ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

TRẦN THỊ TÚ UYÊN

HỆ THỐNG THỦY VÂN SỐ VÀ ỨNG DỤNG THỦY VÂN SỐ TRONG BẢO VỆ BẢN QUYỀN ẢNH SỐ

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội, 2017

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

TRẦN THỊ TÚ UYÊN

HỆ THỐNG THỦY VÂN SỐ VÀ ỨNG DỤNG THỦY VÂN SỐ TRONG BẢO VỆ BẢN QUYỀN ẢNH SỐ

Ngành : Công nghệ thông tin
Chuyên ngành : Truyền dữ liệu và mạng máy tính .
Mã số :

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. NGUYỄN ĐẠI THỌ.

Hà Nội, 2017

MỤC LỤC

Chương 1 TỔNG QUAN VỀ THỦY VÂN SỐ 4
1.1.KHÁI NIỆM THỦY VÂN SỐ 4
1.2.PHÂN LOẠI THỦY VÂN 5
1.2.1.Phân loại thủy vân theo miền nhúng: 5
1.2.2.Phân loại theo đối tượng được nhúng thủy vân : 5
1.2.3.Phân loại thủy vân theo cảm nhận của con người 6
1.3. MÔ HÌNH THỦY VÂN SỐ 7
1.3.1. Tạo thủy vân số 7
1.3.2 Quy trình nhúng thủy vân 8
1.3.3.Trích xuất và tìm kiếm thủy vân 9
1.4.CÁC HƯỚNG ỨNG DỤNG CỦA THỦY VÂN 10
1.5.ĐẶC TÍNH CỦA THỦY VÂN 12
1.6. YÊU CẦU ĐỐI VỚI PHƯƠNG PHÁP THỦY VÂN. 15
Chương 2 KỸ THUẬT THỦY VÂN SỐ 18
2.1. HƯỚNG TIẾP CẬN THEO MIỀN KHÔNG GIAN ẢNH. 18
2.1.1. Thuật toán SW 19
2.1.2. Thuật toán WU-LEE. 21
2.1.3.Thuật toán LBS 25
2.1.4.Thuật toán PCT 29
2.2. HƯỚNG TIẾP CẬN THEO MIỀN TẦN SỐ. 35
2.2.1 . Biến đổi cosin rời rạc (DCT) 36
2.2.2.Biến đổi Fourier rời rạc. 45
2.2.3.Thuật toán thủy vân dựa trên miền DWT. 54
Chương 3. CHƯƠNG TRÌNH THỬ NGHIỆM 61
3.1. PHÁT BIỂU BÀI TOÁN 61
3.2. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG 61
3.2.1. Mô tả chức năng hệ thống 61

3.2.2. Ứng dụng chương trình 61
3.2.3. Hướng dẫn sử dụng 61
KẾT LUẬN 67
TÀI LIỆU THAM KHẢO 69

DANH MỤC TỪ VIẾT TẮT

CHỮ VIẾT TẮT	Ý NGHĨA
SW	Thuật toán thủy vân đơn giản (Simple Watermarking)
WU-LEE	Thuật toán thủy vân đặt theo tên của hai tác giả M.Y.Wu và J.H.LEE.
PCT	Thuật toán thủy vân đặt theo tên của 3 tác giả : Hsiang – Kuang Pan, Yu- Yuan Chen và Yu- chee Treng
LSB	Least Significant Bit
DCT	Biến đổi Cosine rời rạc (Discrete Cosine Transform)
DWT	Biến đổi sóng rời rạc (Discrete Wavelet Transform)

DANH MỤC HÌNH VẼ

Hình 1.1 : Sơ đồ phân loại hệ thống thủy vân

Hình 1.2 : Quy trình nhúng thủy vân.

Hình 1.3: Quy trình trích xuất và tìm kiếm thủy vân.

Hình 2.1 : Minh họa thuật toán SW: nhúng bit 1 vào khối ảnh B

Hình 2.2 : Minh họa chọn điểm ảnh giấu tin vào những khối ảnh màu

Hình 2.3: Minh họa thuật toán WU_LEE nhúng đoạn bit O1

Hình 2.4 : Ví dụ bảng các hệ số DCT

Hình 2.5: Phân chia 3 miền tần số thấp giữa, cao của phép biến đổi DCT.

Hình 2.6: Quy trình nhúng và tách thủy vân theo kỹ thuật thủy vân trên miền DCT Hình 2.7: Ảnh gốc Lena.bmp b Ảnh biên độ . c. Phổ pha .

Hình 2.8: một miền vành đai giữa dải tần.

Hình 2.9: Miền vành đai chia thành những đường tròn đồng tâm và chia góc

Hình 2.10 : Dải tần số trung bình đượcchia thành các cung đồng tâm.

Hình 2.11: Biến đổi Wavelet và cấu trúc dải thông

Hình 2.12: a Thủy vân gốc, b thủy vân tách được từ các khối, c Thủy vân kết hợp

Hình 2.13: Dải thông LL_2 được chia thành các khối nhỏ hơn

Hình 2.14: a Ảnh gốc b ảnh đã thủy vân với Q= 35.

Hình 3.1: Giao diện phần mềm thử nghiệm.

Hình 3.2: Giao diện thủy vân bằng phương pháp LSB.

Hình 3.3: Kết quả trích xuất khi chưa sử dụng tấn công nhiễu

Hình 3.4: Kết quả trích xuất khi sử dụng tấn công nhiễu

Hình 3.5: Giao diện thủy vân bằng phương pháp DCT.

Hình 3.6: Kết quả trích xuất khi chưa sử dụng tấn công nhiễu

Hình 3.7: Kết quả trích xuất khi sử dụng tấn công nhiễu

Hình 3.8: Kết quả trích xuất khi chưa sử dụng tấn công nhiễu

Hình 3.9: Kết quả trích xuất khi sử dụng tấn công nhiễu

MỞ ĐẦU

1. Lý do chọn đề tài

Ngày nay, với sự phát triển mạnh mẽ của các mạng máy tính tốc độ cao, đặc biệt là Internet, các phương tiện kỹ thuật số như phương tiện lưu trữ, phương tiện truyền thông, đã mở ra một kỷ nguyên mới – kỷ nguyên thông tin số. Hầu hết các thông tin ngày nay đều được lưu trữ dưới dạng số hóa. Đồng thời, quá trình toàn cầu hóa mạng Internet đã biến xã hội ảo là nơi diễn ra trao đổi thông tin trong mọi lĩnh vực chính trị, quân sự, quốc phòng, kinh tế, thương mại. Tuy nhiên, công nghệ số cũng tạo ra khả năng sao chép hoàn hảo, không có bất kỳ khuyết điểm và phân phối lại những sản phẩm này trên toàn thế giới, có hoặc không sự cho phép của người sở hữu. Việc trao đổi, phân bố, sao chép và xử lý các sản phẩm số này ngày càng nhanh chóng, đơn giản, nằm ngoài tầm kiểm soát của các tổ chức. Vấn đề đặt ra cho tất cả các phương thức kinh doanh, phân phối tài nguyên số trên mạng là tuân thủ các nguyên tắc về quyền sở hữu trí tuệ, và không cản trở quá trình phân phối, trao đổi tài nguyên số. Nhu cầu được bảo vệ bản quyền và sở hữu trí tuệ các sản phẩm số đã trở thành một vấn đề quan trọng và đang được quan tâm

Hiện nay, có hàng tỉ bức ảnh được phân phối trên các kênh truyền công cộng. Do chúng có đặc tính dễ sao chép, dễ chỉnh sửa nên nhiều đối tượng lợi dụng cố ý đánh cắp, làm sai lệch, giả mạo bức ảnh gốc. Từ đó, có thể gây thiệt hại đến uy tín, thiệt hại về kinh tế cho người sở hữu bức ảnh đặc biệt trong bối cảnh bùng nổ Internet.

Để giải quyết cho các vấn đề an toàn truyền thông vào bảo vệ bản quyền tài liệu số đặc biệt là ảnh số thì việc xây dựng một hệ thống có sử dụng kỹ thuật nhúng thủy vân vẫn là một giải pháp tối ưu. Thuỷ vân số là một phương pháp mới dựa trên lý thuyết tổng hợp của nhiều lĩnh vực khác nhau như mật mã học, lý thuyết thông tin, lý thuyết truyền thông và xử lý tín hiệu số, xử lý ảnh. Bằng cách sử dụng thủy vân, dữ liệu số sẽ bảo vệ khỏi sự sao

chép bất hợp pháp. Tạo thủy vân là một phương pháp nhúng một lượng thông tin nào đó vào trong dữ liệu đa phương tiện cần được bảo vệ sở hữu mà không để lại ảnh hưởng nào đến chất lượng của sản phẩm. Thủy vân luôn gắn kết với sản phẩm đó. Bằng trực giác khó có thể phát hiện được thủy vân trong dữ liệu chứa, nhưng có thể tách chúng bằng các chương trình có cài đặt thuật toán thủy vân. Thủy vân được tách từ dữ liệu số chính là bằng chứng kết luận dữ liệu số có bị xuyên tác thông tin hay vi phạm bản quyền hay không.

Chính vì tính hữu ích trong ứng dụng thực tiễn của thủy vân số nên em quyết định lựa chọn đề tài là: "**Hệ thống thủy vân số và ứng dụng thủy vân số trong bảo vệ bản quyền ảnh số**".

2. Mục đích của luận văn

Mục đích của luận văn là nghiên cứu hệ thống thủy vân số và các hướng ứng dụng của thủy vân số chủ yếu là ứng dụng trong bảo vệ bản quyền ảnh số.Tập trung vào phân tích các thuật toán thủy vân số. Từ đó, xây dựng chương trình thử nghiệm cài đặt một số thuật toán thủy vân nhằm ứng dụng xác thực thông tin và bảo vệ bản quyền cho dữ liệu ảnh số.

3. Đối tượng và phạm vi nghiên cứu

Luận văn tập trung nghiên cứu các kỹ thuật thủy vân trên ảnh số. Ứng dụng mà luận văn xây dựng là hệ thống nhúng và tách thủy vân nhằm xác thực nội dung thông tin và bảo vệ bản quyền ảnh số.

4. Phương pháp thực hiện

Phương pháp thực hiện đề tài là nghiên cứu các vấn đề liên quan đến giấu tin, tập trung nghiên cứu tiến hành xây dựng chương trình và cài đặt chương trình thử nghiệm

5. Kết quả đạt được

Luận văn đã hệ thống lại các kiến thức cơ bản về thủy vân số, nghiên cứu một số thuật toán trên miền không gian và miền tần số.

Đồng thời cài đặt thành công thuật toán thủy vân trên miền tần số và miền không gian nhằm ứng dụng xác thực bản quyền ảnh số của tác giả.

6. Bố cục của luận văn

Chương 1: Tổng quan về thủy vân số

Chương 2: Kỹ thuật thủy vân số

Chương 3: Chương trình thử nghiệm

Chương 1
TỔNG QUAN VỀ THỦY VÂN SỐ

1.1.KHÁI NIỆM THỦY VÂN SỐ

Kỹ thuật thủy vân trên giấy xuất hiện trong các tác phẩm nghệ thuật làm giấy thủ công cách đây khoảng 700 năm. Loại giấy có thủy vân cổ nhất được tìm thấy vào những năm 1929 và nguyên bản của nó bắt nguồn từ thị trấn Fabriano ở Ý đã đóng góp một vai trò rất lớn đối với sự tiến hóa của công nghiệp sản xuất giấy. Vào thời điểm này, kỹ thuật thủy vân được xem là phương pháp hữu hiệu để xác định nguồn gốc sản phẩm, giúp người dung lựa chọn đúng hãng sản xuất giấy mà mình muốn mua.

Thuật ngữ watermark bắt nguồn từ một loại mực vô hình được viết trên giấy và chỉ hiển thị khi nhúng giấy đó vào nước. Thuật ngữ Thủy vân số được cộng đồng thế giới chấp nhận rộng rãi vào đầu thập niên 1990. Khoảng năm 1995, sự quan tâm đến thủy vân số bắt đầu phát triển nhanh.

Thủy vân số *là quá trình sử dụng các thông tin (ảnh, chuỗi bít, chuỗi số) nhúng một cách tinh vi vào dữ liệu số (ảnh số, audio, video hay text) nhằm xác định thông tin bản quyền của tác phẩm đó*. Mục đích của thủy vân số là bảo vệ bản quyền cho phương tiện dữ liệu số mang thông tin thủy vân.

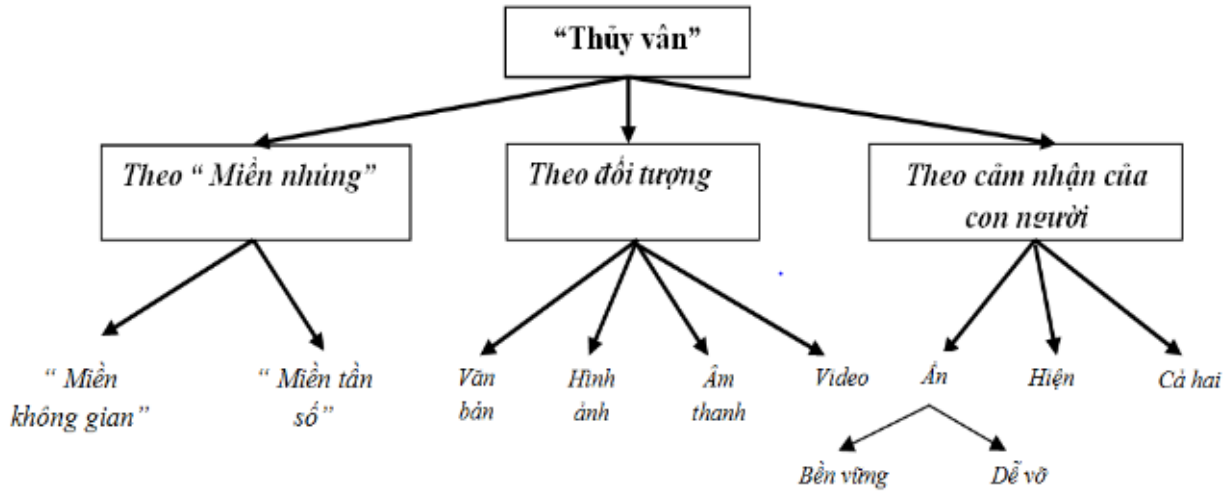
Thao tác đưa thủy vân vào một môi trường số được gọi là thủy vân số. Thủy vân số được xem như là một hình thức ẩn giấu tin. Theo sơ đồ phân loại kỹ thuật giấu tin của A.P. Pentitcolas 1999 theo hai hướng nghiên cứu chính là giấu tin mật và thủy vân số. Có thể xem watermarking là thao tác mà nhúng tin mà trong đó người dùng đầu cuối không cần quan tâm tới thông tin được giấu bên trong đối tượng chứa tin.

Như vậy, Thủy vân số là quá trình nhúng những dữ liệu vào một đối tượng đa phương tiện theo một phương pháp nào đó, để sau đó có thể phát

hiện hoặc trích xuất thủy vân cho mục đích xác thực nguồn gốc của sản phẩm. Thủy vân là một phần đặc trưng của thông tin nhúng vào dữ liệu cần bảo vệ. Một yêu cầu quan trọng đối với thủy vân là rất khó để trích xuất hoặc gỡ bỏ được nó từ đối tượng được nhúng thủy vân mà không biết được chìa khóa bí mật.

1.2.PHÂN LOẠI THỦY VÂN

Thủy vân và kỹ thuật thủy vân tùy theo từng tiêu chí phân loại mà có thể được chia thành nhiều loại khác nhau :



Hình 1.1 : Sơ đồ phân loại hệ thống thủy vân

1.2.1.Phân loại thủy vân theo miền nhúng:

Một trong những tiêu chí để phân loại là "miền nhúng " là nơi chứa thủy vân. Ví dụ, thủy vân có thể được thực hiện trong "miền không gian". Một khả năng khác là thủy vân trong miền tần số.

1.2.2.Phân loại theo đối tượng được nhúng thủy vân :

Kỹ thuật thủy vân có thể được phân loại theo đối tượng đa phương tiện cần nhúng thủy vân như sau:

+ Thủy vân trên ảnh
+ Thủy vân trên video
+ Thủy vân trên âm thanh
+ Thủy vân trên văn bản

1.2.3.Phân loại thủy vân theo cảm nhận của con người

Tùy theo cảm nhận của con người, thủy vân có thể được chia ba loại khác nhau

+ Thủy vân hiện: hiển thị cho người xem thông tin về sản phẩm dưới dạng các hình mờ.

+ Thủy vân ẩn bền vững: được nhúng bằng cách thay đổi trên điểm ảnh sao cho hệ thống cảm giác của con người không thể nhận thấy và phải chịu được các thông tác xử lý tín hiệu thông thường "tấn công" và nó chỉ có thể được phục hồi với cơ chế giải mã thích hợp mà thôi. Xét theo tính bí mật của thủy vân bền vững được phân loại nhỏ hơn như sau :

-*Lược đồ "thủy vân" bí mật* : Cần tới ảnh gốc để trích xuất thủy vân. Có 2 loại lược đồ thủy vân bí mật :

Loại 1: yêu cầu cả ảnh bị biến đổi và ảnh gốc khi trích xuất thủy vân. Ảnh gốc được sử dụng để tìm kiếm vị trí thủy vân trong bức ảnh bị biến đối.

Loại 2: trong đó yêu cầu một bản sao của thủy vân trong quá trình trích xuất và kiểm tra mới có thể biết được thủy vân tcos ở trong bức ảnh cần kiểm tra hay không

Trong hai loại trên khi trích xuất thủy vân cần đòi hỏi có chìa khóa bí mật. Đối với loại thứ nhất thì chìa khóa bí mật ở đây là ảnh gốc, còn đối với loại chìa khóa thứ 2 thì chìa khóa bí mật là dữ liệu bí mật được sử dụng để nhúng vào bức ảnh (hay nói cách khác là thủy vân)

- *Lược đồ thủy vân nửa bí mật*

Không sử dụng ảnh gốc trong quá trình xác định thủy vân. Tuy nhiên, lược đồ này chỉ đưa ra thông tin có sự hiện diện của thủy vân hay không .

- *Lược đồ thủy vân mù*

Trong lược đồ này, không yêu cầu ảnh gốc lẫn thủy vân được nhúng trong quá trình trích thủy vân

- *Lược đồ thủy vân khóa công khai*

Còn được gọi là thủy vân bất đối xứng. Trong lược đồ này, chìa khóa để tìm kiếm và trích xuất thủy vân được công khai với mọi người trái ngược với thủy vân bí mật chìa khóa để tìm kiếm và trích xuất thủy vân là chìa khóa bí mật. Biết được khóa công khai "khó " mà tính được khóa bí mật và khóa bí mật được sử dụng để nhúng và loại bỏ thủy vân.

+ Thủy vân ẩn dễ vỡ : được nhúng theo cách mà bất kỳ biến đổi hay giả mạo đều làm thay đổi hay phá hủy "thủy vân".

+ Thủy vân hiện và ẩn đồng thời : (dual watermark) là sự kết hợp giữa thủy vân ẩn và thủy vân hiện

1.3. MÔ HÌNH THỦY VÂN SỐ

1.3.1. Tạo thủy vân số

Thủy vân có thể là một hình ảnh dạng logo hay văn bản với độ dài cho trước. Thủy vân dạng hình ảnh có khả năng chống chịu trước các phép xử lý ảnh tốt hơn nhiều só với dạng thủy vân dạng ký tự. Thủy vân có thể được biến đổi (bằng mã hóa, chuyển đổi định dạng), trước khi giấu vào ảnh. Các thuật toán nhúng thủy vân dạng logo được gọi là thuật toán thủy vân hợp nhất ảnh. Thủy vân dạng ảnh có lợi ích là dễ dàng nhận biết về mặt trực giác và đưa ra một chứng minh đúng đắn về quyền sở hữu ảnh. Bình thường sẽ có một khóa bí mật K dùng để tang tính bảo mật cho dữ liệu được nhúng. Do tính bền vững được đảm bảo hơn nên thủy vân dạng ảnh được sử dụng nhiều hơn.

