ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

DIGITAL WATERMARKING

BÁO CÁO BÀI TẬP LỚN MÔN XỬ LÝ ẢNH

Ngành: Khoa học máy tính

Mã học phần INT3404E 21

Giảng viên: Nguyễn Thị Ngọc Diệp

Nhóm: 7

Thành viên: Nguyễn Đức Hoàng Long - 20021386
Đặng Hoàng Long - 20020144
Phạm Đức Thắng - 20020156
Ngô Đình Ngọc Quang - 19021355
Nguyễn Trung Tú - 20021462

HÀ NỘI - 2023

TÓM TẮT

Trong thế giới kỹ thuật số ngày nay, việc sao chép, sửa đổi, tái sản xuất và phân phối hình ảnh trở nên dễ dàng hơn bao giờ hết nhờ vào sự phát triển của công nghệ xử lý hình ảnh và mạng internet. Với chi phí thấp và khả năng phân phối gần như ngay lập tức, việc truyền tải hình ảnh kỹ thuật số đã trở nên phổ biến hơn bao giờ hết, và người dùng có thể chia sẻ nội dung của họ trên mạng xã hội, blog hoặc trang web cá nhân một cách dễ dàng.Tuy nhiên, với sự phát triển của công nghệ mạng, các vấn đề liên quan đến quyền riêng tư và tính bảo mật của dữ liệu cũng ngày càng trở nên phức tạp hơn. Việc bảo vệ bản quyền và chống sao chép đang trở thành một vấn đề quan trọng trong việc duy trì thông tin kỹ thuật số, đặc biệt là trong lĩnh vực giải trí và truyền thông.Với mục đích bảo vệ quyền sở hữu trí tuệ và tránh việc sao chép trái phép, các nhà khoa học và kỹ sư đã phát triển các công nghệ bảo vệ bản quyền và chống sao chép. Trong đó, digital watermarking được tạo ra như một công nghệ để nhúng các thông tin bổ sung vào các tài liệu số như ảnh, video, âm thanh, văn bản và các tài liệu điện tử khác. Digital watermarking có thể được sử dụng để nhúng các thông tin bảo mật vào các tài liệu số, nhằm đảm bảo tính xác thực và bảo vệ quyền sở hữu trí tuệ của các tác giả và nhà sản xuất.Với digital watermarking, bất kỳ nội dung kỹ thuật số nào đều có thể được sử dụng để ẩn dữ liệu, các thông tin nhúng này có thể được sử dụng để cung cấp thông tin về người sở hữu tài liệu, ngày tạo ra tài liệu, số phiên bản của tài liệu, v.v. Dựa trên các ứng dụng mong muốn, một số kỹ thuật watermarking phù hợp đã được phát triển để giảm thiểu mối lo ngại này. Tuy nhiên, sẽ là rất khó để đạt được một hệ thống watermarking đồng thời mạnh mẽ và an toàn. Bài báo cáo này cung cấp thông tin về 5 kỹ thuật watermarking bao gồm: Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) và Singular Value Decomposition (SVD).

MỤC LỤC

Chương 1. Tổng quan

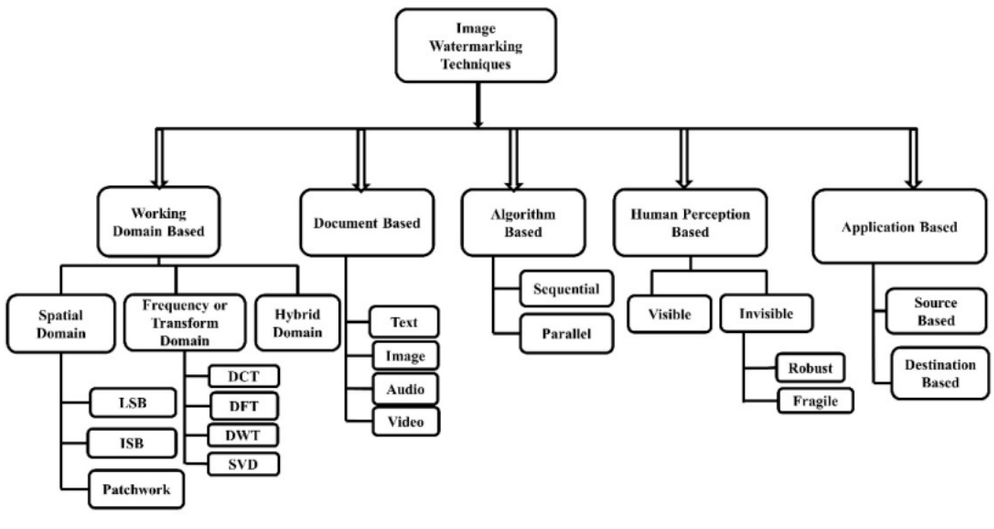
1.1. Digital Watermark là gì?

Quá trình xử lý hình ảnh và internet đã giúp việc sao chép, sửa đổi, tái sản xuất và phân phối hình ảnh kỹ thuật số trở nên dễ dàng hơn với chi phí thấp và khả năng phân phối gần như ngay lập tức mà không làm giảm chất lượng. Công nghệ mạng đã phát triển và tiến bộ nhanh đến mức đe dọa đến quyền riêng tư và tính bảo mật của dữ liệu. Do đó, xác thực nội dung, bảo vệ bản quyền và bảo vệ chống sao chép đóng một vai trò thiết yếu trong việc đối mặt với những thách thức của các mối đe dọa hiện có và sẽ có trong việc duy trì thông tin kỹ thuật số. Digital watermarking được tạo ra như một công nghệ để nhúng các thông tin bổ sung vào các tài liệu số như ảnh, video, âm thanh, văn bản và các tài liệu điện tử khác với mục đích chính là để bảo vệ quyền sở hữu trí tuệ và tránh việc sao chép trái phép, giúp giảm thiểu thiệt hại cho các nhà sản xuất và tác giả. Bất kỳ nội dung kỹ thuật số nào, chẳng hạn như hình ảnh, âm thanh và video, đều có thể dùng để ẩn dữ liệu.

Có một số điểm tương đồng giữa steganography và watermarking vì cả hai phương pháp này đều nhúng thông tin vô hình vào các phương tiện truyền thông kỹ thuật số.Trong các kỹ thuật steganography, việc không thể phát hiện ra sự tồn tại của dữ liệu và khối lượng thông tin được truyền đi là những đặc điểm quan trọng nhất. Các thông báo mật mã thường không đủ mạnh để chống lại sự thay đổi dữ liệu hoặc có khả năng tồn tại hạn chế trước những sửa đổi kỹ thuật có thể xảy ra trong quá trình truyền và lưu trữ, như chuyển đổi định dạng hoặc chuyển đổi kỹ thuật số sang tương tự, v.v. Ngược lại, đối với watermarking, khả năng tồn tại của thông tin được nhúng là tính năng quan trọng nhất; các phương pháp watermarking sẽ cung cấp tính năng bổ sung chống lại mọi thay đổi, biến dạng và nỗ lực xóa thông tin nhúng khỏi ảnh gốc. Mặt khác, khối lượng dữ liệu nhúng không quan trọng. Khối lượng này có thể ít hơn nhiều so với kỹ thuật ghi ảnh giấu tin. Do đó, các phương pháp watermarking thường được được sử dụng khi người dùng quan tâm tới việc bảo vệ dữ liệu được nhúng hơn việc che giấu nó.

