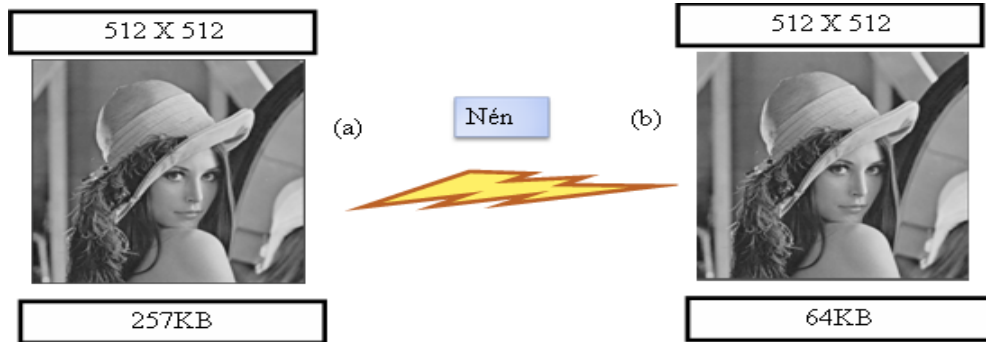
1.3.3. Chống sao chép

Việc áp dụng các bản sao được bảo vệ để ngăn chặn sao chép trái phép các phương tiện truyền thông. Bản sao bảo vệ là rất khó khăn để đạt được trong các hệ thống mở, tuy nhiên, nó là khả thi trong hệ thống đóng. Trong hệ thống như vậy, có thể sử dụng thủy vân để cho biết các dữ liệu có thể được sao chép hay không. Một ví dụ là hệ thống DVD, nơi chứa dữ liệu sao chép thông tin nhúng vào như là một thủy vân. Nếu có một thủy vân “copy never” được nhúng vào trong dữ liệu, tuân thủ một đầu DVD sẽ không cho phép nhân rộng các dữ liệu trong khi nếu có một thủy vân “copy once” trên dữ liệu, bộ đọc DVD sẽ cho phép dữ liệu được sao chép chỉ một lần. Mặc dù chúng ta nhận ra rằng đây là một cách hiệu quả để bảo vệ dữ liệu sao chép bất hợp pháp, nhưng trên thực tế đó là khó khăn để đạt được.

CHƯƠNG II. KỸ THUẬT NÉN ẢNH 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.

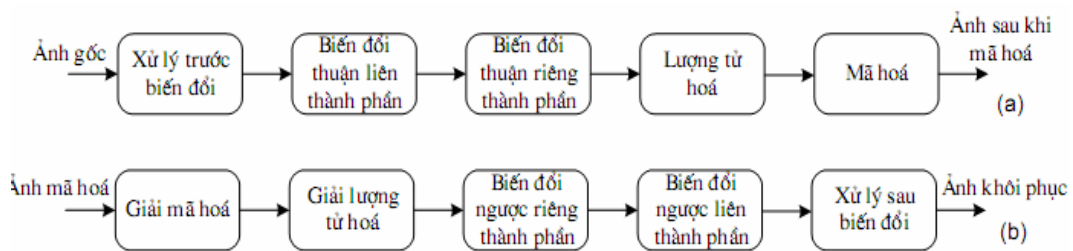
2.3. Các tính năng của JPEG2000

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



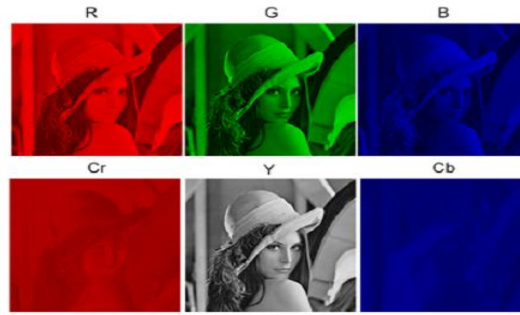
Hình 2.2. Trình tự mã hóa và giải mã JPEG2000

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.

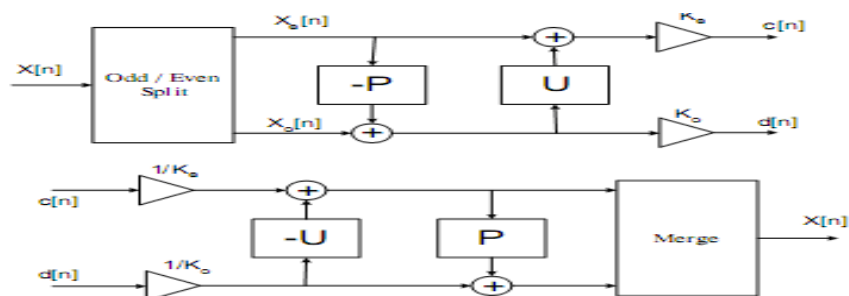


Hình 2.3. Minh họa ảnh với RGB và YcrCb

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 bằng 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 :

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

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

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

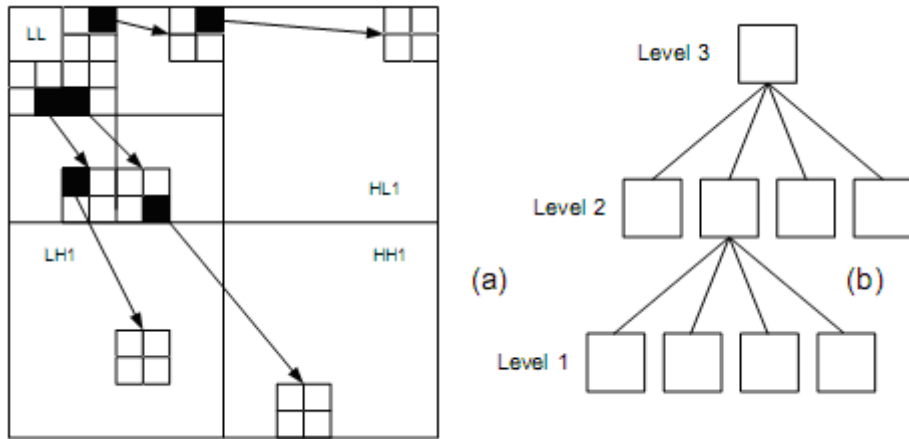
Nguyên tắc quan trọng của phương pháp truyền dẫn ảnh theo kiểu lũy tiến là phương pháp này luôn truyền đi các giá trị mang thông tin quan trọng hơn của ảnh đi trước. Sở dĩ làm như vậy là do các thông tin đó chính là các thông tin sẽ làm giảm thiểu nhiều nhất độ méo dạng của ảnh. Đây chính là lý do tại 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.