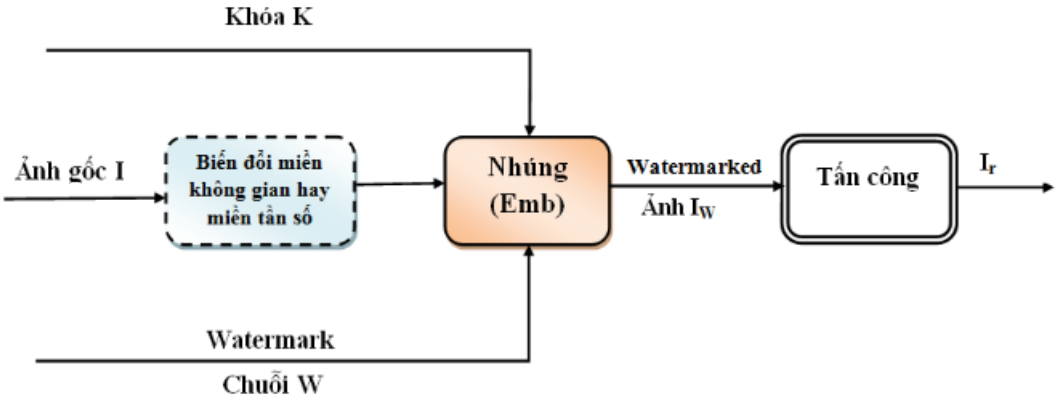
Để tăng thêm tính an toàn và dung lượng thì thủy vân trước khi nhúng vào ảnh mang có thể được mã hóa hay nén lại. Theo cơ chế này, đầu tiên thủy vân số sẽ được nén lại để lượng dữ liệu thủy vân có thể tăng lên, sau đó được mã hóa để tăng tính bảo mật cho thông tin trước khi được giấu vào ảnh mang. Tuy nhiên, giải pháp này làm tăng độ phức tạp của bài toán về phát hiện thủy vân.

1.3.2 Quy trình nhúng thủy vân

Giai đoạn này gồm thông tin khóa thủy vân, thủy vân, dữ liệu chứa và bộ nhúng thủy vân. Dữ liệu chứa bao gồm các đối tượng như văn bản, audio, video, ảnh…. dạng số, được dùng làm môi trường để giấu tin.

Bộ nhúng thủy vân là chương trình được cài đặt những thuật toán thủy vân và được thực hiện với một khóa bí mật

Thủy vân sẽ được nhúng vào trong dữ liệu chứa nhờ một bộ nhúng thủy vân. Kết quả quá trình này là được dữ liệu chứa đã nhúng thủy vân được gọi là dữ liệu có bản quyền và phân phối trên các môi trường khác nhau. Trên đường phân phối có nhiễu và sự tấn công từ bên ngoài. Do đó, yêu cầu các kỹ thuật thủy vân số phải bền vững với cả nhiễu và sự tấn công trên.



Hình 1.2 : Quy trình nhúng thủy vân.

Hình 1.2 trình bày và giải thích quá trình nhúng thủy vân cho ảnh tĩnh. Trong đó, Ảnh gốc được kí hiệu bằng I, "thủy vân" được kí hiệu bở W, hình ảnh chứa "thủy vân" là I_w và K là khóa nhúng. Hàm nhúng E_{MB} có đầu vào là ảnh gốc I, "thủy vân" W và khóa K và tạo ra một ảnh mới có chứa thủy vân mới thể hiện bằng I_w.

Khóa nhúng K là thực sự cần thiết cho việc nâng cao khả năng bảo mật của hệ thống "thủy vân". Trước quá trình nhúng, hình ảnh gốc có thể được chuyển đổi sang miền tần số hoặc nhúng có thể được thực hiện biến đổi sang

miền không gian. Miền được chọn phụ thuộc vào việc lựa chọn kỹ thuật "thủy vân". Nếu quá trình nhúng được thực hiện trong miền tần số, biến đổi nghịch đảo được áp dụng để thu được hình ảnh chứa "thủy vân". Biểu thức toán học cho hàm nhúng có thể được thể hiện như sau :

Đối với kỹ thuật biến đổi theo miền không gian :

$$\mathbf{E_{mb}\ (I, W, K) = I_w}$$

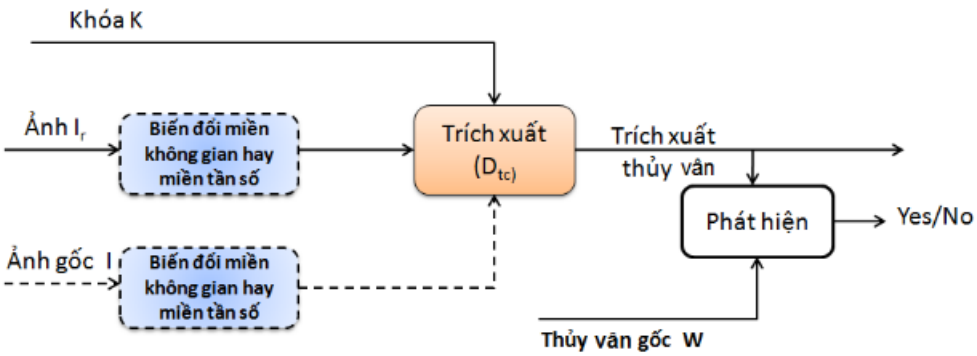
Đối với kỹ thuật biến đổi theo miền tần số :

$$\mathbf{E_{mb}\ (f, W, K) = I_w}$$

Trong đó f là vecto hệ số cho phép biến đổi.

1.3.3. Trích xuất và tìm kiếm thủy vân

Quá trình tách thủy vân được thực hiện thông qua một bộ tách thủy vân tương ứng với bộ nhúng thủy vân cùng với khóa của quá trình nhúng. kết quả thu được là một thủy vân. thủy vân thu được có thể giống với thủy vân ban đầu hoặc sai khác do nhiễu và sự tấn công trên đường đi .



Hình 1.3: Quy trình trích xuất và tìm kiếm thủy vân.

Hình 1.3 trình bày và giải thích quy trình trích xuất và tìm kiếm thủy vân ở trong ảnh tĩnh. Một hàm phát hiện D_{tc} có đầu vào là hình ảnh I_r có chức năng xác định quyền sở hữu sản phẩm. Các hình ảnh I_r có thể chứa thủy vân hoặc không chứa thủy vân. Trong trường hợp tổng quát, hình ảnh có thể bị biến đổi. Hàm phát hiện có khả năng khôi phục thủy vân W_e từ bức ảnh hoặc kiểm tra sự hiện diện của thủy vân W trong bức ảnh đã cho I_r hay

không. Trong quá trình này hình ảnh gốc I cũng có thể yêu cầu, phụ thuộc vào lược đồ thủy vân được lựa chọn.

Biểu thức toán học cho thủ tục trích xuất mù (trích xuất không sử dụng ảnh gốc I) cụ thể như sau :

$$\mathbf{D_{tc}\ (I_r, K) = W}$$

Biểu thức toán học cho thủ tục trích xuất không mù (trích xuất có sử dụng ảnh gốc I) cụ thể như sau :

$$\mathbf{D_{tc}\ (I_r, I, K) = W_e}$$

Thuật toán phát hiện thủy vân mù có đầu ra là một giá trị nhi phân cho biết có sự hiện diện của thủy vân hay không. Bởi vậy, có thể giả sử:

$$\mathbf{D_{tc}\ (I_r, K)} = \begin{cases} 1 \text{ Nếu có thủy vân} \\ 0 \text{ Nếu không có thủy vân} \end{cases}$$

Trong lược đồ tách thủy vân phải được trích xuất một cách chính xác, nguyên mẫu. Lược đồ trích xuất thủy vân có thể chúng mưng được quyền sở hữu, trong khi lược đồ phát hiện thủy vân có thể xác nhận có sự hiện diện của thủy vân hay không.

1.4.CÁC HƯỚNG ỨNG DỤNG CỦA THỦY VÂN

*** Bảo vệ bản quyền ảnh số**

Mặc dù đã có nhiều quy định về bảo vệ bản quyền và đã có những chuyển biến tích cự trong việc thực thi quyền tác giả, nhưng vẫn chưa đủ. Nhưng hành động xâm phạm bản quyền tác giả diễn ra tràn lan, tinh vi và công khai trước sự bất lực của chủ sở hữu. Đặc biệt với dữ liệu số như ảnh số với nhiều định dạng thì vấn đề bảo vệ bản quyền trở nên khó khăn hơn.

Trong việc mua bán và trao đổi các tác phẩm số này nảy sinh các vấn đề cụ thể như sau:

+ Vấn đề thứ 1 là phải bảo đảm quyền tác giả.: Để bảo vệ được bản quyền của người sở hữu ảnh số thì ảnh số đó phải có những thông tin đặc biệt chứng minh nó là thuộc quyền sở hữu của minh.

+ Vấn đề thứ 2 là đảm bảo thông tin sẵn sang cho người dùng hợp pháp và chống phân phối bất hợp pháp nội dung tác phẩm: mua bán,…

+ Vấn đề thứ 3 lần vết thông tin phát hiện người phân phối sản phậm bất hợp pháp: khi vấn đề về vi phạm bản quyền xảy ra hoặc khi chủ sở hữu sản phẩm số nghi ngờ là có bản sao sản phẩm không hợp lệ.

Đây là ứng dụng cơ bản nhất của kỹ thuật thủy vân. Trong thực tế , nhiều tác phẩm đã có tác quyền nhưng vẫn bị sử dụng sai mục đích. Các thông báo tác quyền này thường được đặt ở một vị trí nào đó trên tác phẩm phân phối.

Do các dấu thủy vân có thể vừa không thể nhìn thấy vừa không thể tách rời tác phẩm chứa nó nên sẽ là giải pháp tốt nhất cho việc bảo vệ bản quyền tác giả. Dấu thủy vân (một thông tin nào đó mang ý nghĩa quyền sở hữu tác giả) sẽ được nhúng vào trong các sản phẩm, dấu thủy vân đó chỉ người chủ sở hữu hợp pháp các sản phẩm đó và được dùng làm minh chứng cho bản quyền sản phẩm.

* **Xác thực thông tin và phát hiện xuyên tạc thông tin**: dấu thủy vân không chỉ được dùng để chỉ ra thông tin bản quyền tác giả mà còn được dùng để xác thực thông tin và phát hiện ra xuyên tạc thông tin. Dấu thủy vân sẽ được nhúng trong một tác phẩm sau đó được lấy ra và so sánh với dấu thủy vân ban đầu. Nếu có sự sai lệch chứng tỏ tác phẩm gốc đã bị tấn công và xuyên tạc. Các thủy vân nên được ẩn để tránh sự tò mò của đối phương, hơn nữa việc làm giả các thủy vân hợp lệ hay xuyên tạc thông tin nguồn cũng cần xét đến. Trong các ứng dụng thực tế, người ta mong muốn tìm được vị trí bị xuyên tạc cũng như phân biệt được các thay đổi (ví dụ như phân biệt một đối

tượng đa phương tiện chứa thông tin giấu bị thay đổi, xuyên tạc nội dung hay chỉ bị nén mất dữ liệu). Yêu cầu chung đối với ứng dụng này la khả năng giấu thông tin cao và thủy vân không bền vững.

*** Dấu vân tay hay dán nhãn** : thủy vân trong những ứng dụng này được sử dụng để nhận diện người gửi hay người nhận một thông tin nào đó. Ví dụ các vân khác nhau sẽ được nhúng vào các bản copy khác nhau của thông tin gốc trước khi chuyển cho nhiều người.. Những ứng dụng này, yêu cầu là đảm bảo độ an toàn cao cho các thủy vân, tránh khả năng xóa dấu vết trong khi phân phối.

*** Điều khiển truy nhập:** các thiết bị phát hiện thủy vân (ở đây sử dụng phương pháp phát hiện thủy vân đã giấu mà không cần thông tin gốc) được gắn sẵn vào trong các hệ thống đọc ghi, tùy thuộc vào việc có thủy vân hay không để điều khiển (cho phép/ cấm) truy cập. Ví dụ hệ thống quản lý sao chép DVD được ứng dụng ở nhật .

1.5.ĐẶC TÍNH CỦA THỦY VÂN

Trước đây, đã có một số bài báo thảo luận về đặc tính của thủy vân. Một số thuộc tính thường được thảo luận như: tính phức tạp, tính trung thực hình ảnh, độ tin cậy phát hiện, tính bền vững, dung lượng, bảo mật,…Trong thực tế, không thể để thiết kế một hệ thống thủy vân đảm bảo được tất cả các thuộc tính trên. Do đó, việc đảm bảo cân bằng giữa các thuộc tính là thực sự cần thiết và vấn đề đảm bảo cân bằng phải dựa trên sự phân tích ứng dụng một cách cẩn thận.

- Độ trung thực

Độ trung thực nghĩa là người theo dõi không thể phát hiện ra dấu thủy vân hay nói cách khác dấu thủy vân không làm giảm chất lượng hình ảnh. Để tín hiệu thực sự là không thể cẩm thấy thì thông tin phải được nhúng vào những bít ít quan trọng. Tuy nhiên, tín hiệu lại dễ dàng bị loại bỏ trong quá trình nên có tổn thất thông tin.

Các nghiên cứu trước đây về thủy vân đều tập trung hầu hết vào việc thiết kế thủy vân không thể thấy được và thường nhúng thủy vân vào trong vùng tín hiệu ít quan trọng về mặt cảm nhận, ví dụ như tần số cao hoặc các bít ít quan trọng. Tuy nhiên, gần đây, các kỹ thuật khác (như kỹ thuật trải phổ)lại chèn giấu thủy ký không thấy được vào trong vùng tín hiệu quan trọng về mặt cảm nhận. Đặt dấu thủy ký trong vùng tín hiệu quan trọng về mặt cảm nhận còn có thể nâng cao tính bền vững chống lại các quá trình xử lý tín hiệu.

- Tính bền vững

Hình ảnh được thủy vân có thể phải trải qua nhiều loại xử lý biến đổi khác nhau, ví dụ, tăng độ tương phản, lọc thông, làm mờ,…

Do vậy, dấu thủy ký phải có tính bền vững mới chịu được các phép biến đổi ảnh cũng như biến đổi tín hiệu số thành tín hiệu tương tự, tương tự thành số và nén.

Ngoài ra, ảnh chứa thủy vân phải chịu được các phép biến đổi hình học như di chuyển vị trí, co dãn kích thước và cắt xén.

Thủy vân đạt được tính bền vững thực sự khi: dấu thủy vân ký vẫn còn trong dữ liệu sau khi biến đổi và bộ phát hiện/ trích xuất vẫn có thể phát hiện ra thủy vân. Ví dụ, dấu thủy vân vẫn còn tồn tại trong ảnh sau khi phép biến đổi hình học nhưng thuật toán trích xuất/ phát hiện chỉ phát hiện và đưa ra thủy vân sau khi loại bỏ phép biến đổi. Trong trường hợp, không xác định rõ phép biến đổi để thực hiện biến đổi ngược thì bộ phát hiện/ trích xuất không thể phát hiện và đưa ra thủy vân mặc dù thủy vân vẫn tồn tại trong ảnh số.

Thủy vân có thể được nhúng trong hình ảnh bằng cách thay đổi các giá trị điểm ảnh. Trong trường hợp biến đổi miền không gian, thủy vân đơn giản có thể được nhúng vào trong ảnh bằng cách thay đổi các giá trị điểm ảnh hoặc giá trị các bít quan trọng nhất (LSB), CPT . Tuy nhiên, “thủy vân” bền vững hơn nếu được nhúng vào trong miền biến đổi của hình ảnh bằng cách thay đổi các hệ số.

Vào năm 1997, tác giả Cox et.al trình bày một bài báo về "Thủy vân dựa trên trải phổ bảo vệ cho dữ liệu đa phương tiện" và sau đó hầu hết các nổ lực nghiên cứu về các kỹ thuật biến đổi trên miền tần số được dựa trên bài báo này.

- Tính dễ hỏng

Là thuộc tính đối ngược hoàn toàn với tính bền vững của thủy vân. Thuộc tính này thường được ứng dụng trong lược đồ thủy vân vỡ. Với lược đồ này yêu cầu đặt ra là dấu thủy ký hoặc bị phá hủy bởi bất cứ phương pháp sao chép nào ngoại trừ các phương pháp sao chép hợp pháp. Ví dụ, thủy vân đặt trong một văn bản hợp pháp tồn tại qua bất cứ lần sao chép nào mà không thay đổi nội dung nhưng sẽ bị phá hủy nếu có câu trong nội dung bị thay đổi. Yêu cầu này không giống với chữ ký số trong kỹ thuật mã hóa, trong đó, có thể xác thực tính nguyên vẹn của các bít một cách chính xác nhưng không thể phân biệt các mức biến đổi có thể chấp nhận được.

- Tỉ lệ lỗi sai dương

Tỉ lệ lỗi sai dương là xác suất hệ thống phát hiện nhầm: xác định một mẩu dữ liệu không mang dấu thủy ký là mang dấu thủy ký. Tùy theo ứng dụng mà ảnh hưởng của lỗi là khác nhau, trong một số ứng dụng có thể là rất nghiêm trọng. Do đó, trong ứng dụng, người ta phát tính toán trước sao cho tỷ lệ lỗi sai dương nhỏ hơn mức cho phép.

- Tính dư thừa

Tính dư thừa liên quan đến một thực tế là thủy vân được lặp lại ở những vùng tấn số khac nhau, do đó nếu có một lỗi trên một vùng tần số thì vẫn có thể được khôi phục thông điệp từ các dải tần khác. Tính dư thừa ánh xạ đến tính bền vững, có nghĩa là thủy vân có thể được khôi phục ngay cả khi nó bị biến đổi ở độ nhất dịnh do sự vô ý hay tấn công có chủ ý.

- Đa thủy vân

Một kẻ tấn công có thể thủy vân lại một đối tượng đã đóng dấu thủy vân và sau đó tuyên bố sản phẩm thuộc quyền sở hữu của mình. Một giải

pháp đơn giản nhất trong trường hợp này là gán nhãn thời gian cho thông tin thủy vân với sự có mặt của cơ quan chứng thực hay có thể nhúng thủy vân khác nhau với những người sử dụng khác nhau. Với phương pháp nhúng nhiều thủy vân cho phép lần vết theo nội dung thủy vân nhưng lại tạo điều kiện cho phép tấn công loại bỏ bằng cách lấy trung bình xác suất (tấn công đồng thời).

- Độ phức tạp tính toán

Cũng như bất cứ công nghệ nào sử dụng trong thương mại, độ phức tạp tính toán của lược đồ thủy vân đều rất quan trọng. Điều này, đặc biệt đúng khi sử lý với các dữ liệu thời gian thực.

Mặt khác, cần phải xem xét tính co giãn của độ phức tạp tính toán. Người thiết kế lược đồ thủy vân luôn mong muốn thiết kế được lược đồ mà quy trình nhúng và phát hiện thủy vân có tính co giãn theo các thế hệ của máy tính. Ví dụ, lược đồ thủy vân thế hệ đầu tiên có độ phức tạp tính toán không lớn nhưng độ tin cậy không cao so với lược đồ thủy vân thế hệ tiếp theo. Nhưng khi giải quyết một vấn đề tính toán lớn thì lược đồ thủy vân ở thế hệ sau lại làm việc tốt hơn.

1.6. YÊU CẦU ĐỐI VỚI PHƯƠNG PHÁP THỦY VÂN.

Khi thực hiện thủy vân ảnh số, cần phải có một số tiêu chí để đánh giá chất lượng của giải thuật. Thông thường người ta dựa trên các tính chất sau :

- Bảo đảm tính vô hình

Quá trình thủy vân sẽ làm biến đổi ảnh mang do thủy vân được nhúng vào. Tính "vô hình" thể hiện mức độ biến đổi ảnh mang.

Lược đồ thủy vân hiệu quả, sẽ làm cho thủy vân trở nên "vô hình" trên ảnh mang làm cho người khác khó có thể nhận ra, do vậy đảm bảo được tính bí mật của thủy vân. Tuy nhiên trong thực tế không phải khi nào người ta cũng cố gắng để đạt được tính vô hình cao nhất, ví dụ trong thủy vân hiện

thủy vân được sử dụng để làm biểu tượng xác thực nguồn gốc sản phẩm, do vậy không nhất thiết phải là bí mật, nhiều khi cần lộ ra cho mọi người biết để mà dè chừng.

- Khả năng chống giả mạo (tính toàn vẹn)

Đối với thủy vân thì khả năng chống giả mạo là yêu cầu vô cùng quan trọng vì có như vậy mới bảo vệ được bản quyền, minh chứng cho tính pháp lý của sản phẩm. Để có thể chống lại giả mạo thì bất cứ sự thay đổi nào về nội dung của các ảnh số thì thủy vân này sẽ bị hủy đi. Do đó, rất khó làm giả các ảnh số có chứa thủy vân.

- Tính bền vững

Yêu cầu thứ 3 là thủy vân phải bền vững. Thủy vân phải có khả năng tồn tại cao với các hình thức tấn công có chủ đích và không có chủ đích. Các tấn công không có chủ đích đối với ảnh số bao gồm như nén ảnh, lấy mẫu, lọc, chuyển đổi A/D và D/A

Tấn công có chủ đích có thể là việc xóa, thay đổi hoặc làm nhiễu thủy vân trong ảnh. Để thực hiện được điều này, thủy ấn phải được dấu trong các vùng quan trọng đối với trực giác. Phương pháp thủy vân phải đám bảo sao cho việc không thể lấy lại thủy vân tương đương với việc ảnh bị biến đổi quá nhiều , không còn giá trị về thương mại .

- Dung lượng

Với yêu cầu này, thủy vân nhúng vào ảnh phải đủ dùng trong ứng dụng mà không làm thay đổi quá nhiều chất lượng ảnh.

