TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN TOÁN ỨNG DỤNG VÀ TIN HỌC
NGÀNH TOÁN TIN

****

ĐỒ ÁN 1

TÌM HIỂU KĨ THUẬT THỦY VÂN SỐ TRONG VIỆC BẢO VỆ BẢN QUYỀN ẢNH SỐ

NGUYỄN THỊ QUÝ - 20185396
quy.nt185396@sis.hust.edu.vn

GIẢNG VIÊN HƯỚNG DẪN: TH.S LÊ QUANG HÒA

Hà Nội, 2021

Mục lục

Danh sách hình vẽ

Danh sách bảng

Danh sách thuật ngữ

Tiếng Anh	Tiếng Việt
DCT: Discrete Cosine Transform	phép biến đổi cosine rời rạc
DFT: Discrete Fourier Transform	phép biến đổi fourier rời rạc
DWT: Discrete Wavelet Transform	phép biến đổi sóng rời rạc
IDCT: Inverse Discrete cosine Transform	phép biến đổi cosine rời rạc ngược
IDWT: Inverse Discrete Wavelet Transform	phép biến đổi sóng rời rạc ngược
LSB: Least Significant Bit	thuật toán thủy vân trên các bít ít quan trọng
MSE: Mean squared error	sai số toàn phương trung bình
PNSR: Peak signal-to-noise ratio	hệ số đánh giá chất lượng ảnh
Watermark	thủy vân

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ

Phần đánh giá của giảng viên chấm bài:

.....
.....
.....
.....
.....
.....
.....
.....
.....

Hà Nội, ngày..... tháng..... năm.....
Giảng viên chấm bài

Phần đánh giá của giảng viên hướng dẫn:

.....
.....
.....
.....
.....
.....
.....
.....
.....

Hà Nội, ngày..... tháng..... năm.....
Giảng viên hướng dẫn

.

LỜI CẢM ƠN

Để có thể hoàn thành được đề tài này, trước hết em xin gửi lời cảm ơn sâu sắc tới ThS. Lê Quang Hòa, người đã gợi mở và hướng dẫn em đi vào tìm hiểu đề tài thủy vân ảnh. Em xin cảm ơn thầy đã hết lòng giúp đỡ em, cung cấp những kiến thức bổ ích, cũng như đã truyền cho em rất nhiều cảm hứng, động viên em và các bạn trong quá trình học tập, cũng như tìm hiểu và thực hiện đề tài.

Em cũng xin gửi lời cảm ơn các thầy, cô giáo trường Đại học Bách Khoa Hà Nội nói chung và các thầy, cô giáo viện Toán Ứng dụng và Tin học nói riêng, đã dạy dỗ chúng em, đã tạo cho chúng em môi trường học tập tốt.

Do thời gian thực hiện đề tài vẫn còn ngắn và kiến thức của em vẫn còn nhiều hạn chế dề tài còn nhiều thiếu sót. Em sẽ cố gắng hoàn thiện thêm trong thời gian tới.

Em xin chân thành cảm ơn!

MỞ ĐẦU

Lý do chọn đề tài

Cùng với sự bùng nổ và phát triển của Internet, các phương tiện kỹ thuật số như phương tiện lưu trữ, truyền thông đã mở ra một kỉ nguyên mới - kĩ nguyên thông tin số. Các thông tin ngày nay đều được lưu trữ dưới dạng số hóa, hay thuật ngữ "chuyển đổi số" đã không còn quá xa lạ mà trở nên phổ biến. Việc chuyển đổi số bên cạnh sự tiện lợi, hiện đại cũng mang đến nhiều rủi ro với những vấn nạn như sao chép đã vượt ra khỏi tầm kiểm soát của các tổ chức. Vì thế một vấn đề phát sinh là các phương thức kinh doanh, phân phối tài nguyên phải tuân thủ nghiêm ngặt các quy định về bảo vệ bản quyền số của cục sở hữu trí tuệ nhằm bảo vệ lợi ích và bản quyền của người sở hữu.

Chính vì vậy, nhu cầu bảo vệ bản quyền và sở hữu trí tuệ đã và đang trở thành một vấn đề quan trọng và đang được quan tâm. Ngày nay có nhiều phương pháp được nghiên cứu trong việc xác minh bảo vệ bản quyền, và một trong những phương pháp hữu hiệu và đang được quan tâm nhất là phương pháp thủy vân số. Thủy vân là một phương pháp tổng hợp của nhiều lĩnh vực khác nhau như mật mã học, lý thuyết thông tin, xử lí tín hiệu số. Bằng cách nhúng dấu thủy vân vào dữ liệu số, sẽ giúp đánh dấu bản quyền cho dữ liệu số khi lan truyền trên những kênh truyền không tin cậy. Ngoài việc dấu thủy vân được nhúng nhằm bảo vệ bản quyền, thì thủy vân số ngày nay còn có khả năng trích xuất và khôi phục lại dữ liệu gốc nhằm phục vụ cho một số lĩnh vực như quân đội, y học,... Thủy vân được trích xuất là bằng chứng xác thực bản quyền dữ liệu có thuộc quyền sở hữu hay vi phạm bản quyền hay không.

Chính vì tính hữu ích và cấp thiết của ứng dụng thủy vân số trong thực tiễn em quyết định chọn đề tài “Tìm hiểu kĩ thuật thủy vấn số và ứng dụng thủy vân số trong bảo vệ bản quyền ảnh số" làm đề tài nghiên cứu của mình.

Mục đích thực hiện đề tài

Đồ án đưa ra một cái nhìn khái quát, tổng quan nhất về hệ thống thủy vân, cách thức và hướng ứng dụng của thủy vân trong bảo vệ bản quyền ảnh số. Trình bày một số thuật toán và chỉ ra hướng thủy vân đang được ứng dụng, áp dụng chủ yếu ngày nay nhất là trong việc bảo vệ bản quyền ảnh số.

Đối tượng và phạm vi nghiên cứu

Đồ án tập trung nghiên cứu các kĩ thuật thủy vân trên miền tần số của ảnh số.

Phương pháp thực hiện

Tập trung nghiên cức các khái niệm, phương pháp, thuật toán đã được nghiên cứu, công bố trước đó.Phát triển, xây dựng một số thuật toán thử nghiệm, so sánh độ hiệu quả của các phương pháp và đưa ra kết luận, nhận xét.

Kết quả đạt được

Đồ án đã hệ thống lại các kiến thức cơ bản về thủy vân số, hiểu được ứng dụng của thủy vân số trong bảo vệ bản quyền ảnh số. Cài đặt thành công một số thuật toán thủy vân trên miền tần số nhằm xác thực bản quyền ảnh số của tác giả, và so sánh độ hiệu quả của các thuật toán với nhau.

Bố cục đồ án

Chương 1: Một số khái niệm về thủy vân số về thủy vân số

Chương 2: Kỹ thuật thủy vân số trên ảnh số

Chương 3: Chương trình thử nghiệm

Chương 1

MỘT SỐ KHÁI NIỆM VỀ THỦY VÂN SỐ

1.1 Lịch sử phương pháp thủy vân số

Phương pháp thủy vân đầu tiên là thủy vân trên giấy. Đó là một thông tin nhỏ được nhúng chìm trong giấy để thể hiện bản gốc hoặc bản chính thức. Theo Hartung và Kutter, thủy vân trên giấy đã bắt đầu được sử dụng vào năm 1292 ở Fabriano, Italy – nơi được coi là nơi sinh của thủy vân. Sau đó, thủy vân đã nhanh chóng lan rộng trên toàn Italy và rồi trên các nước châu Âu và Mỹ. Ban đầu, thủy vân giấy được dùng với mục đích xác định nhãn hàng và nhà máy sản xuất. Sau này được sử dụng để xác định định dạng, chất lượng và độ dài, ngày tháng của sản phẩm.

Đến thế kỷ thứ 18, nó bắt đầu được dùng cho tiền tệ và cho đến nay thủy vân vẫn là một công cụ được dùng rộng rãi với mục đích bảo mật cho tiền tệ, chống làm tiền giả. Thuật ngữ "thủy vân" (watermarking) được đưa ra vào cuối thế 18, nó bắt nguồn từ một loại mực vô hình khi viết lên giấy và chỉ hiển thị khi nhúng giấy đó vào nước. Năm 1988, Komatsu và Tominaga đã đưa ra thuật ngữ "thủy vân số" (Digital watermarking).

Vậy 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 số. Mục đích của thủy vân số là bảo vệ bản quyền cho phương tiện dữ liệu số mang thông tin thủy vân. Tùy theo mục đích của hệ thủy vân mà người ta lại chia thành các hướng nhỏ như thủy vân dễ vỡ và thủy vân bền vững.

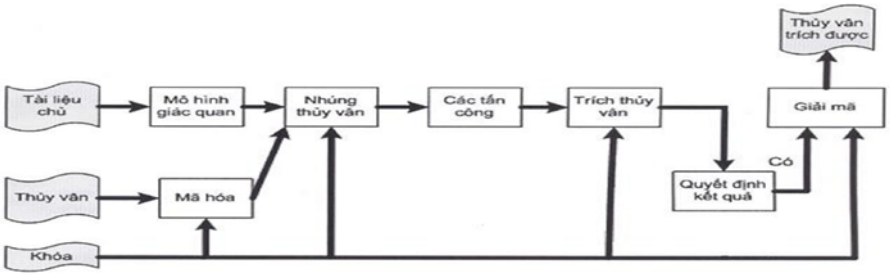
Thủy vân bền vững quan tâm nhiều đến việc nhúng những mẩu tin đòi hỏi độ bền vững cao của thông tin được giấu trước các biến đổi thông thường trên dữ liệu chứa. Hướng này được sử dụng để bảo vệ bản quyền tác giả.