1.2. Phân loại watermarking

Phân loại watermarking được tóm tắt trong hình sau



Hình 1. Phân loại watermarking

1.2.1. Theo loại dữ liệu

Watermarking có thể được phân loại theo loại dữ liệu đầu vào như sau:

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

Các loại này đều được sử dụng để đánh dấu tác giả hoặc bản quyền của tài liệu, đồng thời ngăn chặn việc sao chép hoặc sửa đổi tài liệu, phần mềm. Trong báo cáo này, chúng ta sẽ chỉ tập trung vào Image Watermarking.

1.2.2. Theo khả năng nhận biết

Watermarking dựa theo khả năng nhận biết có thể chia thành 2 loại: visible watermarking và invisible watermarking. Visible watermarking là một trong những kỹ thuật hiện đại được sử dụng rộng rãi. sử dụng ghi nhãn này, chủ sở hữu thường hiển thị trong hình một số dấu hiệu, tên và logo đặc biệt, vì vậy có thể dễ dàng nhận thấy những dấu hiệu này. Ví dụ, một số hãng ảnh và phần mềm các nhà phát triển thường thêm hình mờ của biểu tượng bản quyền hoặc tên của cơ quan để xem trước hình ảnh, do đó không thể sử dụng các bản xem trước cho các bản sao chất lượng cao của sản phẩm kèm theo giấy phép.

Hình 2. Ví dụ của Visible watermarking

Các kỹ thuật watermarking vô hình ẩn một số bản quyền cụ thể, xác thực, hoặc thông tin khác bên trong hình ảnh để nhận dạng tác giả để bảo vệ tác giả quyền và hạn chế khả năng sao chép không giới hạn của kẻ xâm nhập và sử dụng trái phép thông tin. Ngoài ra, những hình mờ này có thể thêm một số thông tin quan trọng khác, ví dụ: đánh dấu người

nhận để theo dõi phân phối hình ảnh, chú thích ẩn, ghi chú chính, v.v… Đây là loại watermark không thể hoặc rất khó để nhìn thấy bằng mắt thường. Báo cáo này giới thiệu các phương pháp để tạo ra một watermark vô hình.

1.2.3. Theo miền làm việc

Phân loại theo miền làm việc, watermarking được chia làm 3 loại: Spatial Domain, Transform or Frequency Domain và Hybrid Domain.

Watermarking miền không gian thực hiện quá trình đánh dấu trực tiếp vào pixel của ảnh gốc giúp bảo vệ thông tin hiệu quả làm thay đổi giá trị pixel của một hoặc nhiều tập hợp ngẫu nhiên được chọn của hình ảnh. Nó tải trực tiếp dữ liệu thô vào các pixel hình ảnh. Các phương pháp thuộc Spatial Domain bao gồm: Least Significant Bit (LSB), Intermediate Significant Bit (ISB), Patchwork,...

Tuy nhiên các kỹ thuật watermark trên miền không gian quá mỏng manh vì chúng có thể dễ dàng thao tác. Những kỹ thuật này kém mạnh mẽ hơn nhiều trước các kiểu tấn công khác nhau so với các thuật toán miền tần số. Những nhược điểm này đã thu hút sự tập trung vào việc nghiên cứu các kỹ thuật watermark trên miền biến đổi giúp ẩn dữ liệu trong không gian biến đổi của tín hiệu, thay vì thời gian, theo cách hiệu quả hơn. Kỹ thuật này chuyển đổi một hình ảnh bằng cách sử dụng một biến đổi được xác định trước để thể hiện ảnh trong miền tần số. Sau đó, nó nhúng watermark bằng cách thay đổi các hệ số miền biến đổi của ảnh gốc sử dụng các phép biến đổi khác nhau, bao gồm Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Hadamard, Biến đổi CAT, FFT, PHT và Fresnel, trong số những biến đổi khác. Cuối cùng, nó trích xuất watermark sử dụng một phép biến đổi nghịch đảo với sự trợ giúp của một khóa chính xác,

Cuối cùng, watermarking hỗn hợp (Hybrid Domain) thường được coi là sự kết hợp của thuật toán miền không gian và miền chuyển đổi. Các thuật toán này đảm bảo cả tính mạnh mẽ và tính năng nhúng dữ liệu nâng cao. Nhiều nghiên cứu đã được thực hiện trên các phương pháp miền lai. Những nghiên cứu này phản ánh các xu hướng hiện tại trong lĩnh vực watermark. Ứng dụng của watermark

Chương 2. Các phương pháp watermarking

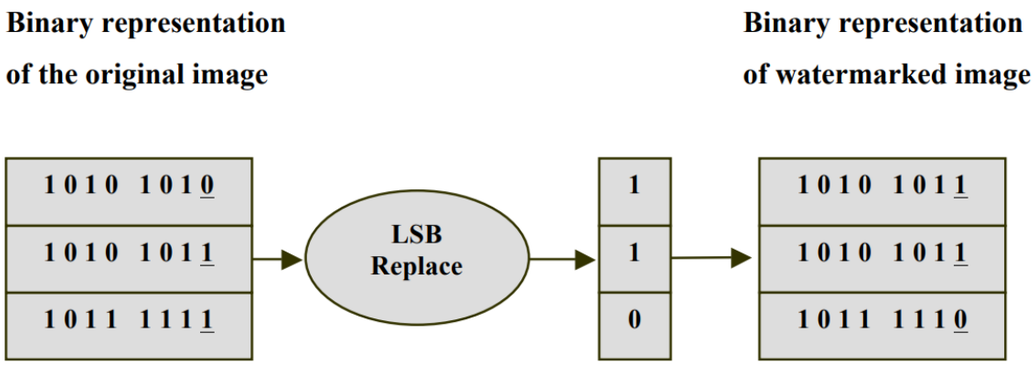
Link Github: LnG-a/digital_watermarking

2.1. Least Significant Bit

LSB (Least Significant Bit) là một kỹ thuật trong watermarking được sử dụng để nhúng dấu nước vào trong hình ảnh. Kỹ thuật này dựa trên việc sửa đổi bit thấp nhất trong giá trị pixel của hình ảnh để lưu trữ thông tin nhúng vào.Kỹ thuật LSB là một trong những kỹ thuật phổ biến nhất được sử dụng trong invisible watermarking. Kỹ thuật này hoạt động bằng cách thay đổi bit cuối cùng của mỗi giá trị pixel trong hình ảnh. Bằng cách sửa đổi bit cuối cùng này, chúng ta có thể lưu trữ thông tin nhúng vào hình ảnh mà không làm thay đổi nhiều về mặt thị giác của hình ảnh. Để nhúng watermark vào trong hình ảnh bằng kỹ thuật LSB, chúng ta cần lựa chọn các bit cần sửa đổi và thực hiện việc sửa đổi đó theo một cách nhất định. Thông thường, chúng ta sẽ sửa đổi các bit thấp nhất của giá trị pixel để đảm bảo rằng sự thay đổi là nhỏ nhất và không gây ra ảnh hưởng đến chất lượng của hình ảnh.