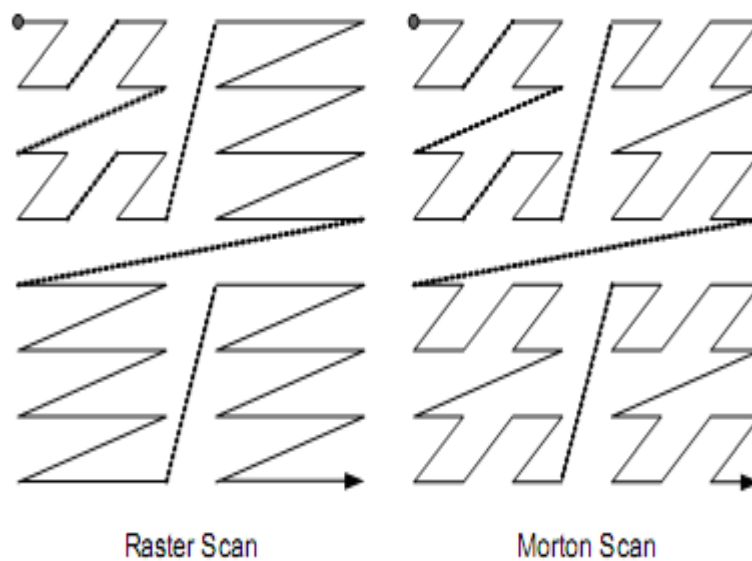


Hình 2.5. Minh họa cây tứ phân (a) và sự phân mức (b)

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.



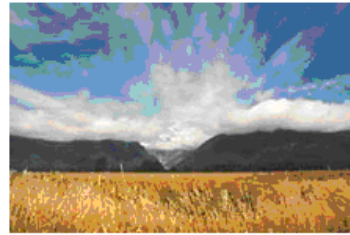
Hình 2.6. Hai cách sắp xếp thứ tự các hệ số biến đổi.

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 kỳ 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.



JPEG



JPEG2000



JPEG



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 9, 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 đỉnh 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.

So sánh tính năng với một số chuẩn nén ảnh như là JPEG – LS, PNG; MPEG 4 VTC qua bảng 2.2 (Dấu + biểu thị chuẩn đó có chức năng tương ứng, số dấu + càng nhiều thì chuẩn đó thực hiện chức năng tương ứng càng tốt) dấu – biểu thị chuẩn tương ứng không hỗ trợ tính năng đó.

	<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 luỹ 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)	+++	+++	++	++	+++

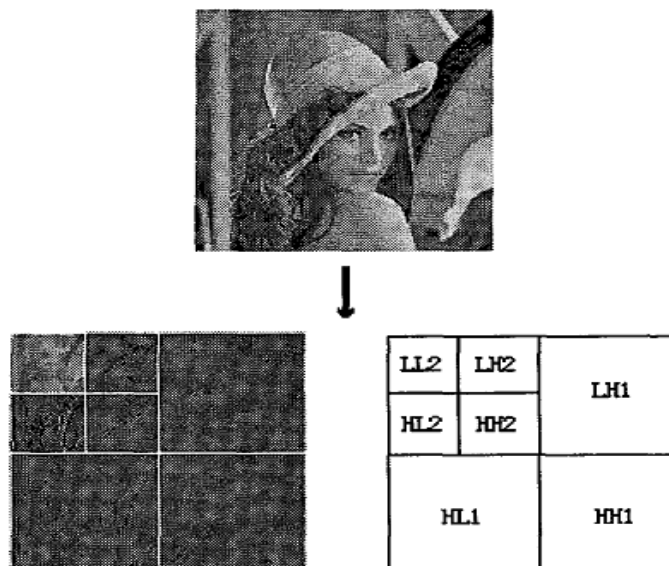
Bảng 2.2. So sánh tính năng của JPEG2000 với các chuẩn nén ảnh tĩnh khác.

CHƯƠNG III. KỸ THUẬT GIẤU 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. Biến đổi cosin rời rạc (DCT) và biến đổi sóng rời rạc (DWT). Đây là 2 phương pháp biến đổi quan trọng. Trong đó, phương pháp biến đổi DWT rõ ràng có ưu điểm hơn hẳn. Nó có thể tách ảnh thành các dải tần số khác nhau mà vẫn giữ được các thông tin về không gian.

3.1. Thủy vân số trong DWT



Hình 3.1. Hai lần phân tách wavelet

Sự phân giải của sóng có thể được sử dụng hiệu quả bởi thuật toán hình chóp. Bằng cách kết hợp 2 bộ lọc low-pass và high-pass, ảnh sẽ được phân tích thành các dải: thấp-thấp (LL), thấp-cao (LH), cao-thấp (HL) và cao-cao (HH). Trong dải LL, chất lượng ảnh vẫn kém đi. Trong dải HH, thì tin giấu dễ bị nhìn thấy và nguy hiểm. Thông thường thủy vân số được nhúng vào dải tần số ở giữa HL hoặc LH. 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, có thể được xây dựng lại được ảnh gốc. Quá trình xây dựng này được gọi là đảo ngược DWT – IDWT.