Việc giấu thủy vân trong ảnh thì ta bắt buộc phải thay đổi dữ liệu ảnh. ta có thể tăng tính bền vững cho thủy vân bằng cách tăng lượng thay đổi ảnh cho mỗi đơn vị cần giấu. nhưng, nếu thay đổi quá nhiều thì tính ẩn không còn được đảm bảo nữa. Còn nếu thay đổi ảnh quá ít thì các yếu tố dùng để xác định thủy vân trong ảnh sau các phép tấn công có thể không đủ để xác định

thủy vân. nếu thông tin được giấu quá nhiều thì cũng dễ làm thay đổi chất lượng ảnh, và làm giảm tính bền vững. Vì vậy, lượng thay đổi ảnh lớn nhất có thể chấp nhận và tính bền vững là nhân tố quyết định cho khối lượng tin được giấu trong ảnh.

Trong thực tế, người ta luôn phải cân nhắc giữa chất lượng (tính bí mật, tính toàn vẹn, tính bền vững) và dung lượng thủy vân.

1.7.KHẢ NĂNG TẤN CÔNG TRÊN HỆ THỐNG THỦY VÂN SỐ.

Thủy vân bền vững phải vượt qua được các tấn công ngẫu nhiên và cố ý.

* Tấn công đơn giản: là dạng tấn công làm hỏng thủy vân đã được nhúng bằng cách thao tác lên toàn bộ dữ liệu được nhúng thủy vân mà không có ý định nhận dạng để lấy tách thủy vân.

* Tấn công phát hiện

Là sự tấn công với mục đích loại bỏ đi mối quan hệ và vô hiệu quá khả năng khôi phục thủy vân, làm cho bộ phát hiện không thể xác định được thủy vân. Điều này được thực hiện chủ yếu bằng cách thay đổi hình dạng hình học như phóng to, thu nhỏ, xoay, cắt xén, xóa hoặc chèn thêm các điểm ảnh và phép biến đổi hình học

* Tấn công nhập nhằng: là sự tấn công với mục đích gây nhầm lẫn bằng cách tạo ra dữ liệu gốc giả hoặc dữ liệu đã được nhúng thủy vân giả. Ví dụ: kẻ tấn công có thể làm giảm tính xác thực của thủy vân bằng cách nhúng một hoặc nhiều thủy vân bổ sung sao cho thủy vân mới không thể phân biệt được với thủy vân ban đầu – thủy vân dùng để xác thực.

* Tấn công loại bỏ : nhằm mục đích phân tích để xác định ra thủy vân hoạc dữ liệu gốc , tách dữ liệu đã được nhúng thủy vân thành dữ liệu gốc và thủy vân.

Chương 2
KỸ THUẬT THỦY VÂN SỐ

Dựa trên những miền dữ liệu được sử dụng để nhúng thủy vân, lược đồ thủy vân có thể được phân thành hai lớp:

Lớp các kỹ thuật thủy vân "miền không gian" (thao tác trên điểm ảnh và lân cận). Hệ thống thủy vân trực tiếp làm thay đổi các phần tử dữ liệu chính, chẳng hạn như trong một bức ảnh số các điểm ảnh được thay đổi để giấu cac dữ liệu về "thủy vân".

Lớp các kỹ thuật thủy vân trên "miền tần số" (thao tác trên tần số). Hệ thống thủy vân làm biến đổi tần số của các phần tử dữ liệu trên một bức ảnh để ẩn đi các dữ liệu về "thủy vân".

2.1. HƯỚNG TIẾP CẬN THEO MIỀN KHÔNG GIAN ẢNH.

Các thuật toán trong miền không gian tập trung vào việc thay đổi trực tiếp trong miền điểm ảnh. Thế mạnh của phương thức thủy vân trong miền điểm ảnh là đơn giản và có độ phức tạp tính toán thấp. Tuy nhiên, kỹ thuật này chỉ đảm bảo thuộc tính ẩn mà không có tính bền vững. Vì vậy, thuật toán này được cài đặt cho ứng dụng xác thực thông tin của ảnh số.

Ý tưởng cơ bản của thuật toán trong kỹ thuật này là chia một ảnh gốc thành các khối nhỏ, số lượng bit giấu trong mỗi khối là tùy thuộc vào từng thuật toán. Thuật toán này dùng cho cả ảnh màu, ảnh đa mức xám và ảnh đen trắng nhưng để dễ trình bày thuật toán chúng ta sử dụng ảnh đen trắng

Ảnh đen trắng hay còn gọi là ảnh nhị phân là ảnh chỉ có hai mức giá trị mức xám là mức 0(đen) và 1 (trắng). Để tạo thủy vân cho ảnh đen trắng ta đem nhúng thủy vân vào ảnh nhị phân. Thông thường việc nhúng thủy vân vào ảnh đen trắng khó thực hiện hơn ảnh đa cấp xám hay ảnh màu. Lý do là ảnh nhị phân chỉ có hai mức xám duy nhất, vì thế nếu thay đổi một bít của điểm ảnh thì đồng nghĩa với thay đổi toàn bộ điểm ảnh.

Có hai cách để nhúng dữ liệu vào ảnh nhị phân là thay đổi giá trị của từng bit riêng lẻ hoặc thay đổi giá trị của một nhóm bít. cách thứ nhất sẽ đảo ngược một điểm đen thành trắng hoặc một điểm trắng thành đen. Cách tiếp cận thứ 2 sẽ làm thay đổi một số đặc trưng của ảnh như độ dày của cạnh, vị trí tương quan giữa các bit…Cách tiếp cận này tùy thuộc nhiều vào kiểu ảnh (kiểu văn bản, kiểu bản đồ). Vì số tham số có thể thay đổi là hữu hạn, đặc biệt là yêu cầu thủy vân ẩn, tổng số dữ liệu có thể dấu được là hữu hạn.

2.1.1. Thuật toán SW

Đây là một thuật toán đơn giản. Cho một file ảnh Bitmap đen trắng F, dữ liệu thủy vân d được biểu diễn dưới dạng nhị phân (dãy bit 0/1). Các bit 1 gọi là điểm đen, các bit 0 gọi là điểm trắng.

Ý tưởng cơ bản của thuật toán này là chia một ảnh gốc thành các khối nhỏ, trong mỗi khối nhỏ sẽ giấu không quá một bit thông tin.

- **Quá trình nhúng thủy vân**

- Chia F thành các khối kích thước m x n.
- Với mỗi khối B trong F ta xét khả năng giấu một bit dữ liệu d_i của d theo các bước :

  + Bước 1: Tính tổng SUM[B] các điểm đen trong khối B, đặt t = SUM[B] mod 2

  + Bước 2: So sánh tính chẵn lẻ giữa t và d_i

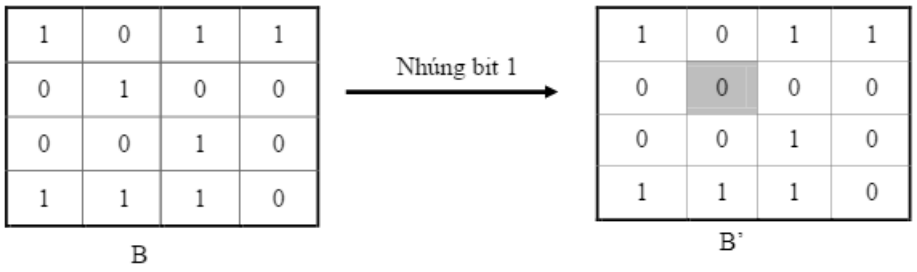
Nếu t và d_i cùng tính chẵn lẻ thì khối B mặc nhiên đã giấu được bit d_i mà không cần làm gì.

Nếu t và d_i khác tính chẵn lẻ thì ta sẽ đảo 1 bit trong B. Chính sách đảo bit: nếu số điểm đen và điểm trắng xấp xỉ nhau thì chọn ngẫu nhiên 1 bit để đảo. Nếu có nhiều điểm đen và có điểm trắng thì sửa điểm trắng thành điểm đen. Ngược lại sẽ sửa điểm đen thành điểm trắng.

Ví dụ minh họa:

Giả sử giấu một bit dữ liệu b = 1 vào khối B.

Ta có SUM (B) = 8. Do SUM (B) mod 2 = 0 nên khối B không thõa mãn yêu cầu để giấu bit 1. Muốn giấu bit 1 vào khối này ta cần phải thay đổi khối bằng cách chọn một bit bất kỳ và đổi từ 0 sang 1 và từ 1 sang 0. Giả sử ta đảo lại bit tại vị trí B [2,2] ta được khối B đã được nhúng bít 1.



Hình 2.1 : Minh họa thuật toán SW: nhúng bit 1 vào khối ảnh B.

Giả sử vẫn với khối B đã cho như trên nhưng ta phải giấu bit dữ liệu b= 0 và khối đó. Ta thấy do Sum (B) = 8 nên Sum (B) mod 2 = 0. Khối B được bảo toàn và bit dữ liệu b = 0 xem như được giấu.

- **Quá trình tách thủy vân**

Trong thuật toán thủy vân này, khóa đơn giản là kích thước của khối, tức là bộ số (m, n). Nếu biết kích thước của khối thì dễ dàng trích lại dữ liệu d theo ccs bước:

Bước 1: Chia ảnh có nhúng thủy vân B' thành các khối có kích thước m x n với mỗi khối B_i' trong B' ta tính Sum [Bi']

Bước 2: tách thủy vân theo cách xét

+ Nếu Sum [Bi'] là chẵn thì bit di = 0

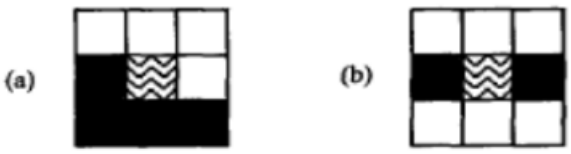
+ Ngược lại , nếu Sum [Bi'] là lẻ thì bit di = 1

- **Nhận xét**

Với thuật toán này việc chọn khối khá là đơn giản: ta có thể bắt đầu từ khối đầu tiên và các khối tiếp theo một cách tuần tự. Tuy nhiên, ta có thể chọn ngẫu nhiên một khối chưa giấu ở mỗi lần giấu, hoặc chọn các khối theo một

thuật toán xác định kèm theo một khóa K. Khi đó, ta đã làm tang được độ an toàn của thuật toán vì khóa bây giờ còn thêm cả chỉ số khối đã giấu tin cho từng bit. Hoặc ta có thể thay đổi kích thước khối mỗi lần giấu, chẳng hạn như khối thứ nhất có kích thước là 8 x 8 thì khối thứ 2 có kích thước 8x12 trong trường hợp này khóa sẽ gồm cả kích thước khối của mỗi lần giấu.

Kỹ thuật trên sẽ gặp phải hiện tượng gây bất thường đối với ảnh sau khi giấu thông tin đặc biệt khi chọn vào những khối ảnh một màu, chẳng hạn như một khối màu đen hoặc toàn trắng. Khi đó, nếu cần đảo giá trị một bit thì vị trí bit đảo sẽ khác biệt hoàn toàn với các bit trong khối và dễ nhận biết có sự thay đổi. Vì vậy, để xác định nên thay đổi bit nào khối bit ta phải tính hệ số ảnh hưởng của bit đó khi nó bị thay đổi. Hệ số này tính bằng cách xét sự thay đổi về tính trơn và tính liên kết với các điểm láng giềng. Tính trơn được đo theo sự chuyển đổi mức xám theo chiều ngang và chiều dọc, đường chéo trong cửa sổ 3x 3. Tính liên kết được tính bằng số nhóm điểm đen và số điểm trắng. Ví dụ: Nếu đảo một điểm ảnh trong hình (a) sẽ ít bị chú ý hơn điểm ảnh trong hình.



Hình 2.2 : Minh họa chọn điểm ảnh giấu tin vào những khối ảnh màu.

2.1.2. Thuật toán WU-LEE.

Thuật toán này của hai tác giả M.Y. WU và J.H. Lee đưa ra cải tiến hơn thuật toán 1 bằng việc đưa thêm khóa K sử dụng trong quá trình nhúng và tách thủy vân đồng thời đưa thêm các điều kiện đảo bit trong mỗi khối. Với thuật toán này, có thể nhúng một bit và mỗi khối bằng cách hiệu chỉnh nhiều nhất 1 bit của khối. Kỹ thuật này có khả năng làm tăng dữ liệu có thể nhúng.

Xét ảnh gốc F , khóa bí mật K và một số dữ liệu được nhúng vào F. Khóa bí mật K là một ma trận ảnh có kích thước m x n . Để đơn giản ta giả sử kích thước của ảnh gốc F là bội số của m x n . Quá trình nhúng thu được ảnh F có một số bit đã bị hiệu chỉnh. Thuật toán thực hiện như sau:

- **Quá trình nhúng thủy vân**

  + Bước 1 : Chia F thành các khối, mỗi khối có kích thước m x n .

  + Bước 2: Với mỗi khối F_i thu được ở bước 1. Kiểm tra điều kiện:

$$\mathbf{0 < SUM (F_i \wedge K) < SUM (K)}$$

Nếu điều kiện trên đúng thì tiếp tục thực hiện bước 3 để nhúng một bit vào F_i. Ngược lại, dữ liệu sẽ không được nhúng vào F_i và F_i sẽ được giữ nguyên.

+ Bước 3: Giả sử bit được nhúng vào F_i là b. Được hiệu chỉnh F_i ta làm như sau:

Trường hợp 1: Nếu SUM (F_i ^ K) mod 2 = b thì không thay đổi F_i và bit b hiện nhiên được nhúng vào khối F_i.

Trường hợp 2: Nếu SUM (F_i ^ K) mod 2 # b và SUM (Fi ^ K) = 1 thì chọn ngẫu nhiên một bit của F_i tại vị trí (i,j) mà F_i (j,k)=0 và K (j,k)=1 và đảo F_i (j,k) thành 1.

Trường hợp 3: Nếu SUM (F_i ^ K) mod 2 # b và SUM (F_i ^ K) = SUM (K) – 1 thì chọn ngẫu nhiên một bit của F_i tại vị trí (j,k) mà K (j,k)=1 và đảo ngược F_i (j,k) thành 0.

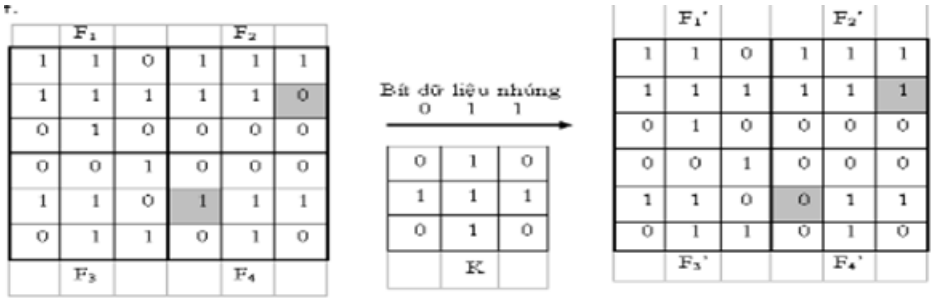
Trường hợp 4: Nếu SUM (F_i ^ K) mod 2 # b và 1< SUM (F_i ^ K) < SUM (K) – 1 thì chọn ngẫu nhiên một bit của F_i tại vị trí (j,k) mà K (j,k)=1 và đảo ngược Fi (j,k).

Trong bước 3 chỉ thực hiện tối đa một phép đảo một bit của Fi để thu được khối Fi’ nhằm đảm bảo tính bất biến.

Ví dụ minh họa:

Giả sử ta cần nhúng dãy bit d = 011 và một ảnh F có kích thước 6 x 6 với một ma trận khóa K có kích thước 3 x 3 như trong hình 2.3. Ta có Sum (K) = 5

Chia ảnh F thành bốn khối nhỏ mỗi khối sẽ có kích thước là 3 x 3 ta thu được F_1 , F_2, F_3, F_4 .



Hình 2.3: Minh họa thuật toán WU_LEE nhúng đoạn bit O1

Áp dụng thuật toán, lần lượt nhúng các bit vào các khối như sau:

- Với F_1, Vì SUM (F_1 ^ K) = 5 = SUM (K) không thỏa mãn điều kiện nhúng nên không nhúng dữ liệu vào trong F1.
- Với F2, SUM (F2 ^ K) = 3 thỏa mãn điều kiện nhúng và bít cần nhúng là 0.

Vì SUM (F2 ^ K) mod 2 = 3 mod 2 # 0 và 1 < SUM (F2 ^ K) < SUM (K) – 1 nên ta chọn ngẫu nhiên một vị trí để đảo bit trong khối F2, chẳng hạn vị trí (2,3) thỏa mãn K [2,3] =1 (theo trường hợp 4). Sau khi đảo bit F2 [2,3] ta thu được khối F2 ‘ như trên hình ảnh (bit bị đảo được tô xám).

- Với F3, SUM (F3 ^ K)= 3 thỏa mãn điều kiện nhúng và bit cần nhúng là 1.

Ta có SUM (F3 ^ K) mod 2 = 3 mod 2 = 1 = b. Khối F3’ thu được giữ nguyên khối F3 nhung với ý nghĩa là khối đã được giấu bit = 1 (theo trường hợp 1)

- Với F4, SUM (F4 ^ K) = 4 thỏa mãn điều kiện nhúng và bit cần nhúng là 1.

Ta có SUM (F4 ^ K) mod 2 = 4 mod 2 = 0 # b và SUM (F4 ^ K) = SUM (K) – 1. Theo trường hợp 3 trong thuật toán, ta chọn vị trí (2,1) để đảo bit trong khối F4 vì với phần tử này ta có F4[2,1] = 1 và K [2,1] =1 . Sau khi đảo bit F 4 [2,1] ta thu được khối F4’ như trên hình vẽ (bit bị đảo được tô xám).

- **Quá trình trích thủy vân**

Phương pháp giấu tin Wu- Lee cho phép giấu nhiều nhất 1 bit dữ liệu trong 1 khối, Giả sử có được bất biến 0 < SUM (Fi ^ K) < SUM (K)

Trong thuật toán nhúng tin, tiến hành đảo 1 bit trong mỗi khối F I, sao cho tổng số bit 1 của Fi ^ K bằng tổng số bit 1 của K tức là :

SUM (Fi ^ K) = [b mod 2]

Do đó, khi xác định được 0 < SUM (Fi ^ K) < SUM (K) thì có nghĩa là khối đó có giấu tin, Bit tin được giấu xác định bởi công thức:

b= [SUM (Fi' ^ K)] mod 2

- **Nhận xét:**

Việc chọn khóa K nhằm làm tăng độ bảo mật của thuật toán. Nếu thuật toán 1 chỉ biết kích thước khối là mx n thì đối phương rất dễ khai thác thủy vân.

Phép toán F i ^ K quy định thuật toán chỉ được phép sửa các bit trong khối Fi ứng với bit 1 trong khóa K. Như vậy, khóa K được xem như một mặt nạ, tạo ra khung nhìn cho thuật toán. Ta có thể thay phép toán ^ bằng một phép toán khác chẳn hạn phép + .

Điều kiện 0< SUM (Fi ^ K) < SUM (K) quy định nếu khối Fi ^ K toàn 0 hoặc giống như khóa K thì không được giấu tin để tránh bị lộ.

Do việc giấu tin vào khối chỉ cần thay đổi tối đa một bit nên việc chọn bit nào trong F để đảo cần tuân thủ theo nguyên tắc: Nếu F i ^ K có nhiều bit 1 thì chọn bit 1 , ngược lại nếu Fi ^ K có quá it bit 1 thì chọn bit 0. Ngược tắc này làm giảm khả năng bit đảo bị phát hiện.

Vì khóa K là bí mật nên thông tin đã nhúng là bí mật. Thuật toán này đã thay đổi nhiều nhất của một bit của khối Fi khi giấu một bit thông tin vào bên trong khối nên với một khối có kích thước m x n đủ lớn thì sự thay đổi của Fi là nhỏ.

Ảnh F được lựa chọn để nhúng tin có quá nhiều điểm trắng hay quá nhiều điểm đen đều làm giảm tỷ lệ bít giấu được.

Thuật toán Wu – Lee đơn giản, lượng tin giấu được không thấp nhưng tính bảo mật không cao, không thích hợp với ảnh có mảng đen và trắng rộng.

2.1.3.Thuật toán LBS

Về cơ bản, kỹ thuật thủy vân LBS dựa trên tần suất xuất hiện của các bit 0 và 1 trong file ảnh gốc và trong thông điệp cần mã hóa, từ đó đưa ra sự thay thế các bit này để thực hiện việc giấu tin .

Cụ thể hơn, trong kỹ thuật thủy vân LSB, bit cuối cùng của mỗi byte được đặt giá trị 0, sau đó tùy thuộc vào giá trị 0 hoặc 1 của dữ liệu mà thay đổi. Nếu bit của dữ liệu là 0 thì giữ nguyên, còn nếu bit của dữ liệu là 1 thì sẽ đổi giá trị này trên ảnh thành 1.

