BỘ GIÁO DỤC
VÀ ĐÀO TẠO

VIỆN HÀN LÂM KHOA HỌC
VÀ CÔNG NGHỆ VIỆT NAM

**HỌC VIỆN KHOA HỌC VÀ CÔNG NGHỆ**


**Phạm Quang Huy**

# NGHIÊN CỨU PHÁT TRIỂN MỘT SỐ KỸ THUẬT THỦY VÂN DỰA TRÊN CÁC VÙNG ĐẶC TRƯNG ĐIỂN HÌNH CỦA ẢNH KỸ THUẬT SỐ

## LUẬN ÁN TIẾN SĨ HỆ THỐNG THÔNG TIN

*Hà Nội - 2024*

BỘ GIÁO DỤC
VÀ ĐÀO TẠO

VIỆN HÀN LÂM KHOA HỌC
VÀ CÔNG NGHỆ VIỆT NAM

**HỌC VIỆN KHOA HỌC VÀ CÔNG NGHỆ**

**Phạm Quang Huy**

# NGHIÊN CỨU PHÁT TRIỂN MỘT SỐ KỸ THUẬT THỦY VÂN DỰA TRÊN CÁC VÙNG ĐẶC TRƯNG ĐIỂN HÌNH CỦA ẢNH KỸ THUẬT SỐ

**LUẬN ÁN TIẾN SĨ HỆ THỐNG THÔNG TIN**
**Mã số: 9 48 01 04**

| **Xác nhận của Học viện Khoa học và Công nghệ** | **Người hướng dẫn 1** *(Ký, ghi rõ họ tên)* | **Người hướng dẫn 2** *(Ký, ghi rõ họ tên)* |
|---|---|---|

***Hà Nội - 2024***

# LỜI CAM ĐOAN

Tôi xin cam đoan luận án: "Nghiên cứu phát triển một số kỹ thuật thủy vân dựa trên các vùng đặc trưng điển hình của ảnh kỹ thuật số" là công trình nghiên cứu của chính mình dưới sự hướng dẫn khoa học của tập thể hướng dẫn. Luận án sử dụng thông tin trích dẫn từ nhiều nguồn tham khảo khác nhau và các thông tin trích dẫn được ghi rõ nguồn gốc. Các kết quả nghiên cứu của tôi được công bố chung với các tác giả khác đã được sự nhất trí của đồng tác giả khi đưa vào luận án. Các số liệu, kết quả được trình bày trong luận án là hoàn toàn trung thực và chưa từng được công bố trong bất kỳ một công trình nào khác ngoài các công trình công bố của tác giả. Luận án được hoàn thành trong thời gian tôi làm nghiên cứu sinh tại Học viện Khoa học và Công nghệ, Viện Hàn lâm Khoa học và Công nghệ Việt Nam.

*Hà Nội, ngày 16 tháng 08 năm 2024*

**Tác giả luận án**

. **Phạm Quang Huy**

# LỜI CẢM ƠN

Thực hiện luận án tiến sĩ là một thử thách lớn, đòi hỏi sự kiên trì và tập trung cao độ. Tôi thực sự hạnh phúc với kết quả đạt được trong đề tài nghiên cứu của mình. Những kết quả đạt được không chỉ là nỗ lực của cá nhân, mà còn có sự hỗ trợ và giúp đỡ của tập thể giáo viên hướng dẫn, cơ sở đào tạo, đơn vị công tác, đồng nghiệp và gia đình. Tôi muốn bày tỏ lòng biết ơn sâu sắc tới Học viện Khoa học và Công nghệ, nơi đã cung cấp môi trường và cơ sở vật chất tuyệt vời cho quá trình nghiên cứu của tôi. Tôi xin bày tỏ lòng kính trọng và cảm ơn đến PGS.TS. Tạ Minh Thanh, người đã có những định hướng giúp tôi thành công trong việc nghiên cứu của mình. Thầy đã động viên và chỉ bảo giúp tôi vượt qua những khó khăn để tôi hoàn thành được luận án này. Tôi cũng xin chân thành cảm ơn tới TS. Đào Nam Anh, Thầy cũng đã cho tôi những kiến thức quý báu về nghiên cứu khoa học. Nhờ sự chỉ bảo của Thầy tôi mới hoàn thành tốt luận án.

**Tác giả luận án**

. **Phạm Quang Huy**

# MỤC LỤC

# DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

| | |
|---|---|
| $\{0,1\}^*$ | Ký hiệu chuỗi bit có độ dài bất kỳ |
| $\{0,1\}^\infty$ | Ký hiệu chuỗi bit có độ dài vô tận |
| $\epsilon$ | Hàm nhỏ không đáng kể |
| $\sigma$ | Chữ ký số |
| WLNS | Phương pháp thủy vân bằng cách học không nổi bật |
| RDH | Phương pháp nhúng dữ liệu có thể đảo ngược (Reversible Data Hiding) |
| JPEG | Một tiêu chuẩn nén hình ảnh (Joint Photographic Experts Group) |
| DCT | Biến đổi cosin rời rạc (the Discrete Cosine Transform) |
| ROI | Các vùng quan tâm (Regions of Interest) |
| LSB | Các bit ít quan trọng nhất (the Least Significant Bits) |
| DWT | Biến đổi sóng rời rạc (the Discrete Wavelet Transform) |
| JND | Độ méo đáng chú ý nhất (Just Noticeable Distortion) |
| SAD | Tổng chênh lệch Tuyệt đối (Sum of Absolute Differences) |
| SSIM | Chỉ số đo lường sự tương đồng cấu trúc (Structural Similarity Index Measure) |
| PSNR | Tỷ lệ tín hiệu tối đa đến nhiễu (Peak Signal to Noise Ratio) |

# DANH MỤC CÁC HÌNH VẼ

# DANH MỤC CÁC BẢNG BIỂU

# MỞ ĐẦU

***Tính cấp thiết của đề tài nghiên cứu:***

Lịch sử hình thành và phát triển của các kỹ thuật liên quan đến bảo hộ quyền tác giả là một quá trình biến đổi liên quan đến việc thích ứng với những tác động của công nghệ. Sự xuất hiện của các cuộc cách mạng công nghệ đã tạo nền tảng và thúc đẩy sự phát triển của quyền tác giả. Đồng thời, quyền tác giả cũng đã có vai trò thúc đẩy sự tiến bộ trong lĩnh vực công nghệ thông qua việc bảo vệ quyền của những người sáng tạo về các tác phẩm văn học, khoa học và nghệ thuật.

Ngay từ giữa thế kỷ XV, việc sáng chế máy in đã tạo ra một sự biến đổi lớn trong việc sao chép sách từ việc thủ công sang sử dụng máy móc. Sự bùng nổ của thị trường sao chép sách tại Anh đã thúc đẩy các nhà xuất bản đặt ra yêu cầu về quyền lợi cho hoạt động biên soạn và in ấn [1]. Đáp ứng nhu cầu này, đạo luật về quyền tác giả đã được ban hành lần đầu tiên tại Anh định rõ rằng quyền tác giả thuộc về người sáng tạo và tác phẩm được bảo hộ trong một khoảng thời gian nhất định.

Mối liên hệ giữa quyền tác giả và công nghệ [2] ngày càng rõ ràng bởi sự phát triển của các công nghệ ghi âm, ghi hình và phát sóng. Các tiến bộ này đã mở rộng phạm vi bảo hộ quyền tác giả đối với tác phẩm kịch, âm nhạc, bản ghi âm và ghi hình. Có thể khẳng định rằng sự hình thành của quyền tác giả có nguồn gốc trực tiếp từ sự phát triển của công nghệ.

Khi internet ra đời, nó đã tạo ra sự thay đổi to lớn trong mọi khía cạnh của đời sống kinh tế và xã hội, bao gồm cả lĩnh vực quyền tác giả. Khi internet phát triển, quyền tác giả lại đối mặt với những thách thức mới do công nghệ mới, cụ thể như sau:

i. Sự biến đổi của môi trường internet

Internet đã làm thay đổi cách thức sao chép, phân phối và lưu trữ tác phẩm văn hóa và nghệ thuật, làm dấy lên nhiều thách thức trong việc bảo vệ quyền tác giả. Dưới đây là ba thách thức chính:

- Sao chép và phân phối dễ dàng: Trong không gian mạng, việc sao chép tác

phẩm trở nên đơn giản và tiện lợi với chi phí thấp hoặc không tốn kém, gây ra sự lan truyền không kiểm soát các tác phẩm bản quyền. Ví dụ, trong 7 ngày Tết Nguyên đán tại Việt Nam, chương trình "Gặp nhau cuối năm - Táo quân 2021" đã ghi nhận hơn 2.000 trường hợp vi phạm bản quyền [3].

- Thay đổi trong cách lưu trữ tác phẩm: Mạng Internet đã biến đổi hình thức vật chất chứa đựng tác phẩm, khiến việc nhận diện bản sao tác phẩm trở nên dễ dàng hơn. Công nghệ số hóa cho phép tạo ra nhiều bản sao hoàn hảo của tác phẩm được bảo hộ, dẫn đến khó khăn trong việc kiểm soát và bảo vệ quyền tác giả.

- Quá trình truyền tải tác phẩm qua mạng: Dữ liệu tác phẩm khi được truyền tải qua mạng thường cần thông qua bộ nhớ truy cập ngẫu nhiên của các máy chủ trung gian để tải xuống hoặc hiển thị trên màn hình người dùng [4]. Điều này có thể dẫn đến việc tạo ra các bản sao lưu trữ tạm thời hoặc vĩnh viễn trên các thiết bị như USB, đĩa CD mà không rõ ràng về quyền sao chép.

Những thách thức này đòi hỏi cần có các giải pháp pháp lý và công nghệ mới để bảo vệ hiệu quả quyền sở hữu trí tuệ trong môi trường số ngày càng phức tạp.

ii. Sự thay đổi trong việc hưởng thụ tác phẩm

Internet đã thay đổi cách thức người dùng tiếp cận và tận hưởng tác phẩm, bản ghi âm và ghi hình. Người sử dụng internet có thể dễ dàng tận dụng tác phẩm trong không gian mạng với tốc độ nhanh chóng và chi phí thấp, bất kể thời gian và địa điểm [3]. Các tác phẩm số có thể được phân phối với số lượng lớn mà không tốn nhiều chi phí. Chủ sở hữu quyền tác giả sử dụng các biện pháp công nghệ để bảo vệ tác phẩm và ngăn chặn việc xâm phạm quyền tác giả trên internet. Họ có quyền tự bảo vệ tác phẩm bằng các giải pháp công nghệ mà không cần phải tuân theo quy định pháp luật. Tuy nhiên, khi các giải pháp công nghệ này được tạo ra bởi con người, chúng cũng có thể bị con người phá vỡ. Do đó, pháp luật liên quan đến bảo hộ quyền tác giả cần cấm các hành vi vô hiệu hóa các giải pháp công nghệ bảo vệ tác phẩm. Quyền tự bảo vệ tác phẩm bằng các giải pháp công nghệ đã được đề cập tại Điều 9, Điều 28 và Điều 198 của Luật Sở hữu Trí tuệ Việt Nam [5], nhưng cần sự điều chỉnh và bổ sung để đảm bảo quyền của người sáng tạo trong môi trường internet.

iii. Sự thay đổi nhanh chóng của các giải pháp công nghệ

Sự phát triển nhanh chóng của công nghệ đã mang lại những thách thức mới trong việc bảo vệ bản quyền trong môi trường internet. Công nghệ đã cho phép chủ sở hữu bản quyền bảo vệ các tác phẩm của họ một cách hiệu quả tương tự như trong môi trường truyền thống. Tuy nhiên, các biện pháp công nghệ bảo vệ này cũng có thể hạn chế quyền tiếp cận thông tin, tri thức và thưởng thức văn hóa, nghệ thuật của công chúng [6].

Quyền tự do ngôn luận và các quyền cơ bản khác của con người phải được bảo đảm không chỉ ở môi trường truyền thống mà còn trên không gian mạng. Sự phát triển của internet không thể là lý do để hạn chế các quyền này. Các vấn đề phát sinh từ sự bảo vệ quyền tác giả trên internet cho thấy sự cần thiết phải cân bằng giữa quyền sáng tạo và quyền tiếp cận của công chúng [6].

Mặc dù các hiệp ước quốc tế [7] và pháp luật quốc gia [5] đã cung cấp những ngoại lệ cho phép người dùng sử dụng các tác phẩm mà không cần sự cho phép của chủ sở hữu bản quyền nhưng các biện pháp bảo vệ công nghệ vẫn thường xuyên được sử dụng để hạn chế những sử dụng này. Các giải pháp công nghệ yêu cầu một sự điều chỉnh liên tục để thích ứng với môi trường số ngày càng phức tạp, đồng thời đảm bảo duy trì sự cân bằng giữa lợi ích của người sáng tạo và lợi ích cộng đồng.

Các kỹ thuật bảo hộ quyền tác giả cần được cải tiến để phù hợp với sự phát triển của công nghệ và đáp ứng nhu cầu của môi trường internet cũng như quy định của pháp luật [8], đảm bảo rằng quyền của người sáng tạo không chỉ được bảo vệ trong môi trường vật chất mà còn cả trong không gian trực tuyến.

Trong bối cảnh hiện nay, một trong những kỹ thuật nổi bật nhằm bảo vệ quyền sở hữu trí tuệ cho các tác phẩm kỹ thuật số, đặc biệt là ảnh và video, là thủy vân số. Thủy vân số là giải pháp được công nhận rộng rãi trong hai thập kỷ qua cho việc nhúng dữ liệu vào ảnh và video, một chiến thuật chính trong phát hiện và khôi phục sự can thiệp vào đa phương tiện [9]. Thủy vân số là việc cài đặt một thông tin nhận dạng vào trong một tác phẩm mà không làm thay đổi đáng kể đến chất lượng của tác phẩm đó. Thông tin này có thể là logo, văn bản hoặc một chuỗi ký tự đặc biệt, không thể gỡ bỏ mà không gây hư hại đến tác phẩm gốc. Kỹ thuật này giúp bảo vệ bản quyền bằng cách cho phép chủ sở hữu có khả năng theo dõi và xác minh nguồn gốc của tác phẩm một cách dễ dàng khi tác phẩm được phát tán trên internet.

Sự phát triển của công nghệ số đã làm tăng đáng kể khả năng sao chép và phân phối các tác phẩm mà không hề suy giảm chất lượng, từ đó đặt ra những thách thức mới cho việc bảo vệ quyền tác giả. Thủy vân số do đó đóng vai trò thiết yếu trong việc ngăn chặn việc sử dụng trái phép các tác phẩm số. Tuy nhiên, thách thức hiện tại là làm thế nào để tạo ra các kỹ thuật thủy vân có khả năng chống lại các phương pháp tấn công ngày càng tinh vi mà không làm ảnh hưởng đến tính thẩm mỹ và chất lượng của tác phẩm gốc. Các phương pháp tấn công này có thể bao gồm việc cố tình làm hỏng dữ liệu thủy vân hoặc cố gắng loại bỏ hoàn toàn nó.

Nghiên cứu tiếp tục trong lĩnh vực thủy vân dựa trên đặc trưng của ảnh số là cần thiết để phát triển các giải pháp mới có khả năng chống lại sự phát triển của các công nghệ gỡ bỏ thủy vân, cũng như để đảm bảo rằng thủy vân không làm giảm chất lượng hình ảnh hoặc nhận thức của người dùng đối với tác phẩm. Hơn nữa, việc tích hợp các giải pháp thủy vân số với các công nghệ nhận dạng và phân tích ảnh tiên tiến hơn sẽ mở rộng khả năng ứng dụng của chúng, từ đó đem lại lợi ích lớn cho ngành công nghiệp nội dung số và bảo vệ quyền sở hữu trí tuệ một cách hiệu quả hơn.