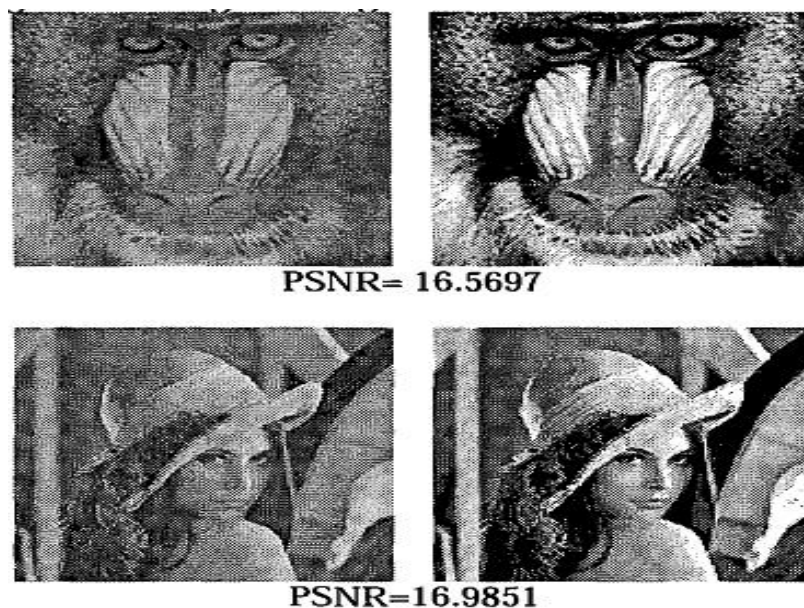
3.2. Sự tương quan giữa các hệ số các dải giữa với sự biến đổi cấp xám.

Các dải LH và HL được gọi là các dải ở giữa 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 (256x256) và lena (512x512) trong hình 3.2 thể hiện sự khác nhau sau khi cân bằng mức xám. PSNR thể hiện sự khác nhau so với các ảnh gốc. PSNR được định nghĩa :

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

Với MSE là số các ô lỗi giữa ảnh gốc và ảnh đã biến đổi.



Hình 3.2. Cân bằng mức xám

Ảnh đã được phân giải 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 được định nghĩa như sau :

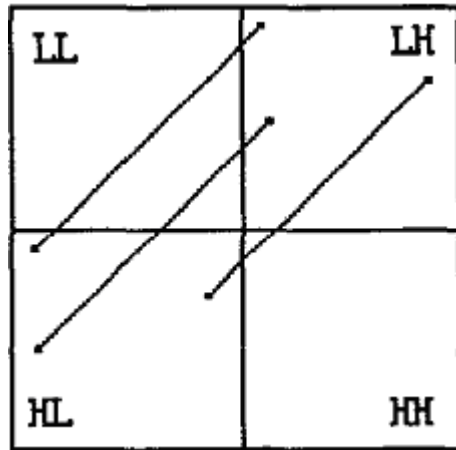
$$Correlation(X,Y) = \frac{\sum (X - \bar{X})(Y - \bar{Y})}{\sqrt{\sum (X - \bar{X})^2} \sqrt{\sum (Y - \bar{Y})^2}}$$

Thông thường trong các dải HL và LH, tin được giấu trong các hệ số ít quan trọng nhất 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 trung gian 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 sử dụng tỉ lệ giữa các giá trị trước và sau tần công để chứng tỏ sự thay đổi của hệ số.

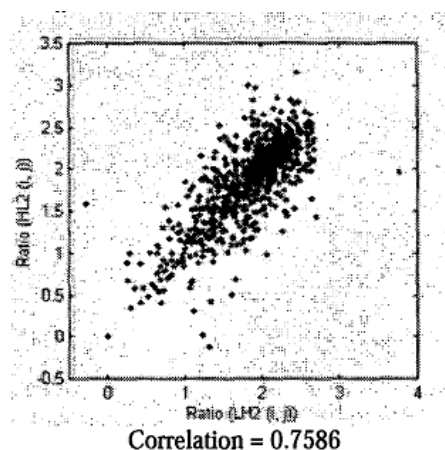
Điều đó có nghĩa là, tại vị trí (i, j):

$$Ratio(LH(i, j)) = \frac{ABS(LH(i, j))_{sau\ tan\ cong}}{ABS(LH(i, j))_{truoc\ tan\ cong}}$$



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 ít quan trọng nhất trong hình 3.4.



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

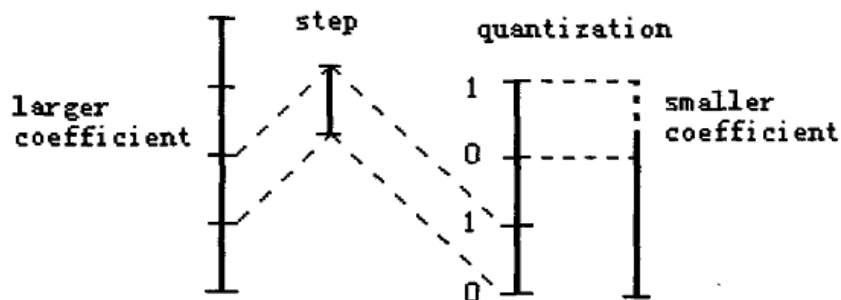
Dưới các tần công khác, sự thay đổi của cặp tần số trung gian cũng thể hiện mối tương quan nhiều hơn hoặc ít hơn. Khi sự tần công bị giảm, tỷ lệ trung

trung bình $\text{Ratio}(\text{LH2}(I,j))$ của một nửa trong số các hệ số lớn nhất là 0.8368, và tỷ lệ trung bình $\text{Ratio}(\text{HL2}(i,j))$ là 0.8461. Khi sự tần công tăng lên, tỷ lệ trung bình $\text{Ratio}(\text{LH2}(I,j))$ của một nửa trong số các hệ số lớn nhất là 1.2621, và tỷ lệ trung bình $\text{Ratio}(\text{HL2}(i,j))$ là 1.2300.