Một trong những ưu điểm của kỹ thuật LSB là tính đơn giản và dễ dàng áp dụng. Nó cho phép lưu trữ nhiều thông tin vào trong một tấm hình ảnh mà không gây ra sự khác biệt đáng kể trong chất lượng của hình ảnh. Bên cạnh đó, kỹ thuật này cũng có thể áp dụng trên nhiều định dạng hình ảnh khác nhau, và nhiều dạng thông tin khác như âm thanh, văn bản, … miễn là chúng được biểu diễn dưới dạng bit. Có một ưu điểm rất quan trọng của LSB đó là tải trọng rất cao. Sử dụng mã ASCII 7 bit tiêu chuẩn để nhúng một chữ cái, người dùng có thể nhúng một bài viết lớn vào một bức tranh. Ví dụ: sử dụng hình ảnh màu (1270x900), bao gồm ba ma trận thang độ xám, có thể nhúng toàn bộ cuốn sách lớn 'Con chó săn của Baskervilles' của Conan Doyle vào một bức tranh, bởi vì cuốn sách này bao gồm 315.572 ký tự. Do đó, như chúng ta có thể thấy, phương pháp này rất hữu ích đối với việc ghi mật mã nếu có một cách để tránh làm sai lệch, thay đổi tiêu chuẩn do nén và các cuộc tấn công độc hại.

Tuy nhiên, phương pháp LSB có một nhược điểm nghiêm trọng. Bất kỳ sự thay đổi biên độ tín hiệu nào thậm chí không đáng kể sẽ thay đổi mặt phẳng LSB trước, do đó, bất kỳ sự thay đổi độ sáng và độ tương phản nào cũng có thể phá hủy tất cả các watermark LSB. Có một số biến dạng khác, chẳng hạn như thêm nhiễu, nén mất dữ liệu hoặc thay đổi kích thước, cũng có thể phá vỡ watermark LSB. Do đó, các watermark như vậy dễ bị ảnh hưởng bởi nhiều loại biến dạng. Đôi khi, việc kẻ xâm nhập có thể phát hiện sự tồn tại của watermark trong ảnh hay không không quan trọng; nếu kẻ trộm nghi ngờ có sự tồn tại thủy vân trong ảnh, chúng có thể sử dụng một tập hợp các quy trình tấn công có thể dễ dàng phá hủy hầu hết watermark LSB nếu có. Và một trong những cách tấn công đơn giản và hiệu quả nhất là loại bỏ (zeroing) toàn bộ mặt phẳng LSB với rất ít thay đổi về chất lượng cảm nhận của hình ảnh sau khi đã sửa đổi.



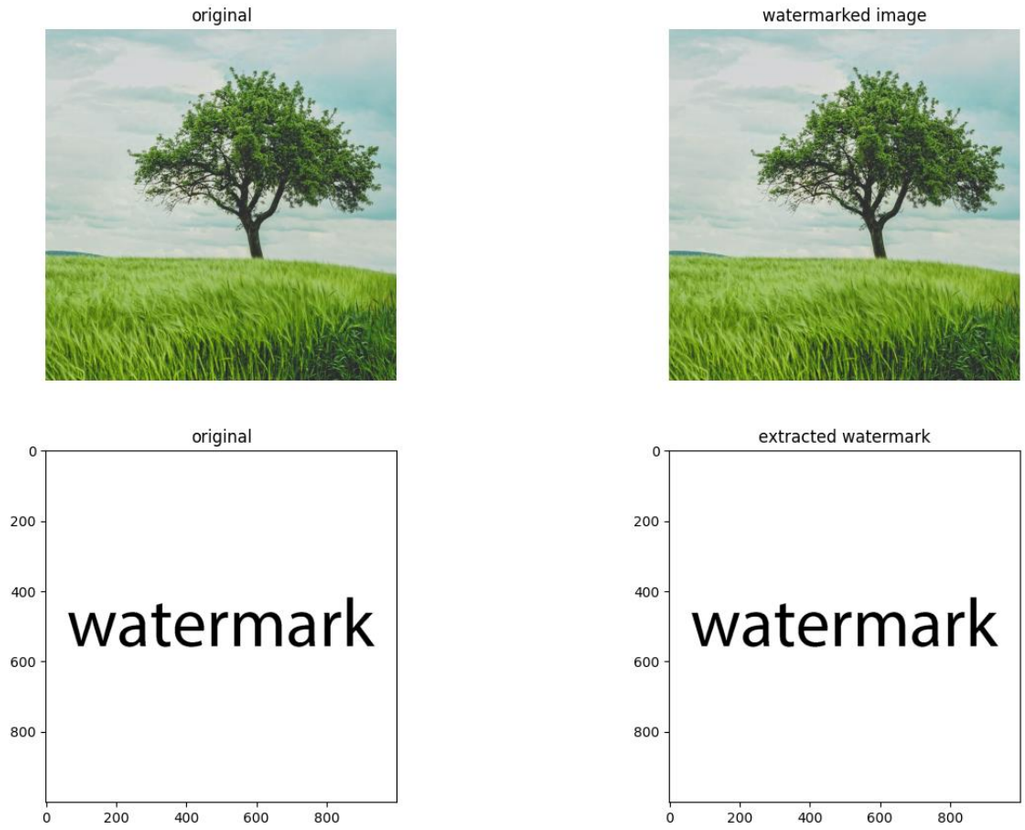
Hình 3. Sơ đồ phương pháp LSB

Để cài đặt phương pháp watermark LSB cho một ảnh màu RGB, ta cần làm như sau:

1. Chọn thông tin watermark: Đầu tiên, chọn thông tin watermark cần nhúng vào ảnh màu RGB. Thông tin watermark có thể là văn bản, hình ảnh hoặc âm thanh. Để thực hiện phương pháp LSB, thông tin watermark cần được biểu diễn dưới dạng các bit.
2. Chia ảnh màu thành các kênh màu: Ảnh màu RGB được biểu diễn dưới dạng ba kênh màu đỏ, xanh lá cây và xanh lam. Do đó, ta cần chia ảnh màu thành ba kênh màu tương ứng.
3. Chèn thông tin watermark vào kênh màu: Sau khi chia ảnh thành ba kênh màu, ta tiến hành chèn thông tin watermark vào từng kênh màu bằng phương pháp LSB như đã mô tả ở trên. Cụ thể, ta thực hiện việc thay đổi bit ít quan trọng nhất của các giá trị pixel trong từng kênh màu bằng các bit từ thông tin watermark.
4. Ghép lại các kênh màu: Sau khi đã nhúng thông tin watermark vào các kênh màu, ta tiến hành ghép lại các kênh màu để tạo thành ảnh màu hoàn chỉnh.
5. Lưu ảnh đã nhúng: Ảnh màu đã nhúng thông tin watermark có thể được lưu lại dưới dạng file ảnh mới, hoặc có thể ghi đè lên file ảnh gốc nếu không muốn tạo ra một file ảnh mới.

Để trích xuất thông tin watermark từ ảnh đã nhúng, ta thực hiện các bước ngược lại như sau:

1. Chia ảnh màu thành các kênh màu: Tương tự như khi nhúng thông tin watermark, ta cần chia ảnh màu thành ba kênh màu đỏ, xanh lá cây và xanh lam.
2. Trích xuất thông tin watermark từ các kênh màu: Đối với từng kênh màu, ta lấy ra các bit LSB của từng giá trị pixel và ghép lại thành thông tin watermark ban đầu.
3. Tái tạo thông tin watermark: Cuối cùng, ta ghép lại các thông tin watermark từ ba kênh màu để tái tạo ra thông tin watermark ban đầu.