Thủy vân dễ vỡ yêu cầu thông tin giấu sẽ bị sai lệch nếu có bất kỳ sự thay đổi nào trên dữ liệu chứa. Hướng này được sử dụng để phát hiện xuyên tạc thông tin.

Ở mỗi loại thủy vân bền vững hoặc thủy vân dễ vỡ lại chia thành hai loại dựa theo đặc tính đó là thủy vân ẩn và thủy vân hiện. Thủy vân hiện cho phép nhìn thấy thông tin đem nhúng vào dữ liệu chứa. Loại này được sử dụng cho mục đích công bố công khai về quyền sở hữu. Ngược lại, thủy vân ẩn không cho phép nhìn thấy nội dung thông tin nhúng và nó được sử dụng với mục đích gài bí mật các thông tin xác nhận quyền sở hữu.

Hình 1.1: Ví dụ về thủy vân ẩn và thủy vân hiện

1.2 Mô hình thủy vân số



Hình 1.2: Mô hình thủy vân do Sviatoslav Voloshynovkiy và các cộng sự đề xuất

Mô hình thủy vân Sviatoslav Voloshynovskiy được chia làm 3 phần chính:

- Nhúng thủy vân
- Các tấn công trên thủy vân
- Trích thủy vân

Thủy vân có thể được mã hóa để tăng cường tính bền vững. Thông thường, tài liệu đã nhúng thủy vân sau khi lan truyền trên các kênh truyền không tin cậy sẽ trải qua một số bước tấn công trước khi được trích thủy vân. Sau quá trình trích được thực hiện, dựa vào kết quả trích xuất để có quyết định tài liệu có được nhúng thủy vân hay không, và nếu có thì thực hiện giải mã trên dữ liệu trích để nhận được giá trị thủy vân.

1.3 Các tính chất quan trọng của thủy vân số

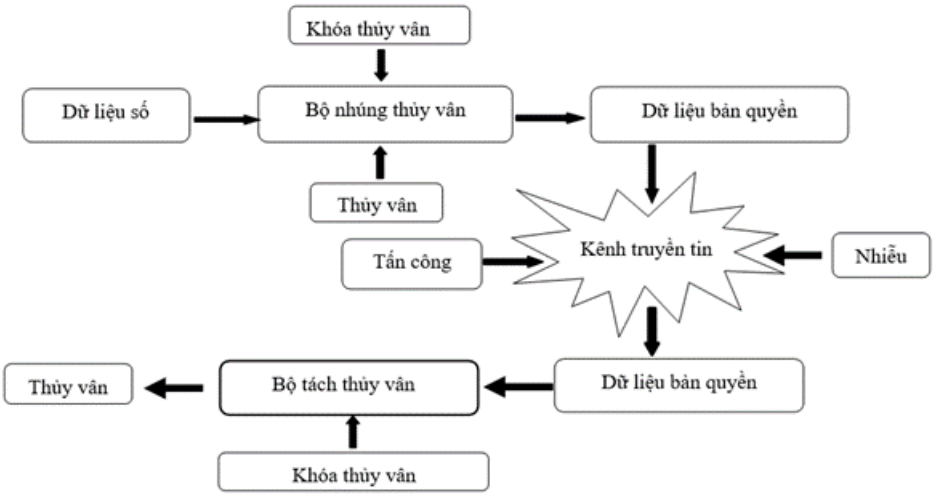
Tính bền vững: Chất lượng của thuật toán nhúng ảnh hưởng đến tính bền vững của thủy vân. Đặc biệt đối với thủy vân bền vững, yêu cầu quan trọng là thủy vân không bị biến đổi qua các cuộc tấn công trên ảnh được nhúng. Đối với ảnh số, các tấn công này có thể là nén ảnh JPG, lọc, cắt, xén, làm nhiễu, ... Ngày nay tính bền vững của thủy vân là một yếu tố rất quan trọng trong các hướng nghiên cứu thủy vân nhằm bảo vệ bản quyền ảnh số.

Tính Vô hình: Đối với thủy vân ẩn thì mọi thuật toán đều cố gắng nhúng thủy vân sao cho chúng không bị phát hiện bởi người sử dụng. Thông thường đối với một thuật toán, tính bền vững cao thì tính vô hình kém và ngược lại, do đó cần có sự cân bằng giữa tính bền vững và tính vô hình để đảm bảo thủy vân đạt được cả tính bền vững cũng như tính vô hình.

Tính bảo mật: Bảo mật đối với khóa thủy vân sao cho không ai có thể dò được thủy vân. Ngày nay, một trong những hướng nghiên cứu chính để làm tăng tính bảo mật của thủy vân là sử dụng các hệ mật mã khóa bất đối xứng. Với độ an toàn và dường như không thể bị tấn công, những hệ mật khóa này làm cho dấu thủy vân có tính bảo mật cao và không thể bị tấn công.

Tính dư thừa: Khi ta thiết lập thuật toán thủy vân vào dữ liệu số, thực tế dấu thủy vân có thể lặp lại ở những vùng tần số khác nhau. Vì vậy, dấu thủy vân có thể được khôi phục lại từ các dải tần khác nếu một vùng tần số nào đó gặp phải lỗi, có nghĩa là thủy vân vẫn có thể được phát hiện ngay cả khi nó bị biến đổi nhất định do sự vô ý hay tấn công có chủ ý.

1.4 Hệ thống thủy vân số



Hình 1.3: Sơ đồ hệ thống thủy vân

Hệ thống thủy vân số là quá trình sử dụng một thủy vân nhúng vào trong một dữ liệu số để được một dữ liệu số có chứa thủy vân hay gọi là dữ liệu có bản quyền. Dữ liệu có bản quyền này sẽ được phân phối trên kênh truyền tin không tin cậy như Internet. Vì thế trong quá trình phân phối, dữ liệu bản quyền có thể bị tấn công trái phép hoặc yếu tố gây nhiễu. Nếu dữ liệu số bản quyền bị nghi ngờ sao chép trái phép hoặc chỉnh sửa thông tin thì có thể xác minh nhờ quá trình tách thủy vân đã nhúng. Như vậy, hệ thống thủy vân số nói chung bao gồm 2 quá trình là quá trình nhúng thủy vân và quá trình tách thủy vân.

Thủy vân mang thông tin bảo mật hoặc bản quyền về dữ liệu chứa.

Khóa thủy vân được dùng cho cả phiên nhúng và phát hiện thủy vân. Khóa thủy vân là duy nhất với mỗi thủy vân. Khóa đó là khóa bí mật, chỉ tác giả mới biết. Điều đó nói lên rằng chỉ tác giả mới phát hiện ra được thủy vân. Tùy từng bộ nhúng thủy vân mà có các yêu cầu với khóa thủy vân. Ngày nay, một trong những hướng phát triển nhằm bảo mật dấu thủy vân đó là sử dụng hệ mã khóa mật bất đối xứng. Với tính bảo mật và khó có thể tấn công của nhứng hệ mã khóa này sẽ luôn đảm bảo dấu thủy vân bền vững và khó có thể bị trích xuất.

1.4.1 Quá 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 đa phương tiến như ảnh số, audio, video,... 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 gọi là dữ liệu có bản quyền và được phân phối trên các môi trường khác nhau. Trong quá trình phân phối dữ liệu nhúng có thể bị tấn

công dù vô ý hay cố ý. Do đó yêu cầu quan trọng cho các kỹ thuật thủy vân số phải bền vững với sự tấn công .

1.4.2 Quá trình trích thủy vân

Thủy vân được trích xuất 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 truyền. Thủy vân thu được là bằng chứng cho bản quyền của tác giả. Vì thế các thuật toán thủy vân phải đảm bảo dấu thủy vân phải ít sai khác sau các cuộc tấn công nhằm đảm bảo tính xác thực.

1.5 Các hướng ứng dụng của thủy vân

Thủy vân hiển: Có thể dùng trong những trường hợp sau:

- Tăng cường bảo vệ quyền tác giả. Trong tình huống như vậy, nơi hình ảnh được làm sẵn thông qua Internet và chủ sở hữu nội dung có liên quan rằng những hình ảnh này sẽ được dùng trong thương mại mà không trả tiền nhuận bút. Ở đây, chủ sở hữu nội dung mong muốn một dấu quyền sở hữu, trực quan rõ ràng, nhưng mà không ngăn chặn hình ảnh được sử dụng cho các mục đích khác (ví dụ như nghiên cứu học thuật).
- Chỉ sở hữu bản quyền. Trong trường hợp này hình ảnh được làm sẵn có thông qua Internet và chủ sở hữu nội dung mong muốn chỉ ra quyền sở hữu của các thành phần cơ bản (ví dụ như bản thảo thư viện).

Thủy vân bền vững: Thủy vân bền vững được áp dụng nhiều trong thực tế:

- Phát hiển hình ảnh biển thủ. Trong kịch bản này, người bán các hình ảnh kỹ thuật số là có liên quan. Hình ảnh thu phí tạo của ông ta có thể được mua bởi một cá nhân sẽ làm cho họ được miễn phí, điều này có thể tước đi các chủ sở hữu của doanh thu giấy phép.
- Làm bằng chứng về quyền sở hữu. Trong kịch bản này, người bán là những hình ảnh kỹ thuật số nghi ngờ một trong những hình ảnh của ông đã được biên tập và xuất bản mà không trả tiền nhuận bút. Ở đây, việc phát hiện thủy vân của người bán trong các hình ảnh được thiết kế để phục vụ, như là bằng chứng cho thấy các hình ảnh được công bố là tài sản của người bán.