Để thực hiện kỹ thuật thủy vân này, cần một ảnh gốc, hay còn gọi là cover image. Do phương pháp này sử dụng những bits của từng pixcel trong ảnh, nó đòi hỏi một định dạng nén không mất thông tin. Khi ta sử dụng ảnh màu 24 bit, từng bit của mỗi màu thành phần R, G, B đều có thể được sử dụng, như vậy có thể giấu được 3 bit trong mỗi điểm ảnh, đồng nghĩa với việc nhúng được nhiều thông tin hơn.

- **Dữ liệu vào**

  + Ảnh gốc

  + Dữ liệu thủy vân

  + Khóa bí mật

- **Dữ liệu ra**

+ Ảnh mang: có chứa thông tin thủy vân. Ảnh mang có sự thay đổi không đáng kể so với ảnh gốc.

+ Để có thể lưu trữ lượng thông tin lớn và sự thay đổi màu sắc của ảnh là không đáng kể, chúng ta sử dụng file bitmap 24 bit . Cụ thể hơn, một pixel

của ảnh được biểu diễn 3 màu đỏ, xanh lá cây và xanh da trời (R|, G, B), mỗi màu sử dụng 8 bit. Tuy nhiên trong lược đồ trình bày dưới đây, chúng ta chỉ sử dụng bit cuối cùng màu xanh da trời để giấu thông tin.

- **Thuật toán nhúng thủy vân:**

+ Bước 1 : Tính tổng số bytes cần dùng để nhúng thủy vân. Giá trị này được lưu trong biến int S.

+ Bước 2: Đọc các kí tự từ file text sau đó chuyển giá trị ASCII của chúng sang dạng nhị phân 8 bit, lưu giữ trong một mạng từ A [7] về A [0] (A[0] là LSB)

+ Bước 3: Tính toán xem có tất cả bao nhiêu bit 0 và 1 xuất hiện trong mỗi byte, lưu tổng các giá trị này lần lượt là i 0 và i1.

+ Bước 4: Lặp lại từ bước 1 -> 4 cho đến khi kết thức toàn bộ văn bản EOF.

+ Bước 5 : Từ ảnh gốc , đọc giá trị RGB của mỗi pixel.

+ Bước 6: Đọc giá trị bit cuối cùng của mỗi pixels. Với ảnh RGB 24 bit thì ta sẽ đọc bit cuối cùng trong số 8 bit của màu xanh da trời.

+ Bước 7: Kiểm tra xem bit này có giá trị 0 hay l, sau đó tính tổng số lần xuất hiện các bit này trong S pixcels, lưu lần lượt vào hai biến c 0 và c 1.

+ Bước 8: Lặp lại từ bước 5 cho đến bước 7 [8*S] lần. Đây là số pixel cần đọc để có thể giấu toàn bộ các byte thông điệp

+ Bước 9: Nếu [(c0 > c1) và (i0 > i1)] và [(c1> c0) và (i1>i0)], đặt gí trị cho flag = 0, ngược lại đạt giá trị flag = 1.

+ Bước 10 : Ghi giá trị của flag vào phía bên trái của bit cuối cùng của pixel đầu tiên trong ảnh giấu.

+ Bước 11: Mở ảnh gốc ở chế độ đọc. Tạo một ảnh mang giống ảnh gốc ở chế độ ghi.

+ Bước 12: đọc Header của file gốc. Ghi thông tin header này lên ảnh mang. Từ ảnh gốc, đọc giá trị RGB của mỗi pixel.

+ Bước 13: đọc bit stream của dữ liệu. Nếu giá trị của cờ là 0 thì giữ nguyên giá trị bit của dữ liệu, sau đó ghi đè lên bit cuối cùng của màu xanh của pixel, ngược lại, nếu giá trị cờ là 1 thì đảo lại bit dữ liệu rời mới ghi lên pixcel (0 thành 1 hoặc 1 thành 0). Ghi pixel này vào ảnh stego.

+ Bước 14: Nếu toàn bộ các LSB đã được sửa đổi thành công, thì ghi nốt các bit còn lại của các pixel vào ảnh mang. Ngược lại, quay lại bước 13.

- **Thuật toán tách thủy vân**

+ Bước 1: Mở ảnh Stego dưới chế độ đọc

+ Bước 2: Đọc bit liền kề bit cuối của pixel đầu tiên trong ảnh. Dựa trên giá trị của nó, đặt giá trị flag là 0 hoặc 1.

+ Bước 3: Đọc từng pixel của ảnh Stego.

+ Bước 4: Nếu flag là 0 thì đọc bit cuối cùng của mỗi pixel và đưa vào một mảng. Ngược lại nếu flag = 1 thì đảo bit rồi mới chuyển vào mảng.

+ Bước 5: Đọc mỗi 8 pixel theo cách trên, sau đó chuyển nội dung của mỗi 8 phần tử của mạng sang hệ thập phân, dây chính là giá trị ASCII của kí tự.

+ Bước 6: Nếu chưa gặp giá trị EOF thì in kí tự và quay lại bước 3.

- **Ví dụ minh họa**

Giả sử thông tin cần nhúng là Hi. Trong bảng mã ASCII, H có mã là 72 và i có mã là 105 :

+ Chuyển sang hệ nhị phân ta có H = 01001000 và i = 01101001

+ Thông điệp Hi được mã hóa có dạng : 0100100001101001

+ Trong chuỗi trên có 6 bit 1 và 10 bit 0

+ cần 16 pixel để lưu giữ 16 bit dữ liệu trên

+ Giả sử có một bảng 16 pixel RGB có giá trị như sau:

```
11001000 01100001 10100001
11001011 11110000 10100001
01001111 01000001 10111101
01001111 11110000 10111001
01000000 01000000 10110000
11001111 01010000 10100001
11001111 11100001 10100000
11000000 11110000 10100001
11001111 10010000 00100000
11001111 11110000 10100001
11001111 11110000 10100001
11000011 11110000 00100000
00001111 11110000 00100000
11001111 11010000 10000001
11001111 10110110 10100001
01001111 01110000 10100001
```

+ Dựa theo thuật toán ta có : i0 = 10 i1 = 6 c0 = 5 c1 =11

+ Ở đây ta có i0> i1 nhưng c0 < c1 , do đó cần thực hiện phép đổi bit trên thông điệp thành 101101111001010 và đặt flag có giá trị bằng 1.

+ Sau quá trình nhúng thủy vân các điểm ảnh của ảnh Stego sẽ có dạng

```
11001000 01100001 1010000 1
11001011 11110000 1010000 0
01001111 01000001 1011110 1
01001111 11110000 1011100 1
01000000 01000000 1011000 0
11001111 01010000 1010000 1
11001111 11100001 1010000 1
11000000 11110000 1010000 1
11001111 10010000 0010000 1
11001111 11110000 1010000 0
11001111 11110000 1010000 0
11000011 11110000 0010000 1
00001111 11110000 0010000 0
11001111 11010000 1000000 1
11001111 10110110 1010000 1
01001111 01110000 1010000 0
```

Quá trình tách thủy vân tiến hành ngược lại :

+ Flag được đọc và nhận giá trị 1

+ Đọc 16 bits cuối của ảnh Stego ta nhận được chuỗi 1011011110010110

+ Do flag = 1 , ta cần thực hiện phép đảo bit để nhận được chuỗi nguyên bản 0100100001101001.

2.1.4.Thuật toán PCT

Việc nhúng thông tin vào ảnh nhị phân là một thách thức không nhỏ. Thuật toán giấu bít thông tin vào khối ảnh nhị phân (WL) được WU và LEE đề xuất. Tuy nhiên, mỗi khối giấu được không nhiều thông tin và khả năng bảo mật cũng không được tốt. Thuật toán CPT của Y. Chen , H. Pan, Y. Tseng cũng có tư tưởng giấu tin theo khối bít.

Theo thuật toán, ảnh được phân hoạch thành nhiều khối có cùng kích thước m x n . Với mỗi khối dữ liệu ảnh, có thể giấu được tối đa r bit thông tin, với r <= [log 2 (m*n + 1)] bằng cách thay đổi không quá 2 bit trong khối dữ liệu ảnh.

So với thuật toán WL, thuật toán CPT có tỷ lệ giấu tin cao hơn nhiều, trong khi số bít cần thay đổi cũng rất ít. Ví dụ với khối 25 * 25 thuật toán WL, ta chỉ giấu được 1 bit, nhung với thuật toán CPT có thể giấu tối đa là 8 bit.

Ngoài cách sử dụng một khóa K, thuật toán CPT còn sử dụng một ma trận trọng số nhằm giấu được một dãy nhiều bít vào mỗi khối, và ma trận trọng số này cũng là thành phần bí mật cùng với ma trận khóa K. Do vậy, độ an toàn, tính bảo mật của thuật toán CPT sẽ cao hơn.

*** Dữ liệu vào:**

+ Ảnh nhị phân A dùng làm môi trường giấu tin. A được coi như một ma trận nhị phân, và được chia thành các ma trận con F cấp m * n. Mỗi ma trận F là một khối bit được dùng làm môi trường giấu tin.

+ (b1,b2….br) là dãy r bít cần giấu vào trong mỗi khối ảnh kích thước m * n và r phải thỏa mãn bất đẳng thức 2 ^r – 1 < = m* n.

+ B là k * r bit dữ liệu cần giấu, được tách thành k chuỗi r bit.

+ K là ma trận nhị phân cấp m * n (KHóa)

+ W là ma trận trọng số cấp m * n. Các phần tử của W cần thỏa mãn điều kiện

$$\{ [W]_{i,j|Ii=1\ldots m=1\ldots n} \} = \{1,2,\ldots\ldots,2^{r}-1\}$$

Số khả năng có thể lựa chọn K và W là $C_{mn}^{2^r-1} * (2^r-1)! * (2^r-1)^{mn-(2^r-1)}$ khả năng (trong đó $C_{mn}^{2^r-1}$ là tổ hợp m*n phần tử). Vì vậy, với m và n, đủ lớn thì khả năng kẻ gian dò tìm ra được W là vô cùng khó nên thuật toán CPT có độ an toàn giấu tin rất cao.

Các ma trận K và W được sử dụng như khóa bí mật: người gửi sử dụng khóa K và ma trận trọng số W trong quá trình giấu tin và người nhận cần phải có khóa K, W để khôi phục lại thông tin đã giấu.

*** Dữ liệu ra**

Ảnh nhị phân A' chứa thông tin cần bảo mật. A' cùng gồm các ma trận con F' cấp m x n , trong đó mỗi F' giấu được r bít, và F' khác F tối đa hai phần tử.

- Các khái niệm cơ bản :

+ Ảnh nhị phân và ma trận nhị phân :

Trước hết ta quan tâm tới đối tượng chính là các ảnh nhị phân hay ảnh 1 bit màu. Đó là những bức ảnh mà mỗi điểm ảnh chỉ là điểm đen hoặc trắng, được quy định bởi một bit. Nếu bit mang giá trị 0 thì điểm ảnh là đen, nếu là 1 thì điểm ảnh là trắng. Do đó để biểu diễn ảnh đen trắng ta có thể dùng ma trận nhị phân, là ma trận mà mỗi phần tử chỉ nhận một trong hai giá trị là 0 hoặc 1.

+ Khóa bí mật :

Là ma trận nhị phân có cùng kích thước với kích thước khối ảnh được dùng chung bởi người giấu tin và người tách thông tin.

+ Ma trận trọng số

Cũng là ma trận số cùng kích thước với khóa và được sử dụng bởi người giấu tin và người tách thông tin.

Ma trận W kích thước m*n được gọi là ma trận trọng số cấp r nếu mỗi phần tử của tập hợp {1,2,….,2^r-1} xuất hiện trong W ít nhất một lần và các phần tử của W chỉ nhận giá trị trong tập hợp {1,2,….,2^r-1} với m, n, r là các số tự nhiên thỏa mãn $2^r - 1 \leq m * n$.

Từ định nghĩa, ta nhận thấy với mỗi m, n, r thỏa mãn $2^r - 1 \leq m * n$. sẽ có :

$$C_{mn}^{2^r-1} * (2^r - 1)! * (2^r - 1)^{mn-(2^r-1)}$$

+ Ví dụ như với m = n = 4, r =2 thì ta có 5.356.925.280 khả năng lựa chọn. Con số này đủ lớn để làm giảm nguy cơ thông tin bị giải mã bởi những kẻ phá hoại.

+ Phép đảo bít là một phép biến đổi trên các bit nhị phân. Đảo bit b tương đương với phép biển đổi thay b bởi 1- b, tức là nếu ban đầu b nhận giá trị 0 thì sau khi đảo nó sẽ nhận giá trị 1 và ngược lại, nếu ban đầu b có giá trị là 1 thì sau khi đảo nó sẽ có giá trị 0.

- **Các phép toán trên ma trận :**

Giả sử cho hai ma trận nhị phân A và B có cùng kích thước

+ Phép cộng C = A + B

Trong đó C[i,j] = A[i,j] + B[i,j] ;

A[i,j]	B[i,j]	C[i,j]
0	0	0
0	1	1
1	0	1
1	1	0

+ Phép nhân C= A x B

Trong đó C[i,j] = A [i,j] * B[i,j] .

- **Thuật toán**

Với khối ảnh Fi, ma trận trọng số W, khóa K, ta cần giấu r bit thông tin b1,b2,….br vào Fi bằng cách đảo nhiều nhất 2 bit của Fi. Mục đích của ta là biến đổi F i thành F i' sao cho thỏa mãn yêu cầu sau: SUM (F_I' K) x W = b1b2…..br (mod 2^r).

Thuật toán được thực hiện tuần tự cho từng khối F theo các bước sau:

+ Tính T = F + W

Trong đó: Phép + là phép toán XOR theo các vị trị tương ứng của hai ma trận nhị phân cùng bậc

Ví dụ :

$$F = \begin{pmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,1 \\ 1\,0\,1\,0 \\ 1\,0\,1\,1 \end{pmatrix} \quad K = \begin{pmatrix} 1\,0\,0\,1 \\ 1\,0\,0\,1 \\ 1\,1\,1\,0 \\ 1\,0\,1\,0 \end{pmatrix} \quad T = F \oplus K = \begin{pmatrix} 0\,0\,1\,0 \\ 1\,1\,1\,0 \\ 0\,1\,0\,0 \\ 0\,0\,0\,1 \end{pmatrix}$$

+ Bước 2 : Tính S = SUM (T x W)

Trong đó X là phép nhân hai phần tử tương ứng của hai ma trận cùng bậc.

Phép SUM là dùng để tính tổng các phần tử của một ma trận .

Ví dụ:

Giả sử :

$$T \otimes W \quad \begin{pmatrix} 0\,0\,3\,0 \\ 1\,2\,5\,0 \\ 0\,1\,0\,0 \\ 0\,0\,0\,2 \end{pmatrix}$$

Thì SUM (T x W) = 3+1+2+5+1+2 =14

+ Bước 3 : Xây dựng tập :

$$Z_\alpha = \{ (j, k) \mid ([W]_{j,k} = \alpha \text{ và } [T]_{j,k} = 0) \text{ hoặc } ([W]_{j,k} = 2^r - \alpha \text{ và } [T]_{j,k} = 1)\}$$

Với mỗi số nguyên α thuộc khoảng từ 1 đến $(2^r - 1)$, tính được tập con tương ứng Z α . Khi đó tập Z là một tập hợp gồm $2^r - 1$ tập con. Mỗi tập Z α là một tập hợp chứa tất cả các chỉ số (j,k) của ma trận. Như vậy nếu thay đổi giá trị của phần tử thứ (j,k) trong ma trận F (thay 0 thành 1 , thay 1 thành 0) sẽ làm cho S tăng thêm α đơn vị (hiểu theo mod 2^r) . Thực tế , có hai khả năng để đạt được :

+ Nếu $[W]_{j,k}$= α và $[T]_{j,k = 0}$ thay đổi giá trị của phần tử $[F]_{j,k}$ thì S tăng thêm α đơn vị .

+ Nếu Nếu $[W]_{j,k}$= α và $[T]_{j,k =}$ 1 thay đổi giá trị của phần tử $[F]_{j,k}$ thì S giảm đi 2^r – α đơn vị hoặc theo mod 2^r thì S tăng thêm α đơn vị.

+ Bước 4:

Gọi F’ là khối ảnh sau khi đã giấu r bit thông tin vào F (F’ khác F tối đa hai phần tử) và S’ = (SUM (F’ + K) * W). Khi đó sẽ thực hiện giấu tin bằng cách thay đổi các bit trong F để biến F thành F’ sao cho đạt được bất biến : S’ = b (mod 2^r) (*)

Trong đó b = (b1b2b3……br) . Ví dụ nếu r = 8 và (b1b2b3…..b8) =11111111 thì b = 255 .

Đặt d = b- S (mod 2^r)

+ Trường hợp 1: Nếu d = 0 thì S = b mod 2^r . Do đó trong trường hợp này giấu được b vào F mà không cần biến đổi F tức là F’ = F và S’ = S

+ Trường hợp 2: Nếu d> 0 thì cần phải biến đổi F sao cho đạt được bất biến. Trong trường hợp này có 2 khả năng xảy ra.:

Nếu Z_d # Rỗng thì cần chọn một cặp (j,k) bất kỳ thuộc Z_d rồi thay đổi giá trị phần tử $[F]_{j,k}$ khi đó S sẽ tăng thêm d đơn vị (theo mod 2^r), do đó đã đạt được bất biến. Trong trường hợp này giấu được b vào trong F chỉ cần thay đổi 1 phần tử trong F.

Nếu Z_d = Rỗng thì thực hiện các bước sau :

Chọn h là số tự nhiên đầu tiên thỏa mãn Z_{hd} # Rỗng và $Z_{(1-h)d}$ # Rỗng .

Chọn cặp (j,k) bất kỳ thuộc Z_{hd} và thay đổi giá trị của phần tử $[F]_{j,k}$, khi đó S tăng thêm h * d .

Chọn cặp (u,v) bất kỳ thuộc Z- (h-1)d và thay đổi giá trị của phần tử $[F]_{u,v}$ khi đó S tăng thêm (1-h)*d = d- h*d

Vậy khi thay đổi giá trị $[F]_{j,k}$ và $[F]_{u,v}$ thì S tăng một lượng là h *d + d – h* d= d. Trong trường hợp này giấu b vào trong F, cần thay đổi tới hai phần tử trong F.

+ Trường hợp 3: Nếu d< 0 thì cần phải biến đổi F sao cho đạt được bất biến. Trong trường hợp này có hai khả năng xảy ra:

Nếu $Z_d + 2^r$ khác rỗng thì cần chọn cặp (j,k) bất kỳ thuộc $Z_d + 2^r$ rồi thay đổi giá trị phần tử $[F]_{j,k}$ khi đó S sẽ tăng d đơn vị (theo mod 2^r) do đó đã đạt được bất biến. Trong trường hợp này giấu được b vào trong F chỉ cần thay đổi một phần tử trong F.

Nếu $Z_d + 2^r$ = rỗng thì thực hiện các bước sau:

Chọn h là số đầu tiên thỏa mãn Z_{hd} khác rỗng và $Z_{(1-h)d} + 2^r$ khác rỗng

Chọn cặp (j,k) bất kỳ thuộc Z_{hd} và thay đổi giá trị của phần tử $[F]_{j,k}$, khi đó S tăng thêm h * d

Chọn cặp (u,v) bất kỳ thuộc $Z_{(1-h)d} + 2^r$ và thay đổi giá trị của phần tử $[F]_{u,v}$ khi đó S cũng tăng thêm (1-h)*d + 2^r = d- h*d + 2^r

Vậy khi thay đổi giá trị của hai phần tử $[F]_{j,k}$ và $[F]_{u,v}$, thì S tăng một lượng là h * d + d- d*h + 2^r = d + 2^r (theo mod 2^r) thì S tăng thêm d. Trong trường hợp này giấu b vào F, cần thay đổi đến hai phần tử trong F.

+ Bước 5

Khôi phục lại thông tin đã giấu. Khi người nhận được F’ từ người gửi và biết ma trận mặt nạ K, ma trận trọng số W người nhận chỉ cần tính S’ =

SUM (F' + K) x W => b = S' mod 2^r , từ đó xác định được dãy bít (b1b2…br) đã giấu trong F

Ví dụ :

$$F = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \quad K = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad W = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 5 & 1 \\ 2 & 1 & 4 & 0 \\ 4 & 3 & 6 & 2 \end{pmatrix}$$

$$T = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad S = SUM\,(T \times W) = 3 + 1 + 2 + 5 + 1 + 2 = 14$$

Giả sử cần nhúng một dãy bit 1010 vào trong F

Ta có L: r= 4, b = $2^3 + 2^1 = 10$;

Đặt d = b – S mod 2^r = 10 – 14 mod 2^4 = - 4

$Z_{d+2^r} = Z_{10}$ = rỗng.