3.3. Thuật toán nhúng và tách thủy vân

3.3.1. Ý tưởng

Sử dụng một hệ số trong cặp tần số trung gian như một mức để lượng tử hóa hệ số còn lại. Bước lượng tử hóa(step) là một phần cố định của hệ số lớn hơn(larger coefficient). Hệ số nhỏ hơn(smaller coefficient) được lượng tử hóa bởi step này.



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

3.3.2. Kỹ thuật nhúng thủy vân

Bước 1: Thủy vân là một 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: Đặt T là ngưỡng cho các hệ số nhỏ, nó là hệ số lớn nhất trong 1/3 các hệ số nhỏ nhất của tất cả các hệ số trong dải tần LH2 và HL2. S 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. 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)) bởi khoảng cách cố định S;
Else
 $Maxcoef = \text{Max}(ABS(HL2(i, j)), ABS(LH2(i, j)))$;
 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

Bước 3: Sau đó thực hiện đảo ngược DWT theo hai chiều để lập thành ảnh thủy vân.

3.3.3. Kỹ thuật tách thủy vân

Ảnh được phân tích thành 2 mức. Khi thủy vân được thêm vào ảnh gốc một cách dư thừa, các hệ số của tần số trung gian 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 vị trí (i, j)

For tất cả hệ số trong dải LH2 và HL2 có trong phần này
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
 $Maxcoef = \text{Max}(ABS(HL2(i, j)), ABS(LH2(i, j)))$;
 $Step = Maxcoef / D$;
 If $Maxcoef = ABS(LH2(i, j))$
 $B(i, j) = HL2(i, j) / Step \bmod 2$;
 Else
 $B(i, j) = LH2(i, j) / Step \bmod 2$;
 End if
End if
End for

CHƯƠNG IV. KỸ THUẬT PHÁT HIỆN ẢNH CÓ GIẤU TIN

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

- 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.

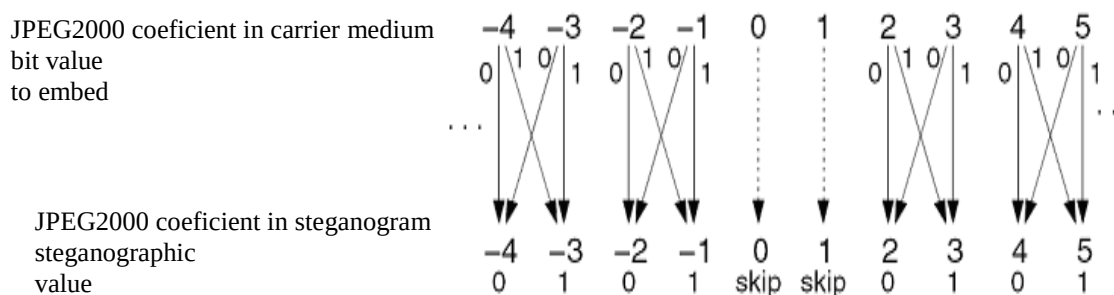
4.2. Kỹ thuật phát hiện bằng thống kê χ^2

Với kỹ thuật giấu Jsteg thay đổi các LSB của các hệ số DWT dẫn đến thay đổi tần suất xuất hiện của các cặp POV như hình vẽ 4.1. Cặp POV được hiểu như sau:

Giả sử một hệ số DWT của ảnh gốc có giá trị là 2 khi giấu một bit thông điệp nó sẽ có giá trị mới là 2 hoặc 3. Một hệ số DWT có giá trị là 3 khi giấu một bit thông điệp sẽ có giá trị mới là 2 hoặc 3. Như vậy (2,3) là một cặp POV.

Trong hình 4.1 chúng ta có các cặp POV sau..., (-4,-3), (-2,-1), (2,3), (4,5),...

Các cặp POV này trong ảnh có giấu tin có tần suất gần bằng nhau trong khi đó điều này hiếm khi xảy ra đối với ảnh chưa giấu tin



Hình 4.1. Mô tả quá trình giấu tin trong hệ số DWT của thuật toán J-steg

Sử dụng thống kê χ^2 (Chi-Squared) [1], [2], [3] có thể kiểm tra một ảnh có giấu tin hay không giấu trên LSB của các hệ số DWT dựa vào các cặp POV. Để phát hiện ra các ảnh này có giấu tin sử dụng kỹ thuật giấu Jsteg như sau:

Thuật toán thống kê POV

Input : stego image

Output: kết luận có giấu tin hay không

Các bước thực hiện

- Tách các hệ số DWT từ ảnh stego lưu trữ vào mảng hai chiều

- Đặt X là vector với x_k bằng tần số xuất hiện của các hệ số DWT có giá trị là chẵn với $DWT > 0$ và có giá trị lẻ với $DWT < 0$.
- Đặt Y là vector với y_k bằng tần số xuất hiện của các hệ số DWT có giá trị là lẻ với $DWT > 0$ và có giá trị chẵn với $DWT < 0$.
- Khởi tạo giá trị ban đầu của X và Y đều bằng 0. Sau đó POV thống kê giá trị hệ số DWT, kiểm tra và điền vào X, Y tương ứng