Hình 4. Kết quả sau khi sử dụng LSB

2.2. Discrete Cosine Transform

Discrete Cosine Transform (DCT) là kỹ thuật tách một hình ảnh thành các các hệ số tần số của các thành phần tần số tương ứng, có thể được biểu diễn dưới dạng tổng của các hàm cosin. Phép biến đổi DCT rất quan trọng trong việc nén ảnh, ví dụ như trong định dạng ảnh JPEG.

DCT hai chiều của một ma trận A có kích thước M x N được tính như sau:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

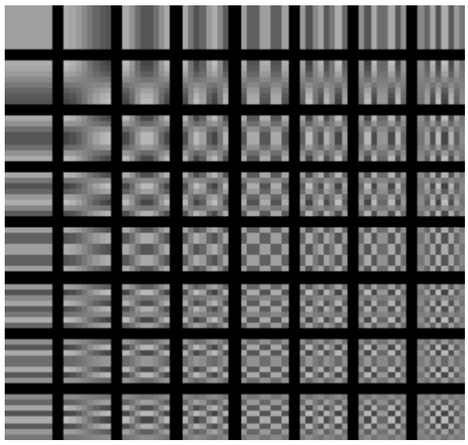
$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

Các giá trị Bpq được gọi là các hệ số DCT của A. Dưới đây là cách lấy nghịch đảo Inverse Discrete Cosine Transform (IDCT) của ma trận B, ta được ma trận A.

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

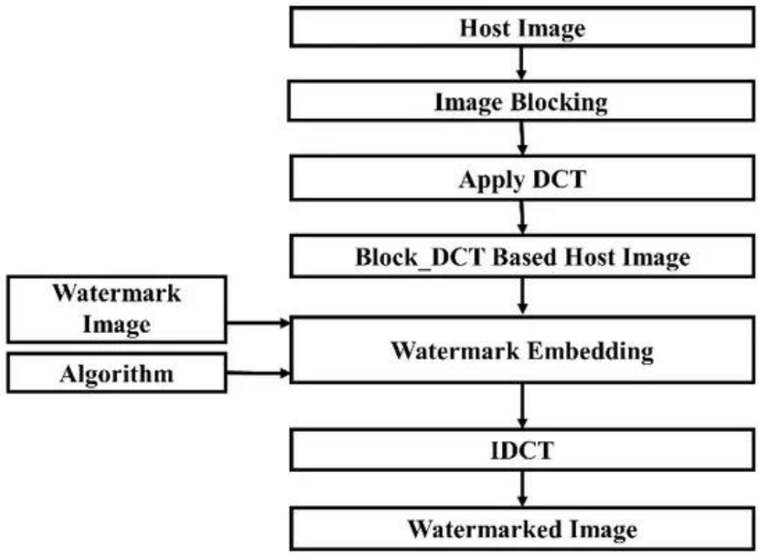
Tích hai hàm cosin có thể được minh họa bằng nhiều ma trận 8x8, mỗi ma trận thể hiện tích giữa các hàm cosine dọc và ngang như trong Hình 1. Trong thực tế, bằng việc kết hợp tổng các ma trận này (với các hệ số tương ứng), ta có thể tái tạo ra được bất kỳ ảnh 8x8 mẫu nào với sai số là rất nhỏ, khó có thể nhận biết được bằng mắt thường. Sửa đổi một số trọng số với sai số nhỏ trong ma trận tần số sẽ không làm biến đổi sâu sắc đến hình ảnh ban đầu. Vì vậy, ta có thể sửa đổi ma trận tần số với sai số được lấy từ ảnh Watermark sau đó convert lại ảnh ban đầu dẫn đến việc khó có thể nhận ra ảnh đã được watermark.



Hình 5. Hình minh họa tập tích hai hàm cosine với tần số khác nhau

Quy trình nhúng watermark vào ảnh gốc diễn ra như sau:

- Xác định kích thước của watermark, nó sẽ xác định số lượng các giá trị trong watermark.
- Chia ảnh ban đầu thành các block có kích thước bằng với kích thước của watermark. Các block này được chuyển đổi sang miền tần số bằng phép biến đổi DCT.
- Chọn các hệ số DCT để nhúng thông tin watermark vào. Các hệ số này được chọn sao cho chúng không ảnh hưởng quá nhiều đến chất lượng của ảnh gốc.
- Thực hiện nhúng watermark vào các hệ số DCT đã chọn theo một quy tắc nhất định.
- Chuyển đổi ngược các hệ số DCT đã được nhúng watermark để lấy lại các block ảnh gốc.
- Lặp lại các bước trên cho tất cả các block trong ảnh gốc.



Hình 6. Quy trình nhúng Watermark vào ảnh gốc theo phương pháp DCT

Quy trình trích xuất watermark từ ảnh diễn ra như sau:

- Chia ảnh đã nhúng thành các block có kích thước bằng với kích thước của watermark.
- Thực hiện phép biến đổi DCT trên mỗi block.
- Chọn các hệ số DCT đã được nhúng watermark và lấy chúng ra.
- Sử dụng các hệ số này để tạo lại watermark ban đầu.

Việc nhúng watermark vào ảnh trong miền DCT có độ chống lại tấn công khá cao. Tuy nhiên, phương pháp này dễ bị tấn công bằng cách xoay, cắt ghép và thay đổi tỷ lệ ảnh. Phép biến đổi DCT cho kết quả tốt hơn so với phép biến đổi Fourier rời rạc (DFT) trong việc tập trung năng lượng vào các hệ số thấp hơn của dữ liệu ảnh.

2.3. Discrete Fourier Transform

Discrete Fourier Transform (DFT) là một phương pháp chuyển đổi một tín hiệu từ miền thời gian sang miền tần số. Nó là một dạng của phép biến đổi Fourier, được áp dụng trên các tín hiệu có độ dài hữu hạn.

Ý tưởng của DFT là chia một tín hiệu đầu vào thành các mẫu rời rạc và áp dụng phép biến đổi Fourier trên các mẫu này. Kết quả là một tín hiệu ở miền tần số, với các thành phần tần số của tín hiệu ban đầu.

Cụ thể, DFT thực hiện phép tính tổng các phần tử của một chuỗi tín hiệu rời rạc với các hệ số phức số phức ở các tần số khác nhau để tạo ra một chuỗi tần số rời rạc mới. Kết quả của DFT thường được biểu diễn dưới dạng phổ tần số, cho phép xác định các thành phần tần số của tín hiệu.

DFT là một công cụ quan trọng trong xử lý tín hiệu và nhiều ứng dụng khác, bao gồm xử lý âm thanh, xử lý hình ảnh và mạng lưới điện.