***Mục tiêu nghiên cứu:***

Luận án hướng đến mục tiêu phát triển các phương pháp thủy vân trong ảnh số có khả năng cải thiện tính bền vững và tính vô hình của thông tin thủy vân, đồng thời cải thiện khả năng phục hồi ảnh gốc sau khi trích rút thủy vân. Mục tiêu cụ thể bao gồm việc đề xuất và thử nghiệm các phương pháp mới nhằm tăng cường khả năng bảo vệ bản quyền, đảm bảo tính toàn vẹn và xác thực dữ liệu trong các ứng dụng truyền thông số.

***Đối tượng nghiên cứu:***

Đối tượng nghiên cứu của luận án bao gồm các kỹ thuật thủy vân hiện có, các mô hình độ nổi bật trong ảnh số, các thuật toán xử lý ảnh số liên quan và đặc biệt là các phương pháp thủy vân thuận nghịch (Reversible Watermarking). Luận án tập trung vào việc phân tích và cải tiến các phương pháp thủy vân nhằm nâng cao hiệu quả và tính bền vững của chúng trong các môi trường có nhiều tác động xấu như nén dữ liệu, chỉnh sửa ảnh, và các dạng tấn công khác. Đối với thủy vân thuận nghịch, luận án nghiên cứu việc bảo toàn thông tin gốc sau khi phát hiện và loại bỏ thủy vân, nhằm đảm bảo tính toàn vẹn và bảo mật của ảnh số.

***Phương pháp nghiên cứu:***

Luận án áp dụng các phương pháp nghiên cứu khoa học tiên tiến bao gồm:

- Phân tích lý thuyết: Tìm hiểu, phân tích các cơ sở lý thuyết liên quan đến kỹ thuật thủy vân và các mô hình độ nổi bật, từ đó xác định các vấn đề còn tồn đọng và đưa ra các giả thuyết nghiên cứu.
- Thực nghiệm: Triển khai các thuật toán đề xuất trên bộ dữ liệu thực tế và mô phỏng, từ đó đánh giá hiệu quả của các phương pháp thủy vân đề xuất thông qua các tiêu chí như độ bền vững, tính tàng hình và khả năng khôi phục dữ liệu.
- Phân tích kết quả: So sánh, đánh giá kết quả thu được từ các phương pháp thủy vân khác nhau, xác định những ưu và nhược điểm của từng phương pháp, từ đó đề xuất những cải tiến cần thiết.

***Bố cục của luận án:***

Ngoài phần mở đầu và phần kết luận, kiến nghị, luận án được chia thành 3 chương chính với bố cục như sau:

**Chương 1**: Tổng quan về các vấn đề bảo vệ bản quyền và các kỹ thuật thủy vân.

Chương 1 của luận án mở đầu cho nghiên cứu về sự tích hợp giữa bảo vệ bản quyền và kỹ thuật thủy vân, hai yếu tố thiết yếu trong lĩnh vực quản lý tài sản trí tuệ. Luận án này trình bày một cái nhìn tổng quan và sâu sắc về chủ đề, qua đó phân tích những thách thức và tiềm năng của kỹ thuật thủy vân trong việc bảo vệ và quản lý quyền sở hữu trí tuệ.

Chương này trình bày về cơ sở lý thuyết của kỹ thuật thủy vân, từ việc nhúng thông tin định danh vào tài liệu đến ứng dụng của nó trong nhiều lĩnh vực. Luận án đánh giá cách thức hoạt động của các kỹ thuật thủy vân khác nhau và khả năng áp dụng của chúng trong việc bảo vệ bản quyền và quản lý tài sản trí tuệ.

Tuy nhiên, như mọi công nghệ, kỹ thuật thủy vân cũng có những hạn chế. Phần tiếp theo sẽ thảo luận về các vấn đề và thách thức mà các nhà nghiên cứu, doanh nghiệp và cơ quan chính phủ gặp phải khi sử dụng kỹ thuật thủy vân để bảo vệ thông tin và dữ liệu. Luận án xem xét các vấn đề liên quan đến hiệu quả, bảo mật và quản lý của kỹ thuật thủy vân.

Trong bối cảnh công nghệ phát triển liên tục và môi trường kỹ thuật thay đổi, việc hiểu biết về kỹ thuật thủy vân và tương tác của nó với quyền sở hữu trí tuệ trở nên cần thiết. Chương này xây dựng nền tảng cho luận án để tiếp tục nghiên cứu về kỹ thuật thủy vân và các vấn đề phức tạp liên quan đến bảo vệ bản quyền và quản lý tài sản trí tuệ trong thế kỷ 21.

**Chương 2**: Phân tích ảnh hưởng độ nổi bật của ảnh trong thủy vân số.

Chương 2 của luận án tập trung vào việc phát triển các phương pháp thủy vân số mới, sử dụng đặc trưng độ nổi bật và không nổi bật của ảnh số để tăng cường bảo mật. Phương pháp này được thiết kế để nhúng thông tin vào những vùng ít thu hút sự chú ý trong ảnh thông qua việc sử dụng công nghệ máy học và đồng thời khai thác các đặc trưng nổi bật để cải thiện khả năng chống giả mạo và tăng cường bảo mật thông tin nhúng.

Kết quả đạt được từ việc triển khai các phương pháp thủy vân mới trong

nghiên cứu này bao gồm:

- Khả năng chống lại các loại tấn công phổ biến: Các thử nghiệm chứng minh phương pháp thủy vân mới có khả năng chống lại nén, cắt xén và thêm nhiễu mà không làm giảm chất lượng thị giác của ảnh.
- Duy trì chất lượng hình ảnh: Nhờ vào việc sử dụng các đặc trưng không nổi bật và nổi bật một cách hiệu quả, phương pháp thủy vân đảm bảo rằng chất lượng thị giác của ảnh gốc không bị ảnh hưởng đáng kể sau quá trình nhúng thông tin.
- Ứng dụng rộng rãi: Phương pháp mới cho phép ứng dụng trong nhiều lĩnh vực đòi hỏi bảo mật cao, như tài liệu pháp lý và hình ảnh y tế, nơi mà việc duy trì chất lượng hình ảnh là cần thiết.

Những kết quả này làm nổi bật tiềm năng của các kỹ thuật thủy vân dựa trên đặc trưng độ nổi bật và không nổi bật trong việc cải thiện bảo mật và hiệu quả của phương pháp thủy vân trong các ứng dụng thực tế.

**Chương 3**: Phát triển kỹ thuật thủy vân đảm bảo tính toàn vẹn của ảnh gốc.

Chương 3 của luận án đề xuất và phát triển các thuật toán mới trong lĩnh vực thủy vân đảo ngược (Reversible Data Hiding - RDH) cho ảnh JPEG nói riêng và ảnh số nói chung, áp dụng thuật toán yếu tố cấu trúc (Structural Element Algorithm - SEA) và thuật toán biến đổi DCT.

Các thuật toán này được thiết kế để tối ưu hóa quá trình nhúng thông tin vào ảnh JPEG, đảm bảo rằng sau khi thông tin bí mật đã được trích xuất, ảnh gốc có thể được phục hồi hoàn toàn mà không có bất kỳ sự thay đổi nào về chất lượng. Điều này rất quan trọng trong các ứng dụng nhạy cảm, nơi mà bảo toàn ảnh gốc là điều cần thiết.

Kết quả đạt được từ việc triển khai các thuật toán này trong nghiên cứu bao gồm:

- Hiệu suất nhúng cao hơn: Các thuật toán mới cho phép nhúng một lượng lớn dữ liệu hơn vào ảnh mà không làm giảm chất lượng hình ảnh nhìn thấy.
- Khả năng phục hồi ảnh gốc tốt hơn: Sau khi dữ liệu bí mật được trích xuất, ảnh gốc có thể được phục hồi hoàn toàn đảm bảo tính nguyên vẹn của ảnh.

- Ổn định trước các cuộc tấn công: Thuật toán được cải tiến để đảm bảo rằng thông tin nhúng có khả năng chống lại các cuộc tấn công số hóa và xử lý hình ảnh khác nhau.

Những kết quả này đóng góp vào sự phát triển của các phương pháp bảo vệ thông tin trong lĩnh vực thủy vân số, đặc biệt là trong các ứng dụng đòi hỏi tính toàn vẹn và bảo mật cao.

**Kết luận và hướng nghiên cứu trong tương lai**.

Phần cuối của luận án tập trung vào việc tổng kết những đóng góp chính của công trình nghiên cứu và đề xuất hướng đi cho các nghiên cứu trong tương lai. Phần kết luận nhấn mạnh tầm quan trọng của việc phát triển kỹ thuật thủy vân số như một giải pháp hiệu quả để bảo vệ quyền sở hữu trí tuệ và an ninh nội dung trong môi trường số. Các phương pháp thủy vân số đã được khám phá trong luận án, bao gồm thủy vân dựa trên đặc trưng độ nổi bật và thủy vân thuận nghịch đã chứng minh được tiềm năng ứng dụng cao trong việc tạo ra các lớp bảo vệ bản quyền mạnh mẽ mà không làm mất đi thông tin gốc của dữ liệu.

# CHƯƠNG 1. TỔNG QUAN NGHIÊN CỨU VÀ MỘT SỐ KIẾN THỨC NỀN TẢNG

## 1.1. Giới thiệu

### 1.1.1. Nguồn gốc và khái niệm về thủy vân số

Thuật ngữ "thủy vân" (watermark) xuất phát từ một loại mực vô hình được viết trên giấy và chỉ xuất hiện khi giấy được ngâm trong nước [10]. Thuật ngữ "thủy vân số" được chấp nhận rộng rãi trên toàn thế giới vào những năm đầu thập kỷ 1990. Khoảng năm 1995, sự quan tâm đối với thủy vân số đã bắt đầu phát triển mạnh.

Cách đây khoảng 700 năm, kỹ thuật thủy vân trên giấy đã xuất hiện trong các tác phẩm nghệ thuật làm bằng giấy thủ công. Loại giấy có thủy vân cổ nhất được phát hiện vào năm 1929 ở thị trấn Fabriano, Ý đã có ảnh hưởng lớn đến quá trình phát triển công nghiệp sản xuất giấy. Kỹ thuật thủy vân đã trở thành phương pháp quan trọng để xác định nguồn gốc sản phẩm giấy, giúp người tiêu dùng lựa chọn đúng hãng sản xuất mà họ muốn mua.

Thủy vân số là một quá trình phức tạp, bao gồm việc nhúng thông tin tinh vi (như ảnh, chuỗi bit hoặc số) vào dữ liệu số (như ảnh số, âm thanh, video hoặc văn bản) để xác định thông tin bản quyền của tác phẩm đó [10]. Mục tiêu của thủy vân số là bảo vệ bản quyền cho dữ liệu số mang thông tin thủy vân.

Việc thêm thủy vân vào một môi trường số được gọi là "thủy vân số". Thủy vân số được coi là một hình thức ẩn giấu thông tin. Theo sơ đồ phân loại kỹ thuật giấu tin của A.P. Pentitcolas [11] vào năm 1999, có hai hướng chính trong nghiên cứu, đó là giấu tin mật và thủy vân số. Thủy vân số có thể được xem là quá trình nhúng thông tin mà người dùng cuối không cần phải quan tâm đến thông tin được ẩn trong đối tượng chứa thông tin.

Vì lẽ đó thủy vân trở thành một quá trình quan trọng trong lĩnh vực nhúng dữ liệu, nơi mà thông tin cần được giữ an toàn và xác thực nguồn gốc của sản phẩm là yếu tố chính. Thủy vân không chỉ là một phần quan trọng của quá trình nhúng thông tin mà còn đóng vai trò phòng thủ với những người cố gắng phá vỡ sự an toàn của dữ liệu.

Mục tiêu chính của thủy vân là tạo ra một kỹ thuật nhúng thông tin mà người ta khó có thể trích xuất hoặc gỡ bỏ mà không có chìa khóa bí mật [10]. Qua đó, việc bảo vệ thông tin cần được bảo vệ trở nên đáng tin cậy hơn. Thủy vân không chỉ là một giải pháp hiệu quả trong việc giữ an toàn thông tin mà còn là một phương tiện để đảm bảo tính xác thực của nguồn gốc, quan trọng trong những trường hợp đề cao sự minh bạch và tính tin cậy.

Trong quá trình này, thủy vân cần được thiết kế sao cho độ phức tạp và khả năng chống phân tích cao, đặt ra thách thức đối với những người muốn xâm phạm sự vững chắc của nó. Một khía cạnh quan trọng khác là khả năng của thủy vân khi thích ứng với nhiều loại dữ liệu và định dạng đa phương tiện khác nhau, đặt ra yêu cầu cao về tính linh hoạt và khả năng tương thích.

Trong ngữ cảnh ngày nay, thủy vân còn trở thành một lĩnh vực nghiên cứu đa dạng và phong phú với nhiều phương pháp tiếp cận và ứng dụng khác nhau [11, 12, 13]. Nghiên cứu liên tục tập trung vào việc phát triển các kỹ thuật thủy vân mới nhằm đáp ứng nhu cầu ngày càng cao về bảo mật thông tin và xác thực dữ liệu trong môi trường số hóa ngày càng phức tạp.

Một trong những thách thức đặt ra là phải tìm ra cách cân bằng giữa khả năng nhúng thông tin một cách hiệu quả và việc duy trì chất lượng và tính toàn vẹn của dữ liệu. Sự phức tạp ngày càng tăng của các dữ liệu đa phương tiện đặt ra yêu cầu cao về đổi mới và sáng tạo trong phát triển các thuật toán thủy vân.

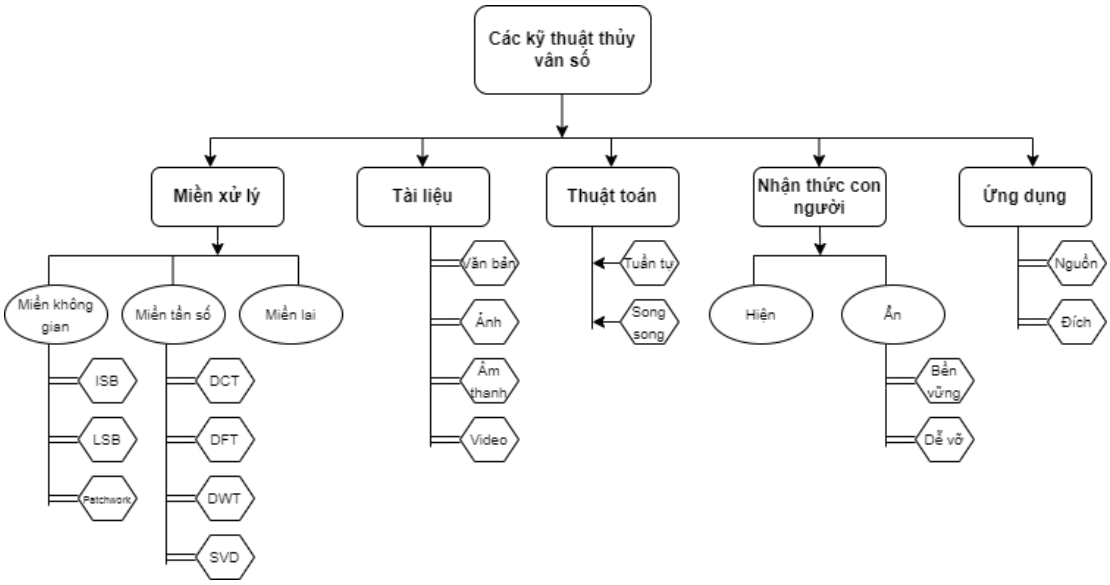
Đồng thời, thủy vân cũng đối mặt với những thách thức về đạo đức và pháp lý [14], đặc biệt là trong bối cảnh ngày càng nhiều tranh cãi xoay quanh quyền riêng tư và sự tự do thông tin. Các nhà nghiên cứu và chuyên gia thủy vân cần tiếp tục đối mặt và đưa ra giải pháp cho những vấn đề này để đảm bảo rằng thủy vân được sử dụng một cách công bằng và hợp pháp.