- Lấy giá trị trung bình của x_k và y_k là $z_k = \frac{x_k + y_k}{2}$

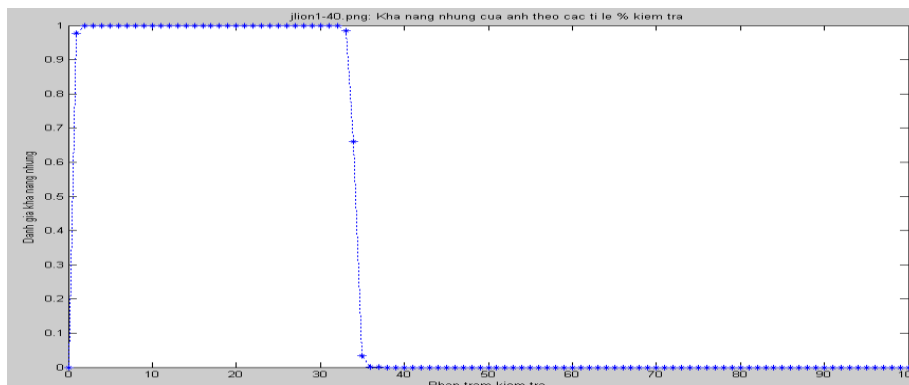
- Sau đó thống kê χ^2 với $n-1$ mức tự do được tính như sau:

$$\chi^2_{n-1} = \sum_{i=0}^{n-1} \frac{(x_i - z_i)^2}{z_i} \quad \text{với } z_i = \frac{x_i + y_i}{2}$$

Theo giả thuyết, thì χ^2_{n-1} là nhỏ đối với ảnh được giấu tin, vì x_i là nhỏ so với z_i . Và đối với ảnh không giấu tin thì χ^2_{n-1} là lớn, vì x_i là lớn so với z_i .

Tính p (giá trị đánh giá xác suất giấu tin) bằng hàm mật độ tích hợp với χ^2_{n-1} như là giới hạn trên của nó:

$$p = 1 - \frac{1}{2^{\frac{n-1}{2}} \Gamma(\frac{n-1}{2})} \int_0^{\chi^2_{n-1}} e^{-\frac{u}{2}} u^{\frac{n-1}{2}-1} du$$



Hình 4.2. Biểu đồ mô tả phát hiện ảnh có giấu tin sử dụng thống kê POV

Đối với một ảnh thông tin giấu được nhúng liên tục (từ góc trên trái của ảnh) thì giá trị của p sẽ gần tới 1 và sau đó rơi xuống 0 khi chúng ta thăm các vùng không giấu. Với kỹ thuật này không những độ phát hiện rất cao mà còn tính toán được độ dài của thông điệp giấu.

Nếu hệ số mang thông điệp được chọn ngẫu nhiên hơn là chọn liên tục, thì kỹ thuật trên ít hiệu quả hơn (trừ trường hợp số lượng giấu từ 70% trên các hệ số DWT của ảnh trở lên).

4.3. Kỹ thuật phát hiện giấu tin trên miền WAVELET.

4.3.1. Ý tưởng.

- Bài viết này đưa ra một kỹ thuật phát hiện giấu tin mới dựa trên cơ sở phân tích histogram thông qua các hệ số wavelet để phát hiện ra sự tồn tại của thông tin được giấu trên miền wavelet. Cách tiếp cận của chúng ta là tập trung vào các phương pháp nhúng thông tin bí mật thông qua các hệ số wavelet lượng tử hóa. Khi phân tích histogram, người ta đã thu được các thông số thống kê sự khác nhau của các hệ số wavelet giữa ảnh chứa thông tin ẩn giấu và ảnh không chứa thông tin ẩn giấu. Và FFT của những thông số này đã được sử dụng để tạo thành tiêu chuẩn định lượng để quyết định xem một ảnh có chứa các thông điệp ẩn giấu hay không.

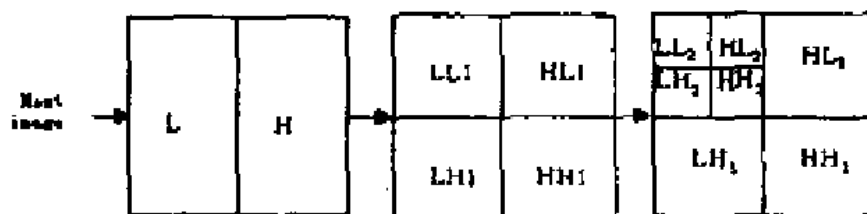
4.3.2. Sự khác biệt về mức năng lượng(energy difference)-Cơ sở sự phát hiện.

Trong kế hoạch thực hiện giấu tin, lượng tử hóa là một phương pháp quan trọng để nhúng thông điệp vào vật chứa. Rất nhiều phương pháp giấu thông điệp vào trong các ảnh nén không mất mát thông tin (BMP, RAS, PGM và nhiều định dạng khác) là dựa trên biến đổi wavelet với mỗi cấp xám hoặc kênh màu với các bit thông điệp. Các phương pháp này sử dụng ý tưởng điều biến lượng tử hóa (quantization modulation idea).

Ví dụ, mọi người có thể xây dựng danh sách các kí hiệu điện tử lượng tử hóa trung bình (a mean quantization code book) khi thi hành kế hoạch. Quá trình lượng tử hóa được thực hiện giữa DWT và MFP (middle

frequency pair – là cặp hệ số trên cùng vị trí trên dải LH và HL của các hệ số DWT).