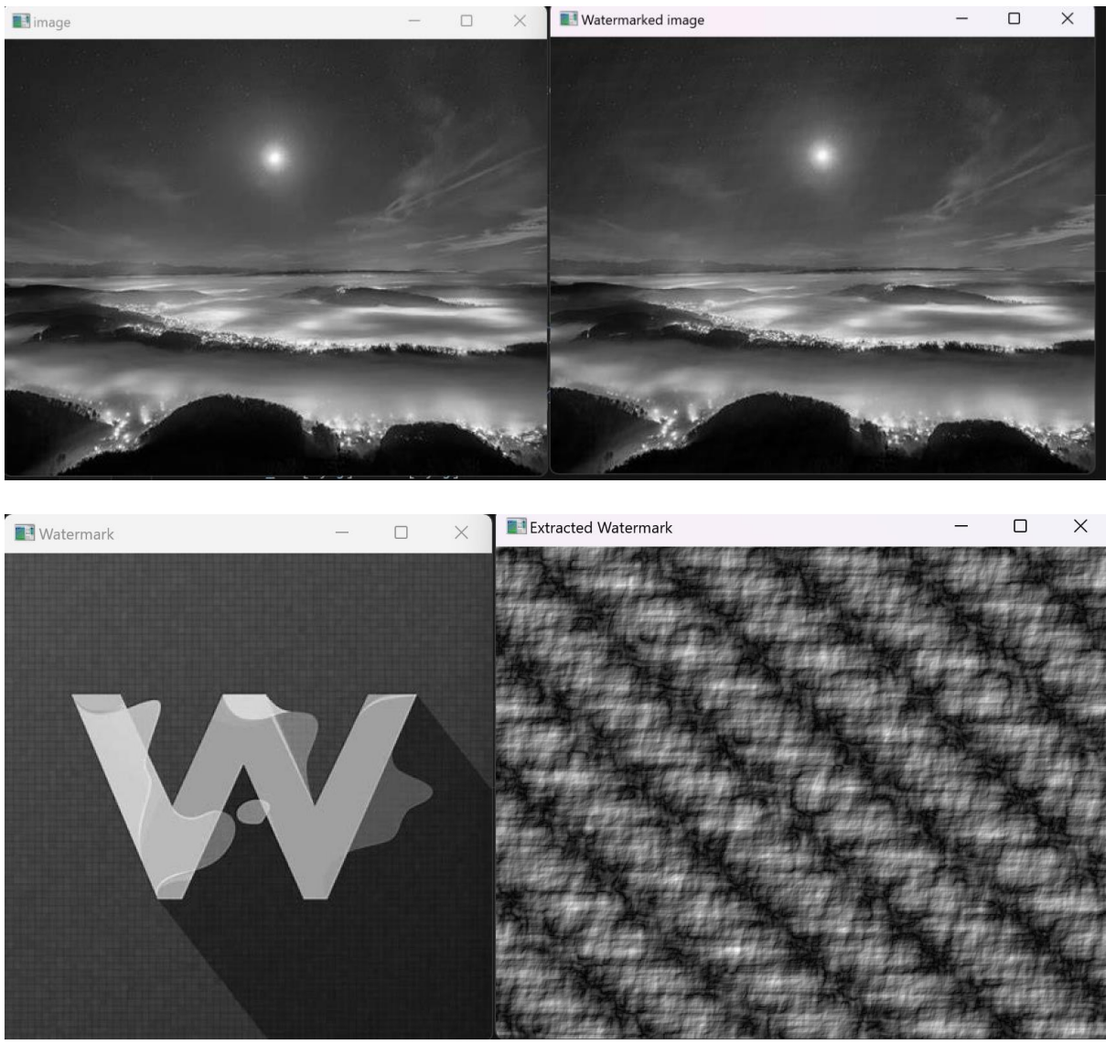
Discrete Fourier Transform (DFT) là một phép biến đổi giúp chuyển đổi một tín hiệu thời gian liên tục sang tín hiệu tần số rời rạc. Trong ứng dụng watermark digital image,

DFT có thể được sử dụng để chèn watermark vào hình ảnh bằng cách thay đổi các giá trị tần số của hình ảnh.

Cụ thể, để chèn watermark, ta có thể thực hiện các bước sau:

- Áp dụng DFT để chuyển đổi hình ảnh từ miền thời gian sang miền tần số.
- Chọn các vị trí tần số trong miền tần số để chèn watermark. Các vị trí này có thể được chọn dựa trên một số tiêu chí như độ bảo mật, độ chịu tấn công của watermark, và độ nhạy cảm của các tần số đó đối với hình ảnh gốc.
- Thay đổi giá trị tần số tại các vị trí đã chọn để chèn watermark. Điều này có thể được thực hiện bằng cách thay đổi pha hoặc biên độ của các tần số đó.
- Áp dụng ngược lại DFT để chuyển đổi hình ảnh từ miền tần số trở lại miền thời gian.
- Kiểm tra độ chính xác của watermark đã chèn bằng cách so sánh hình ảnh kết quả với hình ảnh gốc và xác định vị trí watermark.

Việc chèn watermark bằng cách sử dụng DFT có thể đạt được độ bảo mật tốt và khả năng chịu tấn công cao, tuy nhiên nó có thể làm giảm độ tương phản hoặc độ phân giải của hình ảnh. Do đó, việc chọn vị trí tần số phù hợp để chèn watermark là rất quan trọng để đảm bảo tính bảo mật và độ nhạy cảm của watermark.



Hình 7. Kết quả của phương pháp DFT

2.4. Discrete Wavelet Transform

Phương pháp Discrete Wavelet Transform (DWT) là một trong những phương pháp phổ biến trong lĩnh vực watermarking, nơi mà watermark (dấu nhận dạng) được nhúng vào dữ liệu để bảo vệ quyền sở hữu và đảm bảo tính toàn vẹn của nó. DWT là một kỹ thuật xử lý tín hiệu mạnh mẽ, được sử dụng rộng rãi trong xử lý ảnh và âm thanh, và có thể được áp dụng để nhúng watermark một cách hiệu quả.

DWT là một biến đổi biến đổi tuyến tính, mà phân tích dữ liệu thành các thành phần tần số khác nhau. Quá trình DWT thực hiện việc chia đoạn dữ liệu thành các khối con (sub-band) có độ phân giải khác nhau. Các khối con này bao gồm các thành phần tần số cao và tần số thấp, mô tả thông tin chi tiết và thông tin tổng quát của dữ liệu tương ứng.

Quá trình nhúng watermark bằng DWT thực hiện các bước sau:

- Bước 1: Áp dụng biến đổi sóng rời rạc (DWT) lên ảnh gốc để phân tích thành bốn băng con tần số: LL, LH, HL, HH.
- Bước 2: Áp dụng DWT lên băng con LH để phân tích thành bốn băng con nhỏ hơn: LL2, LH2, HL2, HH2.
- Bước 3: Chọn 22 hệ số miền tần số giữa từ băng con LH2 và HL2 để nhúng watermark. Sử dụng quét theo đường zig-zag trên các khối 8x8 trong các băng con này.
- Bước 4: Chuyển đổi watermark thành một vector nhị phân, gọi là vector thông điệp (message vector - MV).
- Bước 5: Tạo chuỗi ngẫu nhiên PSN (Pseudo-Noise Sequence), có số chiều bằng 22 (tương ứng với số hệ số miền tần số giữa) và liên quan đến một khóa bí mật.
- Bước 6: Nếu MV(i) = 0, thực hiện nhúng PSN vào 22 hệ số miền tần số giữa của các khối 8x8 tương ứng.
- Bước 7: Áp dụng quá trình ngược của DWT (IDWT) lên các băng con LL2, LH2, HL2, HH2 để thu được băng con LH. Áp dụng quá trình ngược IDWT (Inverse Discrete Wavelet Transform) lên các băng con LL, HL, LH, HH để tái tạo ảnh gốc đã nhúng watermark.

Bằng cách sử dụng DWT, các thành phần tần số thấp được chọn để nhúng thông tin watermark, và sau đó IDWT (Inverse Discrete Wavelet Transform) được áp dụng để tái tạo ảnh gốc đã nhúng watermark từ các thành phần tần số đã thay đổi và các thành phần tần số cao không thay đổi.