Trong tương lai, việc phát triển các kỹ thuật thủy vân mới và hiệu quả hơn sẽ đóng vai trò quan trọng trong việc đảm bảo an toàn cho dữ liệu và thông tin quan trọng, đồng thời đưa ra những tiến bộ quan trọng trong lĩnh vực bảo mật thông tin. Công cụ thủy vân không chỉ giúp bảo vệ bản quyền mà còn đóng góp tích cực vào việc xây dựng một môi trường số an toàn và tin cậy.

### 1.1.2. Phân loại thủy vân số

Hình 1.1 [15] trình bày một cái nhìn tổng quan về các tiến bộ gần đây trong việc phân loại thủy vân số, minh họa sự đa dạng và hiệu quả của các

phương pháp được áp dụng.




***Hình 1.1:*** *Phân loại thủy vân số*

*1.1.2.1. Phân loại thủy vân số theo miền xử lý*

Một trong những tiêu chí phân loại thủy vân số là theo miền nhúng thủy vân. Ở đây thủy vân nhúng được xử lý trong miền không gian hoặc miền tần số tùy thuộc vào hướng tiếp cận xử lý dữ liệu.

**Miền không gian** ảnh là miền dữ liệu ảnh gốc tập hợp một ma trận các điểm ảnh, xử lý dữ liệu thủy vân trong miền không gian là tác động trực tiếp lên các điểm ảnh, thay đổi giá trị trực tiếp giá trị của các điểm ảnh [16]. Đây được coi là hướng tiếp cận tự nhiên khi thực hiện giấu tin trong ảnh và một trong những phương pháp thủy vân số phổ biến là thay thế bit ít quan trọng nhất LSB (Least Significant Bit).

**Miền tần số** là việc biến đổi các điểm ảnh của miền không gian thông qua các kỹ thuật biến đổi sang miền mới với các biến số mới [16]. Việc biến đổi sang miền tần số đảm bảo ba vấn đề quan trọng sau:

1. Không hiển thị trên nền ảnh.
2. Không làm ảnh hưởng nhiều tới chất lượng của ảnh khi quan sát.
3. Tồn tại bền vững cùng sản phẩm, khó bị xóa hay sai lệch bởi các tấn công hơn miền không gian.

*1.1.2.2. Phân loại thủy vân số theo môi trường chứa*

Thủy vân số phân loại theo đối tượng đa phương tiện được nhúng thủy vân như sau:

**Thủy vân trên ảnh** [16]

Mục đích: Thủy vân trên ảnh thường được sử dụng để đánh dấu bản quyền, xác thực nguồn gốc của hình ảnh và bảo vệ chúng khỏi việc sao chép trái phép.

Ví dụ: Thủy vân có thể được nhúng bằng cách điều chỉnh các điểm ảnh hoặc thông tin không có ảnh hưởng đến sự nhận biết của con người. Các thuật toán nhúng thủy vân được áp dụng để tạo ra một biểu tượng hoặc dấu nhận dạng độc đáo trên ảnh.

**Thủy vân trên âm thanh** [16]

Mục đích: Thủy vân âm thanh được sử dụng để xác thực và bảo vệ bản quyền cho các tệp âm thanh, podcast hoặc các tác phẩm âm nhạc trực tuyến.

Ví dụ: Thủy vân âm thanh thường được nhúng bằng cách thay đổi một số thuộc tính không đáng kể của tín hiệu âm thanh, chẳng hạn như biên độ, phổ tần số hoặc thời gian.

**Thủy vân trên video** [16]

Mục đích: Thủy vân trên video được sử dụng để bảo vệ quyền tác giả của video và theo dõi nguồn gốc của nó.

Ví dụ: Các kỹ thuật nhúng thủy vân trên video thường kết hợp các biến đổi dựa trên thời gian và không gian, như thay đổi một số frame cụ thể hoặc nhúng thông tin vào khung hình.

**Thủy vân trên văn bản** [16]

Mục đích: Thủy vân trên văn bản thường được sử dụng để bảo vệ bản quyền, xác thực nguồn gốc và kiểm soát sao chép của nội dung văn bản.

Ví dụ: Thủy vân trên văn bản có thể bao gồm việc thay đổi cấu trúc văn bản hoặc nhúng các biểu tượng, mã số, hoặc dấu hiệu đặc biệt vào văn bản.

*1.1.2.3. Phân loại thủy vân số theo thuật toán*

**Tuần tự (Sequential)**:

- Kỹ thuật thủy vân tuần tự thực hiện việc nhúng thông tin thủy vân theo một trình tự nhất định, lần lượt từ điểm này sang điểm khác trong ảnh. Điều

này có thể giúp dễ dàng kiểm soát quá trình nhúng và đảm bảo thông tin được nhúng một cách có hệ thống và đều đặn.

- Các phương pháp tuần tự thường được sử dụng để đảm bảo rằng toàn bộ ảnh đều có thủy vân, làm tăng khả năng phát hiện và bảo vệ thông tin.

**Song song (Parallel)**:

- Kỹ thuật thủy vân song song thực hiện việc nhúng thông tin thủy vân đồng thời vào nhiều điểm hoặc nhiều vùng trong ảnh cùng một lúc. Điều này giúp tăng tốc độ nhúng và có thể giảm thiểu tác động của việc nhúng đến chất lượng tổng thể của ảnh.

- Các phương pháp song song thường được áp dụng khi cần xử lý khối lượng lớn dữ liệu hoặc khi yêu cầu về thời gian xử lý là rất cao.

#### *1.1.2.4. Phân loại thủy vân số theo nhận thức của con người*

**Thủy vân hiện** là một phương pháp nhúng thông tin đặc biệt vào dữ liệu, nơi thông tin này có thể nhìn thấy hoặc được hiển thị một cách rõ ràng cho người xem [16]. Điều này thường được áp dụng để xác nhận bản quyền, thương hiệu hoặc xuất xứ của tác phẩm. Dưới đây là một mô tả chi tiết về thủy vân hiện:

- Mục đích chính: Dùng để xác thực và bảo vệ bản quyền của tác phẩm, thường được sử dụng trong ngành công nghiệp sáng tạo như nhiếp ảnh, thiết kế đồ họa và nghệ thuật số.
- Tính nhạy cảm: Dễ nhận diện và nhìn thấy bởi người xem mà không cần công cụ hỗ trợ.
- Tính ứng dụng: Bảo vệ bản quyền, thương hiệu và quảng cáo. Thường xuất hiện trên hình ảnh, video, hoặc các tác phẩm đa phương tiện.
- Phương pháp nhúng: Thông tin thủy vân được tích hợp trực tiếp vào hình ảnh hoặc tác phẩm với mức độ hiển thị tương đối cao.
- Ưu Điểm: Dễ nhận biết, giúp xác nhận nguồn gốc và bản quyền. Có thể là một phương tiện quảng cáo hiệu quả.
- Nhược Điểm: Có thể làm giảm giá trị thẩm mỹ của tác phẩm. Dễ bị loại bỏ hoặc che đậy.

- Ứng dụng thực tế: Nhiếp ảnh, nghệ thuật số, video và bất kỳ tác phẩm sáng tạo nào cần xác nhận nguồn gốc và bản quyền. Ví dụ cụ thể:

  - Trên hình ảnh: Logo của nhiếp ảnh gia hoặc tên thương hiệu được chèn trực tiếp lên hình ảnh.

  - Trong video: Dấu hiệu thủy vân hoặc logo được hiển thị trong góc video.

- Thách Thức: Tìm ra một sự cân bằng giữa việc xác nhận bản quyền và duy trì tính thẩm mỹ của tác phẩm.

Thủy vân hiện là một phương pháp hiệu quả để bảo vệ quyền sở hữu và xác định nguồn gốc trong môi trường số, nhưng việc sử dụng nó cần sự cân nhắc để tránh ảnh hưởng quá mức đến trải nghiệm người xem.

**Thủy vân ẩn** là một phương pháp nhúng thông tin vào dữ liệu mà không làm thay đổi đồ họa hay âm thanh một cách rõ ràng cho người quan sát [16]. Thường được sử dụng để xác thực và bảo vệ bản quyền trong các tác phẩm số như hình ảnh, video, hoặc âm nhạc. Thủy vân ẩn thường không thể nhìn thấy bằng mắt thường và được thiết kế để giữ tính toàn vẹn của tác phẩm nguyên bản. Thủy vân ẩn thường được chia thành ba loại sau:

1. Thủy vân ẩn bền vững [16]:

   Thủy vân ẩn bền vững là một kỹ thuật thủy vân số được thiết kế để chống lại nhiều loại tấn công xử lý hình ảnh nhằm đảm bảo rằng thông tin thủy vân có thể tồn tại qua các biến đổi và vẫn có thể được trích xuất một cách chính xác. Phương pháp này là lựa chọn tối ưu trong các ứng dụng yêu cầu độ bảo mật và tính bền vững cao như bảo vệ tài liệu, quản lý quyền số và phân phối nội dung số.

   - Mục đích chính: Tập trung vào việc giữ thông tin thủy vân một cách ổn định và bền vững trong điều kiện xử lý và truyền tải dữ liệu.
   - Tính nhạy cảm: Nâng cao khả năng chịu đựng của thủy vân trước các biến đổi và tấn công, đảm bảo tính ổn định của thông tin thủy vân.
   - Tính ứng dụng:Các ứng dụng yêu cầu tính ổn định và bền vững của thủy vân, như quản lý tài liệu, bảo vệ bản quyền và lĩnh vực y tế.
   - Phương pháp nhúng: Sử dụng các kỹ thuật nhúng thông tin một cách cẩn thận để đảm bảo tính ổn định và bền vững.

- Ưu điểm: Bền vững trước các biến đổi, giữ nguyên tính toàn vẹn của thủy vân.
- Nhược điểm: Có thể đối mặt với giảm hiệu suất thẩm mỹ do sự tập trung vào tính ổn định.
- Ứng dụng thực tế: Các lĩnh vực đòi hỏi tính ổn định cao, không chấp nhận sự thay đổi đáng kể trong thông tin thủy vân.

2. Thủy vân ẩn dễ vỡ [16]:

   Thủy vân ẩn dễ vỡ là một phương pháp trong kỹ thuật thủy vân số, được thiết kế để đáp ứng các yêu cầu cụ thể về tính xác thực của hình ảnh hoặc tài liệu. Phương pháp này nhúng thông tin dễ bị phá vỡ bởi bất kỳ sự can thiệp nào đến tệp gốc, như chỉnh sửa hoặc xử lý hình ảnh, làm cho nó trở nên lý tưởng để xác minh tính toàn vẹn của tài liệu.

   - Mục đích chính: Chú trọng vào khả năng giữ lại thông tin thủy vân và khả năng truy xuất, xác thực sau khi dữ liệu trải qua biến đổi hoặc tấn công.
   - Tính nhạy cảm: Có khả năng chịu đựng mất mát thông tin và biến đổi cao hơn, đảm bảo khả năng truy xuất và xác thực.
   - Tính ứng dụng: Các ứng dụng yêu cầu mức độ bảo mật cao như an ninh thông tin, chống sao chép.
   - Phương pháp nhúng: Có khả năng chịu đựng mức độ biến đổi và mất mát thông tin, đảm bảo tính xác thực và truy xuất.
   - Ưu điểm: Bảo mật cao, có khả năng chịu đựng biến đổi và mất mát thông tin.
   - Nhược điểm: Có thể làm thay đổi đáng kể thông tin gốc và tăng kích thước của dữ liệu.
   - Ứng dụng thực tế: Các ứng dụng đòi hỏi mức độ bảo mật cao và khả năng truy xuất cao, như an ninh thông tin và chống sao chép.

3. Thủy vân ẩn bán dễ vỡ [16]:

   Thủy vân ẩn bán dễ vỡ là phương pháp thủy vân được thiết kế để nhúng thông tin vào hình ảnh một cách dễ bị thay đổi hoặc loại bỏ, thường được sử dụng cho các mục đích như trang trí hoặc xác định nguồn gốc, nơi mà

yêu cầu về bảo mật không quá cao. Phương pháp này cho phép tích hợp thông tin vào tài liệu mà không làm ảnh hưởng nhiều đến nội dung chính.

- Mục đích chính: Tập trung vào việc nhúng thông tin thủy vân một cách dễ vỡ, chủ yếu cho mục đích trang trí hoặc xác định nguồn gốc.
- Tính nhạy cảm: Dễ bị thay đổi hoặc loại bỏ mà không ảnh hưởng nhiều đến thông tin chính.
- Tính ứng dụng: Mục đích trang trí, quảng cáo, hoặc xác định nguồn gốc không đòi hỏi sự bảo mật cao.
- Phương pháp nhúng: Sử dụng các kỹ thuật nhúng linh hoạt, không yêu cầu tính ổn định cao.
- Ưu điểm: Dễ dàng nhúng và trích xuất thông tin, không yêu cầu sự ổn định cao.
- Nhược điểm: Không phù hợp cho các ứng dụng đòi hỏi mức độ bảo mật cao.
- Ứng dụng thực tế: Mục đích trang trí, quảng cáo, hoặc trong các tình huống không đòi hỏi sự bảo mật cao.

#### *1.1.2.5. Phân loại thủy vân số theo ứng dụng*

**Dựa trên nguồn (Source Based)**:

Kỹ thuật thủy vân dựa trên nguồn tập trung vào việc nhúng thông tin thủy vân vào hình ảnh dựa trên nguồn gốc của hình ảnh. Điều này giúp bảo vệ và xác định quyền sở hữu, theo dõi nguồn gốc và phát hiện vi phạm bản quyền. Ví dụ, thủy vân có thể được nhúng vào hình ảnh từ một cơ sở dữ liệu nội dung số của công ty để đảm bảo rằng mọi bản sao của hình ảnh đều có thể được theo dõi và xác thực nguồn gốc.

**Dựa trên đích đến (Destination Based)**:

Kỹ thuật thủy vân dựa trên đích đến sử dụng thông tin về nơi mà hình ảnh sẽ được phân phối hoặc sử dụng để tối ưu hóa quá trình nhúng thủy vân. Ví dụ, nếu hình ảnh sẽ được phát trực tuyến qua mạng, kỹ thuật thủy vân có thể tối ưu hóa để đảm bảo thông tin thủy vân không bị mất mát qua các quá trình nén và truyền dẫn mạng. Điều này giúp bảo vệ nội dung khi được sử dụng trong các môi trường khác nhau và đảm bảo thông tin thủy vân vẫn tồn tại sau khi hình ảnh được chia sẻ hoặc phát sóng.

### 1.1.3. Quy trình xây dựng mô hình thủy vân số

#### *1.1.3.1. Cách tạo thủy vân số*

Thủy vân có thể hiện thân dưới dạng hình ảnh biểu tượng hoặc văn bản với độ dài đã được xác định trước. Sự đa dạng của thủy vân hình ảnh khiến nó có khả năng chống chịu xử lý ảnh tốt hơn so với thủy vân dạng ký tự. Thay đổi thủy vân trước khi ẩn vào ảnh có thể được thực hiện thông qua việc mã hóa hoặc chuyển đổi định dạng. Thuật toán nhúng thủy vân cho hình ảnh được gọi là thuật toán thủy vân hợp nhất hình ảnh.

Sự hữu ích của thủy vân hình ảnh là dễ dàng nhận biết một cách trực quan và cung cấp chứng cứ vững chắc về quyền sở hữu hình ảnh. Thường thì một khóa bí mật $K$ sẽ được sử dụng để bảo mật cho dữ liệu thủy vân trước khi nhúng. Bởi vì tính ổn định được đảm bảo, thủy vân hình ảnh thường được sử dụng phổ biến hơn.