Trong phương pháp này, chúng ta sẽ tập trung chủ yếu vào các cách thực hiện dựa trên lượng tử hóa trên miền wavelet. Việc phân tích wavelet có thể được thực hiện một cách hiệu quả bằng thuật toán kim tự tháp. Sự biến đổi wavelet là đồng nhất đối với một hệ thống dải băng con (sub-band) có thứ bậc. Đầu tiên, ảnh được phân tích thành 3 phần tần số cao, thấp và trung bình (các dải con LL1, HL1, LH1, HH1) bằng cách sử dụng bộ lọc các dải (sub-band filter) để lấy mẫu theo các kênh ngang và dọc. Các dải con đánh nhãn HL1, LH1, và HH1 đại diện cho các hệ số wavelet co giãn tốt nhất, còn LL1 đại diện cho các hệ số co giãn kém nhất. Để thu được các hệ số wavelet co giãn kém hơn tiếp theo, dải con LL1 sẽ được phân tích nhỏ hơn và các dải con nhỏ hơn này sẽ được lấy mẫu. Quá trình này được lặp lại vài lần tùy theo yêu cầu của người sử dụng. Hơn nữa từ các hệ số DWT này, ảnh gốc có thể được xây dựng lại. Quá trình đảo ngược này được gọi là quá trình đảo ngược DWT (IDWT).

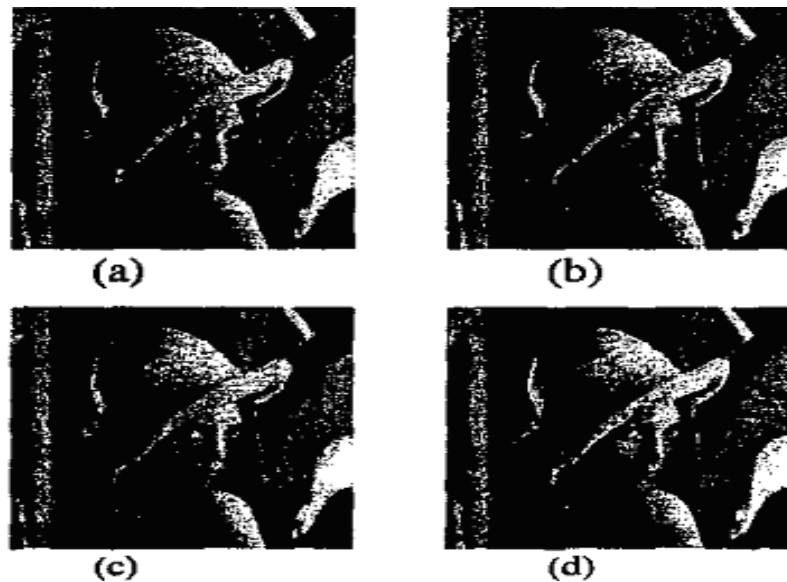


Hình 4.3. Quá trình phân tích wavelet một ảnh

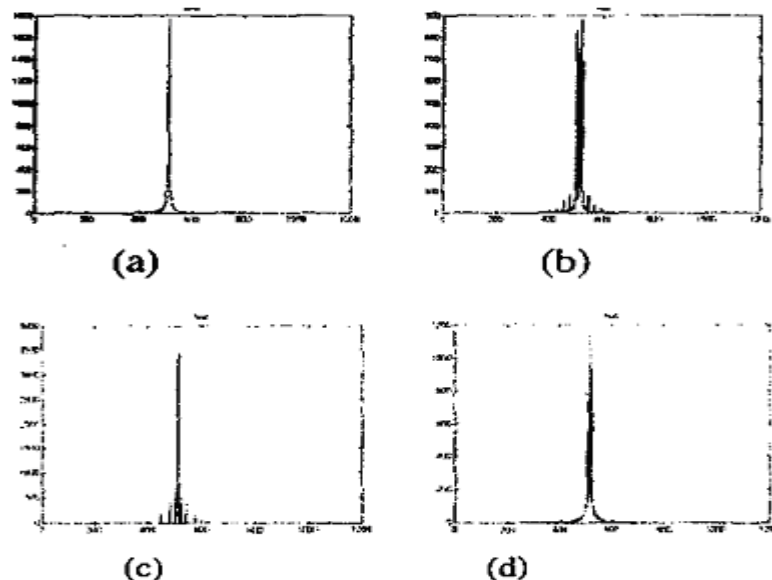
4.3.3. Phân tích histogram

Nhìn chung, các đánh dấu được nhúng vào trong các hệ số wavelet thấp (dải LL) là an toàn với các tấn công trong khi nó có thể gây ra sự giảm sút chất lượng ảnh. Sự thay đổi các hệ số nhiều chi tiết (dải HH) là không thể nhìn thấy được đối với hệ thống thị giác của con người nhưng lại dễ bị tổn hại trước những tấn công. Thủy văn số trên các dải tần số trung gian (dải HL và LH) là cân bằng giữa 2 lựa chọn này. Đầu tiên ta chọn ra các

phương pháp miền wavelet khác nhau để nhúng thông điệp. Ảnh (a) trong hình 4.4 là ảnh chứa, ảnh (b) sử dụng phương pháp QIM trên miền wavelet, ảnh (c) sử dụng phương pháp điều biến thích hợp và HSV, ảnh (d) là ảnh được giấu với phương pháp MFP. Hiển nhiên là các sai khác của ảnh không thể nhìn thấy được. Vì thế, ta thực hiện biến đổi wavelet ảnh sau đó lấy hệ số 3 dải con. Hình 4.5 cho thấy sự phân tích histogram một cách tuần tự.



Hình 4.4. (a) là ảnh gốc. Các ảnh (b),(c),(d) là những ảnh giấu thông tin với các phương pháp tương ứng :QIM, HVS và MFP



Hình 4.5. Phân tích Histogram. Trong đó (a),(b),(c),(d) là histogram của (a),(b),(c),(d) tương ứng trong hình 4.4.

4.3.4. Phân tích quang phổ và sự khác biệt về mức năng lượng.

- Từ hình 4.5, chúng ta nhận thấy hình ảnh histogram của ảnh gốc không giấu tin mịn hơn ảnh có giấu tin. Qua phân tích định lượng các đặc tính của ảnh có tin giấu, chúng tôi giới thiệu phương pháp phân tích quang phổ và energy difference để loại bỏ những đặc tính này.