Thủy vân ẩn dễ vỡ:

- Được sử dung cho máy ảnh tin cậy. Trong kịch bản này, các hình ảnh được chụp bằng một máy ảnh kỹ thuật số để sau này đưa vào trong các bài báo. Ở đây, nó là mong muốn của một hãng đăng tin để xác minh rằng một hình ảnh đúng với chụp gốc và chưa được

chỉnh sửa để làm sai lệch một cảnh. Trong trường hợp này, thủy vân có thể nhìn thấy được nhúng vào thời điểm chụp; sự hiển diện của chúng tại thời điểm công bố nhằm mục đích chỉ ra rằng hình ảnh đã không được tham dự kể từ khi nó được chụp.

- Phát hiện thay đổi luân phiên các hình ảnh được lưu trữ trong một thư viện kỹ thuật số. Trong trường hợp này, hình ảnh (ví dụ như dấu vân tay của con người) đã được quét và lưu trữ trong một thư viện kỹ thuật số; chủ sở hữu nội dung mong muốn khả năng phát hiển bất kỳ thay đổi luân phiên các hình ảnh, mà không cần phải so sánh các hình ảnh vào tài liệu quét.

1.6 Phân biệt giấu tin và thủy vân

Xét về tính chất, thủy vân giống giấu tin ở chỗ cả hai hướng này đều tìm cách nhúng thông tin mật vào một môi trường. Nhưng về bản chất thì thủy vân và giấu tin có những nét khác ở một số điểm sau:

- Mục tiêu của thủy vân là nhúng thông tin không lớn, thường là biểu tượng, chữ ký hay các đánh dấu khác vào môi trường phủ nhằm phục vụ việc xác nhận bản quyền. Ngược lại, giấu tin mật yêu cầu lượng thông tin giấu là lớn.
- Thủy vân khác với giấu tin mật ở chỗ giấu tin sau đó cần tách lại tin còn thủy vân tìm cách biến tin giấu thành một thuộc tính của vật mang.
- Chỉ tiêu quan trọng nhất của một thủy vân là tính bền vững, của giấu tin là dung lượng.
- Thủy vân có thể vô hình hoặc hữu hình trên vật mang còn giấu tin chỉ được vô hình.

1.7 Các kĩ thuật tấn công trên thủy vân

Việc tấn công thủy vân rất đơn giản, đó là việc tác động trực tiếp nên ảnh đã nhúng thủy vân. Tùy mức độ, mục đích tấn công mà ta chia các cuộc tấn công thành:

Tấn công đơn giản: Là dạng tấn công nhằm loại bỏ dấu thủy vân bằng cách tấn công trực tiếp nên toàn bộ dữ liệu nhúng. Việc tấn công này mang tính chất phá hủy mà không có ý định nhận dạng hay trích xuất thủy vân.

Tấn công phát hiện: Là sự tấn công nhằm loại bỏ đi mối quan hệ giữa dấu thủy vân và môi trường nhúng nhằm vô hiệu hóa khả năng khôi phục thủy vân. Việc không phát hiện được dấu thủy vân sẽ làm cho ảnh bị tấn công sai khác với ảnh ban đầu và không có cơ sở để khẳng định bản quyền. Các phép tấn công đơn giản được sử dụng như: nén, xoay, phóng to,...

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. 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 thủy vân ban đầu – thủy vân dùng để xác thực.

Tấn công loại bỏ: Là tấn công nhằm loại bỏ dấu thủy vân ra khỏi dữ liệu gốc và tách thành dữ liệu ban đầu và dấu thủy vân.

Chương 2

KỸ THUẬT THỦY VÂN SỐ

2.1 Một số khái niệm cơ bản về ảnh số

Ảnh số là tập hữu hạn các điểm ảnh với mức xám phù hợp dùng để mô tả ảnh gần với ảnh thật. Số điểm ảnh xác định độ phân giải của ảnh. Ảnh có độ phân giải càng cao thì càng thể hiện rõ nét các đặc điểm của tấm hình và càng làm cho ảnh trở nên thực và sắc nét hơn.

Điểm ảnh (pixel) là một phần tử của ảnh số tại tọa độ (x,y) với độ xám hoặc màu nhất định. Mỗi ảnh được biểu diễn bởi một ma trận điểm ảnh. Kích thước và khoảng cách giữa các điểm ảnh được chọn thích hợp sao cho mắt người cảm nhận được sự liên tục về không gian và màu ảnh gần như ảnh thật.

Mức xám của ảnh là kết quả của sự biến đổi tương ứng một giá trị độ sáng cảu một điểm ảnh với một giá trị nguyên dương. Thông thường nó xác định trong [0,255] tùy thuộc vào giá trị mà mỗi điểm ảnh biểu diễn.

Phân loại ảnh:

- Ảnh màu:Thông thường ảnh màu, 1 pixel được biểu diễn bằng 3 giá trị (R,G,B) trong đó R, G, B là một giá trị xám và biểu diễn bằng 1 byte. Khi đó ta có một ảnh 24bits.
- Ảnh xám: Giá trị xám nằm trong [0,255], mỗi điểm ảnh biểu diễn bởi 1 byte (8bit).
- Ảnh nhị phân: Giá trị xám của tất cả các điểm ảnh chỉ nhận giá trị 1 hoặc 0. Mỗi điểm ảnh biểu diễn bởi 1 bit.

2.2 Thủy vân số trên ảnh số

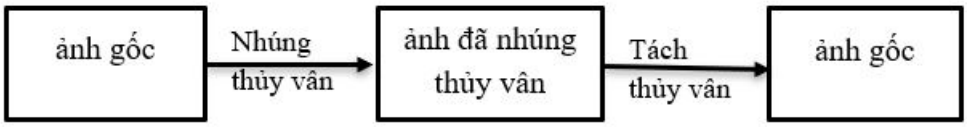
Thủy vân là phương pháp nhúng thông tin vào một tín hiệu kỹ thuật số như âm thanh, hình ảnh, video. Ngày nay, thủy vân được áp dụng rộng rãi và phổ biến trên ảnh số. Bởi sự bao trùm mạnh mẽ của internet, ảnh số được lan truyền trên các kênh truyền không tin cậy.

Vì vậy vấn đề thủy vân trên ảnh số nhằm bảo vệ bản quyền ảnh số rất quan trọng.

Thủy vân trên các ảnh số có nhiều loại:

- Thủy vân ảnh hiện: có thể nhìn ảnh qua chính đối tượng che mờ.
- Thủy vân ảnh dễ vỡ: là thủy vân khi nhúng vào trong ảnh, phân bố trên các môi trường mở và rất dễ bị thay đổi trước các tấn công. Thường áp dụng trong các lĩnh vực nhận thực thông tin và phát hiện xuyên tạc ảnh.
- Thủy vân ảnh bền vững: thủy vân được nhúng phải đảm bảo tính bền vững cùng với sản phẩm nhằm chống việc tẩy xóa, là giả hay biến đổi, phá hủy thủy vân. Dấu thủy vân nhúng vào ảnh như một hình thức dán tem bản quyền. Vì thế nó được áp dụng trong các ứng dụng bảo vệ bản quyền.

Ngoài ra, hiện nay một hướng nghiên cứu mới rất được quan tâm đó là vân thuận nghịch. Thủy vân thuận nghịch có thể khôi phục lại hình ảnh ban đầu mà không có bất kì sự biến dạng nào sau khi dữ liệu được trích ra sản phẩm đã nhúng thủy vân.



Hình 2.1: Mô hình thủy vân số thuận nghịch

Trong một số ứng dụng như y tế, quân sự, an ninh-quốc phòng, ảnh gốc cần phải được khôi phôi lại nguyên vẹn bên cạnh việc phục hồi thủy vân gốc là yêu cầu bắt buộc. Vì thế thủy vân thuận nghịch được nghiên cứu nhiều gần đây bởi nó có nhiều ứng dụng cũng như hàm lượng toán học cao.

Ngày nay thủy vân trên ảnh số được nghiên cứu dựa trên 2 hướng chính là thủy vân trên miền không gian và thủy vân trên miền tần số. Thủy vân trên miền không gian ra đời đầu tiên với các thuật toán đơn giản, tiếp đó là sự phát triển của các phương pháp thủy vân trên miền tần số. Hướng phát triển nghiên cứu này cho thấy ưu điểm rõ rệt về tính ẩn và bền vững của dấu thủy vân. Tuy nhiên mỗi hướng nghiên cứu đều có ưu nhược điểm riêng, cụ thể:

Nội dung	Thủy vân trên miền không gian	Thủy vân trên miền tần số
Đặc điểm	- Tác động trực tiếp lên miền dữ liệu ảnh gốc - Thay đổi giá trị trực tiếp điểm ảnh	- Tác động lên các miền biến đổi - Các phép biến đổi chuyển miền biến số độc lập sang các miền mới và thực hiện nhúng thủy vân trên các miền biến đổi mới.
Ưu điểm	- Thuật toán đơn giản, dễ cài đặt - Không cần vật phủ để trích xuất thủy vân - Dung lượng nhúng nhiều	- Bền vững hơn thủy vân trên miền không gian trước các phép biến đổi ảnh, năng lượng của ảnh tập trung vào các thành phần có tần số thấp nên khi nhúng vào đó thì những biến đổi sẽ phân bố trên toàn bộ ảnh.
Nhược điểm	- Do tác động trực tiếp trên điểm ảnh dẫn đến sự thay đổi lớn, ảnh thủy vân không bền vững để chống lại các phép xử lí ảnh (thủy vân không được phân bố trên toàn bộ ảnh).	- Thuật toán phức tạp hơn - Dung lượng nhúng không nhiều

Bảng 2.1: So sánh thủy vân trên miền không gian và thủy vân trên miền tần số

2.3 Một số kĩ thuật bổ trợ cho các kĩ thuật thủy vân

2.3.1 Phép biến đổi Fourier rời rạc

Phép biến đổi Fourier rời rạc DFT - Discrete Fourier Transform hay còn gọi là biến đổi Fourier hữu hạn, là một biến đổi trong giải tích Fourier cho các tín hiệu thời gian rời rạc sang miền tần số rời rạc.