Chọn h = -12/4

$Z_{h*d} = Z_1 = \{(1,1); (2,4)\}$ khác rỗng $Z_{(h-1)*d} + 2^r = Z_{11} = \{(2,3)\}$ khác rỗng.

$$F' = \begin{pmatrix} \mathbf{0} & 0 & 1 & 1 \\ 0 & 1 & \mathbf{0} & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

S' = SUM ((F' + K) x W) = 10

b = S' mod 2^4 = 10

2.2. HƯỚNG TIẾP CẬN THEO MIỀN TẦN SỐ.

Các thuật toán này sử dụng phương pháp biến đổi cosine rời rạc DCT để chuyển từng khối ảnh từ miền không gian ảnh sang miền tần số,. Thủy vân sẽ được nhúng trong miền không gian tần số của ảnh theo kỹ thuật trải phổ

trong truyền thông. Đây là kỹ thuật phổ biến nhất với nhiều thuật toán và là phương pháp có thể đảm bảo được tính mạnh mẽ và chính xác của thủy sau khi nhúng.

Kỹ thuật thủy vân trên miền tần số sử dụng các phương pháp biến đổi như Cosine rời rạc, biến đổi Fourier rời rạc, … để chuyển miền không gian ảnh sang miền tần số. Thủy vân sẽ được nhúng trong miền tần số của ảnh theo kỹ thuật trải phổ trong truyền thông, kỹ thuật này được đề xuất lần đầu tiên bởi Cox cùng cộng sự trong bài báo về "Thủy vân dựa trên trải phổ bảo vệ cho sự đa phương tiện" và đã được trích dẫn trong nhiều tài liệu. Đây là kỹ thuật phổ biến nhất với nhiều thuật toán được đề xuất và là phương pháp tốt giải quyết vấn đề về tính bền vững của thủy vân.

2.2.1 . Biến đổi cosin rời rạc (DCT)

Biến đổi cosin rời rạc DCT được đưa ra bởi Ahmed và các đồng nghiệp vào năm 1974. Từ đó đến nay, nó được sử dụng phổ biến trong nhiều kỹ thuật xử lý ảnh số nói riêng và xử lý tín hiệu số nói chung. Trong các kỹ thuật thủy vân ảnh dựa trên phép biến đổi dữ liệu ảnh sang miền tần số thì phép biến đổi DCT là được sử dụng nhiều. Nó được sử dụng chuẩn nén JPEG để mã hóa ảnh tĩnh và chuyển MPEG để mã hóa ảnh động.

Biến đổi DCT hai chiều tổng quát là biến đổi trong khối hai chiều bất kỳ M x N. Sau đây trình bày công thức biến đổi DCT2 chiều trên khối kích thước 8 x 8 được sử dụng nhiều nhất hoặc 16 x16

Công thức biến đổi DCT thuận từ I (k,l) -> I (u,v)

$$I(u,v) = \frac{C(u)C(v)}{4} \sum_{k=0}^{7} \sum_{l=0}^{7} I(k,l) \cos\left(\frac{(2k+1)u\pi}{16}\right) \cos\left(\frac{(2l+1)v\pi}{16}\right)$$

I (u,v) được gọi là hệ số DCT và là số thực.

Công thức biến đổi ngược IDCT từ I (u,v) -> I (k,l)

$$I(k,l) = \sum_{k=0}^{7}\sum_{l=0}^{7} \frac{C(u)C(v)}{4} I(u,v)\cos(\frac{(2k+1)u\pi}{16})\cos(\frac{(2l+1)v\pi}{16})$$

Ở đây 0 < = k, l,u, v <= 7

Phép biến đổi DCT ảnh hai chiều thể hiện đặc tính nội dung về tần số của thông tin ảnh. Hầu hết các thuật toán, ảnh gốc được chia thành các khối ma trận ảnh 8 x 8. Áp dụng biến đổi DCT cho mỗi khối ta sẽ thu được khối 8 x 8 chứa các hệ số DCT. Gọi C_b (j,k) là giá trị các hệ số trong đó b là số thứ tự của khối, (j,k) là vị trí của hệ số. Hệ số đầu tiên $C_b(0,0)$ được gọi là Dc và chứa thông tin độ sáng của khối đó. Các hệ số còn lại biểu diễn cho các thành phần tần số cao theo hướng ngang và theo hướng thẳng đứng gọi là hệ số AC

.

	Low	Horizontal						High
Low	1	2	6	7	15	16	28	29
	3	5	8	14	17	27	30	43
	4	9	13	18	26	31	42	44
	10	12	19	25	32	41	45	54
	11	20	24	33	40	46	53	55
	21	23	34	39	47	52	56	61
	22	35	38	48	51	57	60	62
High	36	37	49	50	58	59	63	64

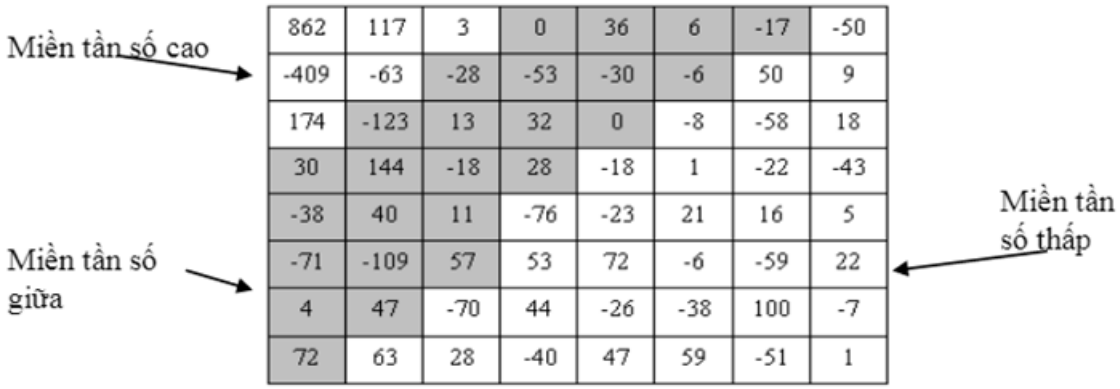
Hình 2.4 : Ví dụ bảng các hệ số DCT

Theo nguyên lý chung, khi biến đổi chi tiết giữa các điểm ảnh càng lớn theo một hướng nào đó trong khối các điểm ảnh (hướng ngang, hướng thẳng đứng hay theo hướng đườngchéo) thì các hệ số biến đổi DCT tương ứng cũng lớn.

Tóm lại, DCT làm giảm độ tương quan không gian của thông tin trong khối ảnh. Điều đó, cho phép biểu diễn thích hợp ở miền DCT do các hệ số DCT có xu hướng có phần dư thừa ít hơn. Hơn nữa, các hệ số DCT chứa

thông tin về nội dung tần số không gian của thông tin trong khối. Nhờ các đặc tính tần số không gian của hệ thống nhìn của mắt người, các hệ số DCT có thể được mã hóa phù hợp, chỉ các hệ số DCT quan trọng nhất mới được mã hóa để truyền đi.

Khối hệ số DCT có thể chia thành ba miền ; miền tần số thấp, miền tần số giữa và miền tần số cao. Miền tần số thấp chứa các thông tin quan trọng ảnh hưởng đến tri giác. Các thông tin trong miền tần số cao thường không mang tính tri giác cao, khi nén JPEG thì thường loại bỏ thông tin trong miền này

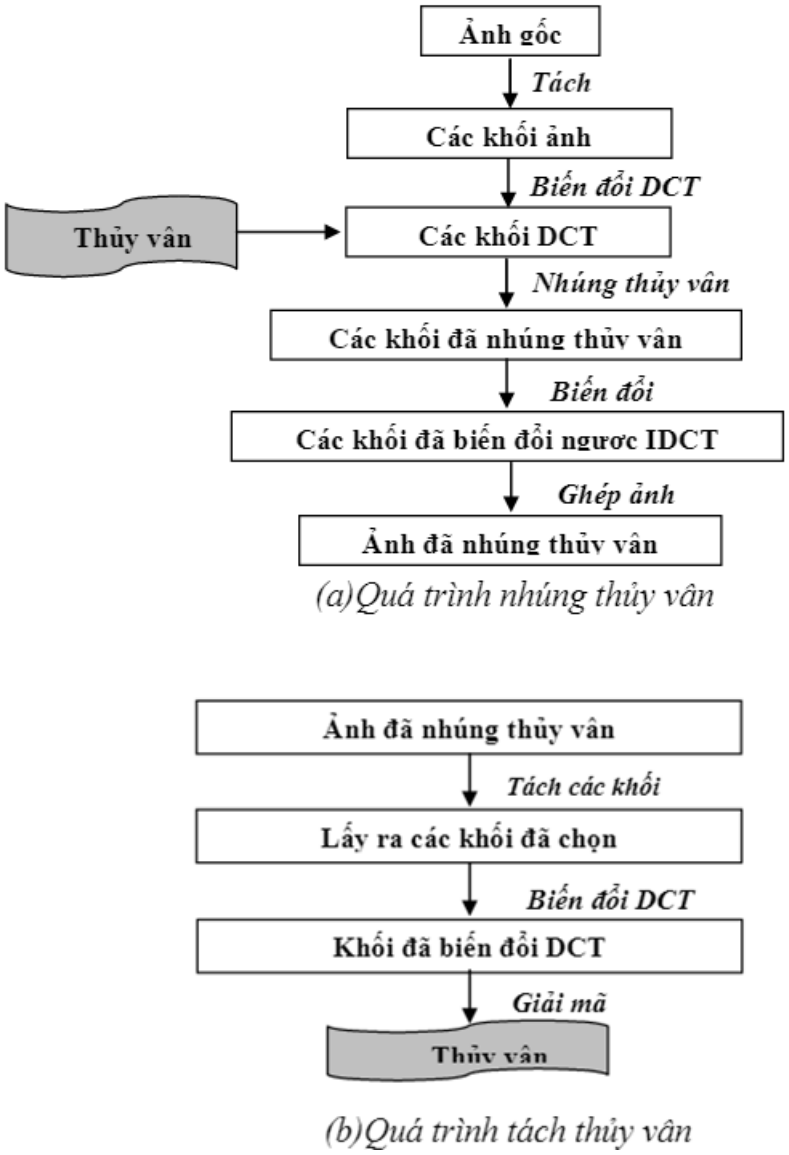


862	117	3	0	36	6	-17	-50
-409	-63	-28	-53	-30	-6	50	9
174	-123	13	32	0	-8	-58	18
30	144	-18	28	-18	1	-22	-43
-38	40	11	-76	-23	21	16	5
-71	-109	57	53	72	-6	-59	22
4	47	-70	44	-26	-38	100	-7
72	63	28	-40	47	59	-51	1

Hình 2.5: Phân chia 3 miền tần số thấp giữa, cao của phép biến đổi DCT.

Trong các thuật toán thủy vân, miền hệ số DCT tần số cao thường không được sử dụng do nó thường không bền vững với các phép xử lý ảnh hoặc nén ảnh JPEG. Miền tần số thấp cũng khó được sử dụng do một sự thay đổi dù nhỏ trong miền này cũng ảnh hưởng đến chất lượng tri giác của ảnh. Vì vậy, miền tần số ở giữa thường hay được sử dụng nhất và cũng cho kết quả tốt nhất.

Thủy vân trên miền DCT là một kỹ thuật được sử dụng phổ biến với nhiều thuật toán. Nhìn chung, các thuật toán đều thực hiện các bước giống nhau trong quy trình nhúng và tách thủy vân như hình 2.6. Tuy nhiên, các thuật toán khác nhau thì khác nhau về cách lựa chọn vị trí nhúng thủy vân và phương thức nhúng.



Hình 2.6: Quy trình nhúng và tách thủy vân theo kỹ thuật thủy vân trên miền DCT

2.2.1.1. Thuật toán DCT1

Thuật toán được nhóm tác giả Nguyễn Xuân Huy và Trần Quốc Dũng đưa ra trên bài báo : "Một thuật toán thủy vân trên miền DCT - An Image Watermarking Algorithm Using DCT domain ". Nội dung bài viết đề xuất một thuật toán nhúng thủy vân vào trong ảnh sao cho thỏa mãn các tính chất và yêu cầu của một hệ thủy vân trên ảnh số. Thuật toán chọn miền tần số để giấu tin nhằm nâng cao tính bền vững của thủy vân.

*** Mô tả thuật toán**

- input :

+ Một chuỗi các bit thể hiện bản quyền

+ Một ảnh.

- out put

+ Một ảnh sau khi thủy vân . Khóa để giải mã

*** Quá trình thủy vân**

- Chia ảnh có kích thước m x n thành (mxn)/64 khối 8x 8 , mỗi bit sẽ được giấu trong một khối.

- Chọn một khối bất kì B và biến đổi DCT khối đó thu được B'

- Chọn hai hệ số ở vị trí bất kì trong miền tần số ở giữa của khối DCT, giả sử đó là b '(i,j) và b' (p,q). Ta tính :

$$d = \| b'(i,j) - b'(p,q) \| \bmod a$$

trong đó a là một tham số thỏa mãn điều kiện a = 2 (2t +1), t là một số nguyên dương.

Bít s_i sẽ được nhúng sao cho thỏa mãn điều kiện sau:

$$\begin{cases} d >= 2t+1 & \text{nếu } s_i = 1 \\ d < 2t+1 & \text{nếu } s_i = 0 \end{cases}$$

- Nếu d < 2t + 1 và s_i = 1 thì một trong hai hệ số DCT b'(i,j) hoặc b'(p,q) có trị tuyệt đối lớn hơn sẽ bị thay đổi để d > = 2t + 1 theo công thức sau:

$$max(|b'(i,j)|, |b'(p,q)|) + (INT(0,75 *a) - d)$$

Với hàm max (|b'(i,j) | , |b'(p,q)|) là hàm chọn ra hệ số có trị tuyệt đối lớn hơn, hệ số được chọn sẽ được cộng thêm một lượng là INT (0,75 *a) – d .

Hoặc cũng có thể biến đổi một trong hai hệ số theo công thức

$$min(|b'(i,j)|, |b'(p,q)|) - (INT(0,25 *a) + d)$$

Với hàm min (|b'(i,j) | , |b'(p,q)|) là hàm chọn ra hệ số có trị tuyệt đối nhỏ hơn, hệ số được chọn sẽ bị trừ đi một lượng là INT (0,25 *a) + d .

INT () là hàm làm lấy phần nguyên của một số thực.

- Tương tự, nếu d > = 2t + 1 và s_i = 0 thì một trong hai hệ số DCT b'(i,j) hoặc b'(p,q) có giá trị tuyệt đối lớn hơn sẽ được thay đổi để thõa mãn d < 2t + 1 như sau :

$$max(|b'(i,j)|,|b'(p,q)|) - (d - INT(0,25*a))$$

Với hàm max (|b'(i,j) | , |b'(p,q)|) là hàm chọn ra hệ số có trị tuyệt đối lớn hơn, hệ số được chọn sẽ bị trừ đi một lượng là INT d – INT (0,25 *a).

Hoặc

$$min(|b'(i,j))|,|b'(p,q)|) + INT(1,25*a) - d$$

- **Quy trình trích để lấy lại thông tin** :
  - In put : + Một ảnh đã nhúng thủy vân
    + khóa để giải mã
  - Out put

Thủy vân là một dãy bit đã nhúng

Thực hiện : Đọc khối DCT từ ảnh chứa thủy vân và vị trí hai hệ số đã biến đổi, sau đó tính:

$$d = ||b'(i,j)|-|b'(p,q)|| \ mod \ a \text{ với } (a = 2(2t+1))$$

Nếu d >= 2t+1 thì gán si =1

Nếu d<2t +1 thì gán si = 0

2.2.1.2. Thuật toán DCT 2

*** Mô tả thuật toán**

Cùng ý tưởng nhúng thủy vân vào miền tần số giữa của khối biến đổi cosin rời rạc, tác giả chris Shoemarker đã sử dụng phép biến đổi DCT để phân tích khối được chọn từ ảnh gốc thành các miền tần số, rồi chọn một cặp hệ số

trong miền tần số giữa để thực hiện quá trình nhúng một bit thủy vân. Quá trình nhúng luôn bảo đảm sau khi nhúng bit thủy vân thì khoảng cách về giá trị giữa hai hệ số được chọn có giá trị lớn hơn hoặc bằng k cho trước.

- **Quá trình thủy vân**

Thủy vân là một chuỗi các bit hoặc một ảnh nhị phân được nhúng vào ảnh gốc. Ảnh gốc có kích thước m x n sẽ được chia thành m x n / 64 khối 8 x 8 , mỗi bit của thủy vân sẽ được nhúng trong một khối .

Chọn một khối ảnh gốc Fi , thực hiện phép biến đổi DCT với Fi để được Fi'

Chọn hai hệ số thuộc miền tần số giữa của Fi', giả sử đó là Fi'(u,v) và Fj '(p,q), đọc thủy vân cần nhúng giả sử đó là s_i

Nếu bit cần nhúng $s_i = 0$ và nếu Fi' (u,v) < Fi' (p,q) thì đổi chỗ hai hệ số này.

Nếu bit cần nhúng $s_i = 1$ và nếu Fi' (u,v) >= Fi' (p,q) thì đổi chỗ hai hệ số này.

Nếu Fi' (u,v) > Fi' (p,q) và nếu Fi' (u,v) - Fi' (p,q) < k thì tăng Fi' (u,v) đồng thời giảm Fi' (p,q) k/2 lần.

Nếu Fi' (u,v) <= Fi' (p,q) và nếu Fi' (p,q) - Fi' (u,v) < k thì tăng Fi' (p,q) đồng thời giảm Fi' (u,v) k/2 lần

Dùng phép biến đổi ngược IDCT với mỗi khối đã nhúng thủy vân Fi' . Ghép các khối ảnh để được ảnh đã nhúng thủy vân.

- **Quá trình trích để lấy lại thông tin :**

Đọc vào khối DCT đã nhúng thủy vân Fi' và vị trí hai hệ số đã biến đổi (u,v) và (p.q) , sau đó tính k = Fi' (u,v) – Fi' (p,q) .

Nếu k > 0 thì gán $s_i = 0$

Nếu k < 0 thì gán $s_i = 1$

Ghép dãy bit s_i để được thủy vân đã nhúng.

- **Nhận xét**

Sau khi thử nghiệm cho thấy, hệ thống thủy vân trên đáp ứng tốt tính chất bảo đảm tính bền vững của thủy vân trước đa số các phép biến đổi ảnh thông thường. Hệ số k được gọi là hệ số tương quan giữa tính ẩn của thủy vân với tính bền vững của thủy vân. Hệ số k càng lớn, tính bền vững của thủy vân càng cao, đồng thời chất lượng ảnh sau khi nhúng thủy vân ẩn bền vững đó là mâu thuẫn giữa chất lượng thương mại của ảnh sau khi nhúng thủy vân với tính bền vững của thủy vân trước các tấn công. Trong thực tế, có thể xây dựng một hệ thống thủy vân với đề xuất về thông số giữa việc chọn hệ số k, chất lượng ảnh sau khi nhúng thủy vân và đồ bền vững của thủy vân trước các tấn công để người sử dụng tùy theo mục đích mà lựa chọn các thông số phù hợp.

Khóa để giải mã trong việc phát hiện thủy vân gồm kích thước khối và vị trí cặp hệ số được chọn trong khối. Do đó, độ phức tạp của việc dò tìm thủy vân khi không biết khóa phụ thuộc rất nhiều vào kỹ thuật chọn cặp hệ số trong quá trình nhúng thủy vân. Có thể chọn cố định một cặp số cho tất cả các khối, cũng có thể chọn vị trí thay đổi cho mỗi khối , khi đó vị trí tương ứng cảu cặp hệ số trong mỗi khối sẽ là một phần trong khóa để phát hiện thủy vân.

Quá trình tách thủy vân không cần sử dụng ảnh gốc.

2.2.1.3 Thuật toán DCT3

*** Mô tả thuật toán :**

Trong thuật toán DCT3 này tác giả BenHam lựa chọn vị trí nhúng tin có sự loại bỏ các khối không phù hợp. Các khối bị loại bỏ là các khỏi nhẵn hoặc khối sắc không cao.

Các khối được chọn nhúng thủy vân là các khối sắc lớn.

Khối nhẵn : chúng ta có thể phát hiện ra các khối này bằng cách đếm số lượng hệ số cao tần có giá trị là “0”. Nếu tất cả các hệ số này hay chỉ cần tồn tại ít nhất 1 hệ số ở nửa trên đường zig zắc bằng “0’ thì khối đó được xem là khối nhẵn.

Khối sắc : Được phát hiện bằng cách tìm giá trị tuyệt đối lớn nhất của hệ số AC tần số thấp. Ngưỡng được sử dụng là 100.

Thuật toán sử dụng 3 hệ số để nhúng 1 bit.