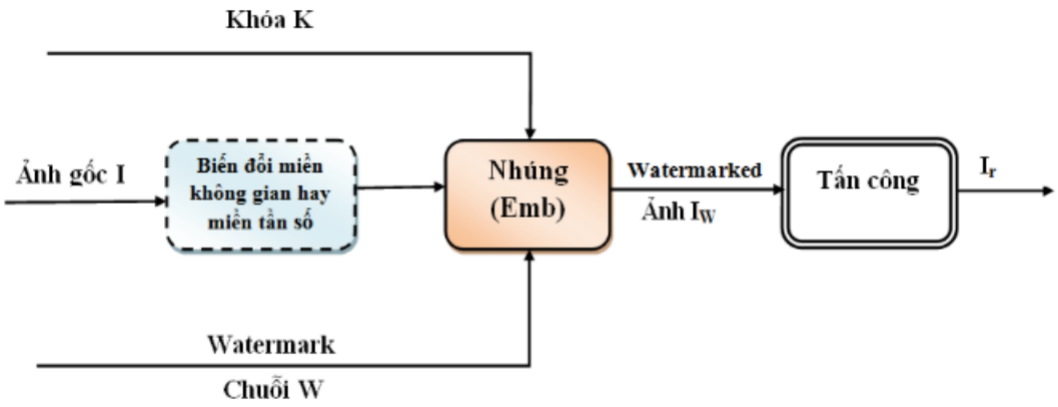
Để tăng tính bảo mật và hiệu quả dung lượng, thủy vân trước khi ẩn vào ảnh có thể được nén hoặc mã hóa. Theo cơ chế này, trước tiên dữ liệu thủy vân sẽ được nén để tăng kích thước, sau đó sẽ được mã hóa để đảm bảo tính bảo mật trước khi ẩn vào ảnh. Tuy nhiên, việc này làm tăng độ phức tạp trong việc phát hiện thủy vân.

#### *1.1.3.2. Quá trình nhúng thủy vân*

Trong giai đoạn này, các phần thông tin về khóa thủy vân, dữ liệu ẩn chứa thông tin và bộ công cụ được sử dụng để thực hiện việc nhúng thủy vân. Dữ liệu chứa có thể là các hình ảnh, tệp âm thanh, video hoặc các dạng dữ liệu số khác được sử dụng như môi trường để ẩn thông tin.

Bộ công cụ nhúng thủy vân là một chương trình có các thuật toán thủy vân được thực hiện bằng sự hỗ trợ của một khóa bí mật.

Quá trình nhúng thủy vân [17] vào dữ liệu chứa sẽ được thực hiện thông qua việc sử dụng bộ công cụ nhúng thủy vân. Kết quả của quá trình này là dữ liệu chứa đã được nhúng thủy vân hay còn được gọi là dữ liệu có chứa thông tin bản quyền và có thể được phân phối trên nhiều môi trường khác nhau. Trong quá trình phân phối, dữ liệu có thể bị nhiễu và tấn công từ bên ngoài. Vì vậy, yêu cầu đối với các kỹ thuật thủy vân số là phải đảm bảo tính bền vững trong bối cảnh gặp nhiễu và bị tấn công.




***Hình 1.2:*** *Quá trình nhúng thủy vân*

Trong hình 1.2, quá trình nhúng thủy vân cho ảnh tĩnh được mô tả và giải thích. Quá trình sử dụng ký hiệu $I$ để đại diện cho ảnh gốc, $W$ để biểu thị thủy vân, $I_W$ là hình ảnh chứa thủy vân và $K$ là khóa nhúng. Một hàm nhúng $Emb$ được áp dụng trên đầu vào là ảnh gốc $I$, thủy vân $W$ và khóa $K$ để tạo ra một hình ảnh mới $I_W$ chứa thủy vân.

Khóa $K$ chính là yếu tố quan trọng đối với sự tăng cường bảo mật của hệ thống thủy vân. Trước khi thực hiện quá trình nhúng, ảnh gốc có thể được chuyển đổi vào miền tần số hoặc thực hiện biến đổi trong miền không gian, phụ thuộc vào kỹ thuật thủy vân được lựa chọn. Khi quá trình nhúng thực hiện trong miền tần số, biến đổi nghịch đảo thường áp dụng để tạo ra hình ảnh chứa thủy vân. Biểu thức toán học cho hàm nhúng có thể được biểu diễn như sau:

- Đối với kỹ thuật biến đổi theo miền không gian :

$$Emb(I, W, K) = I_W \tag{1.1}$$

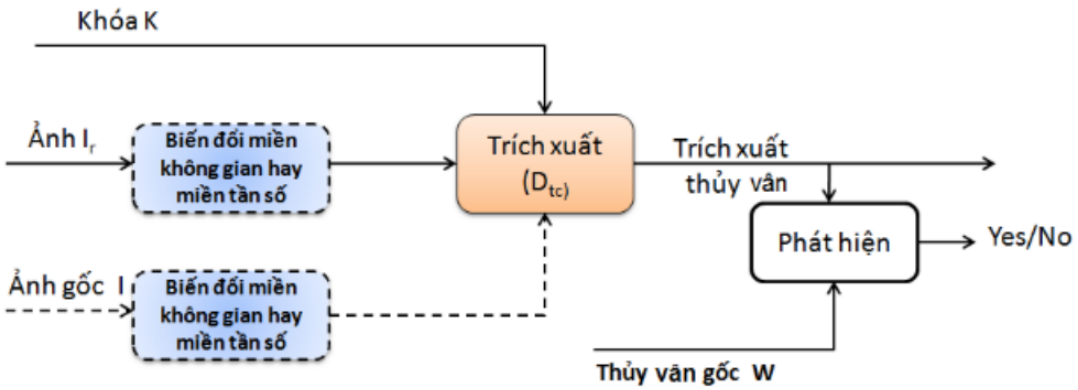
- Đối với kỹ thuật biến đổi theo miền tần số :

$$Emb(f, W, K) = I_W \tag{1.2}$$

  trong đó $f$ là vector hệ số cho phép biến đổi.

#### *1.1.3.3. Quá trình trích xuất thủy vân*

Việc trích rút thủy vân [17] được tiến hành thông qua một bộ trích xuất thủy vân tương ứng với bộ nhúng thủy vân và khóa sử dụng trong quá trình nhúng. Kết quả thu được là một thủy vân. Thủy vân thu được có thể tương




***Hình 1.3:*** *Quá trình trích xuất thủy vân*

đồng hoặc có sự khác biệt so với thủy vân ban đầu, phụ thuộc vào sự ảnh hưởng của nhiễu và các cuộc tấn công trên đường truyền.

Hình 1.3 trình bày và giải thích quá trình trích xuất và nhận diện thủy vân trong ảnh tĩnh. Một hàm phát hiện $D_{tc}$ nhận đầu vào là hình ảnh $I_r$ và khóa $K$ có chức năng xác định quyền sở hữu sản phẩm. Hình ảnh $I_r$ có thể chứa hoặc không chứa thủy vân. Trong mô hình tổng quát, hình ảnh cũng có thể bị biến đổi. Hàm phát hiện $D_{tc}$ 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 $I_r$.

Công thức toán học cho quy trình trích xuất thủy vân ẩn (không sử dụng hình ảnh gốc $I$) cụ thể như sau:

$$D_{tc}(Ir, K) = W \tag{1.3}$$

Công thức toán học cho quy trình trích xuất thủy vân hiện (sử dụng hình ảnh gốc $I$) cụ thể như sau:

$$D_{tc}(I_r, I, K) = W_e \tag{1.4}$$

Thuật toán phát hiện thủy vân ẩn tạo ra một đầu ra nhị phân, biểu thị sự có hay không có thủy vân. Do đó, có thể giả định:

$$D_{tc}(Ir, K) = \begin{cases} 1 \text{ nếu có thủy vân} \\ 0 \text{ nếu không có thủy vân} \end{cases} \tag{1.5}$$

Trong lược đồ trích xuất thủy vân, việc tách thủy vân cần phải thực hiện một cách chính xác để khôi phục lại thủy vân gốc. Lược đồ trích xuất thủy vân xác nhận quyền sở hữu, trong khi thuật toán phát hiện thủy vân xác nhận sự

hiện diện của thủy vân.

### 1.1.4. Các đặc trưng của thủy vân số

Trong quá khứ, đã có nhiều nghiên cứu [10, 16, 18] đề cập đến các đặc tính của thủy vân. Các thuộc tính này bao gồm tính phức tạp, tính chân thực của hình ảnh, độ tin cậy trong phát hiện, tính bền vững, dung lượng, bảo mật và nhiều khía cạnh khác. Tuy nhiên, không thể thiết kế một hệ thống thủy vân đảm bảo được tất cả các thuộc tính này cùng một lúc. Do đó, việc tạo cân bằng giữa các yếu tố là vô cùng quan trọng và việc thực hiện cân bằng này cần dựa trên sự phân tích cẩn thận về ứng dụng cụ thể.

**Tính chân thực**

Tính chân thực đề cập đến khả năng người quan sát không phát hiện ra sự tồn tại của thủy vân, hoặc nói cách khác, thủy vân không gây ảnh hưởng đến chất lượng hình ảnh. Để thực sự giấu thông tin mà không thể cảm nhận được, cần phải nhúng thông tin vào các vùng ít quan trọng về mặt thị giác. Tuy nhiên, thông tin nhúng dễ dàng bị mất đi trong quá trình này.

Những nghiên cứu trước đây về thủy vân thường tập trung vào việc thiết kế thủy vân không thể thấy được, thường nhúng thủy vân vào các vùng tần số cao hoặc các bit ít quan trọng. Gần đây, các kỹ thuật khác như kỹ thuật trải phổ đã chèn giấu thủy vân không thể thấy được về thị giác vào các vùng tín hiệu quan trọng. Đặt thủy vân trong các vùng này cũng có thể cải thiện tính bền vững chống lại các xử lý tín hiệu.

**Tính bền vững**

Hình ảnh có thể trải qua nhiều biến đổi khác nhau như tăng độ tương phản, lọc thông, làm mờ và nhiều thay đổi khác. Do đó, thủy vân cần phải có tính bền vững để chịu được các biến đổi ảnh và cả biến đổi tín hiệu số thành tín hiệu tương tự và ngược lại. Hơn nữa, ảnh chứa thủy vân cần phải chịu được biến đổi hình học như di chuyển vị trí, co dãn kích thước và cắt xén.

Tính bền vững thực sự đạt được khi dấu thủy vân vẫn tồn tại trong dữ liệu sau khi trải qua các biến đổi và bộ phát hiện/trích xuất vẫn có thể phát hiện thủy vân. Thủy vân có thể được nhúng vào hình ảnh bằng cách thay đổi các giá trị điểm ảnh hoặc các bit ít quan trọng nhất (LSB). Tuy nhiên, tính bền vững cao hơn nếu thủy vân được nhúng vào miền biến đổi của hình ảnh bằng cách thay đổi các hệ số.

**Tính dễ hỏng**

Tính dễ hỏng đối nghịch hoàn toàn với tính bền vững của thủy vân. Thuộc tính này thường được áp dụng trong lược đồ thủy vân dễ vỡ. Trong lược đồ này, yêu cầu là thủy vân bị phá hủy bởi bất kỳ phương pháp sao chép nào, trừ khi được thực hiện bằng các phương pháp sao chép hợp pháp. Ví dụ, thủy vân đặt trong một văn bản hợp pháp tồn tại qua bất kỳ sao chép nào mà không thay đổi nội dung nhưng sẽ bị phá hủy nếu một số 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 bit một cách chính xác nhưng không thể phân biệt các mức biến đổi có thể chấp nhận được.

**Đa thủy vân và độ phức tạp tính toán**

Một kẻ tấn công có thể tiếp tục nhúng thủy vân vào một đối tượng đã chứa thủy vân và sau đó tuyên bố sản phẩm là của họ. Một giải pháp đơn giản trong tình huống này là đánh dấu thời gian cho thông tin thủy vân hoặc nhúng nhiều thủy vân khác nhau cho các người dùng khác nhau. Sử dụng nhiều thủy vân cho phép theo dõi theo nội dung thủy vân nhưng cũng tạo điều kiện cho việc tấn công bằng cách loại bỏ thông tin thông qua trung bình xác suất (tấn công đồng thời).

Độ phức tạp tính toán của lược đồ thủy vân cũng rất quan trọng, tương tự như bất kỳ công nghệ nào sử dụng trong thương mại. Điều này đặc biệt quan trọng khi làm việc với dữ liệu thời gian thực. Hơn nữa, cần xem xét tính linh hoạt của độ phức tạp tính toán. Người thiết kế lược đồ thủy vân luôn hy vọng có một thiết kế có thể linh hoạt theo từng thế hệ. Ví dụ, lược đồ thủy vân thế hệ đầu tiên có độ phức tạp tính toán thấp nhưng độ tin cậy thấp so với lược đồ thủy vân thế hệ tiếp theo. Khi giải quyết vấn đề tính toán lớn, lược đồ thủy vân thế hệ sau có thể hoạt động tốt hơn.

Việc hiểu rõ và cân nhắc kỹ các yếu tố này là vô cùng quan trọng để tạo ra các giải pháp thủy vân hiệu quả và bền vững trong thực tế.

### 1.1.5. Các tiêu chí đánh giá thủy vân số và độ đo tương ứng

Khi thực hiện thủy vân ảnh số, cần phải áp dụng một loạt tiêu chí [15, 16, 17, 19] để đánh giá chất lượng của thuật toán. Thông thường, người ta dựa vào những tính chất sau đây:

**Tính bí mật:** Trong quá trình thủy vân, ảnh sẽ trải qua biến đổi do việc

nhúng thủy vân vào. Tính "vô hình" thể hiện mức độ biến đổi trên ảnh. Một lược đồ thủy vân hiệu quả sẽ làm cho thủy vân trở nên "vô hình" trên ảnh, làm cho việc nhận ra khó khăn và bảo vệ tính bí mật của thủy vân. Tuy nhiên, trong thực tế, không cần phải luôn đạt độ vô hình tối đa. Ví dụ, trong trường hợp thủy vân được sử dụng làm biểu tượng xác thực nguồn gốc sản phẩm, việc tiết lộ có thể cần thiết để giữ cho mọi người được thông báo.

**Tính toàn vẹn:** Khả năng chống giả mạo đối với thủy vân là yêu cầu cực kỳ quan trọng vì chỉ khi có khả năng này thì bản quyền mới được bảo vệ và sản phẩm được thừa nhận pháp lý. Để chống lại giả mạo, bất kỳ thay đổi nào về nội dung của ảnh số sẽ làm hủy thủy vân. Do đó, làm giả các ảnh số có chứa thủy vân trở nên rất khó.

**Tính bền vững:** Tiêu chí thứ ba là thủy vân cần phải có tính bền vững. Thủy vân cần phải tồn tại mạnh mẽ trước cả các tấn công có chủ đích và không có chủ đích. Tấn công không có chủ đích đối với ảnh số bao gồm việc nén, lấy mẫu, lọc và các biến đổi tương tự. Tấn công có chủ đích có thể liên quan đến việc xóa, thay đổi hoặc làm nhiễu thủy vân trong ảnh. Để đạt được điều này, thủy vân phải được ẩn trong các vùng quan trọng đối với thị giác. Phương pháp thủy vân cần đảm bảo rằng không thể khôi phục lại thủy vân tương đương mà ảnh đã bị biến đổi quá nhiều và không làm mất giá trị thương mại.

**Dung lượng:** Trong việc đánh giá thủy vân số, đây là một tiêu chí quan trọng đo lường khả năng lưu trữ và quản lý dữ liệu thủy vân số. Dung lượng xác định khối lượng dữ liệu mà hệ thống thủy vân số có thể chứa, bao gồm cả việc quản lý, tổ chức và bảo quản dữ liệu. Điều này đảm bảo khả năng lưu trữ và sử dụng dữ liệu một cách hiệu quả để phục vụ các mục tiêu và ứng dụng cụ thể, đồng thời cũng quan trọng trong việc dự đoán khả năng mở rộng và bảo mật dữ liệu thủy vân số.