Quá trình trích xuất watermark bằng DWT

Quá trình trích xuất watermark từ dữ liệu đã được nhúng bằng phương pháp DWT cũng được thực hiện bằng cách áp dụng DWT và so sánh các thành phần tần số của dữ liệu đã nhúng và dữ liệu trích xuất. Các bước trong quá trình trích xuất watermark bao gồm:

- Bước 1: Áp dụng biến đổi sóng rời rạc (DWT) lên ảnh chứa watermark để phân tích thành bốn băng con tần số: LL, LH, HL, HH.
- Bước 2: Áp dụng DWT lên băng con LH để phân tích thành bốn băng con nhỏ hơn: LL2, LH2, HL2, HH2.

- Bước 3: Tạo chuỗi ngẫu nhiên PSN (Pseudo-Noise Sequence) có số chiều bằng 22 (tương ứng với số hệ số miền tần số giữa) và liên quan đến cùng khóa bí mật được sử dụng trong quá trình nhúng.
- Bước 4: Áp dụng quá trình ngược của DWT (IDWT) lên các băng con LL2, LH2, HL2, HH2 để thu được băng con LH.
- Bước 5: Áp dụng quá trình ngược IDWT lên các băng con LL, HL, LH, HH để tái tạo ảnh gốc đã chứa watermark.
- Bước 6: Chọn 22 hệ số miền tần số giữa từ băng con LH sau quá trình tái tạo ảnh gốc.
- Bước 7: Trích xuất thông điệp watermark từ các hệ số miền tần số giữa được chọn.
- Bước 8: Chuyển đổi thông điệp watermark từ dạng vector nhị phân thành thông điệp ban đầu.

Quá trình trích xuất watermark dựa trên quá trình nhúng bằng DWT: bằng cách sử dụng DWT và chọn các hệ số miền tần số giữa đã nhúng watermark, thông điệp ban đầu được trích xuất từ ảnh chứa watermark.

Ưu điểm của DWT trong watermarking:

- *Khả năng chịu được nhiễu*: DWT có khả năng chịu được nhiễu và biến đổi nhỏ trong dữ liệu mà không gây ra sự thay đổi lớn trong watermark.
- *Bảo vệ chống lại các cuộc tấn công*: DWT trong watermarking cung cấp một mức bảo vệ tốt chống lại các cuộc tấn công như biến đổi affine và nén dữ liệu. Watermark nhúng trong các thành phần tần số thấp có khả năng giữ nguyên được nguyên vẹn hơn trong quá trình biến đổi và nén dữ liệu.
- *Hiệu suất cao*: DWT được tính toán nhanh chóng và có hiệu suất cao trong việc xử lý ảnh và âm thanh.

Hạn chế của DWT trong watermarking bao gồm:

- *Mất mát thông tin*: Quá trình DWT có thể gây mất mát thông tin trong dữ liệu gốc. Việc phân tích và tái tạo dữ liệu bằng DWT có thể dẫn đến mất mát một phần của dữ liệu ban đầu, dẫn đến giảm chất lượng và độ chính xác của dữ liệu đã nhúng watermark.
- *Sự nhạy cảm với nhiễu*: DWT không đảm bảo tính ổn định đối với nhiễu. Nếu dữ liệu chứa watermark bị nhiễu, có thể gây ra sự thay đổi không mong muốn trong watermark và làm giảm khả năng trích xuất đúng của nó.
- *Khả năng phát hiện watermark*: DWT không cung cấp khả năng phát hiện lỗi của watermark. Nếu watermark bị thay đổi hoặc bị hủy hoại, DWT không thể phát hiện được sự thay đổi này, dẫn đến việc trích xuất không chính xác hoặc không thành công.
- *Không đảm bảo bảo mật*: DWT không cung cấp bảo mật cao cho watermark. Dữ liệu đã nhúng watermark có thể dễ dàng bị tấn công và watermark bị loại bỏ hoặc sửa đổi bởi kẻ tấn công thông qua các phương pháp tấn công như cắt, lọc hoặc biến đổi dữ liệu.

- *Sự không đồng nhất trong việc nhúng*: DWT có thể tạo ra sự không đồng nhất trong việc nhúng watermark vào các khối con dữ liệu. Điều này có thể dẫn đến sự hiện diện của hiệu ứng "blocky" hoặc các biểu đồ không mong muốn trong dữ liệu đã nhúng.

2.5. Singular Value Decomposition

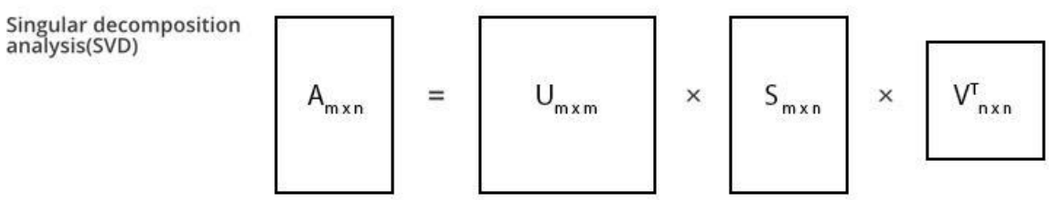
Trong toán học đại số, Singular Value Decomposition (SVD) là một phép phân tích nhân tử của một ma trận. Nó có một số tính chất đại số thú vị và biểu diễn những thông tin quan trọng về mặt hình học và lý thuyết của các phép biến đổi tuyến tính. Biến đổi SVD được sử dụng rộng rãi trong thống kê và xử lý tín hiệu số.

Biến đổi SVD của một ma trận A kích thước m x n được biểu diễn bởi công thức:

$$A = UWV^T$$

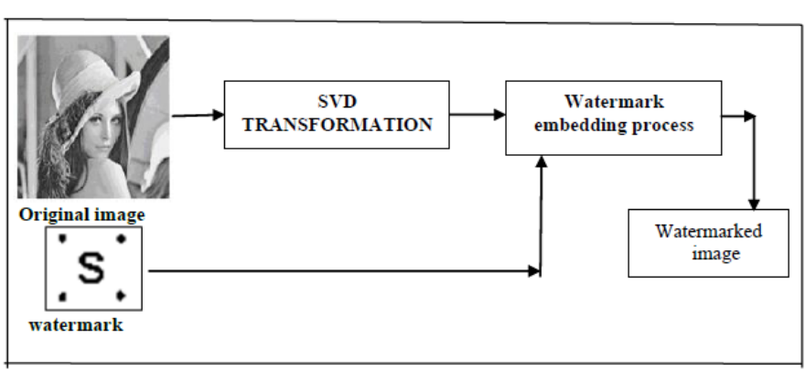
trong đó:

- U: ma trận trực giao kích thước m x m chứa các vector riêng của AA^T
- V: ma trận trực giao thích thước n x n chứa các vector riêng của A^TA
- S: ma trận đường chéo m x n chứa giá trị đơn (căn bậc 2 của các giá trị riêng) của A^TA