- **Quá trình thủy vân :**

Để nhúng bit s_i vào trong khối, 3 hệ số chọn ngẫu nhiên

$$c_b(j_{i,1},k_{i,1}),\ c_b(j_{i,2},k_{i,2}),\ c_b(j_{i,3},k_{i,3})$$

$$|c_b(j_{i,1},k_{i,1})| - |c_b(j_{i,2},k_{i,2})| > \varepsilon \text{ nếu } s_i=0$$

$$|c_b(j_{i,1},k_{i,1})| - |c_b(j_{i,2},k_{i,2})| < \varepsilon \text{ nếu } s_i=1$$

$$|c_b(j_{i,2},k_{i,2})| - |c_b(j_{i,3},k_{i,3})| > \varepsilon \text{ nếu } s_i=0$$

$$|c_b(j_{i,2},k_{i,2})| - |c_b(j_{i,3},k_{i,3})| < \varepsilon \text{ nếu } s_i=1$$

47

$$|c_b(j_{i,1},k_{i,1})| - |c_b(j_{i,3},k_{i,3})| > \varepsilon \text{ nếu } s_i=0$$

$$|c_b(j_{i,1},k_{i,1})| - |c_b(j_{i,3},k_{i,3})| < \varepsilon \text{ nếu } s_i=1$$

Nếu thay đổi một trong 3 hệ số là quá lớn thì đơn giản là bỏ qua khối đó và bit đó sẽ được nhúng vào khối tiếp theo. H là hệ số có giá trị cao nhất trong 3 hệ số, M là hệ số ở giữa, L là hệ số thấp nhất.

Bit thủy vân	$c_b(j_{i,1},k_{i,1})$	$c_b(j_{i,2},k_{i,2})$	$c_b(j_{i,3},k_{i,3})$
1	H	M	L
1	M	H	L
1	H	H	L
0	M	L	H
0	L	M	H
0	L	L	M
Bỏ qua	H	L	M
Bỏ qua	L	H	M
Bỏ qua	M	M	M

- **Quá trình trích để lấy lại thông tin:**

Lặp lại các vị trí nhúng tương ứng và các hệ số đã chọn. Lấy thủy vân theo điều kiện

$s_i = 0$ *nếu* $|c_b(j_{i,1}, k_{i,1})| > |c_b(j_{i,2}, k_{i,2})|$

$s_i = 1$ *nếu* $|c_b(j_{i,1}, k_{i,1})| < |c_b(j_{i,2}, k_{i,2})|$

- **Nhận xét**

Độ trung thực của ảnh thủy vân bằng thuật toán này cao do thuật toán sử dụng 3 hệ số thỏa mãn ràng buộc để nhúng 1 bit nên khó phát hiện sự thay đổi của ảnh .

2.2.2.Biến đổi Fourier rời rạc.

2.2.2.1.Phép biến đổi Fourier rời rạc

1/. Biến đổi DFT một chiều

Biến đổi Fourier 1-D cho tín hiệu thời gian rời rạc f (kT) theo công thức:

$$F(n) = \sum_{k=0}^{N-1} f(kT) e^{-j2\pi/N nk}$$

Công thức này có thể viết lại dưới dạng

$$F(n) = \sum_{n=0}^{N-1} f(k) W_N^{-nk}$$

ở đây f(k) = f(kT) và $W_N = e^{-j2/N}$. W_N = được gọi là hạt nhân của phép biến đổi.

Tổng quát, F (n) có dạng :

$$F(n) = A(n)\, e^{j\phi(n)}$$

Kí hiệu A (n) , ϕ (n) gọi là phổ khuyếch đại và phổ pha của F (n)

2/.Biến đổi ngược DFT

Hàm f(k) là biến đổi người DFT của F (n) cho bởi theo biểu thức

$$f(k) = \frac{1}{N} \sum_{n=0}^{N-1} F(n) e^{j\frac{2\pi}{N} nk}$$

Chứng minh : Từ định nghĩa của DFT

$$\frac{1}{N}\sum_{n=0}^{N-1}F(n)W_N^{nk} = \frac{1}{N}\sum_{n=0}^{N-1}\left[\sum_{m=0}^{N-1}f(m)W_N^{-nm}\right]W_N^{kn}$$
$$= \frac{1}{N}\sum_{m=0}^{N-1}f(m)\sum_{n=0}^{N-1}W_N^{n(k-m)} \qquad (2.1)$$

Đặt $S = \sum_{n=0}^{N-1}W_N^{n(k-m)}$

Nếu (k=m) thì S = N

Nếu (k # m) chúng ta có thể viết :

$$S = 1 + W_N^{(k-m)} + W_N^{2(k-m)} + \ldots + W_N^{(N-1)(k-m)}$$

Hoặc

$$S = \frac{1 - W_N^{N(k-m)}}{1 - W_N^{(k-m)}}$$
$$= \frac{1 - e^{j(2\pi(k-m))}}{1 - e^{j\cdot\frac{2\pi}{N}\cdot(k-m)}}$$

Khi $e^{j2\pi(k-m)} = 1$ và $e^{j2\pi N(k-m)} \# 1$ với (k# m), vì vậy S = 0 với (k # m).

Vì vậy, biểu thức (2.1) có thể rút gọn thành

$$\frac{1}{N} = \sum_{n=0}^{N-1}F(n)W_N^{nk} = \frac{1}{N}f(k).N$$

Kết quả này giống như biểu thức

Khi f(k) có thể rút ra từ F(n) và ngược lại, chúng gọi là cặp biến đổi. Cặp biến đổi có dạng :

$$f(k) \Leftrightarrow F(n)$$

Mặc dù f(k) được xác định trên miền k € [0, N] , nó vẫn tín hiệu tuần hoàn với chu kỳ NT.

3/.Biến đổi DFT hai chiều

Một DFT hai chiều của tín hiệu lấy mẫu hai chiều h (k1, k2) cho bởi

$$H(n_1,n_2)=\sum_{k_1=0}^{N-1}\sum_{k_2=0}^{N-1}h(k_1,k_2)e^{-j2\pi/N.(n_1k_1+n_2k_2)}$$
$$=DFT\{h(k_1,k_2)\}$$

ở đây , n_1 = 0,1,2,…. N-1

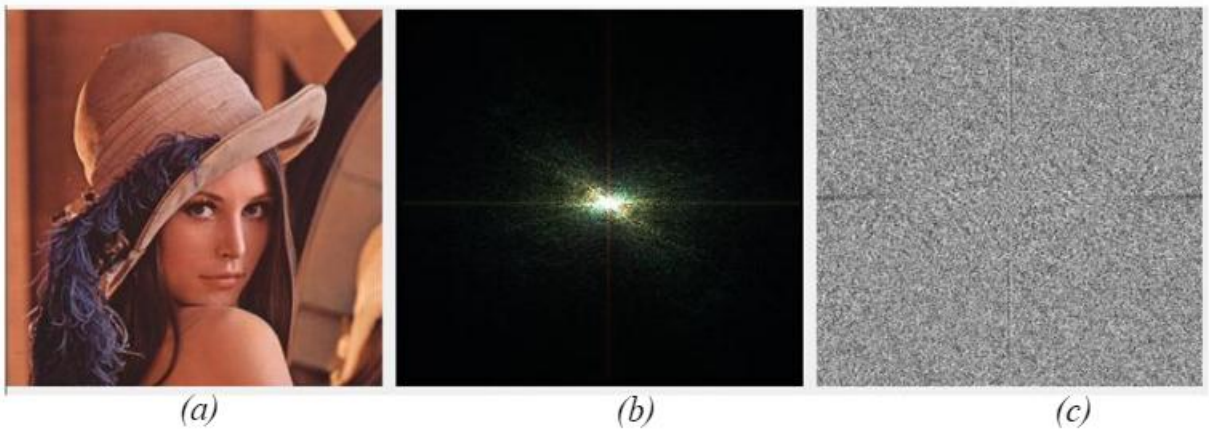
n_2 = 0,1,2,…. N-1

Biểu thức $e^{-j2\pi/N(n1k1+n2k2)}$ trong hai dấu tổng gọi là hạt nhân của phép biến đổi. H (n1,n2) , trong trường hợp tổng quát, đầy đủ có thể biểu diễn theo : H (n1, n2) = A (n1,n2) $e^{j\phi(n1,n2)}$

Trong không gian ba chiều A (n1, n2) và ϕ (n1, n2) nằm tại vị trí n1 và n2 và gọi là phổ tần và phổ pha của H (n1, n2) .

Hàm h (k1, k2) là biến đổi ngược 2 – D DFT (IDFT) của hàm H (n1, n2) và được cho bởi biểu thức

$$h(k_1,k_2)=\frac{1}{N^2}\sum_{n_1=0}^{N-1}\sum_{n_2=0}^{N-1}H(n_1,n_2)e^{j2\pi/N.(n_1k_1+n_2k_2)}$$



(a) (b) (c)

Hình 2.7: Ảnh gốc Lena.bmp b Ảnh biên độ . c. Phổ pha .

2.2.2.2.Lược đồ thủy vân sử dụng biến đổi DFT

1/. Kỹ thuật thủy vân sử dụng hệ số giá trị đỉnh trong DFT

Trong phương pháp thủy vân được trình bày , trước tiên ta dịch chuyển điểm tần số không F(0,0) tới trung tâm của miền tần số DFT và nhúng "thủy vân" vào khoảng vòng ở giữa dải thông . Kí hiệu B chỉ tần số con, trong miền DFT giữa hai vòng có bán kinh được lựa chọn trước R_1 và R_2 trong đó $R_1 < R_2$ như hình 2.18 và hình 2.19 .

Tiếp theo, ta chia B theo n đường tròn đồng tâm có khoảng cách đều nhau với bán kinh tăng dần $r_1, r_2 ..... r_n$ và mỗi đường viền vào m góc sắp thứ tự $\theta_1, \theta_2, ... \theta_m$. như hình 2.19 . Sau đó, để nhúng thủy vân ta chọn n x m vị trí $P = \{p_1, p_2 ..... p_{nx\,m}\}$, gọi là vị trí có thể nhúng, trong miền tần số với tọa độ được mô tả bởi

$$p_k = (u_k, v_k) = (r_i \cos\theta_j, r_i \sin\theta_j), \qquad (2.2)$$

Trong đó, $1 \le i \le n$, $1 \le j \le m$, và $1 \le k \le l$ với $l = n \times m$

Chúng ta điều chỉnh giá trị hệ số của một số những vị trị thành đỉnh cục bộ trong miền tần số, để tạo thành thủy vân theo cách được mô tả ở bước tiếp theo

Trước tiên, chúng ta lựa chọn số h của đỉnh, là một trong số l vị trí có thể được sử dụng để nhúng "thủy vân" W (là chuỗi số được lựa chọn trước và giá trị dương w). Những đỉnh có thể được xem xét để nhúng thủy vân w

Để quyết định đỉnh nào nên sử dụng, một tổ hợp các thao tác được thực hiện để lấy tất cả các mã có thể R = {r1, r 2, ….. r g}. Với mỗi mã r i chỉ định một tập hợp của h vị trí, trong đó g = C (l,h) với C (l,h) là số tổ hợp, có nghĩa là số cách lựa chọn h từ l khả năng có thể xảy ra. Trong thuật toán, chúng ta chọn h = l/2 bởi vì C (l,h) sẽ tạo ra giá trị lớn nhất cho trường hợp cụ thể l = m x n.

Ví dụ , nếu l = 4 và h = 2, chúng ta có P = {p1, p2, p3, p4} và g = C (4,2) = 6 điều đó có nghĩa rằng chúng ta có 6 mã có thể R = {r1, r 2, ….. r 6} được sử dụng cho thủy vân, trong đó $r_1 = \{p_1, p_2\}$, $r_2 = \{p_1, p_3\}$, $r_3 = \{p_1, p_4\}$, $r_4 = \{p_2, p_3\}$, $r_5 = \{p_2, p_4\}$, $r_6 = \{p_3, p_4\}$

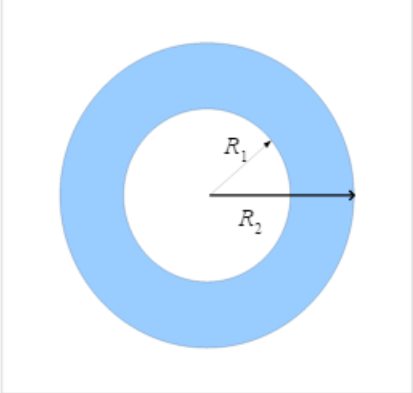
Sau khi, lựa chọn một thủy vân W với giá trị nguyên w không lớn hơn g, chúng ta nhận được mã r_w trong R và chỉnh sữa giá trị hệ số M (u_k, v_k) của vị trí nhúng tương ứng p_k cụ thể bởi r_w tạo thành đỉnh cục bộ M ‘ (u_k, v_k) theo công thức sau : M ‘ $(u_k, v_k) = M (u_k, v_k) + c$ (2.3)

Trong đó, c là hằng số để xác định năng lượng của thủy vân

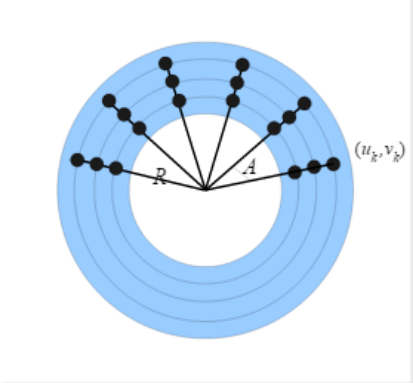
Chú ý rằng, khi thay đổi giá trị hệ số tạo thành đỉnh tại mỗi $p_k = (u_k, v_k)$ bởi một lượng c, chúng ta phải giữ thuộc tính đối xứng dương của DFT, bằng việc thay đổi giá trị hệ số tương ứng tại $p'_k = (-u_k, -v_k)$ cùng số lượng c. Mặt khác, đỉnh tạo ra tại p_k sẽ được trung hòa bằng việc không thay đổi gia trị hệ số đối xứng tại p_k ‘ sau khi biến đổi nghịch đảo DFT. Đó là công việc chúng ta phải thực hiện theo công thức sau :

$$M' ((-u_k, -v_k) = M (-u_k, -v_k) + c$$

Tại mỗi thời điểm khi chúng ta thực hiện phép toán ở công thức :



Hình 2.8: một miền vành đai giữa dải tần.



Hình 2.9: Miền vành đai chia thành những đường tròn đồng tâm và chia góc

2/. Kỹ thuật đồng bộ vị trí đỉnh để chống lại tấn công xoay và co dãn

Để chống lại dạng tấn công xoay và co dãn , một mở rộng cục bộ P_s được gọi là đồng bộ hóa đỉnh, được tạo ra trong miền biến đổi DFT như là một tin hiệu để đồng bộ hóa các vị trí đỉnh P = {p 1, p2.,…. P mxn} đã được đề cập trước đây theo cách sau .

P_s được nhúng vào trong dải tần trung bình B được mô tả bởi công thức :

$$p_s = (u_s, v_s) = (r_s \cos\theta_s, r_s \sin\theta_s)$$

Trong đó r_s được lựa chọn lớn hơn R_2 (bán kính ngoài của dải tần B) và θ_s là góc được lựa chọn trước. Chúng ta điều chỉnh giá trị DCT của P_s và dạng đối xứng của nó thành giá trị đỉnh bởi công thức 2.3 và 2.4

Chúng ta sẽ sử dụng đỉnh đồng bộ P_s như thế nào trong quá trình trích xuất thủy vân để tính toán góc xoay của một bức ảnh phủ (stego - image) đã bị tấn công bằng phương pháp xoay . Như đã đề cập về thuộc tính DFT trước đây nếu ảnh phủ bị xoay thì vị trí của P_s sẽ bị thay đổi theo với cùng một góc xoay.

Chúng ta sẽ phải tính toán đầu tiên là góc mới θ'_s của P_s và sự khác nhau giữa θ'_s và θ_s để xác định xem ảnh phủ có bị xoay hay không :

Nếu $\Delta\theta \neq 0$ thì ảnh đã bị xoay, ngược lại thì không. Nếu bị xoay thì chúng ta sẽ phải đi tìm góc θ_k' của những đỉnh cục bộ khác và tính toán góc nguyên mẫu của chúng bở công thức

$$\theta_k'' = \theta_k' - \Delta\theta$$

Mặt khác, như đã đề cập trước đây, nếu một ảnh phủ được cấu trúc lại, giá trị hệ số DFT hầu như không bị ảnh hưởng. Điều đó có nghĩa rằng bán kính của đỉnh cục bộ sẽ không thay đổi.

3/.Quá trình nhúng thủy vân

Trong quá trình nhúng thủy vân, đầu tiên chúng ta chia hình ảnh đầu vao thành các khối vuông M x M được chọn trước, trong đó M là lũy thừa cơ số 2 . Tiếp theo, chúng ta sử dụng phép biến đổi Fourier nhanh trong hệ cơ số

2 để biến đổi hình ảnh đầu vào trong miền DFT nhanh hơn. Sau đó, chúng ta sử dụng miền DFT của các kênh màu đỏ và màu xanh của hình ảnh đầu vào để nhúng một chuỗi số thủy vân. Thủy vân được chuyển đổi thành một dòng bit và sau đó được chia thành hai nửa. Mỗi nửa được chuyển trở lại được một số nguyên như là một phần của thủy vân để được nhúng vào một trong các kênh màu đỏ và màu xanh theo ý tưởng mô tả trong phần trước. Thuật toán chi tiết của quá trình này được mô tả như sau :

*** Đầu vào :**

Một ảnh mầu C và một thủy vân W

*** Đầu ra :**

Một ảnh mang tin S.

*** Qui trình nhúng thủy vân**

+ Bước 1: Thay đổi tỷ lệ C để nhận được một ảnh C ‘ kích thước M x M . Trong đó M là lũy thừa cơ số 2.

+ Bước 2 : Biến đổi kênh màu đỏ và xanh da trời của C ‘ trong miền tần số bởi biến đổi DFT để nhận được C_r’ và C_b ‘

+ Bước 3 : Biến đổi W thành dãy nhị phân, chia kết quả nhận được thành hai con, và biến đổi chúng thành hai số nguyên W_r và W_b

+ Bước 4: Nhúng W_r và W_b như một thủy vân W’ vào C_r’ và C_b ‘ , tương ứng bằng cách thực hiện thao tác sau :

4.1 Chia tập hợp bán kính R = {r1,r2,…..rn}cho n đường tròn đồng tâm cách đều nhau có viên trong dải thông trung bình B của miền tần số giữa giữa hai đường tròn được lựa chọn trước có bán kính R_1 và R_2 với $R_1 < R_2$.

4.2 Chia m góc $O = \{\theta_1, \theta_2, \ldots \theta_m\}$ thành các khoảng đều nhau từ 0 đến 180^o. Ngoài ra, lấy l = m x n .

4.3 Thu được l vị trí nhúng $P = \{p_1, p_2, \ldots p_l\}$ với p_k (k = 1,2,3…. l) tại $(r_i\cos\theta_j, r_i\sin\theta_j)$ trong I và j thõa mãn k = (i-1)x m + j và

những vị trí đối xứng của chúng Q = $\{q_1, q_2, \ldots q_l\}$ với mỗi q_k đối xứng với p_k.

4.4 Áp dụng tổ hợp các phép toán được đề cập trước đây để nhận được g mã R = $\{r_1, r_2, \ldots r_g\}$ với mỗi r_k (k = 1,2,…. .g) chỉ rõ một tập hợp vị trí đỉnh, trong đó g = C (l, h) với h = l/2 .

4.5 Theo giá trị w của W' , lấy r_w ở ngoài R và điều chỉnh giá trị hệ số vị trị bên trong r_w và vị trí đối xứng của nó được tính bởi công thức (2.3) và 2.4

4.6 Thêm đỉnh đồng bộ hóa P_s theo lược đồ mô tả trong phần trên.

+ Bước 5 : Biến đổi C'_r và C'_r trở lại vào miền tần số bằng phép biến đổi ngược DFT

+ Bước 6: Thay đổi tỷ lệ C' với kích thước nguyên mẫu của C.

+ Bước 7 : Kết quả thu được ảnh có chứa thủy vân S

4/.Quá trình trích xuất thủy vân

Trong quá trình trích xuất, ảnh chứa tin được thay đổi tỷ lệ thành một ảnh các khối vuông kích thước Mx M được chọn trước, trong đó M là một số trong hệ cơ số 2 số như đã đề cập trước đó. Các kênh màu đỏ và màu xanh da trời được biển đổi trong miền DFT được sử dụng bằng cách FFT . Do thuộc tính đối xưng của giá trị hệ số của DFT, chúng ta chỉ cần tìm kiếm đỉnh cục bộ trong vùng trên của nữa ảnh phổ Fourier . Sauk hi thu thập tất cả các đỉnh, việc tìm kiếm đỉnh có bán kính dài nhất được thực hiện để có sự đồng bộ đỉnh P_s, đỉnh mà sau đó được sử dụng để đồng bộ hóa vị trí các đỉnh. Sau đó, các góc của các đỉnh h còn lại trong P = $\{p_1, p_2, \ldots p_n\}$ được tạo bởi biểu thức để nhận được vị trí mới của chúng p ' = $\{ p_{1'}, p_{2'}, \ldots p_{n'} \}$.