Trong thực tế, luôn phải cân nhắc cân bằng giữa chất lượng (tính bí mật, tính toàn vẹn, tính bền vững) và dung lượng thủy vân để tạo ra các giải pháp hợp lý và hiệu quả.

Bảng 1.1 dưới đây giới thiệu một số độ đo thường dùng trong việc đánh giá hiệu quả của các phương pháp thủy vân số. Mỗi độ đo cung cấp một góc nhìn khác nhau về hiệu quả của thủy vân, từ việc đánh giá chất lượng hình ảnh sau khi nhúng thủy vân đến khả năng chống chịu trước các tấn công và khả năng khôi phục thông tin thủy vân.

***Bảng 1.1:*** *Một số độ đo phổ biến trong thủy vân*

| **Độ đo** | **Mô tả** | **Ưu điểm** | **Nhược điểm** | **Đánh giá tiêu chí** |
|---|---|---|---|---|
| MSE (Mean Squared Error) | MSE được sử dụng để đánh giá sự thay đổi chất lượng hình ảnh sau khi nhúng thủy vân vào ảnh gốc.MSE đo lường trung bình bình phương các sai số giữa các pixel của ảnh gốc và ảnh đã nhúng thủy vân. | 1. Đơn giản và dễ tính toán: MSE là một trong những độ đo dễ hiểu và dễ tính toán nhất, phù hợp với nhiều loại dữ liệu.<br>2. Phổ biến: MSE là độ đo phổ biến trong nhiều lĩnh vực, từ học máy đến xử lý tín hiệu và thủy vân số. | 1. Không phản ánh trực quan sự khác biệt: MSE chỉ đưa ra một giá trị tổng thể về sự khác biệt nhưng không cung cấp thông tin chi tiết về vùng nào của ảnh bị biến dạng.<br>2. Nhạy cảm với giá trị ngoại lệ: MSE có thể bị ảnh hương lớn bởi các giá trị ngoại lệ, gây ra sự biến dạng lớn ở một vài pixel. | Tính bí mật |
| RMSE (Root Mean Squared Error) | rMSE được sử dụng đế đánh giá mức độ biến đổi của ảnh sau khi nhúng thủy vân so với ảnh gốc, qua đó đánh giá mức độ bí mật của thủy vân. | 1. Dễ hiểu và dễ tính toán: Công thức tính rMSE đơn giản và trực quan, giúp người sử dụng dễ dàng hiểu và tính toán.<br>2. Độ nhạy cao đối với sai số lớn: rMSE đặc biệt nhạy cảm với các sai số lớn do bình phương sai số, giúp phát hiện các biến đổi lớn giữa ảnh gốc và ảnh đã nhúng thủy vân. | 1. Không phản ánh rõ ràng tính bí mật: rMSE đo lường mức độ biến đổi tổng quát nhưng không phản ánh rõ ràng tính bí mật của thủy vân theo cảm nhận của mắt người. Một ảnh có rMSE thấp vẫn có thể có các biến đổi dễ nhận thấy bằng mắt thường. | Tính bí mật |

| | | | | |
|---|---|---|---|---|
| | | 3. Phản ánh chính xác mức độ khác biệt tổng quát: rMSE cung cấp một thước đo chính xác về mức độ khác biệt tổng quát giữa ảnh gốc và ảnh đã nhúng thủy vân, giúp đánh giá chất lượng ảnh sau khi nhúng thủy vân.<br>4. So sánh dễ dàng giữa các thuật toán: Giá trị rMSE có thể được sử dụng đề so sánh hiệu quả của các thuật toán thủy vân khác nhau, từ đó chọn ra thuật toán tối ưu nhất. | 2. Không đánh giá được khả năng chống tấn công: rMSE không cung cấp thông tin về khả năng chống lại các tấn công (như nén, cắt xén, hay thêm nhiễu) của thủy vân. Một thủy vân có rMSE thấp có thể không bền vững trước các loại tấn công này.<br>3. Nhạy cảm với dữ liệu ngoại lệ: Do tính chất bình phương sai số, rMSE rất nhạy cảm với các điểm dữ liệu ngoại lệ (outliers). Các điểm ảnh có sai số lớn sẽ ảnh hưởng mạnh đến giá trị rMSE, làm méo mó kết quả đánh giá.<br>4. Không thể hiện phân bố sai số: rMSE chỉ cung cấp một giá trị tổng quát về sai số trung bình, không cung cấp thông tin về phân bố sai số trong toàn bộ ảnh. Điều này có thể dẫn đến việc bỏ qua các vùng cụ thể trong ảnh có sự thay đổi lớn. | |

| | | | | |
|---|---|---|---|---|
| Precision | Precision được sử dụng để đánh giá khả năng của một thuật toán trong việc chính xác nhận diện các pixel hoặc vùng ảnh có chứa thủy vân. | 1. Độ chính xác cao trong phát hiện thủy vân: Precision cao nghĩa là thuật toán ít dự đoán sai, đảm bảo rằng phần lớn các điểm ảnh được nhận diện là có thủy vân thực sự chứa thủy vân.<br>2. Giảm thiểu kết quả sai lầm (False Positives): Precision giúp giảm số lượng các kết quả sai lầm, nghĩa là giảm thiểu việc nhận diện nhầm các vùng không chứa thủy vân thành có thủy vân, điều này rất quan trọng trong các ứng dụng yêu cầu độ chính xác cao.<br>3. Hiệu quả trong các ứng dụng nhạy cảm: Trong các ứng dụng mà việc nhận diện sai có thể gây ra hậu quả nghiêm trọng, như xác thực tài liệu pháp lý hay hình ảnh y tế, precision là một chỉ số quan trọng để đánh giá hiệu quả của thuật toán. | 1. Không phản ánh đầy đủ hiệu suất tổng thể: Precision không xem xét số lượng các điểm ảnh hoặc vùng ảnh thực sự có thủy vân nhưng không được nhận diện (False Negatives). Do đó, precision có thể không phản ánh đầy đủ hiệu suất tổng thể của thuật toán.<br>2. Cần kết hợp với Recall để có cái nhìn toàn diện: Precision cần được kết hợp với recall (độ nhạy) để đánh giá hiệu suất tổng thể của thuật toán. Recall đo lường khả năng nhận diện chính xác tất cả các điểm ảnh hoặc vùng ảnh có thủy vân, trong khi precision đo lường độ chính xác trong các dự đoán của thuật toán.<br>3. Không phù hợp khi số lượng điểm ảnh có thủy vân ít: Trong các trường hợp mà số lượng điểm ảnh có thủy vân rất ít so với tổng số điểm ảnh, precision có thể trở nên ít ý nghĩa vì số lượng False Positives có thể bị che khuất bởi số lượng lớn True Negatives. | Tính toàn vẹn, tính bền vững |

| | | | | |
|---|---|---|---|---|
| Recall | Recall đo lường khả năng của hệ thống trong việc phát hiện đúng các bit thủy vân đã nhúng vào ảnh sau khi ảnh đã trải qua các biến đổi hoặc tấn công. | 1. Đánh giá khả năng phục hồi thông tin: Recall cung cấp thông tin về khả năng phục hồi lại các bit thủy vân đã nhúng, giúp đánh giá mức độ bảo vệ thông tin của thuật toán thủy vân.<br>2. Chỉ số quan trọng trong môi trường có nhiều tấn công: Recall đặc biệt hữu ích trong các bối cảnh mà ảnh chứa thủy vân có thể bị biến đổi hoặc tấn công, vì nó phản ánh khả năng của hệ thống trong việc duy trì và phát hiện thông tin thủy vân.<br>3. Đơn giản và dễ hiểu: Công thức tính Recall đơn giản và dễ hiểu, giúp người dùng dễ dàng áp dụng và đánh giá | 1. Không phản ánh độ chính xác toàn diện: Recall chỉ tập trung vào khả năng phát hiện các bit thủy vân đã nhúng, không phản ánh tỷ lệ phát hiện nhầm (false positives). Do đó, một hệ thống có Recall cao nhưng cũng có nhiều phát hiện nhầm vẫn có thể không hiệu quả.<br>2. Không đánh giá được tính bí mật: Recall không cung cấp thông tin về mức độ bí mật của thủy vân. Một hệ thống có Recall cao có thể vẫn làm ảnh hưởng đến chất lượng thị giác của ảnh gốc<br>3. Không cung cấp thông tin về phân phối lỗi: Recall không cung cấp thông tin về phân phối các bit thủy vân bị mất hoặc không phát hiện được trong toàn bộ ảnh, do đó không thể đánh giá được các vùng cụ thể trong ảnh bị ảnh hưởng nhiều. | Tính toàn vẹn |

| | | | | |
|---|---|---|---|---|
| F-measure | F-measure là sự kết hợp hài hòa giữa Precision và Recall nhằm cung cấp một thước đo duy nhất phản ánh hiệu suất của mô hình. | 1. Cân bằng giữa Precision và Recall: F-measure cung cấp một thước đo duy nhất kết hợp cả Precision và Recall, giúp đánh giá toàn diện hiệu suất của thuật toán phát hiện thủy vân. Đặc biệt hữu ích trong các bài toán mà cân cân bằng giữa việc giảm thiểu False Positives và False Negatives.<br>2. Đơn giản và trực quan: Công thức tính toán F-measure đơn giản và dễ hiểu, giúp người dùng dễ dàng áp dụng và giải thích kết quả.<br>3. Phù hợp với các bài toán mất cân bằng dữ liệu: F-measure có thể được sử dụng hiệu quả trong các bài toán có phân phối lớp không đều, nơi mà một lớp có số lượng mẫu lớn hơn nhiều so với lớp khác. | 1. Không phản ánh được độ phức tạp của mô hình: F-measure chỉ cung cấp một cái nhìn tổng quát về hiệu suất của mô hình mà không phản ánh được độ phức tạp hoặc khả năng chống lại các tấn công khác nhau của thuật toán thủy vân.<br>2. Không xem xét độ quan trọng của các lỗi: F-measure coi trọng các lỗi False Positive và False Negative như nhau, trong khi trong một số trường hợp, một loại lỗi có thể quan trọng hơn loại khác.<br>3. Không cung cấp thông tin về phân bố lỗi: F-measure chỉ cung cấp một giá trị duy nhất mà không cung cấp thông tin chi tiết về phân bố của các lỗi trong dữ liệu.<br>4. Không đánh giá chất lượng hình ảnh: F-measure không phản ánh mức độ thay đổi của chất lượng hình ảnh sau khi nhúng thủy vân, điều này rất quan trọng trong các ứng dụng thủy vân số. | Tính toàn vẹn, tính bền vững |

| | | | | |
|---|---|---|---|---|
| JW Distance | JW Distance có thể được sử dụng để đánh giá sự tương đồng giữa các chuỗi nhúng thủy vân và chuỗi gốc. | 1. Nhạy cảm với tiền tố: JW Distance nhạy cảm với các tiền tố phù hợp, điều này có nghĩa là nó ưu tiên các chuỗi có các ký tự phù hợp ở đầu chuỗi. Điều này có thể hữuu ích trong nhiều ứng dụng cụ thể.<br>2. Tính toán sự tương đồng linh hoạt: JW Distance cung cấp một phép đo linh hoạt về sự tương đồng giữa hai chuỗi ký tự, cho phép điều chỉnh để phản ánh tốt hơn các đặc điểm cụ thể của dữ liệu.<br>3. Khả năng phân biệt tốt: Trong nhiều trường hợp, JW Distance có khả năng phân biệt tốt hơn so với các phương pháp đo lường tương đồng khác, đặc biệt là khi các chuỗi có các ký tự phù hợp ở đầu chuỗi. | 1. Không phù hợp cho dữ liệu không có cấu trúc chuỗi: JW Distance chủ yếu được thiết kế cho các chuỗi ký tự. Do đó, nó không phù hợp để so sánh các dạng dữ liệu không có cấu trúc chuỗi, chẳng hạn như hình ảnh hoặc tín hiệu âm thanh.<br>2. Độ phức tạp tính toán cao: Việc tính toán JW Distance có thể đòi hỏi nhiều tài nguyên tính toán, đặc biệt khi so sánh các chuỗi dài hoặc trong các ứng dụng yêu cầu xử lý thời gian thực. | Tính toàn vẹn |

| | | | | |
|---|---|---|---|---|
| | | 4. Ứng dụng rộng rãi: JW Distance đã được chứng minh là hiệu quả trong nhiều ứng dụng khác nhau, từ xử lý ngôn ngữ tự nhiên đến nhận dạng chuỗi ký tự trong thủy vân số. | 3. Nhạy cảm với sai sót ở cuối chuỗi: JW Distance ưu tiên các ký tự phù hợp ở đầu chuỗi, nhưng có thể ít nhạy cảm hơn với các sai sót ở cuối chuỗi. Điều này có thể dẫn đến các kết quả không mong muốn trong một số trường hợp cụ thể. 4. Không phản ánh sự khác biệt tổng thể: JW Distance chủ yếu tập trung vào các ký tự phù hợp và hoán đổi, không phản ánh đầy đủ sự khác biệt tổng thể giữa hai chuỗi ký tự khi có nhiều sai khác nhỏ trải rộng trên toàn bộ chuỗi. | |
| SAD (Sum of Absolute Differences) | SAD được sử dụng đế đánh giá mức độ thay đổi giữa ảnh gốc và ảnh đã được nhúng thủy vân. | 1. Dễ hiểu và dễ tính toán: Công thức tính SAD đơn giản và trực quan, giúp người sử dụng dễ dàng hiểu và tính toán. | 1. Không phản ánh rõ ràng tính bí mật: SAD đo lường mức độ biến đổi tổng quát nhưng không phản ánh rõ ràng tính bí mật của thủy vân theo cảm nhận của mắt người. | Tính bí mật, tính bền vững |

| | | | | |
|---|---|---|---|---|
| | | 2. Không bị ảnh hưởng bởi ngoại lệ: Do chỉ sử dụng giá trị tuyệt đối, SAD không bị ảnh hưởng nhiều bởi các điểm dữ liệu ngoại lệ (outliers) như rMSE.<br>3. Phản ánh sự khác biệt tổng quát: SAD cung cấp một thước đo tổng quát về sự khác biệt giữa hai hình ảnh, giúp đánh giá mức độ biến đổi tổng quát.<br>4. Hiệu quả trong tính toán thời gian thực: Vì tính toán đơn giản, SAD thường được sử dụng trong các ứng dụng yêu cầu tính toán nhanh chóng và thời gian thực. | 2. Không đánh giá được khả năng chống tấn công: SAD không cung cấp thông tin về khả năng chống lại các tấn công (như nén, căt xén, hay thêm nhiễu) của thủy vân.<br>3. Không nhạy cảm với sai số lớn: SAD không nhạy cảm với các sai số lớn như rMSE, do đó có thể không phản ánh chính xác các biến đối lớn giữa hai hình ảnh.<br>4. Không thể hiện phân bố sai số: Tương tự như rMSE, SAD chỉ cung cấp một giá trị tổng quát về sai số, không cung cấp thông tin về phân bố sai số trong toàn bộ ảnh. | |
| PSNR (Peak Signal-to-Noise Ratio) | PSNR được sử dụng để đánh giá mức độ khác biệt giữa ảnh gốc và ảnh đã nhúng thủy vân, qua đó đánh giá mức độ bí mật của thủy vân. | 1. Dễ hiểu và dễ tính toán: Công thức tính PSNR đơn giản và dễ hiểu, giúp người sử dụng dễ dàng áp dụng trong các bài toán thực tế. | 1. Không phản ánh rõ ràng tính bí mật: PSNR đo lường mức độ khác biệt tổng quát nhưng không phản ánh rõ ràng tính bí mật của thủy vân theo cảm nhận của mắt người. Một ảnh có PSNR cao vẫn có thể có các biến đổi dễ nhận thấy bằng mắt thường. | Tính bí mật |