- Đầu tiên ta thực hiện biến đổi fourier các hệ số dải con. C biểu thị các hệ số dải con (sub-band), $Curve_c$ biểu thị đường cong của C , $\hat{C}$ biểu thị các hệ số biến đổi fourier, $Curve_{\hat{c}}$ biểu thị đường cong của $\hat{C}$. Các vùng được bao quanh với các đường $Curve_c$ $Curve_{\hat{c}}$ được gọi là energy của ảnh và được biểu thị bằng $Energy_c$ và $Energy_{\hat{c}}$. Ta có:

$$\hat{C} = FFT(C)$$

- Sau đó, ta tìm giá trị nhỏ nhất địa phương trong đường $Curve_{\hat{c}}$, các điểm giá trị nhỏ nhất địa phương này được biểu thị bằng L_{min} .

$$L_{min} = LocalMin(Curve_{\hat{c}})$$

$Curve_{Lmin}$ biểu thị cho đường cong được tạo thành bởi L_{min} , tính toán sự khác nhau về energy giữa hai đường $Curve_{Lmin}$ và $Curve_{\hat{c}}$:

$$EnergyDifference = Energy_{\hat{c}} - Energy_{Lmin}$$

Sau rất nhiều thực nghiệm, chúng tôi nhận ra rằng sai phân của các ảnh có tin giấu là cao hơn các ảnh không có tin giấu với phương pháp điều biến lượng tử hóa.

4.3.5. Sự lựa chọn các bộ lọc wavelet

Trong quá trình giấu, những người khác nhau có thể lựa chọn các bộ lọc và các mức phân tách khác nhau, vì thế chúng tôi lên danh sách đa số các bộ lọc phổ biến nhất để làm cho phương pháp phát hiện này có thể được áp dụng một cách rộng rãi hơn. Và trong thí hành, hãy lựa chọn từ 2 cho đến 4 mức, chúng tôi lựa chọn độ chênh lệch energy lớn nhất làm căn cứ để quyết định sự tồn tại của thông điệp được giấu trong ảnh

4.3.6. Ước lượng ngưỡng tối ưu

Sau khi tính toán độ chênh lệch energy của ảnh, ta lấy ra một giá trị T_0 xác định làm ngưỡng để quyết định xem ảnh có được giấu thông tin hay không. Thực tế là ngưỡng càng lớn thì tỉ lệ sai càng cao. Ngược lại, nếu

ngưỡng ở mức thấp thì tỉ lệ cảnh báo đúng là cao. Ta rút ra công thức sau làm cân bằng 2 tỉ lệ này.

$$T_0 = \mathit{arg}(\min(\mathit{CostFun}(T)))$$

Hàm CostFun() là hàm giá trị của T. Hàm giá trị được định nghĩa như sau:

$$\mathit{CostFun}(T) = 1 / ((\mathit{meanvalue1} - T)^2 + (\mathit{meanvalue2} - T)^2)^{1/2}$$

Trong đó : Meanvalue1 và meanvalue2 theo thứ tự biểu thị cho giá trị trung bình của thư viện ảnh không có tin giấu và thư viện ảnh có tin giấu.

CHƯƠNG V. KẾT QUẢ THỰC NGHIỆM

5.1. Môi trường cài đặt

- Ngôn ngữ cài đặt: là ngôn ngữ lập trình Java.
- Môi trường soạn thảo: Jcreator 4.5.
- Môi trường chạy chương trình: môi trường dòng lệnh của DOS.

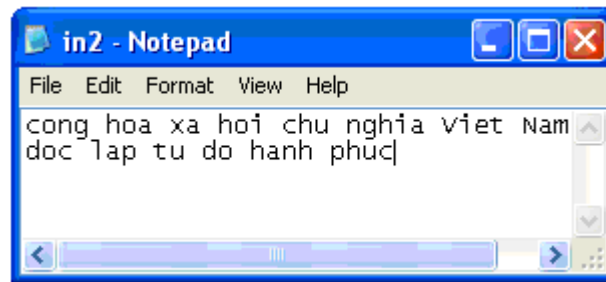
5.2. Kết quả thử nghiệm

- Tập ảnh thử nghiệm gồm 20 ảnh đã được chuyển đổi sang định dạng PGM có kích cỡ 512x512 pixel.



Hình 5.1. Tập ảnh thử nghiệm

- Tiếp tục sử dụng 20 ảnh trên để giấu thông điệp bằng kỹ thuật giấu MFP(middle frequency pair) với 2 thông điệp sau:



Hình 5.2. Thông điệp giấu – 58 byte (464 bit)

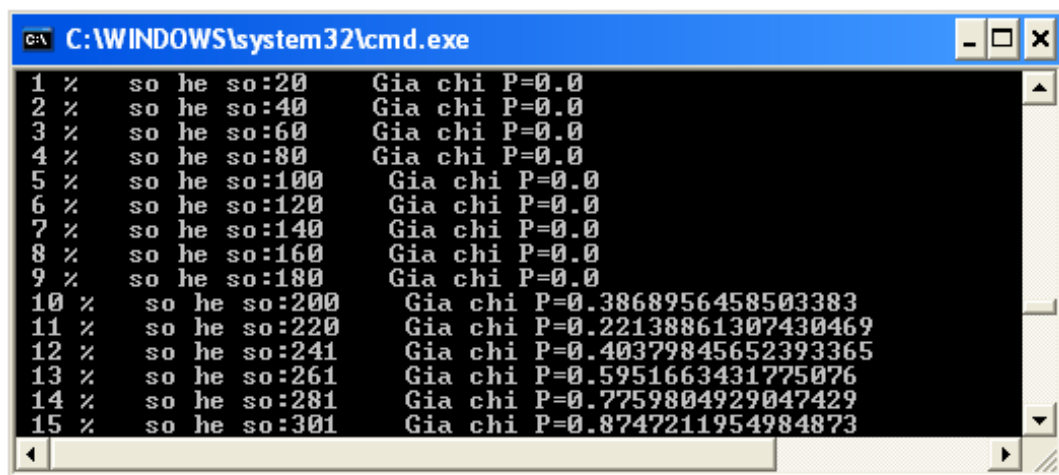
- Sau đó sử dụng 2 chương trình phát hiện được cài đặt theo hai kỹ thuật phát hiện: kỹ thuật phát hiện giấu tin trên miền wavelet và kỹ thuật phát hiện bằng thống kê χ^2 . Kết quả phát hiện được thể hiện trong bảng 5.1.