Tín hiệu 1 chiều:

- Phép biến đổi Fourier rời rạc cho tín hiệu một chiều (1D DFT)

$$F(u) = \frac{1}{M} \sum_{x=0}^{M-1} f(x) e^{\frac{-i2\pi ux}{M}} \tag{2.1}$$

Biến đổi $e^{i\theta} = \cos\theta + i\sin\theta$ ta được:

$$F(u) = \frac{1}{M}\sum_{x=0}^{M-1} f(x)[\cos\frac{2\pi ux}{M} - i\sin\frac{2\pi ux}{M}] \tag{2.2}$$

Hay viết gọn lại:

$$F(u) = |F(u)|e^{-i\phi(u)}|F(u)| = [R^2(u) + I^2(u)]^{\frac{1}{2}} \tag{2.3}$$

Trong đó $|F(u)| = [R^2(u) + I^2(u)]^{\frac{1}{2}}$ được gọi là biên độ (phổ) của biến đổi Fourier

- Phép biến đổi Fourier ngược (1D IDFT)

$$f(x) = \frac{1}{M}\sum_{u=0}^{M-1} F(u)e^{\frac{i2\pi ux}{M}} \tag{2.4}$$

Tín hiệu 2 chiều:

- Phép biến đổi Fourier cho tín hiệu 2 chiều (2D DFT):

$$G(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} g(x,y)e^{-i\frac{2\pi(ux)}{M}}e^{-i\frac{2\pi(vy)}{N}} \tag{2.5}$$

Trong đó u, v là các tọa độ trục tần số,g(x,y) là ảnh gốc, G(u,v) là ảnh Fourier
$F(u,v)| = [R^2(u,v) + I2(u,v)]^{\frac{1}{2}}$ là phổ biên độ của ảnh Fourier

- Phép biến đổi ngược (2D IDFT)

$$g(x,y) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} G(u,v)e^{i\frac{2\pi(ux)}{M}}e^{i\frac{2\pi(vy)}{N}} \tag{2.6}$$

2.3.2 Phép biến đổi Cosin rời rạc

Phép biến đổi Cosin rời rạc (DCT) biểu thị một chuỗi hữu hạn của điểm dữ liệu xét về tổng số cosin các chức năng dao động ở các tần số.

DCT được đề xuất đầu tiên bởi Nasir Ahmed vào năm 1972, vận dụng rộng rãi trong xử lí tín hiệu và nén dữ liệu.

Một DCT là một biến đổi liên quan đến Fourier tương tự như biến đổi Fourier rời rạc, nhưng chỉ sử dụng số thực.

DCT biến đổi dữ liệu dưới dạng biên độ thành dữ liệu dưới dạng tần số. Mục đích: loại bỏ

sự dư thừa dữ liệu trong không gian DCT và chia làm 2 loại:

- DCT một chiều
- DCT hai chiều

Biến đổi DCT hai chiều tổng quát là biến đổi trong hai khối bất kì. Tuy nhiên các biến đổi DCT trên các miền 8×8 hay 16×16 được sử dụng nhiều nhất. Ta sẽ tìm hiểu phép biến đổi DCT trên khối 8×8 được sử dụng trong chuẩn nén JPEG.

Công thức biến đổi DCT thuận từ I(x,y) -> I(u,v) trên miền 8×8

$$I(u,v) = \frac{C(u)C(v)}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} I(x,y) \cos(\frac{(2x+1)u\pi}{16}) cos(\frac{(2y+1)v\pi}{16}) \tag{2.7}$$

Trong đó:

+ I(x,y) : hình ảnh đầu vào kích thước 8×8

+ I(x,y) : là cường độ pixel trong hàng i và cột j

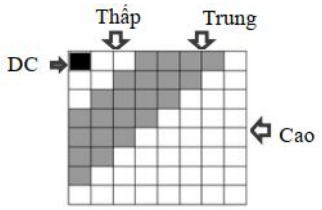
+ I(u,v) : là hệ số DCT và là số thực

Công thức biến đổi DCT ngược từ I(u,v) -> I(x,y)

$$I(x,y) = \frac{C(u)C(v)}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} I(u,v) \cos(\frac{(2x+1)u\pi}{16}) cos(\frac{(2y+1)v\pi}{16}) \tag{2.8}$$

Đặc điểm của phép biến đổi DCT trên ảnh hai chiều: Thể hiện đặc tính nội dung về tần số của thông tin ảnh. Hệ số góc trên là lớn và đặc trưng cho giá trị trung bình thành phần một chiều gọi là hệ số DC, còn các hệ số khác có giá trị nhỏ hơn biểu diễn cho các thành phần tần số cao theo hướng ngang và theo hướng thẳng đứng gọi là các hệ số AC.

Thực tế, hầu hết trong các thuật toán, ảnh gốc thường chia thành các khối ảnh có kích thước 8×8 và thực hiện các phép biến đổi DCT trên từng khối đó. Cấu trúc khối DCT thường gồm 3 miền: miền tần số cao, miền tần số trung, và miền tần số thấp:



Hình 2.2: Khối DCT cấu trúc 8×8

Theo tính chất của phép biến đổi Cosine rời rạc, năng lượng của ảnh thường tập trung vào

các hệ số góc trên bên trái của khối, đặc biệt là phần tử DC. Miền tần số thấp chứa các thông tin quan trọng ảnh hưởng lớn đến tri giác đến tri giác. Nghĩa là, một thay đổi nhỏ trên miền này cũng tác động ảnh hưởng đến trị giác. Các thông tin trong miền tần số cao thường không mang tính trị giác cao, khi nén JPEG thì thường loại bỏ thông tin trong miền này.

Trong các thuật toán thủy vân, biến đôi DCT trên miền tần số cao thường không được sử dụng do nó thường không bền vững với các phép xử lí ảnh hoặc nén ảnh. Miền tần số thấp cũng rất khó sử dụng do một sự thay đổi dù nhỏ cũng ảnh hưởng lớn đến tri giác và không đảm bảo tính ẩn của dấu thủy vân. Vì vậy, người ta thường tác động đến miền tần số trung để cân bằng tính bền vững và tính che giấu của ảnh thủy vân.

2.3.3 Phép biến đổi sóng nhỏ rời rạc DWT

Phép biến đổi wavelet rời rạc DWT - Discrete Wavelet Transform xuất hiện từ năm 1976 khi Crochisere, Weber và Flanagan đã dùng phép biến đổi wavelet rời rạc để mã hóa tiếng nói.

Đây là phép biến đổi mới nhất được áp dụng cho ảnh số nhằm khắc phục các hạn chế của phép biến đổi Fourier. 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.

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.

- Phép biến đổi thuận:

$$DWT_f(m,n) = \alpha_0^{\frac{-m}{2}} \int_{-\infty}^{\infty} f(t)\psi^*(\alpha_0^{-m}t - nb_0)dt \tag{2.9}$$

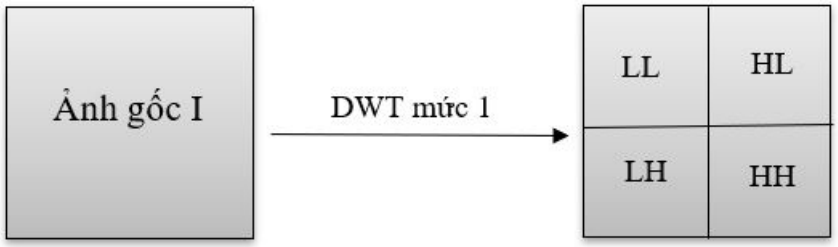
- Phép biến đổi nghịch:

$$f(t) = \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{+\infty} < \psi_{m,n}, f > \tilde{\psi}_{m,n}(t) \tag{2.10}$$

  Trong đó, $\psi(t)$ là hàm wavelet mẹ, điều kiện $\psi(t)$ là một hàm thông dài đảm bảo sự tồn tại của biến đổi sóng ngược. Thông thường người ta chọn $a_0 = 2$ và $b_0 = 1$.

Trong phép biến đổi DWT hai chiều, một ảnh gốc I sẽ được phân tích thành 4 băng tần có kích thước bằng $\frac{1}{2}$ ảnh gốc: LL (low frequency component in horizontal and direction), LH

(low frequency component in horizontal direction and high frequency in vertical direction), HL (high frequency component in horizontal direction and low frequency in vertical direction), HH (high frequency component in horizontal direction and high frequency in vertical direction). Hình 2.3 biểu diễn cho sự phân tích ảnh gốc $I(N \times N$ thành 4 băng tần LL, LH, HL, HH có kích thước $(\frac{N}{2}, \frac{N}{2})$.



Hình 2.3: Một ví dụ về phép biến đổi DWT hai chiều ở mức 1

Các kĩ thuật thủy vân sử dụng phép biến đổi DWT thường nhúng watermark vào một hoặc một số băng tần với các hệ số tương quan khác nhau. Do LL có tần số thấp và chứa các thông tin quan trọng của ảnh nên một sự thay đổi nhỏ cũng ảnh hưởng đến chất lượng hình ảnh. Băng tần HH có tần số cao nên không bền vững trước các sự tấn công như nén JPEG. Do đó để cân bằng tính bền vững và tính ẩn của ảnh thủy vân, các thuật toán hiện nay đều sử dụng các băng tần HL, LH để nhúng thủy vân.