| | | | | |
|---|---|---|---|---|
| | | 2. Đánh giá chất lượng ảnh tốt: PSNR cung cấp một thước đo rõ ràng về mức độ khác biệt giữa ảnh gốc và ảnh đã nhúng thủy vân, cho phép đánh giá chất lượng của ảnh sau khi nhúng thủy vân.<br>3. Tiêu chuẩn phổ biến: PSNR là một tiêu chuẩn phổ biến trong lĩnh vực xử lý ảnh và video, cho phép so sánh dễ dàng giữa các nghiên cứu và các thuật toán khác nhau.<br>4. Nhạy cảm với sai số lớn: Tương tự như rMSE, PSNR cũng nhạy cảm với các sai số lớn, giúp phát hiện các biến đổi lớn giữa ảnh gốc vả ảnh đã nhúng thủy vân. | 2. Không đánh giá được khả năng chống tấn công: PSNR không cung cấp thông tin về khả năng chống lại các tấn công (như nén, cắt xén, hay thêm nhiễu) của thủy vân. Một thủy vân có PSNR cao có thể không bền vững trước các loại tấn công này.<br>3. Nhạy cảm với dữ liệu ngoại lệ: PSNR cũng nhạy cảm với các điểm dữ liệu ngoại lệ (outliers). Các điểm ảnh có sai số lớn sẽ ảnh hưởng mạnh đến giá trị PSNR, làm méo mó kết quả đánh giá.<br>4. Không thể hiện phân bố sai số: PSNR chỉ cung cấp một giá trị tổng quát về sai số trung bình, không cung cấp thông tin về phân bố sai số trong toàn bộ ảnh. Điều này có thể dẫn đến việc bỏ qua các vùng cụ thể trong ảnh có sự thay đổi lớn. | |

| | | | | |
|---|---|---|---|---|
| SSIM (Structur al Similarity Index Measure) | SSIM (Structural Similarity Index Measure) là một chỉ số đánh giá chất lượng hình ảnh được thiết kế để cải thiện độ đo truyền thống như MSE (Mean Squared Error) hoặc PSNR (Peak Signal-to-Noise Ratio) | 1. Phản ánh tốt hơn cảm nhận của mắt người: SSIM mô phỏng cách mắt người nhìn nhận hình ảnh, giúp phản ánh chính xác hơn sự thay đổi về chất lượng hình ảnh so với các độ đo truyền thống như MSE hay PSNR.<br>2. Đánh giá toàn diện: SSIM đánh giá sự tương đồng dựa trên ba yếu tố: độ sáng, độ tương phản và cấu trúc, cung cấp cái nhìn toàn diện hơn về chất lượng hình ảnh.<br>3. Nhạy cảm với biến đổi cấu trúc: SSIM nhạy cảm với các thay đổi về cấu trúc trong hình ảnh, điều mà mắt người cũng nhạy cảm. Điều này làm cho SSIM trở thành công cụ hữu ích trong việc đánh giá các biến đổi gây ra bởi thủy vân.<br>4. Kết quả dễ hiểu: Giá trị SSIM nằm trong khoảng từ -1 đến 1, với giá trị 1 biểu thị hai hình ảnh là hoàn toàn giống nhau, giúp dễ dàng hiểu và diễn giải kết quả. | 1. Tính toán phức tạp hơn: So với các độ đo như MSE hay PSNR, việc tính toán SSIM phức tạp hơn và yêu cầu nhiều tài nguyên tính toán hơn.<br>2. Nhạy cảm với thay đổi nhỏ trong hình ảnh: SSIM có thể nhạy cảm với các biến đổi nhỏ hoặc các điểm nhiễu, dẫn đến việc đánh giá chất lượng bị ảnh hưởng bởi các chi tiết không quan trọng.<br>3. Không tối ưu cho các ứng dụng cụ thể: SSIM được thiết kế để đánh giá tổng thể sự tương đồng giữa hai hình ảnh, nhưng trong một số ứng dụng cụ thể, các yếu tố khác có thể quan trọng hơn mà SSIM không đánh giá được. | Tính bí mật, tính toàn vẹn, tính bền vững |

| | | | | |
|---|---|---|---|---|
| | | | 4. Không đánh giá được tính bí mật của thủy vân: Mặc dù SSIM tốt hơn MSE và PSNR trong việc phản ánh sự thay đổi theo cách mắt người nhận thức, nhưng nó vẫn không đảm bảo đánh giá được tính bí mật của thủy vân theo cách toàn diện. | |
| NC (Normalized Correlation) | NC là một chỉ số được sử dụng trong thủy vân số để đánh giá mức độ tương quan giữa thủy vân nhúng và thủy vân trích xuất. NC đo lường sự tương đồng giữa hai tín hiệu, giúp xác định xem thủy vân có được trích xuất chính xác hay không. | 1. Đo lường trực tiếp mức độ tương đồng: NC trực tiếp đánh giá mức độ tương đồng giữa thủy vân gốc và thủy vân trích xuất, giúp xác định hiệu quả của quá trình nhúng và trích xuất thủy vân.<br>2. Dễ tính toán và hiểu: Công thức tính NC đơn giản và dễ hiểu, giúp người sử dụng dễ dàng tính toán và diễn giải kết quả.<br>3. Nhạy cảm với sai lệch nhỏ: NC có thể phát hiện các sai lệch nhỏ giữa thủy vân gốc và thủy vân trích xuất, giúp đánh giá chi tiết tính chính xác của quá trình trích xuất thủy vân. | 1. Không phản ánh tính bí mật: NC chỉ đánh giá mức độ tương đồng giữa hai thủy vân, không phản ánh trực tiếp tính bí mật của thủy vân trong ảnh.<br>2. Không đánh giá được chất lượng ảnh sau nhúng thủy vân: NC không cung cấp thông tin về mức độ biến đổi của chất lượng ảnh sau khi nhúng thủy vân. Một thủy vân có NC cao không đảm bảo rằng chất lượng ảnh không bị suy giảm. | Tính toàn vẹn, tính bền vững |

| | | | | |
|---|---|---|---|---|
| Capacity | Capacity (dung lượng) đề cập đến lượng thông tin có thể được nhúng vào một phương tiện (ảnh, âm thanh, video) mà không làm giảm đáng kể chất lượng của phương tiện đó. Capacity được đo lường bằng số bit thông tin có thể nhúng vào mỗi đơn vị dữ liệu (chẳng hạn như mỗi điểm ảnh trong một bức ảnh). | 1. Đánh giá tính thực tế của thuật toán: Capacity cung cấp một thước đo rõ ràng về tính khả thi và hiệu quả của một thuật toán thủy vân trong việc nhúng thông tin vào phương tiện số.<br>2. Tối ưu hóa không gian nhúng: Giúp tối ưu hóa việc sử dụng không gian nhúng, đảm bảo rằng càng nhiều thông tin càng tốt được nhúng vào mà không gây ra sự suy giảm chất lượng đáng kể.<br>3. Linh hoạt trong ứng dụng: Dung lượng cao cho phép ứng dụng thủy vân trong các lĩnh vực yêu cầu nhúng nhiều thông tin, chẳng hạn như lưu trữ dữ liệu y tế hoặc truyền tải dữ liệu bảo mật. | 1. Giảm chất lượng phương tiện: Dung lượng cao có thể dẫn đến sự suy giảm chất lượng của phương tiện gốc nếu không được quản lý tốt, gây ra sự mất mát về thị giác hoặc âm thanh.<br>2. Độ phức tạp tính toán cao: Tăng dung lượng thường đi kèm với sự gia tăng độ phức tạp tính toán, yêu cầu thuật toán tinh vi hơn để đảm bảo thông tin được nhúng một cách hiệu quả mà không gây suy giảm chất lượng.<br>3. Khả năng chống tấn công thấp hơn: Nhúng quá nhiều thông tin có thể làm giảm khả năng chống tấn công của thủy vân. Một lượng lớn dữ liệu nhúng có thể dễ bị phát hiện và loại bỏ bởi các phương pháp tấn công khác nhau. | Dung lượng, tính bí mật, tính toàn vẹn, tính bền vững |

| | | | | |
|---|---|---|---|---|
| | | | 4. Sự cân bằng giữa dung lượng và bảo mật: Tăng dung lượng thường đi kèm với việc giảm mức độ bảo mật và tính bí mật của thủy vân. Cần phải tìm ra sự cân bằng tối ưu giữa dung lượng và các yếu tố này để đảm bảo hiệu quả tổng thể của thuật toán thủy vân. | |

### 1.1.6. Các ứng dụng của thủy vân số

#### *1.1.6.1. Bảo vệ quyền sở hữu ảnh số*

Mặc dù đã có nhiều biện pháp về bảo vệ quyền sở hữu [7] và đã có sự tiến bộ trong việc thực thi quyền tác giả nhưng thực tế vẫn còn những hạn chế. Các hành động vi phạm quyền tác giả vẫn diễn ra rộng rãi, tinh vi và không ngại công khai khiến cho chủ sở hữu thất vọng. Dữ liệu số như ảnh số với nhiều định dạng, vấn đề bảo vệ quyền tác giả trở nên phức tạp hơn.

Xuất phát từ quá trình mua bán và giao dịch các tác phẩm số này, những vấn đề cụ thể đã xuất hiện như sau:

+ Bảo đảm quyền tác giả: Để đảm bảo quyền sở hữu của chủ sở hữu ảnh số, ảnh đó cần phải chứa các thông tin đặc biệt để chứng minh quyền sở hữu của họ.

+ Cung cấp thông tin hợp pháp và ngăn chặn việc phân phối trái phép nội dung tác phẩm: Giao dịch mua bán, chia sẻ, phân phối tác phẩm số đòi hỏi việc đảm bảo thông tin sẵn sàng cho người dùng hợp pháp, đồng thời ngăn chặn việc phân phối trái phép nội dung.

+ Theo dõi thông tin để phát hiện người phân phối trái phép: Khi vi phạm quyền tác giả xảy ra hoặc chủ sở hữu nghi ngờ có bản sao sản phẩm không hợp lệ, cần theo dõi thông tin để phát hiện người phân phối trái phép. Đây là áp dụng cơ bản nhất của kỹ thuật thủy vân. Tuy nhiên, trong thực tế,

nhiều tác phẩm đã có quyền sở hữu nhưng vẫn bị sử dụng sai mục đích. Các thông báo về quyền sở hữu thường được đặt ở một vị trí nào đó trên sản phẩm phân phối.

Với khả năng tạo dấu, thủy vân không thể nhìn thấy hoặc tách rời được khỏi tác phẩm, việc này trở thành giải pháp tốt nhất để bảo vệ quyền sở hữu tác giả. Dấu thủy vân - chứa thông tin về quyền sở hữu tác giả, được nhúng vào sản phẩm và chỉ người sở hữu hợp pháp của sản phẩm mới có thể sử dụng nó, đồng thời nó là bằng chứng cho quyền sở hữu tác phẩm.

#### *1.1.6.2. Xác minh thông tin và phát hiện xuyên tạc thông tin*

Dấu thủy vân không chỉ đóng vai trò trong việc bảo vệ quyền sở hữu tác giả mà còn có thể ứng dụng trong việc xác minh thông tin và phát hiện sự xuyên tạc thông tin trong các tác phẩm số [17]. Việc nhúng dấu thủy vân vào tác phẩm cho phép tạo ra một dạng chữ ký số, giúp kiểm tra tính toàn vẹn của tác phẩm và ngăn chặn các hành động xuyên tạc thông tin.

Quá trình này thường bắt đầu bằng việc nhúng một dấu thủy vân vào tác phẩm và sau đó so sánh nó với dấu thủy vân ban đầu để kiểm tra sự thay đổi. Nếu có sự không tương thích, điều này có thể cho thấy tác phẩm gốc đã bị tấn công và thông tin đã bị xuyên tạc. Để đảm bảo tính hiệu quả và an toàn của dấu thủy vân, việc ẩn dấu thủy vân trở nên quan trọng để tránh sự tò mò của người khác và ngăn chặn việc làm giả dấu thủy vân một cách bất hợp pháp hoặc gian lận thông tin nguồn.

Trong thực tế, người dùng thường mong muốn có khả năng xác định vị trí bị xuyên tạc trong tác phẩm cũng như phát hiện bất kỳ sự thay đổi nào. Ví dụ, có thể phân biệt một đối tượng đa phương tiện chứa thông tin giấu bị thay đổi, xuyên tạc nội dung hoặc chỉ bị nén mất dữ liệu. Điều quan trọng trong các ứng dụng này là khả năng ẩn thông tin cao và đồng thời đảm bảo rằng dấu thủy vân không bền vững, nghĩa là khó có thể loại bỏ mà không làm mất đi tính toàn vẹn của tác phẩm.

#### *1.1.6.3. Xác thực người dùng*

Trong các ứng dụng cụ thể, dấu thủy vân không chỉ đơn thuần là một công cụ để bảo vệ quyền sở hữu tác giả mà còn trở thành một phương tiện quan trọng trong việc nhận dạng người gửi hoặc người nhận thông tin [15]. Điều này

thường được thực hiện bằng cách nhúng các dấu thủy vân khác nhau vào các bản sao khác nhau của thông tin gốc trước khi chúng được chuyển giao đến nhiều người khác nhau.

Ví dụ, nếu có nhu cầu chia sẻ thông tin với nhiều đối tượng khác nhau, mỗi đối tượng có thể nhận được một bản sao của thông tin với một dấu thủy vân duy nhất. Điều này giúp xác định người gửi cụ thể hoặc đối tượng nhận thông tin. Trong tình huống này, mức độ bảo mật và an toàn của dấu thủy vân trở nên quan trọng để đảm bảo rằng người nhận không thể xóa hoặc thay đổi dấu vết một cách không hợp pháp trong quá trình phân phối thông tin.

Đối với ứng dụng như vậy, yêu cầu cơ bản là phải đảm bảo tính an toàn cao cho dấu thủy vân. Cần có các biện pháp bảo mật mạnh mẽ để ngăn chặn bất kỳ sự thay đổi hay loại bỏ nào từ phía người nhận thông tin, đồng thời giữ cho tính xác định của dấu thủy vân không bị mất đi trong quá trình truyền tải và chia sẻ thông tin. Điều này đặt ra một thách thức cao về mặt kỹ thuật và an ninh thông tin trong việc phát triển và triển khai các hệ thống thủy vân trong các ứng dụng có tính chất như mô tả trên.

#### *1.1.6.4. Điều khiển truy cập*

Trong hệ thống quản lý thông tin, việc kiểm soát truy cập là một khía cạnh quan trọng để đảm bảo tính toàn vẹn và an toàn của dữ liệu. Một trong những cách tiếp cận để thực hiện điều khiển truy cập hiệu quả là sử dụng các thiết bị phát hiện dấu thủy vân [16] tích hợp trực tiếp vào hệ thống đọc và ghi. Trong trường hợp này, chúng ta áp dụng phương pháp phát hiện dấu thủy vân mà không cần thông tin gốc, nghĩa là quá trình xác nhận dấu thủy vân được thực hiện mà không yêu cầu sự so sánh với dữ liệu nguồn.

Cụ thể, các thiết bị phát hiện dấu thủy vân tích hợp vào hệ thống có khả năng xác định sự hiện diện hoặc vắng mặt của dấu thủy vân trong tập tin hoặc thông tin đang được truy cập. Điều này có thể thực hiện thông qua quá trình phân tích và so sánh các đặc điểm dấu thủy vân đã nhúng mà không cần truy cập đến thông tin nguồn. Khi dấu thủy vân được xác định, hệ thống sẽ thực hiện quyết định về việc cho phép hoặc từ chối truy cập tới tài nguyên hoặc thông tin tương ứng.

Điều này mang lại lợi ích lớn về mặt bảo mật, vì quá trình kiểm soát truy cập dựa trên tính nhất quán của dấu thủy vân mà không cần phải lưu trữ thông

tin gốc. Đồng thời, việc tích hợp các thiết bị phát hiện dấu thủy vân vào hệ thống đọc và ghi giúp tăng cường hiệu suất và giảm độ trễ trong quá trình xác nhận truy cập, tạo ra một hệ thống quản lý thông tin an toàn và hiệu quả.