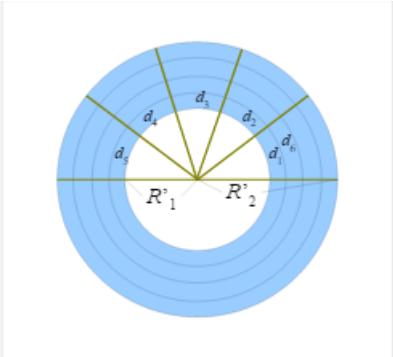
Ngoài ra , chúng ta tách riêng khu vực dải tần số trung bình B bởi hai vòng tròn với bán kinh lần lượt là R_1 và R_2 vào n đường tròn đồng tâm cách đều và vào m khoảng gốc để làm cho B trở thành một tập hợp của l cung D =

$\{d_1, d_2, \ldots\ldots d_l\}$ trong đó l = m x n . Sau đó P' và D được so sánh để rút ra h cung tạo thành một tập hợp A theo cách sau :

k= 1,2,3,….. l và i= 1,2,….. h

Nếu $p_{i'}$ rơi vào cung d_k , đưa d_k vào trong A.

Điều này, có nghĩa rằng nếu có một đỉnh trong một vùng d_k, d_k được đua vào A. Cuối cùng, chúng ta sử dụng tính toán tổ hợp với D và h như là đầu vào để nhận được g mã phù hợp $R = \{r_1, \ldots\ldots r_g\}$, trong đó g = C (l, h) với h = l/2 . Sau đó, chúng ta kiểm tra nếu có bất kỳ r'_j mà là bằng A với $1 \leq j \leq g$, thì số nguyên j là sau đó lấy như là giá trị trích xuất thủy vân và hoàn tất quá trình trích xuất.



Hình 2.10 : Dải tần số trung bình đượcchia thành các cung đồng tâm.

- **Đầu vào :**

  Một ảnh chứa thủy vân S

- **Đầu ra :**

  Một thủy vân W

- **Quy trình tách thủy vân :**

+ Bước 1: Thay đổi tỷ lệ S để nhận được ảnh khối vuông S' kích thước M x M , trong đó M là một số trong hệ cơ số 2 .

+ Bước 2: Biến đổi kênh màu đỏ, màu xanh da trời của S' trong miền tần số để nhận được phổ Fourier của S'_{red} và S'_{blue}

+ Bước 3: Tìm kiếm đỉnh trong phần nửa trên của S'_{red} và S'_{blue} tương ứng bởi các thao tác sau

3.1 Sử dụng một giá trị ngưỡng điều chỉnh T để tìm kiếm đỉnh trong miền tần số trung bình theo phương pháp được mô tả.

3.2 Lựa chọn đỉnh có bán kính dài nhất làm đỉnh đồng bộ hóa, và tính toán góc thay đổi $\Delta\theta$ của nó với góc nguyên gốc của đỉnh đồng bộ hóa.

3.3. Xây dựng lại các góc của h đỉnh còn lại bằng công thức 2.6 để nhận được vị trí mới của chúng $P' = \{p_1', \ldots\ldots p_h'\}$.

3.4 . Chia dải tần số trung bình giữa R_1 và R_2 thành n đường tròn đồng tâm khoảng cách đều nhau và m góc làm cho dải tần trung bình trở thành l cung $D = \{d_1, \ldots\ldots d_l\}$, trong đó $l = m \times n$

3.5 So sánh P ‘ và D để lựa chọn h vùng cho tập hợp A theo cách chỉ ra bởi công thức 2.7

3.6 Áp dụng một tổ hợp tính toán để nhận được g mã $R' = \{r'_1, \ldots\ldots r'_n\}$, với mỗi mã r'_j (j = 1,2,…., g) chỉ rõ một tập h vùng của D, trong đó g = C (l,h). Sau đó, kiểm tra nếu bất kì r'_j bằng với A với $1 \leq j \leq g$. Thì j là chuỗi số cần tìm.

+ Bước 4 : Liên kết hai chuỗi số nhị phân tạo ra từ S'_{red} và S'_{blue}

+ Bước 5: Biến đổi dãy bit đã liên kết thành chuỗi số.

+ Bước 6: Kết quả thu được là thủy vân W.

2.2.3.Thuật toán thủy vân dựa trên miền DWT.

2.2.3.1.Phép biến đổi sóng rời rạc.

Trong phép biến đổi này, Wavelets là các hàm được định nghĩa trong khoảng hữu hạn và có giá trị trung bình bằng 0. Ý tưởng cơ bản của phép biến đổi con sóng con là khai triển hàm f(t) bất kỳ như một xếp chồng của các con sóng con hay các hàm cơ sở. Các hàm cơ sở này có được từ một con sóng con nguyên mẫu được gọi là con sóng mẹ bằng cách lấy tỷ lệ và dịch.

Trong thực tế tính toán, biến đổi con sóng con rời rạc thuận và nghịch (DWT và IDWT) thường được thực hiện bởi phương trình sau :

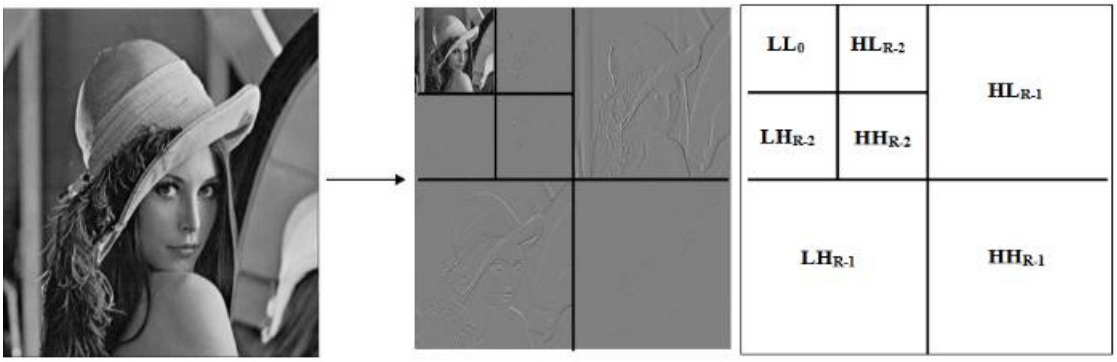
Biến đổi thuận: $$DWT_f(m,n) = \alpha_0^{-m/2} \int_{-\infty}^{+\infty} f(t)\psi^*(\alpha_0^{-m}t - nb_0)dt$$

Biến đổi nghịch: $$f(t) = \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{+\infty} < \psi_{m,n}, f > \tilde{\psi}_{m,n}(t)$$

Trong đó, ψ(t) là hàm wavelet mẹ. Điều kiện ψ(t) là một hàm thông dải đảm bảo sự tồn tại của biến đổi sóng con ngược. Thông thường, người ta chọn a_0=2 và b_0 =1.

Trong các thuật toán nghiên cứu có các thông số đáng chú ý sau đây: Tại một miền phân giải cấp 1 thì các hệ số của băng tần xấp xỉ (LL1 được mô tả tại hình 2.13) sẽ được gọi là v1 (x,y) . Các hệ số của băng tần HH1 sẽ được gọi là f 1,1 (x,y)của LH1 sẽ là f 2,1 (x,y) và của HL1 là f 3,1 (x,y)

Với vài thuật toán các hệ số này sẽ được thăm theo đường zig zag. Khi đó, ta sẽ gọi các hệ số này lần lượt theo thứ tự như sau : v1 (i), f 1,1, (i) , f 2,1 (i) , f 3,1 (i)



Hình 2.11: Biến đổi Wavelet và cấu trúc dải thông.

Trong một số trường hợp, sơ đồ dùng biến đổi sóng con đã tỏ ra ưu thế so với biến đổi Fourier rời rạc DFT hay biến đổi cosin rời rạc DCT. Do đặc tính đa phân giải, sơ đồ mã hóa Wavelets đặc biệt thích hợp cho các ứng dụng mà tính vô hướng và suy biến đóng vai trò quan trọng. Minh chứng cho điều này là biến đổi sóng con đã được dùng như một tiêu chuẩn trong nén

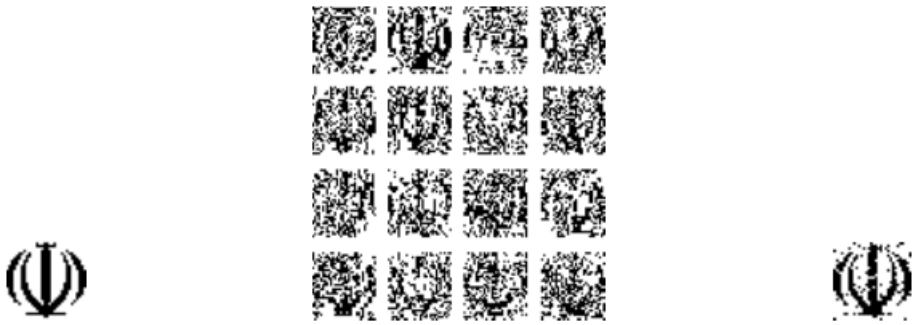
JPEG2000. Ngoài ra, tính đa phân giải của Wavelets còn hữu ích trong việc phân phối thông điệp vào đối tượng bao phủ trong khi vẫn đảm bảo tính bền vững và chất lượng hiện thị. Do đó, lược đồ thủy vân sử dụng DWT vẫn đảm bảo được tính bền vững của thủy vân sau khi nén có mất mát thông tin theo chuẩn nén JPEG2000.

Tổng quát, biến đổi sóng con thực hiện triển khai tần số không gian đa tỷ lệ của một ảnh. Khai triển này tạo ra các hệ số xấp xỉ và các hệ số chi tiết ngang, dọc và chéo. Quá trình khai triển lại tiếp tục với các hệ số xấp xỉ ở mức phân tích cao hơn. Các hệ số xấp xỉ sau cùng chứa thông tin về băng tần thấp nhất trong khi các hệ số chi tiết chứa thông tin về băng tần cao hơn.

2.2.3.2.Lược đồ thủy vân sử dụng biến đổi DWT

Ngày nay, có nhiều thuật toán thủy vân sử dụng biến đổi sóng con và các kỹ thuật lượng tử hóa, thủy vân sử dụng miền biến đổi wavelet có lợi thế làm cho các thủy vân mạnh mẽ hơn chống lại được nhiều dạng tấn công như thay đổi thành phần tần số cao của hình ảnh, nén , lọc thông thấp qua, tuy nhiên nó không thể chống lại cuộc tấn công như cắt ảnh hay phá hủy một thành phần hình ảnh chứa thủy vân.

Hầu hết các phương pháp thủy vân dựa trên biến đổi wavelet chia dải thông con thành các khối nhỏ và sau đó nhúng từng bit logo thủy vân nên chúng hoàn toàn trong mỗi khối con, tức là mỗi bit của thủy vân được lưu trữ trong một hệ số của một khối con và kích thước của khối con phải lớn hơn kích thước của hình ảnh thủy vân. Khi một vùng của hình ảnh phủ bị phá hủy. Thủy vân nguyên vẹn có thể được trích xuất thủy vân hoàn chỉnh. Ví dụ như hình 2.14 cho thấy kết quả của thủy vân kết quả được trích xuất từ một ảnh đã bị nén (với thuật toán JPEG2000) và bị cắt đi một phần



(a) (b) (c)

Hình 2.12: a Thủy vân gốc, b thủy vân tách được từ các khối, c Thủy vân kết hợp

a) Thuật toán nhúng

Đầu vào là ảnh mang I có kích thước Nx N, ảnh nhị phân logo thủy vân W kích thước Mx M

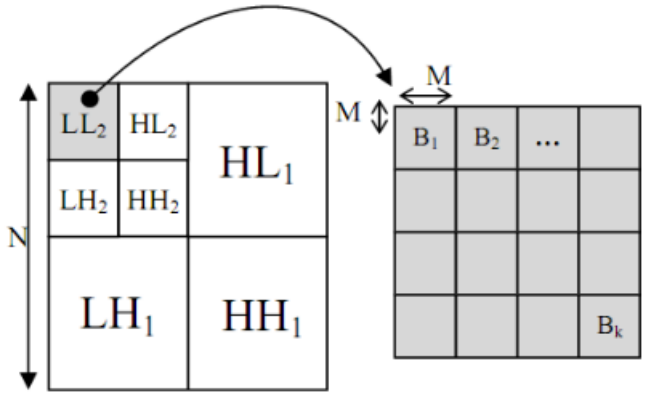
$$I = \{ I(i,j) \mid 1 \le i \le N , 1 \le j \le N \}$$

$$W = \{ W(i,j) \mid 1 \le i \le M , 1 \le j \le M , W(i,j) \in \{0,1\} \}$$

- Quy trình nhúng thủy vân :

+ Bước 1: Hình ảnh mang được phân ra thành n mức sử dụng biến đổi wavelet rời rạc. Sau đó, chúng ta chọn dải thông con LL_n để nhúng thủy vân.

+ Bước 2: Chia dải thông con được lựa chọn thành các khối nhỏ hơn B_k với kích thước M x M . Như hình dưới đây :



Hình 2.13: Dải thông LL_2 được chia thành các khối nhỏ hơn

+ Bước 3: Logo thủy vân được chèn vào tất cả các khối con bằng cách lượng tử hóa các hệ số của khối theo công thức sau

$$q'_k(i,j) = \begin{cases} mQ & mQ < q_k(i,j) \le (m+0.5)Q \\ (m+1)Q & (m+0.5)Q < q_k(i,j) \le (m+1)Q \end{cases} \quad W(i,j) = 1$$

$$q'_k(i,j) = (m+0.5)Q \quad W(i,j) = 0$$

Trong đó $q_k(i,j)$ được sử dụng để biểu diễn các hệ số wavelet của khối con B_k và $q'_k(i,j)$ được sử dụng để biểu diễn các hệ số sau khi được lượng tử hóa. W (i,j) là logo thủy vân, m là một số nguyên và Q là kích thước bước lượng tử hóa.

Lựa chọn một giá trị Q tốt cho lược đồ thủy vân là rất quan trọng bởi việc tăng Q có thể làm tăng tính bền vững của thủy vân trước các cuộc tấn công nhưng lại suy giảm chất lượng ảnh mang hay nói cách khác ảnh hưởng đến tính vô hình của thủy vân. Vì vậy Q và PSNR có mối quan hệ với nhau và Q tỉ lệ nghịch với PSNR. Trong đó PSNR được tính theo công thức

$$PSNR = 10\log_{10}\frac{L_{\max} \times L_{\max}}{MSE}$$

Với L_{max} là giá trị cực đại của các điểm ảnh và MSE là tỷ lệ lỗi trung bình được định nghĩa :

$$MSE = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}[I_o(i,j) - I_w(i,j)]^2}{N_1 \times N_2}$$

Trong đó I_o và I_w biểu diễn giá trị điểm ảnh tương ứng trên ảnh gốc và ảnh chứa thủy vân và N_1 , N_2 là kích thước của ảnh.

Ngoài ra ngưỡng giá trị Q còn khác nhau phụ thuộc vào ảnh mang và miền tần số. Ví dụ như trong hình dưới

Hình 2.14: a Ảnh gốc b ảnh đã thủy vân với Q= 35.

+ Bước 4: Cuối cùng với những hệ số giá trị mới, sử dụng biến đổi sóng con ngược để thu được hình ảnh chứa thủy vân.

Việc lựa chon n mức phân giải sóng con, phải đảm bảo cân bằng giữa tính bền vững và tính vô hình. Với một lựa chọn tốt, thủy vân có thể có được tính bền vững cao hơn chống lại được sự suy giảm chất lượng hình ảnh.

Chọn giá trị n nhỏ có thể làm tăng tốc độ thực hiện của thuật toán nhưng lại làm giảm tính bền vững và làm suy giảm chất lượng hình ảnh. Ngược lại nếu lựa chọn giá trị n lớn có thể tăng tính bền vững nhưng sẽ làm giảm kích thước của miền LL_n do đó có thể gây ra giảm số lượng các khối con K. Như vậy rõ ràng có một mối quan hệ giữa N, M, n, K. Theo kết quả thực nghiệm tác giả chỉ ra rằng trường hợp tối ưu khi N = M x K x 2n

b) Thuật toán trích xuất

Trong khi hầu hết các phương pháp trích xuất thủy vân đều đòi hỏi hình ảnh gốc, thuật toán được trình bày là một trong những thuật toán trích xuất mù không yêu cầu ảnh gốc trong quá trình trích xuất thủy vân. Trong thuật toán, để trích xuất thủy vân cần khóa bí mật chính là kích thước bước lượng tử Q, mức phân giải n số lượng các khối con K .

c. Quy trình trích xuất thủy vân

+ Bước 1: Những hình ảnh mang được phân giải theo n mức sử dụng biến đổi wavelet n rời rạc. Dải thông con LL_n của hình ảnh phân giải được chia thành các khối con B_k với kích thước M x M.

+ Bước 2: Những điểm ảnh của logo thủy vân tương ứng với mỗi khối con B_k được trích xuất theo công thức sau

$$W_k(i,j) = \begin{cases} 1 & (m-0.25)Q \le q_k(i,j) \le (m+0.25)Q \\ 0 & (m+0.25)Q < q_k(i,j) < (m+0.75)Q \end{cases}$$

Trong đó, $q_k(i,j)$ được sử dụng biểu diễn các hệ số con sóng con của khối con B_k, m là một số nguyên và Q là kích thước bước lượng tử.

+ Bước 3: Nếu không xảy ra các biến đổi với hình ảnh chứa thủy vân, thì tất cả các logo thủy vân được trích xuất giống như logo được nhúng ban đầu. Nhưng nếu đã xảy ra bất kỳ biến đổi nào hình ảnh mang, thủy vân được trích xuất nên được kết hợp lại một cách phù hợp để có kết quả cuối cùng. Kết hợp thủy vân được thực hiện theo công thức sau đây :

Trong đó $W_{k(i,j)}$ được sử dụng để biểu diễn thủy vân được trích xuất từ khối con B_k và W (i,j) được sử dụng để biểu diễn thủy vân được kết hợp. K là số khối con.

Chương 3.
CHƯƠNG TRÌNH THỬ NGHIỆM

3.1. PHÁT BIỂU BÀI TOÁN

Chương trình thủy vân với ba phương pháp: nhúng thủy vân vào bit có trọng số thấp (LSB), phương pháp biến đổi sóng con (DWT) và phương pháp biến đổi cosin rời rạc DCT. Chương trình bao gồm module nhúng và trích xuất thủy vân, ngoài ra có thêm sự so sánh tính bền vững của dấu thủy vân giữa ba phương pháp bằng việc thêm tấn công nhiễu gauss với ảnh đã được nhúng thủy vân.

3.2. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG

3.2.1. Mô tả chức năng hệ thống

- Chức năng nhận ảnh gốc
- Chức năng nhận ảnh cần thủy vân
- Chức năng nhúng thủy vân
- Chức năng trích xuất thủy vân
- Chức năng tấn công nhiễu
- Chức năng thủy vân bằng phương pháp LSB
- Chứng năng thủy vân bằng phương pháp biến đổi DWT.
- Chức năng thủy vân bằng phương pháp DCT

3.2.2. Ứng dụng chương trình

Chương trình được dùng để nhúng ảnh vào một ảnh gốc nhằm bảo vệ bản quyền ảnh số của tác giả.

So sánh tính bền vững của dấu thủy vân giữa ba phương pháp LSB, DCT, DWT bằng việc thêm tấn công nhiễu gauss với ảnh đã được nhúng thủy vân.