Phép biến đổi sóng có rất nhiều lợi thế so với các biến đổi khác, đó là :

+ Biến đổi sóng là một mô tả đa độ phân giải của ảnh. Quá trình giải mã có thể được xử lý tuần tự từ độ phân giải thấp cho đến độ phân giải cao.
+ Biến đổi DWT gần gũi với hệ thống thị giác người hơn biến đổi DCT. Vì vậy, có thể nén với tỉ lệ cao bằng DWT mà xác định sự biến đổi khó nhận thấy hơn nếu dùng DCT với tỉ lệ này.

2.4 Các thuật toán thủy vân trên ảnh

2.4.1 Thuật toán thủy vân trên miền không gian

Ý tưởng

Thuật toán thủy vân nhúng các bit trên miền không gian của ảnh.

Thuật toán thủy vân dựa vào các bít ít quan trọng LSB là một thuật toán tiêu biểu cho lớp các thuật toán trên miền không gian ảnh.

Cụ thể, 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.

Chẳng hạn với 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. Sử dụng một tính chất của mắt người là sự cảm nhận về màu B (Blue) kém hơn so với hai màu R, G. Vì thế trong thuật toán này thường chọn bit cuối cùng trong 8 bit biểu diễn màu B của mỗi điểm giấu thủy vân. Thay đổi bit cuối cùng trong 8 bit biểu diễn màu B chỉ làm cho giá trị biểu diễn màu B tăng hoặc giảm đi 1. Do đó, các bit ít quan trọng nhất trong trường hợp này là bit thứ 24 của mỗi điểm ảnh.

Nhận xét

- Các thuật toán nhúng thủy vân trên miền không gian đơn giản, dễ cài đặt.
- Dung lượng nhúng lớn.
- Tuy nhiên việc thay đổi trực tiếp trên các điểm ảnh gốc tác động lớn đến chất lượng ảnh, thủy vân nhúng tập trung mà không phân bố trên toàn ảnh. Chất lượng ảnh thủy vân thấp và dễ bị tấn công bởi các phép biến đổi.

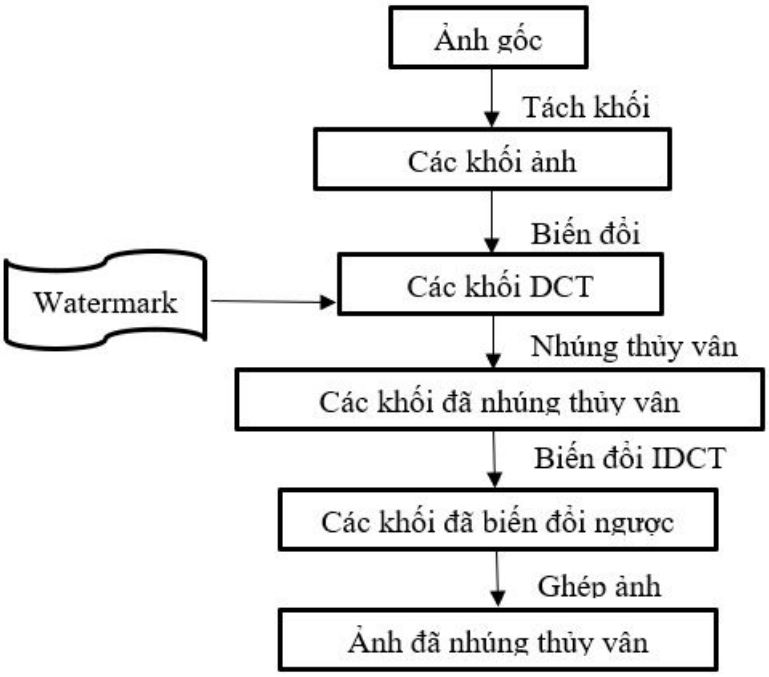
2.4.2 Thuật toán thủy vân DCT trên miền tần số

2.4.2.1 Ý tưởng chung

Các thuật toán dùng phép biến đổi DCT thường chia ảnh gốc thành các khối, thực hiện phép biến đổi DCT với từng khối ảnh gốc để được miền tần số thấp, miền tần số giữa và miền tần số cao. Đa số các thuật toán thủy vân bền vững hiện nay đều chọn nhúng thủy vân trên miền số trung để đảm bảo tính ẩn và độ bền vững của thủy vân.

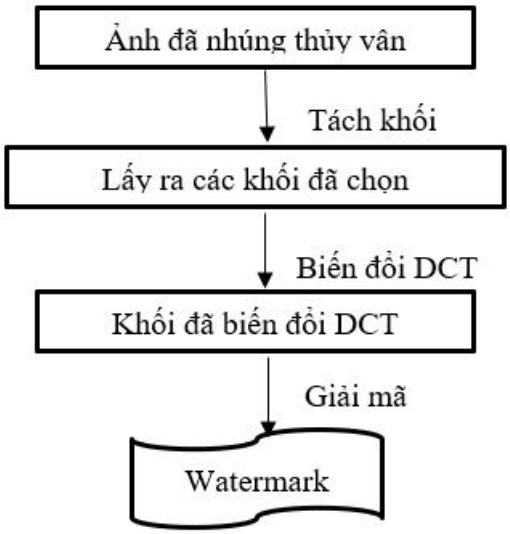
Cho đến nay có nhiều thuật toán DCT, tuy nhiên các thuật toán đều theo một sơ đồ chung.

Quá trình nhúng thủy vân



Hình 2.4: Sơ đồ chung quá trình nhúng thủy vân bằng DCT

Quá trình trích xuất thủy vân



Hình 2.5: Sơ đồ chung quán trình trích xuất thủy vân bằng DCT

2.4.2.2 Thuật toán DCT 1

Ý tưởng

Thuật toán được đề xuất năm 2002 của 2 tác giả Nguyễn Xuân Huy và Trần Quốc Dũng. Thuật toán nhúng mỗi bit thủy vân vào vị trí giữa hai hệ số bất kì trong miền tần số giữa của khối DCT.

Mô tả thuật toán

- Input
  Một chuỗi các bít thể hiện bản quyền
  Một ảnh
- Output:
  Một ảnh sau khi thủy vân
  Khóa để giải mã.

Thuật toán

- Quá trình thủy vân
  - Bước 1: Chia ảnh gốc ban đầu có kích thước $m \times n$ thành $(m \times n)/64$ khối 8×8, mỗi bit sẽ được giấu trong một khối.
  - Bước 2: Chọn một khối I bất kì và biến đổi DCT khối đó thu được $I^{'}$.
  - Bước 3: 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:
    $$d = ||b^{'}(i,j) - b^{'}(p,q)|| \mod a \tag{2.11}$$
    Trong đó a là tham số thỏa mã $a = 2(2t+1)$, t là một số nguyên dương
    Bit s_i sẽ được nhúng sao cho thỏa mãn điều kiện sau:
    $$\begin{cases} d \geq 2t+1 & \text{nếu } s_i = 1 \\ d < 2t+1 & \text{nếu } s_i = 0 \end{cases}$$
    + Nếu $d < 2t+1$ và $s_i = 1$ thì một trong hai hệ số DCT $b^{'}(i,j)$ hoặc $b^{'}(p,q)$ có giá trị tuyệt đối lớn hơn sẽ bị thay đổi để $d \geq 2t+1$ theo công thức sau:
      $$max(|b^{'}(i,j)|, |b^{'}(p,q)|) + (INT(0.75 \times a) - d) \tag{2.12}$$
      Với hàm $max(|b^{'}(i,j)|, |b^{'}(p,q)|)$ là hàm chọn ra hệ số có giá trị tuyệt đối lớn hơn, hệ số được chọn sẽ được cộng thêm một lượng $(INT(0.75 \times a) - d)$

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

$$min(|b^{'}(i,j)|, |b^{'}(p,q)|) - (INT(0.25 \times a) + d) \quad (2.13)$$

Với hàm $min(|b^{'}(i,j)|, |b^{'}(p,q)|)$ là hàm chọn ra hệ số có giá trị tuyệt đối nhỏ hơn, hệ số được chọn sẽ được trừ thêm một lượng $(INT(0.25 \times a) + d)$

+ Tương tự, nếu $d \geq 2t+1$ 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 bị thay đổi để $d < 2t+1$ theo công thức sau:

$$max(|b^{'}(i,j)|, |b^{'}(p,q)|) - (d - INT(0.25 \times a)) \quad (2.14)$$

Hoặc

$$min(|b^{'}(i,j)|, |b^{'}(p,q)|) + (INT(1.25 \times a) - d) \quad (2.15)$$

- Bước 4: Quay lại bước 2 cho đến khi nhúng hết các bit giấu vào các khối .
- Bước 5: Biến đổi IDCT các khối.
- Bước 6: Ghép các khối ta được ảnh nhúng thủy vân.

• Quá trình trích xuất thủy vân

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

$$d = ||b^{'}(i,j) - b^{'}(p,q)|| \mod a \quad \text{với } a = 2(2t+1) \quad (2.16)$$

- Nếu $d \geq 2t+1$ thì gán $s_i = 1$
- Nếu $d < 2t+1$ thì gán $s_i = 0$

2.4.2.3 Thuật toán DCT 2

Thuật toán do R.Munir đề xuất năm 2008 với thuật toán thủy vân sử dụng cặp khóa bí mật công khai trên miền DCT. Đây là một thuật toán thủy vân bền vững áp dụng trong việc xác thực bản quyền tác giả.