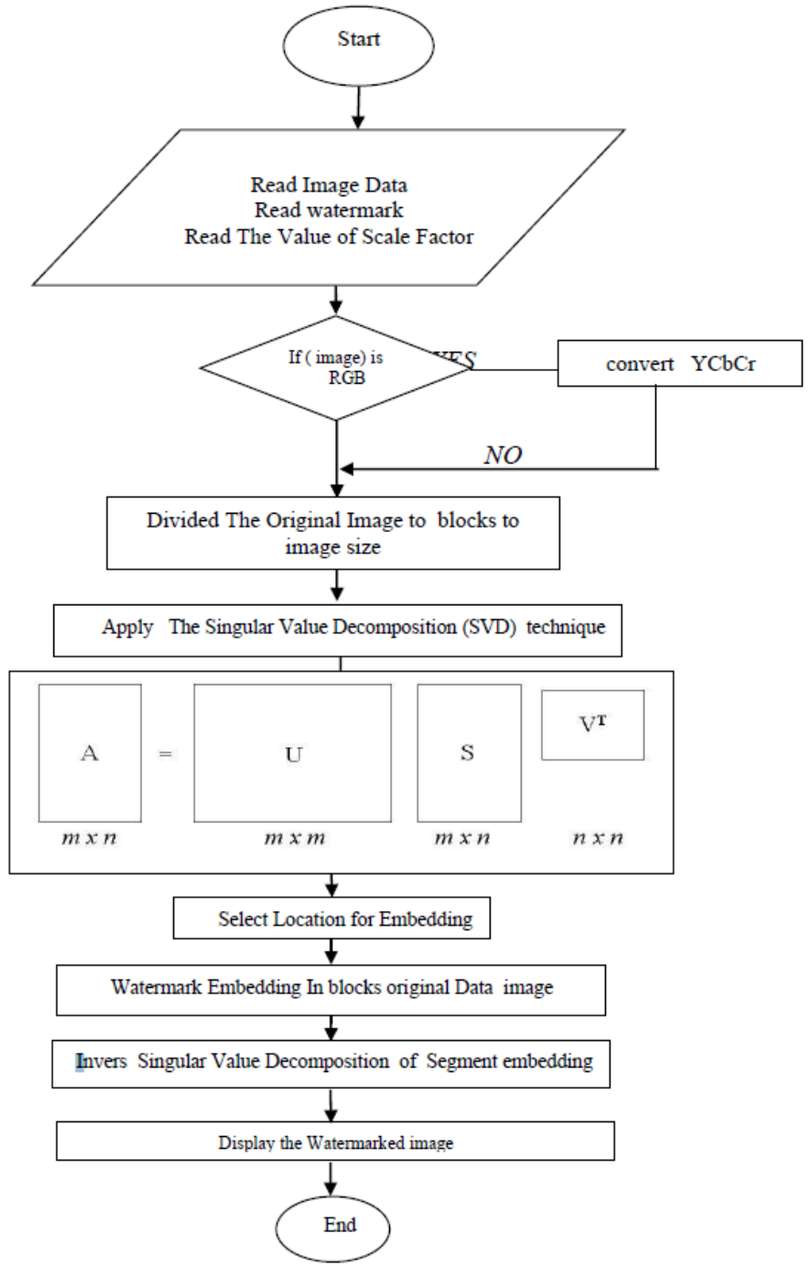


Để áp dụng SVD trong việc chèn watermark cho ảnh, ta thực hiện các bước như sau:

1. Chuyển ảnh gốc về thang màu grayscale, sau đó chia ảnh thành các block.
2. Áp dụng SVD lên từng block.
3. Tính toán coefficient của từng block và chọn ra vị trí để chèn watermark.
4. Chèn watermark vào block đã chọn.
5. Cuối cùng là tái tạo hình ảnh bằng cách sử dụng SVD nghịch đảo.



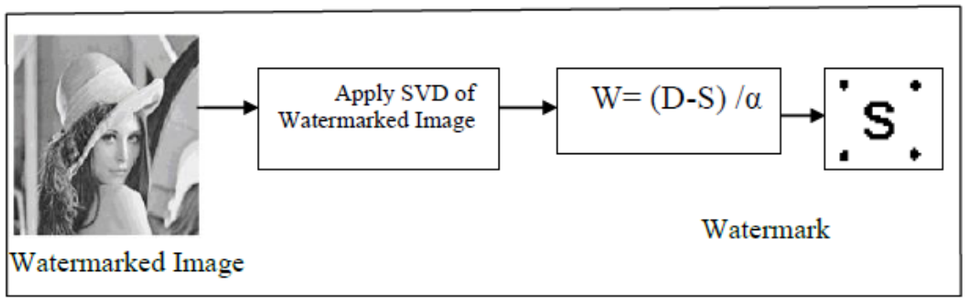
Hình 8. Quá trình chèn watermark vào ảnh sử dụng SVD



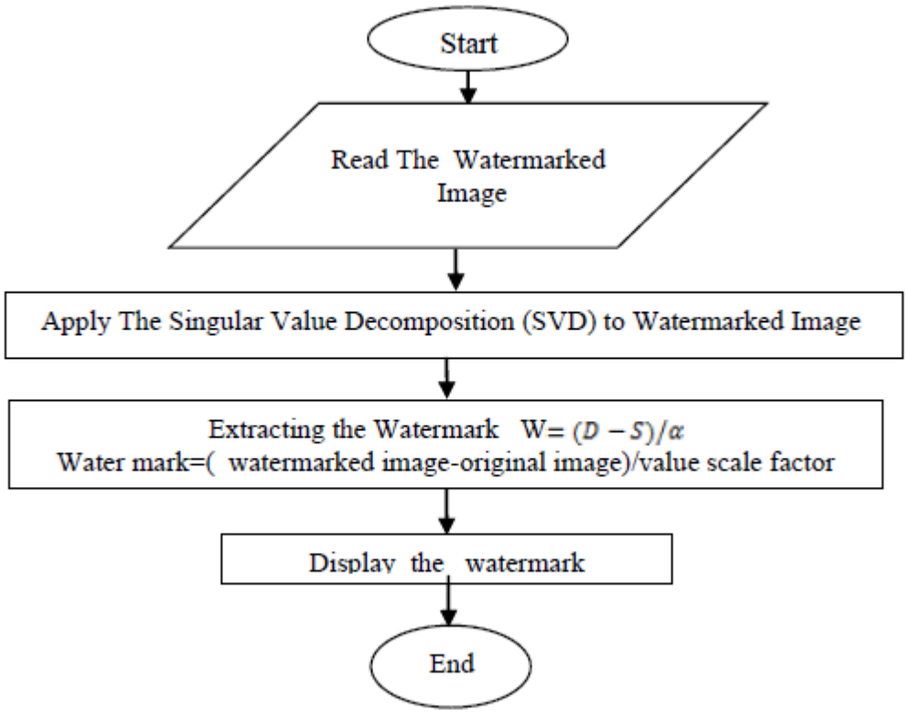
Hình 9. Flowchart quá trình chèn watermark vào ảnh sử dụng SVD

Quá trình trích xuất watermark được thực hiện theo các bước:

1. Áp dụng SVD vào ảnh cần trích xuất watermark.
2. Sử dụng công thức tính $W = (D - S) / \alpha$



Hình 10. Quá trình trích xuất watermark của ảnh sử dụng SVD



Hình 11. Flowchart quá trình trích xuất watermark của ảnh sử dụng SVD

Chương 3. Kết quả

3.1. Phương pháp đánh giá:

Báo cáo này sử dụng PSNR (Peak Signal-to-Noise Ratio) để đánh giá các thuật toán. PNST là một độ đo chất lượng hình ảnh hoặc video. Nó được sử dụng để so sánh chất lượng của hai hình ảnh hoặc video, một hình ảnh hoặc video được coi là gốc và một hình ảnh hoặc video được nén hoặc xử lý. Chỉ số này tính toán sự khác biệt giữa hai hình ảnh bằng cách so sánh các giá trị màu tại cùng một vị trí trên hai hình ảnh. PSNR được tính bằng cách lấy tỷ lệ giữa đỉnh của tín hiệu (tức giá trị màu lớn nhất có thể) và sai số bình phương trung bình giữa hai hình ảnh. Kết quả được đưa ra dưới dạng đơn vị đo dB (decibel). PSNR thường được sử dụng trong các ứng dụng nén hình ảnh và video để đánh giá chất lượng của tệp nén so với tệp gốc. Ở đây PSNR được sử dụng để đánh giá chất lượng ảnh sau khi được chèn watermark. PSNR càng cao thì chất lượng ảnh sau càng giống với ảnh ban đầu.