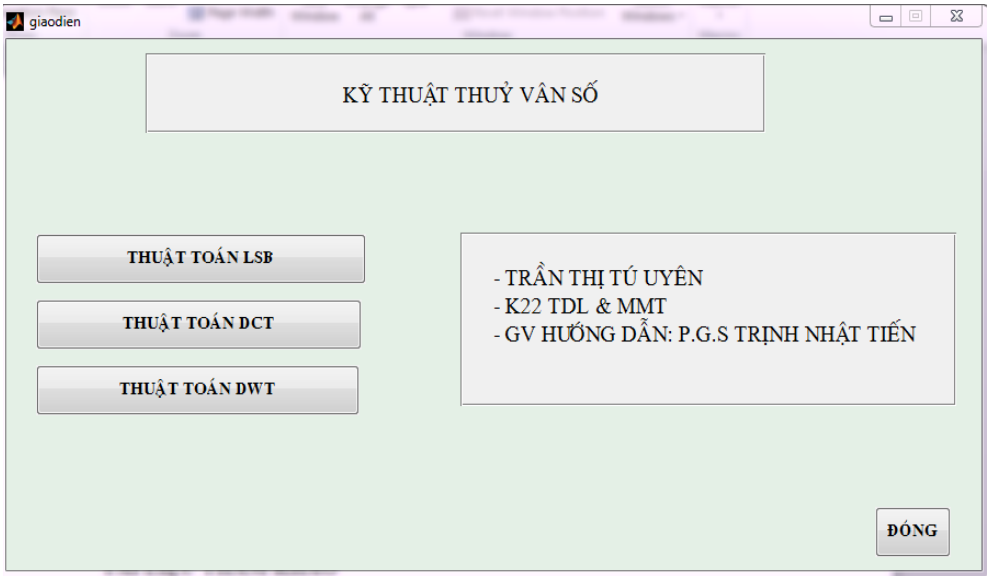
3.2.3. Hướng dẫn sử dụng

- Môi trường chạy

- Chương trình được cài đặt trên công cụ và ngôn ngữ MATLAB.
- Có thể download Matlab tại địa chỉ: http://www.mathworks.com/downloads/

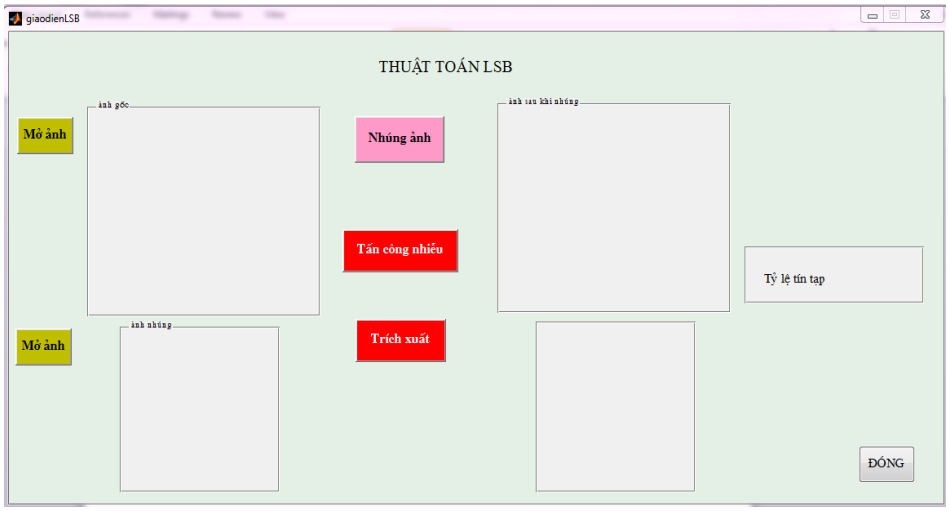
➢ Chạy chương trình

- Mở matlab, trỏ thư mục hiện tại đến thư mục chứa source code
- Mở file giaodien.m, bấm nút **Run** trên thanh công cụ để chạy chương trình. Giao diện chương trình như hình bên dưới:



Hình 3.1: Giao diện phần mềm thử nghiệm.

- **Thủy vân bằng phương pháp LSB**

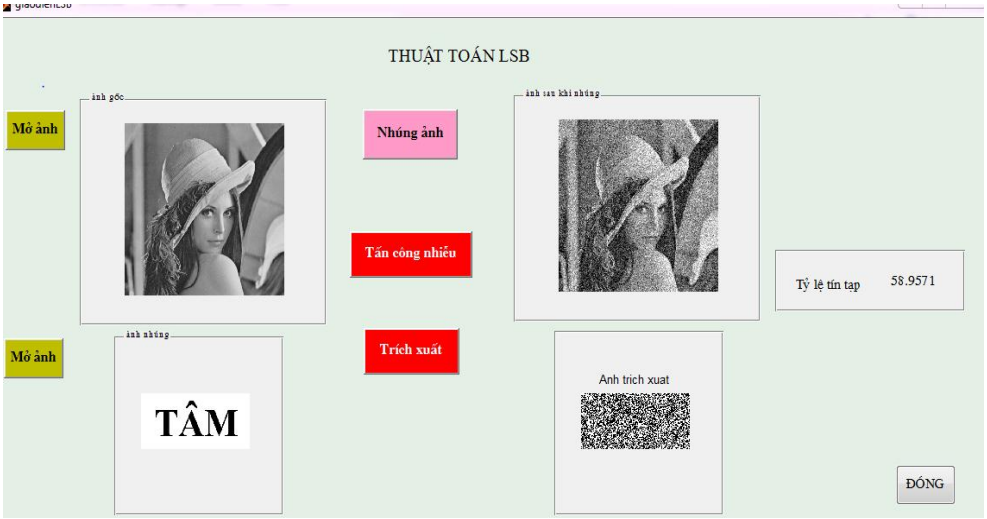


Hình 3.2: Giao diện thủy vân bằng phương pháp LSB.

- Bấm nút Mở ảnh để chọn ảnh mang
- Bấm nút Mở ảnh để chọn dấu thủy vân
- Sau đó nhấn nút Nhúng ảnh để thủy vân ảnh. Ta được hình ảnh hiện thị sau khi nhúng trên màn hình.
- Bấm nút Trích xuất để tách thủy vân. Ta được hình ảnh hiện thị dấu thủy vân

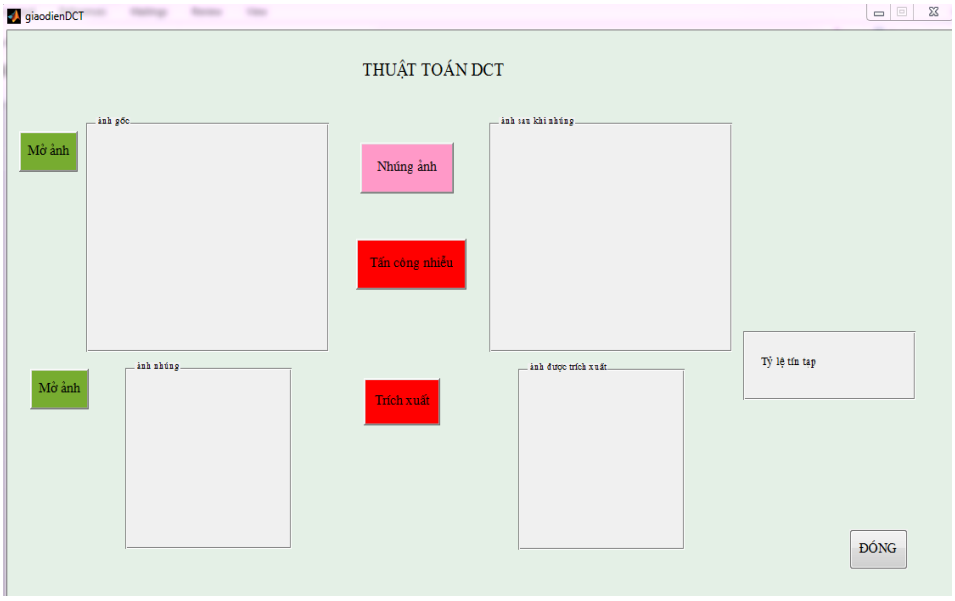
Hình 3.3: Kết quả trích xuất khi chưa sử dụng tấn công nhiễu

- Bấm nút Tấn công nhiễu để làm nhiễu ảnh đã thủy vân
- Bấm nút Trích xuất để kiểm tra thủy vân tách được. Ấn nút Đóng để thoát giao diện LSB.



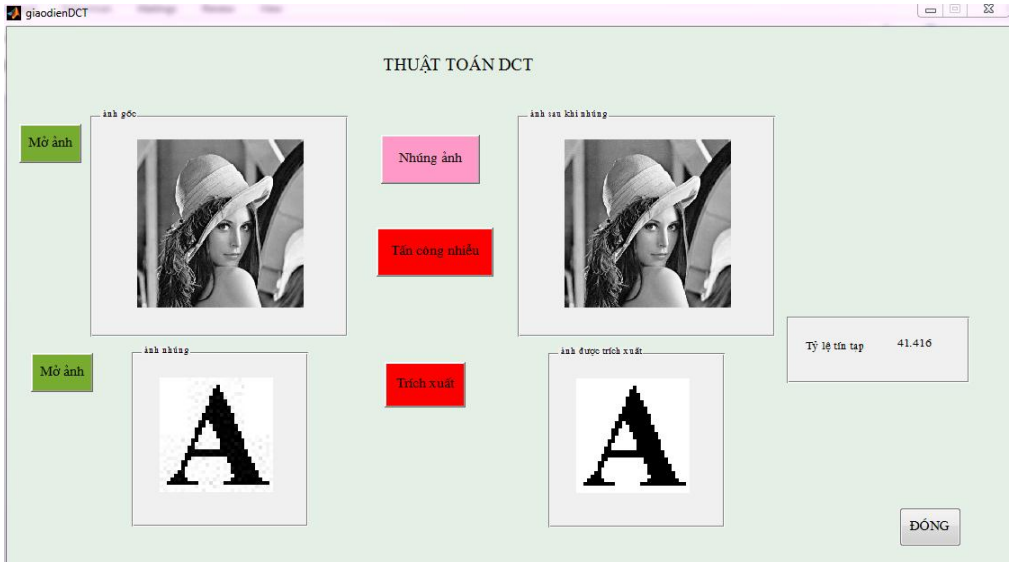
Hình 3.4: Kết quả trích xuất khi sử dụng tấn công nhiễu

- **Thủy vân bằng phương pháp biến đổi DCT**



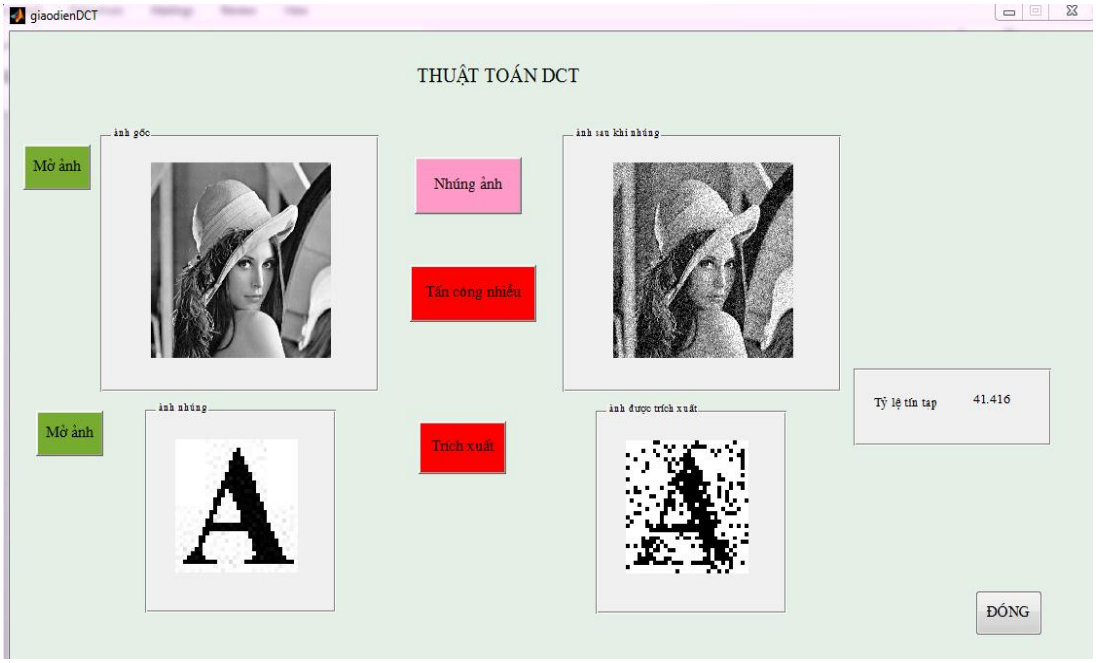
Hình 3.5: Giao diện thủy vân bằng phương pháp DCT.

- Bấm nút Mở ảnh để chọn ảnh mang
- Bấm nút Mở ảnh để chọn dấu thủy vân
- Sau đó nhấn nút Nhúng ảnh để thủy vân ảnh. Ta được hình ảnh hiện thị sau khi nhúng trên màn hình.
- Bấm nút Trích xuất để tách thủy vân. Ta được hình ảnh hiện thị dấu thủy vân



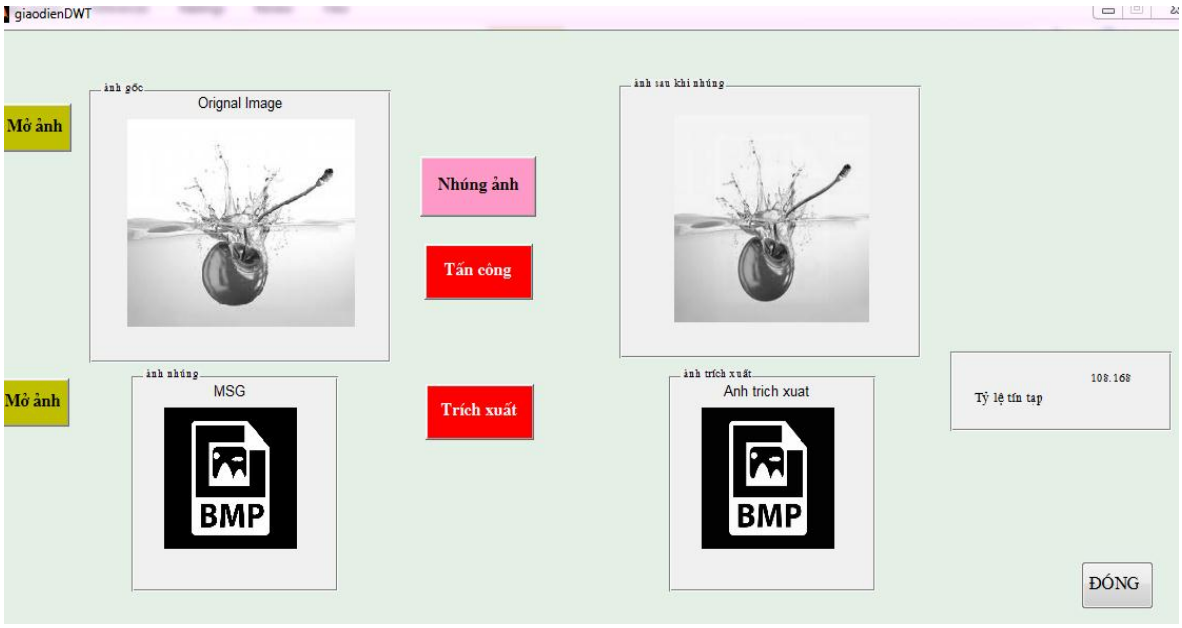
Hình 3.6: Kết quả trích xuất khi chưa sử dụng tấn công nhiễu

- Bấm nút Tấn công nhiễu để làm nhiễu ảnh đã thủy vân
- Bấm nút Trích xuất để kiểm tra thủy vân tách được. Ấn nút Đóng để thoát giao diện DCT.

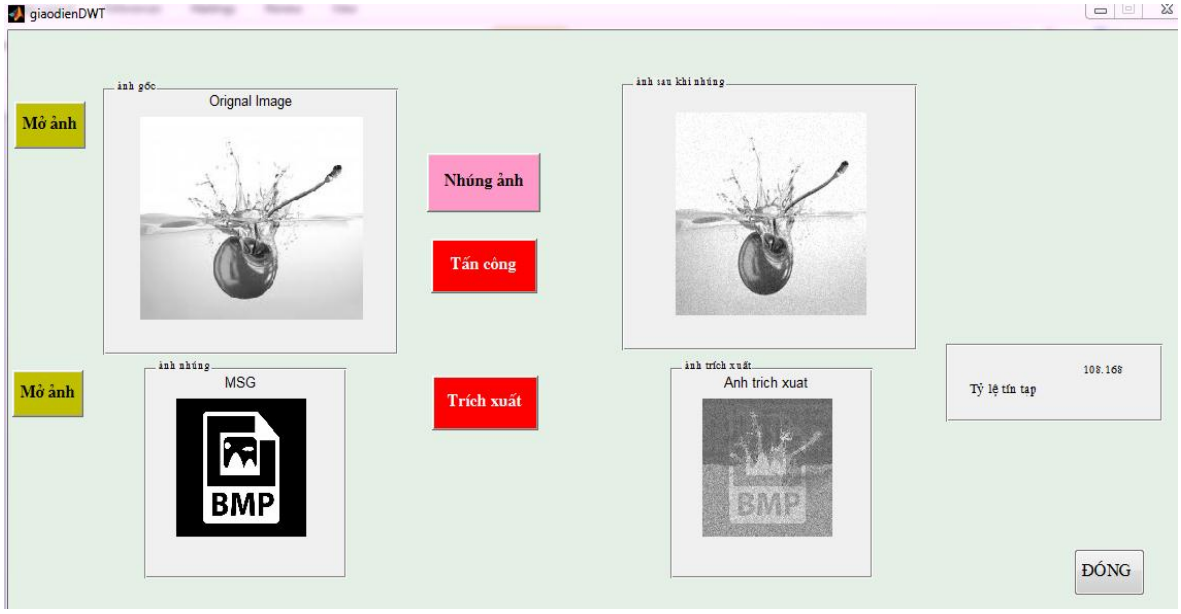


Hình 3.7: Kết quả trích xuất khi sử dụng tấn công nhiễu

- **Thủy vân bằng phương pháp biến đổi DWT**



Hình 3.8: Kết quả trích xuất khi chưa sử dụng tấn công nhiễu



Hình 3.9: Kết quả trích xuất khi sử dụng tấn công nhiễu

KẾT LUẬN

Sau một thời gian nghiên cứu và tìm hiểu cùng với sự nỗ lực của bản than và sự hướng dẫn tận tình của thầy giáo hướng dẫn, tôi đã hoàn thành luận văn của mình. Nội dung chủ yếu của luận văn là nghiên cứu về hệ thủy vân số, các hướng ứng dụng của thủy vân số chủ yếu là ứng dụng trong bảo vệ bản quyền ảnh số. Từ đó, xây dựng chương trình thử nghiệm cài đặt một số thuật toán thủy vân nhằm ứng dụng xác thực thông tin và bảo vệ bản quyền cho dữ liệu ảnh số.

Qua quá trình tìm hiểu nghiên cứu luận văn đã đạt được một số kết quả như sau:

Những kết quả chính có Luận văn:

Tổng hợp nghiên cứu về hệ thống thủy vân khái niệm, phân loại, ứng dụng, mô hình, các khả năng tấn công, yêu cầu đối với phương pháp thủy vân.
Nghiên cứu các thuật toán thủy vân số đang được ứng dụng phổ biến trong ảnh số.

Tiến hành viết phần mềm trên MATLAB sử dung 3 kỹ thuật LSB, DCT, DWT với đầu vào là một ảnh đen trắng và ảnh nhúng là một ảnh. Kết hợp phương pháp tấn công gây nhiễu nhằm so sánh tính bền vững của ảnh thủy vân trích xuất đối với các thuật toán.

Đánh giá kết quả đạt được thông qua phần mềm thực nghiệm

Những đóng góp cho khoa học và thực tiễn của Luận văn:

Các kết quả nhận được cho thấy được mô hình thủy vân xây dựng đã thành công khi nhúng một ảnh mang vào một ảnh đầu vào mà không làm thay đổi chất lượng hình ảnh. Việc cài đặt 3 kỹ thuật thủy vân trên phần mềm đã so sánh được các thuật toán trên miền không gian và miền tần số. Khẳng định được các thuật toán trên miền tần số có tính bền vững hơn thuật toán trên miền không gian.

Do vậy, Luận văn hoàn toàn có tính khả thi, có ý nghĩa quan trọng trong việc bảo vệ bản quyền, sở hữu trí tuệ , không những áp dụng được trong thương mại mà còn mở ra một tiếp cận mới cho vấn đề bảo vệ bản quyền ảnh số.

TÀI LIỆU THAM KHẢO

TIẾNG VIỆT

1. Trịnh Nhật Tiến, Bài giảng An toàn dữ liệu, 2008
2. Nguyễn Xuân Huy, Trần Quốc Dũng , Một thuật toán thủy vân ảnh trên miền DCT, Hội thảo quốc gia Các vấn đề chọn lọc Công nghệ thông tin và Truyền thông, 2002.
3. Nguyễn Quang Hoan, Giáo trình xử lý ảnh, Học viện bưu chính viễn thông 2006
4. Luận văn Kỹ thuật thủy vân số, Nguyễn Minh Nhật, Đại học Duy Tân – Đà Nẵng.
5. Luận án tiến sĩ, Nghiên cứu giải pháp nâng cao chất lượng thủy vân sử dụng biến đổi cosine rời rạc, Nguyễn Lê Cường, Học viện Công nghệ Bưu Chính Viễn Thông, 2012.
6. Luận án tiến sĩ, Nghiên cứu và phát triển kỹ thuật thủy vân cơ sở dữ liệu quan hệ, Lưu Thị Bích Hương, Viện Công nghệ thông tin, 2014.

TIẾNG ANH

7. Shen Tao, Xu Dêh, Li Chengming, Sun Jianguo , Watermarking Gis Data for Digital Map CopyRight Protection, 2009
8. Yasser Dakoury, Ismail Abd El- Ghafar and Ashraf Tammam, Protecting GIS Data Using Cryptography and Digital Watermarking, No.1, 2010.
9. Sonnleitner E., and Kung J. (2013), “Watermarking Generative Information Systems for Duplicate Traceability”. International Journal Applied Mathematics & Information Sciences, Vol 7, No. 5, 1789-1801.