Ý tưởng thuật toán

- Sử dụng các hệ số DCT thuộc tần miền trung (trừ phần tử DC) để nhúng dấu thủy vân. Sử dụng cặp khóa bí mật công khai để nhúng tin.
- Một số kí hiệu
  + I ảnh gốc ban đầu cần nhúng thủy vân

+ $I^{'}$ ảnh sau nhúng thủy vân
+ $W = (\omega_1, \omega_2, ..., \omega_n)$ dấu thủy vân
+ $P = (p_1, p_2, ..., p_n)$ khóa công khai
+ $S = (s_1, s_2, ..., s_n)$ khóa bí mật
+ $D = (d_1, d_2, ..., d_n)$ các hệ số DCT được chọn để nhúng thủy vân

Thuật toán

- Quá trình nhúng thủy vân
  - Bước 1: Chia ảnh gốc ban đầu thành các khối 8×8 và thực hiện phép biến đổi DCT trên các khối đó, sau đó xác định dãy $D = (d_1, d_2, ..., d_n)$ (trong miền tần số trung bình trên các khối DCT của ảnh I) dùng để nhúng thủy vân.
  - Bước 2: Tạo khóa công khai $P = (p_1, p_2, ..., p_n)$ là dãy số thực được tạo ngẫu nhiên theo phân phối chuẩn $N(0, 1)$.
  - Bước 3: Xác định khóa bí mật $S = (s_1, s_2, ..., s_n)$ là một hoán vị ngẫu nhiên của P.
  - Bước 4: Xác định dấu thủy vân $W = (\omega_1, \omega_2, ..., \omega_n)$ theo công thức:

$$\omega_i = \lambda p_i + (1 - \lambda) s_i \qquad \text{với} \quad 0 < \lambda < 1 \tag{2.17}$$

  - Bước 5: Nhúng thủy vân theo công thức:

$$d_i^{'} = d_i + \sigma |d_i| \omega_i \qquad \text{với} \quad 0 < \sigma < 1 \tag{2.18}$$

  - Bước 6: Thực hiện phép biến đổi IDCT trên các khối DCT đã nhúng thủy vân, ghép lại ta được ảnh $I^{'}$.
- Thuật toán kiểm tra dấu thủy vân
  - Chẳng hạn, qua một số phép tấn công, ảnh $I^{'}$ trở thành ảnh I^*. Để kiểm tra dấu thủy vân trên ảnh I^* có thuộc quyền sở hữu của tác giả ảnh $I^{'}$ hay không. Ta sử dụng hệ số tương quan giữa khóa P và dãy D^* (dãy hệ số DCT của ảnh I^*) được tính như sau:

$$Corr(D^*, P) = \frac{1}{n} \sum_{i=1}^{n} d_i^* p_i \tag{2.19}$$

  - Hệ số tương quan $Corr(D^*, P)$ được so sánh với ngưỡng T: nếu $Corr(D^*, P) >$

T thì kết luận I^* có nhúng thủy vân và vẫn thuộc về tác giả có ảnh $I^{'}$. Trong các thực nghiệm ta chọn $T = 0.5$.

- Cải tiến thuật toán

  - Ta thấy, mục đích của việc tấn công nhằm tạo ra ảnh mới I^* gần giống với ảnh $I^{'}$ đã được khẳng định bản quyền tác giả. Trong trường hợp ảnh I^* sai khác ít so với $I^{'}$ thì hệ số tương quan $Corr(D^*, P)$ xấp xỉ bằng $Corr(D^{'}, P)$. Như vậy, tính bền vững phụ thuộc vào $Corr(D^{'}, P)$. Cụ thể, giá trị này càng lớn thì tính bền vững của thuật toán càng cao, hệ số này nhỏ thì tính bền vững thấp.

  - Qua phân tích ta nhận thấy $Corr(D^{'}, P)$ phụ thuộc vào việc xây dựng khóa bí mật S. Như vậy, thuật toán cải tiến tính bền vững của thuật toán bằng cách xây dựng khóa bí mật S dựa trên sự hoán vị ngẫu nhiên trong các tập con.

  - Thuật toán cải tiến thực hiện các bước giống như thuật toán R.Munir và chỉ khác ở cách xây dựng khóa bí mật S. Thuật toán xây dựng khóa $S = (s_1, s_2, ..., s_n)$ từ khóa công khai $P = (p_1, p_2, ..., p_n)$ như sau:

    + Bước 1: Phân hoạch tập N thành các tập con
      $N^k = \{\alpha(k,1), \alpha(k,2), ..., \alpha(k,\beta_k)\}$, $k = 1...m$ thỏa mãn cả hai tính chất:

      1. $max\{p_j | j \in N^k\} \leq min\{p_j | j \in N^{k+1}\}$
      2. Các phần tử p_j với $i \in N^k$ có cùng dấu

    + Bước 2: Hoán vị ngẫu nhiên tập N^k để nhận được dãy

      $$R^k = (\sigma(k,1), ..., \sigma(k,\beta_k)$$

    + Bước 3: Xác định khóa bí mật $S = (s_1, s_2, ..., s_n)$ theo công thức:

      $$s_{\sigma(k,i)} = p_{\alpha(k,i)}, \quad \text{với} \quad i = 1, ..., \beta_k, k = 1...m$$

    Ví dụ: Xây dựng khóa bí mật S từ khóa công khai
    $P = (0.6, -0.4, 0.2, -0.6, 0.5, 0.4, 0.5, -0.8, 0.2, -0.4)$
    $N = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

    + Giả sử phân hoạch N thành 3 tập con:
      $N^1 = \{2, 4, 8, 10\}$, $N^2 = \{3, 6, 9\}$, $N^3 = \{1, 5, 7\}$

    + Ba hoán vị ngẫu nhiên tương ứng của N^1, N^2, N^3 là
      $R^1 = \{4, 2, 10, 8\}$, $R^2 = \{9, 3, 6\}$, $R^3 = \{5, 7, 1\}$

+ Khóa bí mật S là :
$S = (0.5, -0.6, 0.4, -0.4, 0.6, 0.2, 0.5, -0.4, 0.2, -0.8)$

- Thực nghiệm thực tế đã chứng minh thuật toán cải tiến R.Munir bằng cách xây dựng khóa bí mật dựa trên hoán vị ngẫu nhiên trên các tập con đã đảm bảo tính bền vững của ảnh thủy vân và chống được một số phép tấn công điển hình như: thêm nhiễu, cắt, lọc, nén JPEG, thay đổi kích thước, xoay, ...

2.4.3 Thuật toán thủy vân trên miền DWT

Thủy vân số trên miền DWT là phương pháp mới, nó cho thấy khả năng bền vững của ảnh thủy vân không chỉ trong việc chống lại các tấn công thông thường mà còn chống lại các loại biến đổi cấp xám.

Các loại biến đổi cấp xám khác với các tấn công khác ở chỗ chúng thường không gây ra sự suy giảm về mặt chất lượng ảnh. Đôi khi cân bằng histogram được sử dụng như một quá trình nâng cao chất lượng ảnh. Nhưng chúng thường gây ra những thay đổi trầm trọng về ảnh do đó chúng sẽ làm hỏng thủy vân được nhúng vào trong ảnh.

Ý tưởng

- Sử dụng một hệ số trong cặp tần số giữa để lượng tử hóa hệ số còn lại. Bước lượng tử hóa là phần cố định của hệ số lớn hơn. Lựa chọn hệ số nhỏ hơn để thực hiện lượng tử hóa. $\frac{1}{3}$các giá trị lớn nhất của tất cả các hệ số được lựa chọn là các hệ số quan trọng để thực hiện việc lượng tử hóa. Đối với các hệ số nhỏ sử dụng một bước duy nhất để lượng tử hóa.

- Đầu vào là ảnh I kích thước $m \times n$, ảnh nhị phân thủy vân W kích thước $r \times l$.

Thuật toán

- Kỹ thuật nhúng thủy vân

  - Bước 1: Ảnh gốc được chia thành 2 mức. Nhúng thủy vân vào các dải LH_2 và HL_2. Thủy vân được nhúng ít nhất $\frac{m \times n}{r \times l}$ lần.

  - Bước 2: Ngưỡng T của các hệ số nhỏ đặt băng tầm quan trọng của hệ số lớn nhất trong $\frac{1}{3}$ các gái trị lớn nhất của tất cả hệ số trong dải LH_2 và HL_2 . S (step) là khoảng chia cố định và D là số chia cố định. Thủy vân được nhúng vào dải LH_2 và HL_2 cho đến khi tất cả các hệ số đều được lượng tử hóa. Mỗi vị trí (i, j) được lượng tử hóa theo 1 bit thủy vân. Nếu bit này = 1, hệ số được làm tròn đến con số lẻ gần nhất, nếu không nó được làm tròn đến con số chẵn gần nhất.

  - Bước 3: Thực hiện IDWT 2 chiều để lập thành ảnh thủy vân.

- Kỹ thuật tách thủy vân

Thuật toán:
For tất cả hệ số trong dải LH_2 và HL_2
IF $ABS(HL_2(i,j) < T \& ABS(LH_2(i,j) < T$:
Lượng tử hóa $LH_2(i,j)$ và $HL_2(i,j)$ bằng khoảng cách cố định S;
Else:
$max = Max(ABS(HL_2(i,j), ABS(LH_2(i,j))$
If $max = ABS(HL_2(i,j)$
Lượng tử hóa $LH_2(i,j)$ bằng $\frac{max}{D}$
Else:
Lượng tử hóa $HL_2(i,j)$ bằng $\frac{max}{D}$
End if
End if
End for.