- Dòng lệnh chạy chương trình:

```
java JJ2KDecoder -i image01.j2k -o 1.pgm -rate 1
```

- Đối số JJ2KDecoder: là tên file chạy khởi đầu của chương trình thực hiện phát hiện thông tin ẩn giấu trong ảnh.
- Đối số -i: cho biết ảnh đầu vào (input).
- Đối số image01.j2k: tên file ảnh đầu vào.
- Đối số -o: cho biết ảnh đầu ra (output).
- Đối số 1.pgm: tên file ảnh đầu ra.
- Đối số rate: cho biết là thực hiện giấu hay tách lấy thông điệp. Với 1 là thực hiện tách.

- Giao diện chính của chương trình:



Hình 5.3. Giao diện chính của chương trình.

STT	Image	Kỹ thuật phát hiện bằng thống kê χ^2		Kỹ thuật phát hiện giấu tin trên miền WAVELET	
		Ảnh gốc JPEG2000	Ảnh đã giấu tin	Ảnh gốc JPEG2000	Ảnh đã giấu tin
1	Image01	K	C	K	C
2	Image02	K	C	K	C
3	Image03	C	C	K	C
4	Image04	K	K	K	C
5	Image05	K	C	C	C
6	Image06	C	C	K	K
7	Image07	K	K	K	C
8	Image08	K	C	C	C
9	Image09	K	C	K	C
10	Image10	C	C	K	K
11	Image11	K	K	K	C
12	Image12	C	C	K	C
13	Image13	K	C	C	K
14	Image14	K	K	K	C
15	Image15	K	C	K	C
16	Image16	C	C	K	C
17	Image17	K	K	C	C
18	Image18	C	C	K	C
19	Image19	K	C	K	C
20	Image20	K	C	K	C

Bảng 5.1. Kết quả phát hiện dùng kỹ thuật phát hiện bằng thống kê χ^2 và Kỹ thuật phát hiện giấu tin trên miền WAVELET.

Trong đó: k là phát hiện ảnh không giấu tin

c là phát hiện ảnh có giấu tin

5.3. Đánh giá thuật toán

- Từ bảng 5.1, chúng ta thấy rằng với một số ảnh chưa giấu tin nhưng chương trình phát hiện vẫn có kết quả là có giấu tin. Ngoài ra, ta thấy rằng phương pháp phát hiện giấu tin trên miền wavelet có tỷ lệ phát hiện thành công cao hơn phương pháp phát hiện bằng thống kê χ^2 .

KẾT LUẬN

Phát hiện thông tin ẩn giấu trong dữ liệu đa phương tiện đặc biệt là trong ảnh số là một vấn đề đang được quan tâm hiện nay trong nhiều lĩnh vực. Để phát hiện và phân biệt được một ảnh số nào đó có mang tin mật hay không đòi hỏi rất nhiều yếu tố và kỹ thuật phức tạp. Trong lĩnh vực thuỷ văn số (watermarking) thường sử dụng kỹ thuật DWT để biến đổi miền dữ liệu của ảnh sang miền tần số sau đó nhúng một lượng thông tin số vào trong các hệ số DWT đó. Vấn đề phát hiện và phân loại các ảnh số có giấu thông tin trên các miền biến đổi DWT là vấn đề rất đang được quan tâm.

Vì thời gian có hạn nên đề tài mới chỉ tìm hiểu và nghiên cứu một số kỹ thuật phát hiện ảnh có giấu tin trên miền biến đổi DWT rất cơ bản nhưng đã mở ra một hướng đi mới cho các nghiên cứu tiếp theo trong lĩnh vực steganalysis.

TÀI LIỆU THAM KHẢO

1. Westfeld and A. Pfitzmann. “Attacks on Steganographic Systems”, In: LNCS vol.1768, Springer-Verlag, Berlin, pp. 61–75, 2000.
2. Christy A.Stanley. “Pair of Values and the chi-Squared Attack”, Department of Mathematics, Iowa State University, may-2005
3. T. Zhang and X. Ping. “A Fast and Effective Steganalytic Technique Against JSteg-like Algorithms”. Proc. 8th ACM Symp. Applied Computing, ACM Press, 2003.
4. Quan Yuanm Hongxun Yao, Wen Gao and Sanghyun Joo. “Blind Watermarking Method Based on DWT Middle Frequency Pair”. Proceeding of IEEE ICME, vol 2,pages: 473-476(2002).
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”.
6. Shaohui Liu, Hongxun Yao, Wen Gao. “Steganalysis of Data Hiding Techniques in Wavelet Domain”.
7. Munira Poonawala, Mamta Sharma. “Digital Watermarking Technology”.
8. R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. “A digital watermark”. proceeding of IEEE International Conference On Image Processing, volume: 2, pp. 86-90, 1994.
9. JJ2000-4.1-src. <http://jpeg2000.epfl.ch>
10. <http://www.paintshoppro.com>
11. Ming-Sing Hsyeh, Din-Chang Tseng, Yong-Huai Huang. “Hiding Digital Watermark Using Miltiresolution Wavelet Transform”, IEEE Transactions on Industrial Electronics, volume: 48, No. 5, Pages: 875-882, 10/2001.