### 1.1.7. Những tình huống tấn công thủy vân số thường gặp

Trong môi trường ngày nay, khi sự quan trọng của bảo vệ thông tin và dữ liệu cá nhân ngày càng được nhấn mạnh, các phương pháp thủy vân số đang trở thành một công cụ quan trọng trong lĩnh vực bảo mật thông tin. Tuy nhiên, như mọi công nghệ khác, các hệ thống thủy vân số cũng đối mặt với những thách thức và rủi ro đáng kể từ các tình huống tấn công [20] ngày càng tinh vi và phức tạp.

Chính vì vậy, trong phần giới thiệu nội dung này, luận án sẽ giới thiệu về những tình huống tấn công thủy vân số thường gặp, cách mà các kẻ tấn công không ngừng thay đổi và áp dụng các chiến lược đa dạng để xâm phạm tính toàn vẹn và bảo mật của dữ liệu được nhúng dấu thủy vân.

Luận án sẽ khám phá các kịch bản tấn công giả mạo thủy vân, nơi mà sự thay đổi hay chèn thêm thông tin giả mạo có thể đe dọa tính xác định và đáng tin cậy của dấu thủy vân. Đồng thời, luận án sẽ xem xét các tình huống liên quan đến việc loại bỏ hay thay đổi dấu thủy vân cũng như những kỹ thuật tấn công khác như tận dụng lỗ hổng bảo mật hay gỡ bỏ dấu thủy vân một cách tinh tế.

Những thách thức này không chỉ đặt ra những yêu cầu cao về mặt kỹ thuật mà còn đòi hỏi sự đổi mới liên tục trong lĩnh vực bảo mật để ngăn chặn và phòng tránh những tình huống tấn công này. Hãy cùng bắt đầu quá trình nghiên cứu về những thách thức của các tình huống tấn công thủy vân số thường gặp.

**Tấn công đơn giản:** Tấn công đơn giản là hình thức tấn công tối giản nhất nhằm vào việc khiến thủy vân đã được nhúng vào dữ liệu bị hủy hoại mà không cần xác định thủy vân cụ thể để trích xuất. Điều này có thể dẫn đến việc mất mát dữ liệu quan trọng mà không thể khôi phục.

Một ví dụ cụ thể về tấn công đơn giản có thể được minh họa trong bối cảnh sử dụng thủy vân số để bảo vệ quyền tác giả trên hình ảnh trực tuyến. Giả sử Alice là một nhiếp ảnh gia chia sẻ những tác phẩm nghệ thuật của mình trên mạng. Để đảm bảo quyền sở hữu và nguồn gốc của tác phẩm, Alice quyết định nhúng thủy vân số vào từng bức ảnh trước khi đăng tải.

Một kẻ tấn công là Bob muốn gây hại cho danh tiếng của Alice hoặc muốn lợi dụng tác phẩm một cách trái phép. Thay vì cố gắng phá vỡ dấu thủy vân một cách chính xác, Bob áp dụng một tuyến tấn công đơn giản. Bob có thể sử dụng các công cụ chỉnh sửa hình ảnh thông dụng để thay đổi một số pixel ngẫu nhiên trong bức ảnh mà không cần biết đến vị trí hay nội dung cụ thể của dấu thủy vân.

Mặc dù Bob không thể trích xuất thông tin chính xác từ dấu thủy vân, tuy nhiên việc thay đổi ngẫu nhiên này có thể gây hại nặng nề đến tính nhất quán và tin cậy của dấu thủy vân. Nếu bức ảnh đã bị biến đổi, dấu thủy vân sẽ không còn đúng với thông tin gốc khiến cho mục đích bảo vệ quyền tác giả của Alice bị đe dọa và dẫn đến việc mất mát dữ liệu không thể khôi phục được.

**Tấn công phát hiện:** Tấn công phát hiện nhằm vô hiệu hóa khả năng khôi phục thủy vân bằng cách phá vỡ mối quan hệ giữa dữ liệu và thủy vân. Thủy vân không thể được xác định bởi các hệ thống phát hiện khi chúng tạo ra các biến đổi hình dạng phức tạp, chẳng hạn như phóng to, thu nhỏ, xoay, cắt xén, xóa hoặc chèn thêm điểm ảnh kết hợp với các biến đổi hình học.

Giả sử một nhiếp ảnh gia chia sẻ bức ảnh nghệ thuật số độc đáo trên các nền tảng trực tuyến. Họ sử dụng thủy vân số để bảo vệ ảnh khỏi việc sao chép không phù hợp và để xác minh nguồn gốc.

Một kẻ tấn công có ý định sử dụng ảnh nghệ thuật này mà không cần phải mua bản quyền hoặc có sự cho phép của nhiếp ảnh gia. Họ áp dụng một loạt các biến đổi trực tiếp vào ảnh, bao gồm việc thay đổi màu sắc, độ tương phản và kích thước. Họ cũng xoay và làm mờ một số chi tiết quan trọng.

Khi người ta cố gắng phân tích ảnh để xác định thủy vân, sự phức tạp của biến đổi làm cho dấu thủy vân gốc trở nên khó nhận diện. Các hệ thống phát hiện sẽ gặp khó khăn trong việc xác định và khôi phục thủy vân, dẫn đến khả năng giả mạo và sử dụng trái phép ảnh nghệ thuật của nhiếp ảnh gia.

**Tấn công gây nhầm lẫn:** Loại tấn công này nhằm tạo ra sự nhầm lẫn bằng cách tạo ra dữ liệu gốc giả mạo hoặc dữ liệu đã chứa thủy vân giả mạo. Ví dụ, tấn công này có thể làm mất đi tính xác thực của thủy vân bằng cách nhúng thêm một số lượng thủy vân độc quyền mới, không thể phân biệt được với thủy vân gốc - thủy vân được sử dụng để xác thực.

Giả sử một nhiếp ảnh gia nổi tiếng tạo ra một bức ảnh độc đáo và quyết định chia sẻ nó trên các nền tảng trực tuyến. Họ sử dụng thủy vân số để bảo vệ ảnh khỏi việc bị sao chép và để xác minh nguồn gốc của tác phẩm.

Một kẻ tấn công có mục tiêu làm giả mạo tính xác thực của ảnh nghệ thuật để sử dụng nó một cách trái phép. Họ tạo ra một bản sao giả mạo của ảnh với thủy vân giả mạo được nhúng vào. Thủy vân giả mạo này được tạo ra để trông giống hệt như thủy vân gốc và không thể phân biệt được từ góc nhìn bình thường.

Khi người ta cố gắng xác định tính xác thực của ảnh, sự giống nhau giữa thủy vân gốc và thủy vân giả mạo tạo ra sự nhầm lẫn. Điều này có thể dẫn đến việc sử dụng trái phép ảnh giả mạo thay vì tác phẩm gốc của nhiếp ảnh gia.

**Tấn công loại bỏ:** Loại tấn công này nhằm vào việc phân tích dữ liệu để trích xuất thủy vân hoặc dữ liệu gốc. Kẻ tấn công cố gắng tách dữ liệu đã nhúng thủy vân ra khỏi dữ liệu gốc và thủy vân để truy cập thông tin quan trọng.

Giả sử một nhiếp ảnh gia nổi tiếng sử dụng thủy vân số để bảo vệ bản quyền của các tác phẩm nghệ thuật số độc quyền của mình trước khi chia sẻ chúng trên các nền tảng trực tuyến. Mỗi tác phẩm nghệ thuật số được nhúng một dấu thủy vân số để xác minh nguồn gốc và ngăn chặn sự sao chép không phù hợp.

Một kẻ tấn công muốn sử dụng tác phẩm nghệ thuật của nhiếp ảnh gia để bán lậu. Họ áp dụng các phương pháp phức tạp để phân tích và loại bỏ dấu thủy vân từ tác phẩm mà không làm suy giảm chất lượng hoặc sự độc đáo của chúng.

Bằng cách loại bỏ thủy vân, kẻ tấn công có thể tái sử dụng tác phẩm nghệ thuật một cách trái phép, đe dọa uy tín và giá trị thương hiệu của nhiếp ảnh gia, cũng như gây tổn thất về mặt tài chính khi người mua không nhận ra sự giả mạo.

Do đó, việc bảo đảm tính bền vững cho thủy vân số đòi hỏi sự hiểu biết sâu rộng về các loại tấn công này và triển khai biện pháp bảo mật hiệu quả để ngăn chặn và đối phó với chúng. Tính toàn vẹn và khả năng chống lại các cuộc tấn công thủy vân số ngày càng trở nên quan trọng để bảo vệ thông tin quan trọng và duy trì tính bền vững của hệ thống thủy vân số.

## 1.2. Tổng quan về các nghiên cứu liên quan và một số hạn chế còn tồn tại

### 1.2.1. Độ nổi bật trong ảnh

Chú ý thị giác [21] là một khái niệm quan trọng trong lĩnh vực tâm lý học nhận thức, thị giác học và khoa học máy tính, đặc biệt là trong lĩnh vực xử lý ảnh và thị giác máy tính. Khái niệm này mô tả khả năng của bộ não con người hoặc hệ thống máy tính để xác định và tập trung vào những phần quan trọng của một hình ảnh hoặc cảnh quan, bỏ qua những thông tin không cần thiết hoặc không liên quan. Chú ý thị giác giúp người xem lọc và ưu tiên thông tin thị giác, cho phép xử lý hiệu quả và nhanh chóng những tác vụ như nhận diện khuôn mặt, đọc và di chuyển trong môi trường.

Trong thực tế, chú ý thị giác [21] hoạt động như một bộ lọc thông minh, điều chỉnh liên tục dựa trên yếu tố ngữ cảnh và mục tiêu của cá nhân. Ví dụ, khi bạn đang tìm kiếm một người bạn trong đám đông, bộ não của bạn sẽ tự động bỏ qua nhiều thông tin không liên quan để tập trung vào những đặc điểm cụ thể có thể giúp bạn nhận diện người bạn đó.

Trong lĩnh vực máy tính, các thuật toán chú ý thị giác thường được sử dụng để cải thiện hiệu suất của các mô hình thị giác máy tính bằng cách mô phỏng cách mà con người tập trung vào các phần quan trọng của hình ảnh. Điều này không chỉ giúp tăng cường độ chính xác của các tác vụ như nhận dạng đối tượng và phân tích cảm xúc từ khuôn mặt mà còn giúp giảm bớt lượng dữ liệu cần xử lý, từ đó tăng hiệu quả tính toán.

Độ nổi bật thị giác [21] là một khái niệm trung tâm trong lĩnh vực thị giác máy tính, nhằm mô tả khả năng một đối tượng, một khu vực hoặc một đặc điểm cụ thể trong không gian thị giác thu hút sự chú ý tự nhiên và tức thì của quan sát viên. Điều này thường được xác định bởi những yếu tố như độ tương phản về màu sắc, kích thước, định hướng hoặc chuyển động so với môi trường xung quanh, tạo nên một "điểm nổi bật" giúp tách biệt đối tượng từ nền. Trong tâm lý học nhận thức, hiện tượng này giải thích cơ chế mà qua đó bộ não con người lọc và ưu tiên xử lý thông tin thị giác, nhưng trong khoa học máy tính, nó mang ý nghĩa thiết yếu trong việc phát triển các hệ thống thị giác máy tính và xử lý hình ảnh.

Khái niệm về độ nổi bật của hình ảnh đã được sáng tạo đầu tiên bởi Laurent Itti, Christof Koch và Ernst Niebur vào năm 1998 [22], cho phép ước

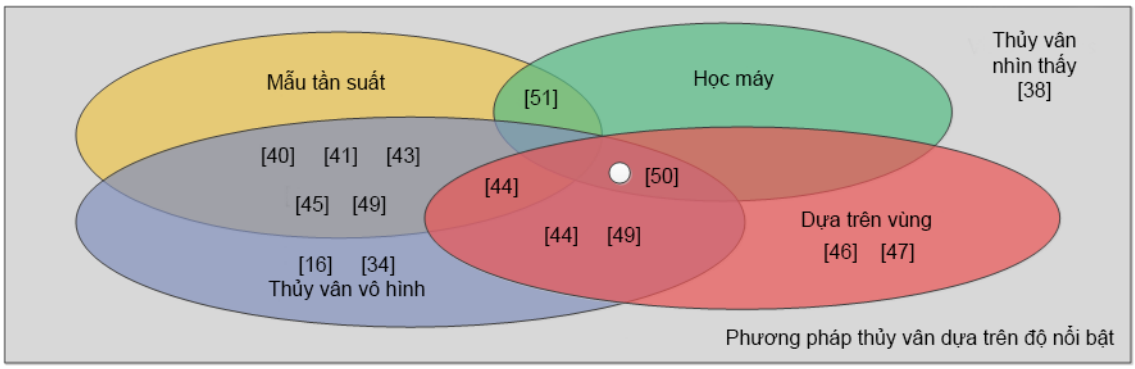
tính sự chú ý của người xem đối với hình ảnh. Trong quá trình nhúng thủy vân, khái niệm này được sử dụng để phân tích vị trí để mã hóa thông tin. Trong lúc nhúng một thủy vân nhìn thấy để thông báo về bản quyền, phương pháp của [23] trong hình 1.4 tìm kiếm vùng tập trung cho mỗi khung hình video với kỳ vọng rằng vùng này sẽ thu hút sự chú ý của người dùng nhất. Do đó, các vùng xa khỏi vùng tập trung được chọn để nhúng một thủy vân nhìn thấy nhằm tránh chồng lấn vùng tập trung nhưng vẫn hiển thị thông báo về bản quyền.

Sự nghiên cứu về độ nổi bật thị giác trong lĩnh vực thị giác máy tính tập trung vào việc mô phỏng và tái tạo cách thức mà con người xử lý thông tin thị giác, nhằm cải thiện khả năng của máy tính trong việc nhận biết và hiểu các cảnh quan hình ảnh phức tạp. Các thuật toán nhận diện độ nổi bật thị giác được thiết kế để tự động xác định các khu vực quan trọng trong hình ảnh, hỗ trợ cho một loạt các ứng dụng từ phân tích nội dung hình ảnh, cải thiện chất lượng hiển thị, đến tối ưu hóa giao diện người dùng và điều hướng robot.

Trong thủy vân số, việc lựa chọn khu vực nổi bật thị giác để nhúng thủy vân đòi hỏi sự cân nhắc tỉ mỉ; vùng ảnh có độ nổi bật cao có thể thu hút sự chú ý của người xem nhưng cũng làm tăng nguy cơ thủy vân bị phát hiện và gỡ bỏ bởi những người có ý định xâm phạm bản quyền. Do đó, cần phải tìm một sự cân bằng giữa việc nhúng thủy vân vào các vùng ít nổi bật để tránh sự chú ý không mong muốn, trong khi vẫn đảm bảo thủy vân có thể được phục hồi một cách chính xác khi cần thiết.

Các nghiên cứu về độ nổi bật thị giác trong thủy vân số thường tập trung vào việc phát triển các mô hình đánh giá độ nổi bật thị giác, từ đó giúp các thuật toán thủy vân tự động xác định các khu vực lý tưởng để nhúng thủy vân dựa trên các tiêu chí như độ phức tạp về mặt hình học, độ tương phản màu sắc và các đặc điểm cấu trúc của ảnh. Việc này không chỉ cải thiện độ bền và khả năng chống gỡ bỏ của thủy vân mà còn giúp thủy vân duy trì được tính không gây rối và không làm giảm chất lượng trải nghiệm hình ảnh cho người dùng.