Hình 2.6: Thuật toán nhúng thủy vân vào trong các dải LH_2 và HL_2

Ảnh thủy vân được tách thành 2 mức. Các bit thủy vân $b(i,j)$ lấy ra được tại các vị trí (i,j) trong tần số giữa là:

Thuật toán:
For tất cả hệ số trong dải LH_2 và HL_2
If $ABS(HL_2(i,j) < T \& ABS(LH_2(i,j) < T$
$b(i,j) = \frac{\frac{LH_2(i,j)}{S} \mod 2 + \frac{HL_2(i,j)}{S} \mod 2}{2}$
Else
Max = $Max(ABS(HL_2(i,j), ABS(LH_2(i,j))$
step = $\frac{max}{D}$
IF Max = $ABS(HL_2(i,j)$
$b(i,j) = \frac{LH_2(i,j)}{step} \mod 2$
Else
$b(i,j) = \frac{HL_2(i,j)}{step} \mod 2$
End if
End if
End for.

Hình 2.7: Thuật toán tách thủy vân vào trong các dải LH_2 và HL_2

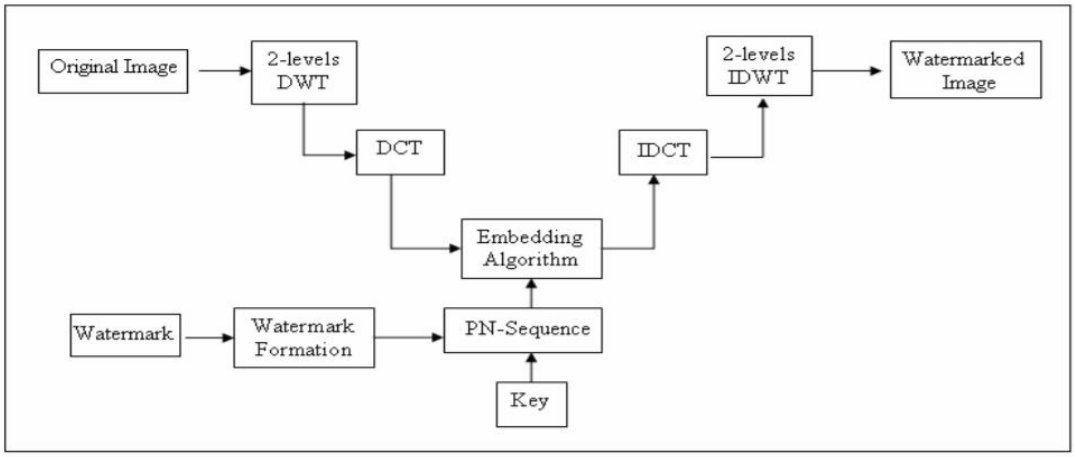
2.4.4 Thuật toán thủy vân kết hợp DCT - DWT

Ý tưởng

Áp dụng kết hợp hai phép biến đổi DCT và DWT để có thể bù đắp hạn chế của nhau. Thủy vân được thực hiện bởi thay hệ số wavelet của các băng con DWT được lựa chọn, sau đó áp dụng biến đổi DCT trên các dải băng con đó.

Thuật toán

- Sơ đồ nhúng thủy vân theo DCT-DWT kết hợp



Hình 2.8: Sơ đồ nhúng thủy vân theo DCT-DWT kết hợp

Cụ thể:

- Bước 1: Áp dụng DWT để chia ảnh gốc thành 4 dải : LL_1, HL_1, LH_1, và HH_1.
- Bước 2: Áp dụng DWT một lần nữa cho băng tần phụ HL_1 để có 4 dải con nhỏ hơn và chọn dải HL_2, hoặc áp dụng DWT cho băng con HH_1 và chọn băng con HH_2.
- Bước 3: Chia băng con HL_2 (hoặc HH_2) thành các khối 4×4.
- Bước 4: Áp dụng DCT cho từng khối trong các băng con đã chọn
- Bước 5: Định dạng lại dấu thủy vân thành ảnh nhị phân 0, 1
- Bước 6: Tạo hai chuỗi giả ngẫu nhiên không tương quan. Một chuỗi nhúng watermark bit 0 (PN_0), và chuỗi khác nhúng watermark bit 1 (PN_1). Số phần tử trong hai chuỗi dải ngẫu nhiên phải bằng số phần tử dải giữa của các dải con DWT được biến đổi DCT.
- Bước 7: Nhúng các bit thủy vân vào miền tần số trung của các khối DCT 4×4 được chọn. Với D là ma trận hệ số tần số trung được chọn, việc nhúng thực hiện

như sau:

Nếu bit nhúng là 0 thì:

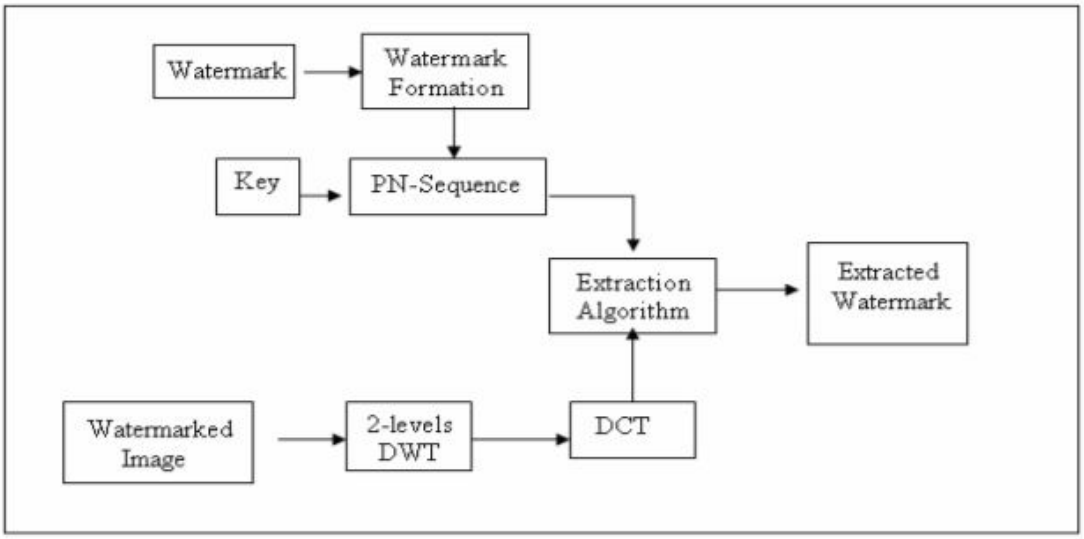
$$D^{'} = D + \alpha PN\_0 \tag{2.20}$$

Nếu bit nhúng là 1 thì:

$$D^{'} = D + \alpha PN\_1 \tag{2.21}$$

- Bước 8: Áp dụng IDCT cho các khối đã được nhúng thủy vân
- Bước 9: Áp dụng IDWT cho ảnh đã được nhúng ta được ảnh thủy vân.

• Sơ đồ trích xuất thủy vân



Hình 2.9: Sơ đồ trích thủy vân theo DCT-DWT kết hợp

Cụ thể:

- Bước 1: Áp dụng DWT chia ảnh thủy vân thành 4 băng con
- Bước 2: Áp dụng DWT một lần nữa cho băng tần phụ HL_1 để có 4 dải con nhỏ hơn và chọn dải HL_2, hoặc áp dụng DWT cho băng con HH_1 và chọn băng con HH_2.
- Bước 3: Chia băng con HL_2 (hoặc HH_2) thành các khối 4×4.
- Bước 4: Áp dụng DCT trong mỗi khối chọn và trích xuất thủy vân ở miền tần số trung.
- Bước 5: Tạo lại hai chuỗi giả ngẫu nhiên PN_0 và PN_1
- Bước 6: Với mối khối trong băng tần phụ HL_2 (hoặc HH_2), tính hệ số tương

quan giữa dải tần số trung và dải ngẫu nhiên PN_0 và PN_1. nếu hệ số tương quan với PN_0 cao hơn với PN_1 thì bit trích xuất là 0, ngược lại là 1.

- Bước 7: Tạo lại dấu thủy vân bằng các bit trích xuất.

2.5 Tham số đánh giá lược đồ thủy vân

PSNR: Được sử dụng để đo chất lượng tín hiệu khôi phục của các thuật toán nén có mất mát dữ liệu. Hệ số PSNR càng cao thì chất lượng dữ liệu khôi phục càng tốt.

PSNR được tính theo công thức:

$$PSNR = 20\log_{10}(\frac{MAX}{\sqrt{MSE}}) \tag{2.22}$$

Trong đó MAX là giá trị cực đại của điểm ảnh và MSE được xác định theo công thức:

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(I(i,j) - I^{'}(i,j))^2 \tag{2.23}$$

Với I là ảnh gốc, $I^{'}$ là ảnh sau nhúng thủy vân.

Giá trị thông thường của PSNR trong ảnh nén và video nằm từ 30 đến 50dB, giá trị càng cao thì càng tốt. Khi 2 ảnh đồng nhất thì MSE sẽ bằng 0. Trong trường hợp này tỉ số PSNR không xác định.

ERR: là tỉ lệ sai khác giữa thủy vân trích được W^* so với thủy vân gốc W được tính theo công thức:

$$ERR = \frac{1}{t}\sum_{i=1}^{t}|W_i - W_i^*| \tag{2.24}$$

Lược đồ có ERR càng nhỏ chứng tỏ lược đồ đó càng bền vững.

Độ bền là thước đo khả năng miễn dịch của dấu thủy vân sau các cuộc tấn công. Để kiểm tra ảnh thủy vân sau tấn công còn thuộc quyền sở hữu của tác giả hay không ta sử dụng hệ số tương quan:

$$Corr(w,\hat{w}) = \frac{\sum_{i=1}^{N} w_i\hat{w}_i}{\sqrt{\sum_{i=1}^{N} {w_i}^2}\sqrt{\sum_{i=1}^{N} {\hat{w}_i}^2}} \tag{2.25}$$

Trong đó N là số pixel trên dấu thủy vân, w và $\hat{w}$ là dấu thủy vân gốc và trích xuất tương ứng. $Corr(w,\hat{w})$ có giá trị trong khoảng từ 0 đến 1, thông thường hệ số này lớn hơn 0.7 thì chấp nhận được.