PSNR được tính bằng công thức sau:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

Trong đó, MAX là giá trị tối đa của pixel, ví dụ như 255 cho ảnh 8-bit. MSE là giá trị mean square error được tính theo công thức:

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

Với I là ảnh gốc và K là ảnh sau khi chèn watermarked.

Ngoài ra báo cáo cũng sử dụng chỉ số SSIM (Structural Similarity Index) là một độ đo chất lượng được sử dụng để so sánh độ tương đồng cấu trúc giữa hai hình ảnh. SSIM đánh giá chất lượng hình ảnh dựa trên ba yếu tố: độ tương phản, độ sáng và độ tương tự cấu trúc. Nó được xây dựng dựa trên việc nghiên cứu về cách mà não bộ con người xử lý thông tin hình ảnh.Để tính toán giá trị SSIM giữa hai hình ảnh A và B, ta chia mỗi hình ảnh thành nhiều khối và tính toán SSIM cho từng khối. SSIM được tính bằng cách so sánh các giá trị trung bình của các khối, độ lệch chuẩn và độ tương quan giữa các khối. Các giá trị này được tổng hợp lại để tính toán giá trị SSIM cuối cùng.SSIM là một độ đo phổ biến trong xử lý hình ảnh và video, và thường được sử dụng để đánh giá chất lượng nén hình ảnh, và ở đây là watermark. Tuy nhiên, SSIM cũng có nhược điểm. Vì nó chỉ đánh giá độ tương đồng cấu trúc giữa hai hình ảnh mà không đánh giá các chi tiết khác như màu sắc, nên nó không thể đánh giá được chất lượng hình ảnh một cách toàn diện.

3.2. Kết quả

Phương pháp	PSNR	SSIM
LSB	31.40	97.06
DCT	44.89	99.75
DFT	39.85	98.37
DWT	32.64	98.14
SVD	25.70	99.27

Bảng 3.1 Kết quả các phương pháp

Từ bảng trên ta thấy phương pháp LSB có chỉ số SSIM là 97.06 và chỉ số PSNR là 31.40. Điều này cho thấy kết quả xử lý hình ảnh bằng phương pháp LSB chưa đạt được độ chính xác cao về mặt cấu trúc và chất lượng, so với các phương pháp khác trong bảng dữ liệu. Phương pháp DCT có chỉ số SSIM cao nhất trong các phương pháp được nêu ra là 99.75 và chỉ số PSNR là 44.89, cho thấy phương pháp này đạt được độ chính xác cao về cấu trúc và chất lượng hình ảnh. Các phương pháp DFT, DWT và SVD cũng cho thấy kết quả tương đối tốt với giá trị SSIM và PSNR cao. Tuy nhiên, trong khi giá trị SSIM của SVD khá cao, chỉ số PSNR của phương pháp này thấp hơn nhiều so với các phương pháp còn lại.

Chương 4. Kết luận

Phương pháp watermarking đã trở thành một trong những công nghệ bảo vệ quan trọng trong việc bảo vệ bản quyền và phòng chống sao chép trái phép. Trong bài báo cáo này, chúng ta đã tìm hiểu về năm phương pháp watermarking khác nhau, bao gồm LSB, DCT, DFT, DWT và SVD. Mỗi phương pháp đều có những ưu điểm và hạn chế riêng, và sự lựa chọn của phương pháp nào sẽ phụ thuộc vào yêu cầu cụ thể của ứng dụng.Phương pháp LSB là phương pháp đơn giản nhất và dễ hiểu nhất, tuy nhiên nó cũng dễ bị tấn công và loại bỏ watermark. Phương pháp DCT và DFT có khả năng chống lại các cuộc tấn công phức tạp hơn, đồng thời cũng có hiệu suất tốt trong việc chèn watermark vào các ảnh. Tuy nhiên, hai phương pháp này cũng có một số hạn chế, bao gồm khả năng mất mát dữ liệu khi sử dụng và chi phí tính toán lớn hơn so với các phương pháp khác. Phương pháp DWT và SVD là hai phương pháp watermarking hiệu quả và được sử dụng phổ biến trong các ứng dụng thương mại. Cả hai phương pháp đều có khả năng chống lại các cuộc tấn công phức tạp, đồng thời cũng có thể tối ưu hóa được hiệu suất trong việc chèn watermark vào các ảnh.Các phương pháp này cũng có một số hạn chế, bao gồm khả năng bị tấn công nếu kẻ tấn công biết trước thông tin về watermark. Tóm lại, việc chọn phương pháp watermarking phù hợp sẽ phụ thuộc vào yêu cầu cụ thể của ứng dụng. Nếu ứng dụng đòi hỏi tính an toàn cao hơn, các phương pháp như DCT và DFT có thể là lựa chọn tốt. Tuy nhiên, nếu ứng dụng cần tính linh hoạt cao hơn, các phương pháp như DWT và SVD sẽ là sự lựa chọn tốt hơn. Bất kể phương pháp nào được sử dụng, việc sử dụng watermarking sẽ giúp bảo vệ quyền sở hữu trí tuệ và giúp người sử dụng kiểm soát việc phân phối và sử dụng nội dung của mình. Tuy nhiên, việc sử dụng watermarking cũng cần được thực hiện đúng cách và trong phạm vi pháp lý. Việc chèn watermark vào nội dung không được phép sử dụng các tài liệu có bản quyền mà không được sự cho phép của chủ sở hữu. Nếu không tuân thủ các quy định pháp lý, người sử dụng có thể phải đối mặt với những hậu quả pháp lý nghiêm trọng.Để tổng kết, watermarking là một công nghệ bảo vệ quan trọng trong việc bảo vệ bản quyền và phòng chống sao chép trái phép. Năm phương pháp watermarking khác nhau bao gồm LSB, DCT, DFT, DWT và SVD, mỗi phương pháp đều có ưu điểm và hạn chế riêng. Việc sử dụng phương pháp nào phụ thuộc vào yêu cầu cụ thể của ứng dụng và cần tuân thủ các quy định pháp lý liên quan để tránh các hậu quả pháp lý nghiêm trọng. Sử dụng đúng và hiệu quả công nghệ watermarking sẽ giúp người sử dụng bảo vệ quyền sở hữu trí tuệ và kiểm soát việc phân phối và sử dụng nội dung của mình.

TÀI LIỆU THAM KHẢO

[1] Digital Watermarking Techniques In Image Processing (researchgate.net)

[2] Information | Free Full-Text | Digital Image Watermarking Techniques: A Review (mdpi.com)

[3] Digital watermarking algorithm using LSB | IEEE Conference Publication | IEEE Xplore