Chương 3

XÂY DỰNG CHƯƠNG TRÌNH THỬ NGHIỆM

3.1 Phát biểu bài toán

Xây dựng chương trình thử nghiệm thủy vân số trên miền không gian và tần số, cụ thể là thuật toán DCT-1, thuật toán DWT, thuật toán DCT-DWT kết hợp sau đó rút ra nhận xét đánh giá.

Mục đích: Kiểm tra kết quả thủy vân của thuật toán, dựa vào kết quả sẽ tiến hành đánh giá, nhận xét phương pháp, đưa về kết luận về chất lượng thuật toán.

3.2 Phương pháp thực nghiệm

Xây dựng chương trình trên nền tảng Python.

Các thử nghiệm được thực hiện trên bộ dữ liệu gồm 9 ảnh, định dạng *.PNG. Trong đó 8 ảnh sẽ lần lượt là ảnh gốc, và 01 ảnh là ảnh nhúng thủy vân. Các ảnh đều được lưu chung vào trong một thư mục để dùng chung cho cả 3 thuật toán.

Hình 3.1: Ảnh gốc

Hình 3.2: Dấu thủy vân

Các thử nghiệm được tiến hành lần lượt từ ảnh thứ nhất đến ảnh cuối cùng, sau đó thực hiện phép tính thống kê đánh giá khách quan, tổng quát dựa trên nhiều ảnh khác nhau.

Đánh giá chất lượng của ảnh ở đầu ra thông qua 2 tham số MSE và PSNR so với ảnh gốc ban đầu . Cụ thể: Đo giá trị PSNR giữa ảnh gốc (ảnh ban đầu) và ảnh chứa dấu thủy vân, để minh chứng về ảnh hưởng của phép biến đổi của thủy vân với môi trường. So sánh giá trị PSNR của các thuật toán khác nhau để đưa ra nhận xét về chất lượng của thủy vân.

3.3 Kết quả thử nghiệm

- Ảnh đã nhúng thủy vân, dấu thủy vân trích xuất qua các thuật toán:

Hình 3.3: Ảnh sau nhúng thủy vân, dấu thủy vân trích xuất thuật toán DCT-DWT

Hình 3.4: Ảnh sau nhúng thủy vân, dấu thủy vân trích xuất thuật toán DWT

Hình 3.5: Ảnh sau nhúng thủy vân, dấu thủy vân trích xuất thuật toán DCT

- Bảng chỉ số PSNR của các ảnh qua mỗi thuật toán:

Ảnh	DCT	DWT	DCT-DWT
ảnh1.png	44.58	49.18	70.03
ảnh2.png	45.11	49.69	69.37
ảnh3.png	44.33	48.74	69.65
ảnh4.png	45.23	49.63	70.04
ảnh5.png	44.06	48.14	70.54
ảnh6.png	43.43	48.23	69.33
ảnh7.png	44.44	48.59	69.01
ảnh8.png	43.99	48.25	70.55
TB	44.39	48.81	69.82

Bảng 3.1: Bảng chỉ số PSNR

3.4 Nhận xét, đánh giá

Qua bảng chỉ số PSNR ta có thể rút ra một số kết luận:

- Các chỉ số PSNR của cả hai thuật toán DCT-1 và DWT dao động trong khoảng 45-50dB, cho thấy thuật toán thủy vân đã làm thay đổi môi trường, tuy nhiên độ thay đổi này là nhỏ. Với chỉ số PSNR này mắt thường khó có thể phân biệt được ảnh gốc và ảnh đã thay đổi.
- Các chỉ số PSNR của thuật toán giấu tin trên miền DWT cao hơn thuật toán giấu tin trên miền DCT.
- Thuật toán cải tiến kết hợp DCT - DWT nhằm loại bỏ các khuyết điểm của 2 phép biến đổi DCT, DWT trên cơ sở bù đắp khuyết điểm của nhau cho thấy độ hiệu quả rõ rệt thể hiện ở chỉ số PSNR nằm trong khoảng 70dB. Đây là một chỉ số lớn, mắt thường không thể nhận biết được sự thay đổi của ảnh.
- Thuật toán thủy vân kết hợp DCT-DWT cho dấu thủy vân trích xuất với chất lượng cao hơn 2 thuật toán DCT và DWT.

Như vậy ta thấy, các thuật toán giấu tin trên các miền DCT, DWT đã cho ta thấy độ hiệu quả của nó khi chỉ số PSNR luôn nằm mức chấp nhận được. Vì vậy, ngày nay hướng nghiên cứu thủy vân trên miền tần số luôn là hướng nghiên cứu chính và được áp dụng hiệu quả trong nhiều lĩnh vực nhất là bảo vệ bản quyền ảnh số.

KẾT LUẬN

Sau quá trình nghiên cứu và tìm hiểu cùng với sự hướng dẫn của thầy giáo hướng dẫn, ThS.Lê Quang Hòa em đã hoàn thành bài báo cáo của mình. Nội dung chủ yếu của báo cáo là nghiên cứu về hệ thống thủy vân số, các hướng ứng dụng của thủy vân số trong bảo vệ bản quyền ảnh số. Thủy vân số là một vấn đề mới, và do khả năng kiến thức của em còn hẹp nên báo cáo chỉ dừng lại ở việc tìm hiểu lí thuyết thủy vân và một số thuật toán áp dụng đơn giản để đưa ra nhận xét giữa các hướng nghiên cứu thủy vân hiện nay.

Qua quá trình nghiên cứu đề tài, đã đạt được một số kết quả sau:

- 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 và so sánh thủy vân và giấu tin mật.
- Tìm hiểu một số thuật toán thủy vân đã được nghiên cứu trong ảnh theo hai hướng chính là thủy vân trên miền không gian và thủy vân trên miền tần số.
- Xây dựng được chương trình và chạy thử nghiệm trên Python, từ đánh giá độ hiệu quả của các thuật toán thủy vân trên miền tần số.

Đề tài chỉ ở mức đơn giản, đây sẽ là nền tảng cho các bước nghiên cứu mới của em trong thời gian tới. Từ đề tài, chúng ta nhận thấy được thủy vân số đã và vẫn đang càng được nghiên cứu theo hướng bền vững và phát triển các thuật toán trên miền tần số với tính giấu tin cao. Cho thấy, thủy vân ngày càng có ý nghĩa quan trọng trong kỹ thuật số bảo vệ bản quyền, không những áp dụng trong thương mại mà còn mở ra một tiếp cận mới cho vấn đề bảo vệ bản quyền dữ liệu số.

Tài Liệu Tham Khảo

[1] Đ. V. Tuấn, T. Đ. Hiên, C. T. Luyên, and P. V. Ất, "Một thuật toán thủy vân bền vững khóa công khai cho ảnh màu dựa trên hoán vị ngẫu nhiên trong các tập con," *Tạp chí Thông tin và Truyền thông*, Jun. 2013.

[2] V. T. C, V. P. Hưng, T. H. Nam, N. T. Sơn, and Đ. T. Nghị, "Một thuật toán thủy vân ảnh số mạnh dựa trên DWT DCT SVD và đặc trưng SIFT," *Kỷ yếu Hội nghị Quốc gia lần thứ XII về Nghiên cứu cơ bản và ứng dụng của Công Nghệ thông tin (FAIR)*, 2019.

[3] N. X. Huy and T. Q. Dũng, "Một thuật toán thủy vân ảnh trên miền DCT JPEG," *Tạp chí Thông tin và Truyền thông*, 2002.

[4] T. N. Tiến, "Bài giảng an toàn dữ liệu," 2008.

[5] N. X. Huy and T. Q. Dũng, "Giáo trình giấu tin và thủy vân trong ảnh," *Đại học quốc gia hà Nội*, 2003.

[6] T. T. T. Uyên, "Luận văn thạc sĩ: Hệ thống thủy vân số và ứng dụng thủy vân số trong bảo vệ bản quyền ảnh số," *Đại học quốc gia hà Nội*, 2017.

[7] Đ. T. Cần, " Đồ án tốt nghiệp: Hệ thống thủy vân số và một số thuật toán thủy vân số thuận nghịch," *Đại học bách khoa Hà Nội*, 2021.

[8] P. T. T. Trang, "Báo cáo khoa học: Kĩ thuật phát hiện thông tin ẩn giấu trong ảnh JPEG2000," *Đại học Dân lập Hải Phòng*, 2009.

[9] R. Munir, B. Riyanto, S. Sutikno, and W. P. Agung, "Derivation of Barni Algorithm into Its Asymmetric Watermarking Technique Using Statistica Approach," *International Journal on Electrical Engineering and Informatics*, vol. 1, no. 2, 2009.

[10] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-Domain System for Robust Image Watermarking," *Signal Processing 66*, vol. 1, no. 2, pp. 357–372, 1998.

[11] A. A. Haj, "Combined DWT-DCT Digital Image Watermarking," *Journal of Computer Science*, vol. 3, no. 9, 2007.

[12] M. Wu and B. Liu, "Data Hiding in Binary Image for Authentication and Annotation," *IEEE Transactions on Multimedia*, vol. 6, no. 4, Aug. 2004.

[13] Q. Yuan, H. Yao, W. Gao, and S. Joo, “Blind watermarking method based on DWT middle frequency pair,” *IEEE International Conference*, vol. 2, pp. 473–476, 2002.