Ngoài ra, trong kỹ thuật thủy vân dựa trên nội dung, việc áp dụng kiến thức về độ nổi bật thị giác còn giúp tối ưu hóa quá trình nhúng thủy vân theo nội dung cụ thể của ảnh, cho phép nhúng thủy vân một cách linh hoạt trong các vùng quan trọng mà không làm ảnh hưởng đến thông điệp hoặc giá trị thẩm mỹ của hình ảnh. Điều này làm tăng khả năng ứng dụng của thủy vân số trong các lĩnh vực đòi hỏi bảo vệ bản quyền cao như nghệ thuật kỹ thuật số, ảnh chụp chuyên nghiệp và tài liệu quảng cáo, mở ra một hướng đi mới cho việc bảo vệ




***Hình 1.4:*** *Bản đồ về các phương pháp thủy vân dựa trên độ nổi bật liên quan đến tính bí mật, mẫu tần số, khu vực hình ảnh và học máy*

sáng tạo nội dung trong kỷ nguyên số.

Ngược lại với dấu thủy vân có thể nhìn thấy, các vùng thích hợp thu được từ bản đồ độ nổi bật trong nguyên tắc sẽ được sử dụng cho việc nhúng thủy vân vô hình. Do đó, các vùng nổi bật và không nổi bật được dành cho việc nhúng thủy vân với độ thích hợp thấp và cao tương ứng [24]. Trong thực tế, ngoài sự khác biệt liên quan đến sự tương phản không gian, đặc điểm nổi bật cho việc nhúng thủy vân có thể tính tới sự thích nghi với độ sáng và JND (Just Noticeable Distortion) [25, 26]. JND là một khái niệm quan trọng liên quan đến ngưỡng nhận thức của con người. JND đề cập đến mức độ thay đổi nhỏ nhất trong tín hiệu (âm thanh, hình ảnh, video) mà con người có thể nhận ra. JND được sử dụng để đảm bảo rằng thủy vân được nhúng vào phương tiện số mà không thể bị phát hiện bởi người dùng bình thường nhưng vẫn có thể được phát hiện và truy xuất bởi các hệ thống tự động. Điều này đảm bảo rằng chất lượng của phương tiện không bị ảnh hưởng đáng kể sau khi thủy vân được thêm vào trong khi vẫn bảo vệ bản quyền và tính xác thực của nội dung. Một vùng có thể được lựa chọn từ đặc điểm nổi bật như vậy để nhúng thủy vân trong miền biến đổi cosine rời rạc (DCT).

Có một lượng lớn tài liệu về việc nhúng thủy vân dựa trên phân tích độ nổi bật bao gồm mẫu tần số [18, 27, 28] để tính toán các đặc điểm của hình ảnh tham chiếu hoặc hình ảnh gốc cũng như các giá trị nhúng liên quan đến các mẫu tần số. Ví dụ, một hình ảnh gốc được phân rã thành các dải con thông qua biến đổi sóng con trong một phương pháp tiếp cận hình ảnh nhận thức chất lượng để đạt được các đặc trưng [29, 30, 31] và bằng cách sử dụng các bit ít quan trọng nhất (the least significant bits - LSB) [32]. Khi một phiên bản biến dạng của hình ảnh như vậy thu được, các thông điệp ẩn có thể được giải mã và sử dụng

để đánh giá chất lượng của hình ảnh bị biến dạng bằng cách áp dụng phương pháp đánh giá chất lượng thấp hơn tham chiếu. Lưu ý rằng bản đồ biên của các vùng quan tâm (Regions of Interest - ROI) có thể xác định tiềm năng của vùng cho thủy vân dễ vỡ, sau đó được nhúng vào miền biến đổi sóng rời rạc [30].

Cụ thể, miền tần số được tạo ra từ ô tự duyệt (automata) 2D là các hệ thống động có không gian và thời gian rời rạc. Một bản đồ nổi bật của dải tần số thấp thấp nhất (LL band) của miền được giới thiệu cho việc nhúng thủy vân [29]. Biến đổi sóng rời rạc (the Discrete Wavelet Transform - DWT) được sử dụng để chia hình ảnh thành các tần số [31]. Vì vùng tần số thấp thích hợp cho việc ẩn thông tin, thủy vân được xây dựng bởi vùng này được nhúng vào miền không gian bằng cách thích nghi với các bit ít quan trọng nhất (the Least Significant Bits - LSB) [32]. Tương tự, sự kết hợp dựa trên độ nổi bật thị giác của JND và DCT có thể tạo ra một giải pháp thủy vân mạnh mẽ. Trong trường hợp nhúng thủy vân cho video, luận án ước lượng sự chú ý hình ảnh dựa trên sóng hình nén toàn cầu để nhúng thông tin phù hợp với sự chú ý hình ảnh [33]. Phương pháp này kết hợp cả đặc điểm không gian và thời gian để tạo ra đặc điểm nổi bật về không gian - thời gian dựa trên sự tương đồng cụ thể của các dải tần số thời gian chuyển động cao được tạo ra trong quá trình phân giải sóng không gian. Phương pháp này kết hợp cả gợi ý không gian và gợi ý thời gian để đạt được đặc điểm độ nổi bật thời không dựa trên sự tương đồng cụ thể của các dãy con thời gian băng thông cao được tạo ra trong phân rã sóng không gian.

Việc ẩn thông tin trong vùng hình ảnh là một giải pháp hiệu quả trong việc nhúng thủy vân, đặc biệt là liên quan đến sự có sẵn của các mô hình về độ nổi bật. Một bản đồ thủy vân cụ thể đã từng được trình bày bằng cách kết hợp độ nổi bật thấp và tính đa dạng - độ sáng để xác định những nơi tốt nhất để nhúng thủy vân [34]. Ở đây, các yếu tố tần số trung bình DCT của những vị trí đó được sử dụng để ẩn dữ liệu. Một giải pháp tinh tế khác thông qua sự tương ứng giữa thủy vân và hình ảnh chứa nó đã được đề xuất [35]. Cụ thể, cần phải chia thông tin thủy vân thành các nhóm và tìm vị trí thích hợp trong hình ảnh gốc cho từng nhóm thủy vân để ẩn thông tin. Đồng thời, việc triển khai thủy vân theo phương pháp trải phổ trong miền DCT được áp dụng cho những khối ảnh cụ thể, mang lại tính bền vững và tính bí mật cao [36]. Một ước tính về độ nổi bật cho một khu vực có thể được sử dụng làm đo lường định lượng về tính hợp lệ và được ghi nhận rằng khu vực địa phương có đặc điểm nổi bật nhất thường có khả năng tạo ra các khu vực không giao nhau [31]. Trong trường hợp

thủy vân nhị phân, định lý số dư Trung Quốc được áp dụng trong miền biến đổi. Sự phát triển của ROI để tạo ra thủy vân mạnh mẽ và thủy vân dễ vỡ được đề cập [37], nơi ROI được trích xuất từ các khung $I$ của cảnh video để thực hiện thủy vân video và chia sẻ bí mật.

Các kỹ thuật học máy hiệu quả cho xử lý tín hiệu, bao gồm cả việc nhúng thủy vân. Bằng cách trích xuất các vùng nổi bật, các vùng không nổi bật được tổng hợp để nhúng thủy vân. Các hệ số entropy mờ cho các vùng không chỉ cung cấp xếp hạng về tính phù hợp mà còn giúp cho việc nhúng thủy vân tối ưu bằng cách nhúng các lượng bit khác nhau [38]. Trong phương pháp khác, độ sáng, đặc điểm biên và độ nổi bật được sử dụng làm thuộc tính cho phân tích mờ của yếu tố độ thích hợp nhúng [39]. Việc nhúng thông tin được thực hiện trong miền DCT của biến đổi sóng. Các phương pháp thủy vân dựa trên độ nổi bật đã được đề cập ở trên và mối quan hệ của chúng với tính không thể thấy được, mẫu tần số, cơ sở vùng và học máy được báo cáo trong hình 1.4, thể hiện các mối quan hệ thông qua một bản đồ các miền. Theo góc nhìn của miền trong ảnh, phương pháp của luận án là dựa trên vùng cung cấp một giải pháp nhúng thủy vân không thể thấy được với phương pháp học máy.

#### *1.2.1.1. Công trình "Learning to Detect Salient Objects from Human Drawings" [40]*

Công trình "Learning to Detect Salient Objects from Human Drawings" [40] đề xuất một cách tiếp cận độc đáo để phát hiện đối tượng nổi bật trong ảnh dựa trên bản vẽ phác thảo do con người tạo ra. Bằng việc sử dụng bản vẽ như một nhãn yếu (weak label), công trình này khám phá khả năng chú ý tự nhiên của con người qua quá trình phác thảo và áp dụng cơ chế này vào việc học máy. Mô hình được thiết kế dựa trên kiến trúc encoder-decoder với cơ chế chú ý 2D giúp mô hình tập trung vào các vùng quan trọng của ảnh khi tạo ra bản vẽ. Kết quả là một hệ thống có khả năng xác định vùng nổi bật mà không cần đến dữ liệu gán nhãn chính xác và chi tiết, giảm thiểu nhu cầu về công sức và chi phí cho việc chuẩn bị dữ liệu.

- Ưu điểm của phương pháp này bao gồm:
  - Giảm thiểu nhu cầu về dữ liệu gán nhãn chi tiết: Việc sử dụng bản vẽ phác thảo như nhãn yếu giúp giảm bớt công sức cần thiết cho việc gán nhãn dữ liệu, một trong những thách thức lớn trong lĩnh vực học sâu.

  - Khám phá thông tin chú ý tự nhiên của con người: Phương pháp tận dụng cơ chế chú ý tự nhiên khi con người tạo ra bản vẽ, mở ra cơ hội để hiểu và ứng dụng thông tin chú ý này vào các nhiệm vụ thị giác máy tính.
  - Hiệu suất cạnh tranh: Mặc dù chỉ sử dụng nhãn yếu, kết quả thử nghiệm cho thấy mô hình có hiệu suất cạnh tranh so với các phương pháp phát hiện đối tượng nổi bật hiện đại.

- Nhược điểm:
  - Thu thập dữ liệu bản vẽ có thể tốn kém và thời gian: Mặc dù giảm bớt nhu cầu về dữ liệu gán nhãn chi tiết, việc thu thập bản vẽ phác thảo từ người dùng vẫn đòi hỏi thời gian và công sức nhất định.
  - Hạn chế về đa dạng và số lượng đối tượng: Mô hình có thể gặp khó khăn trong việc phát hiện chính xác khi đối mặt với ảnh có nhiều đối tượng nổi bật hoặc trong các tình huống phức tạp không thường gặp trong dữ liệu huấn luyện.
  - Tính tổng quát của mô hình: Phương pháp dựa trên giả định rằng bản vẽ phác thảo có thể tốt mô tả sự chú ý của con người, điều này có thể không luôn chính xác trong mọi trường hợp và với mọi người dùng.

Tóm lại, "Learning to Detect Salient Objects from Human Drawings" là một nghiên cứu đột phá, mở ra hướng tiếp cận mới trong việc hiểu và ứng dụng thông tin chú ý tự nhiên của con người vào các nhiệm vụ thị giác máy tính. Tuy nhiên, để tối ưu hóa và mở rộng khả năng ứng dụng, cần có thêm nghiên cứu và phát triển, đặc biệt là trong việc cải thiện quy trình thu thập dữ liệu và tăng cường tính tổng quát của mô hình.

#### *1.2.1.2. Công trình "High payload watermarking based on enhanced image saliency detection" [41]*

Công trình "High payload watermarking based on enhanced image saliency detection" [41] đề xuất một phương pháp đánh dấu ảnh dựa trên sự chú ý (saliency) để đạt được khả năng chứa dữ liệu cao và chất lượng ảnh sau khi đánh dấu cao. Phương pháp này kết hợp việc phát hiện đối tượng nổi bật, mã hóa màu sắc của ảnh đánh dấu bằng các phương pháp mã hóa đối xứng chaos

và mã hóa homomorphic Okamoto-Uchiyama. Đặc biệt, phương pháp cho phép nhúng ảnh đánh dấu có cùng kích thước và độ sâu bit với ảnh gốc, đây là điều chưa từng có trước đây. Kết quả thử nghiệm cho thấy phương pháp này không những duy trì được độ bền vững mà còn đạt được chất lượng ảnh cao và khả năng chứa dữ liệu lớn, vượt trội so với các phương pháp hiện hành.

- Ưu điểm:
  - Khả năng chứa dữ liệu cao: Phương pháp này cho phép nhúng ảnh đánh dấu có cùng kích thước với ảnh gốc, mang lại khả năng chứa dữ liệu đáng kể.
  - Chất lượng ảnh cao: Sử dụng các kỹ thuật mã hóa nâng cao như mã hóa homomorphic Okamoto-Uchiyama và mã hóa hỗn loạn đối xứng giúp bảo vệ thông tin đánh dấu mà không làm giảm chất lượng ảnh đáng kể.
  - Bảo mật: Việc sử dụng các phương pháp mã hóa mạnh mẽ và phức tạp tăng cường độ bảo mật cho thông tin đánh dấu.
  - Tính linh hoạt: Có khả năng nhúng nhiều ảnh đánh dấu vào cùng một ảnh gốc với điều kiện chấp nhận giảm chất lượng của ảnh đánh dấu.
- Nhược điểm:
  - Tính phức tạp cao: Quy trình mã hóa và nhúng đòi hỏi nhiều bước xử lý phức tạp, dẫn đến tăng thời gian xử lý.
  - Thách thức trong quản lý khóa: Việc sử dụng nhiều phương pháp mã hóa khác nhau cùng với việc nhúng khóa vào ảnh gốc cần có cơ chế quản lý khóa hiệu quả để đảm bảo an toàn thông tin.
  - Giảm chất lượng ảnh khi nhúng nhiều ảnh đánh dấu: Mặc dù có khả năng nhúng nhiều ảnh đánh dấu, nhưng chất lượng của các ảnh đánh dấu sẽ bị giảm khi tăng số lượng ảnh đánh dấu.

Phương pháp đánh dấu ảnh dựa trên sự chú ý này mở ra một hướng tiếp cận mới với khả năng chứa dữ liệu lớn và độ bảo mật cao. Tuy nhiên, tính phức tạp cao và thách thức trong quản lý khóa là những vấn đề cần được giải quyết trong các nghiên cứu tiếp theo.

#### *1.2.1.3. Công trình "Research on region selection strategy for visible watermark embedding" [42]*

Bài báo "Research on region selection strategy for visible watermark embedding" [42] đề xuất một phương pháp chọn vùng thích nghi để nhúng thủy vân hiển thị, sử dụng mô hình chú ý dựa trên độ nổi bật để phân biệt chính xác giữa các vùng nổi bật và không nổi bật của ảnh gốc. Phương pháp này nhấn mạnh việc chọn vùng nhúng dựa trên độ phức tạp của kết cấu ảnh, đảm bảo sự nhận diện và tính thẩm mỹ của thủy vân đồng thời xem xét đến độ an toàn của việc nhúng thủy vân.

- Ưu điểm bao gồm khả năng bảo vệ nội dung quan trọng không bị che khuất và giảm nguy cơ bị tấn công loại bỏ thủy vân hàng loạt.
- Nhược điểm là công trình thiếu chi tiết về cách xử lý các trường hợp cụ thể hoặc tối ưu hóa thủy vân cho các loại ảnh khác nhau.

#### *1.2.1.4. Một số hạn chế còn tồn tại*

Sử dụng độ nổi bật trong ảnh để tối ưu hóa quá trình nhúng thủy vân số mang lại lợi ích trong việc giảm thiểu tác động đến chất lượng thị giác của ảnh, tuy nhiên phương pháp này cũng gặp phải một số hạn chế đáng kể:

1. Phụ thuộc mô hình độ nổi bật: Việc áp dụng độ nổi bật phụ thuộc lớn vào độ chính xác của mô hình cảm nhận thị giác được sử dụng, có thể không phản ánh đúng đặc tính cảm nhận của tất cả người xem.
2. Tăng độ phức tạp tính toán: Tính toán độ nổi bật đòi hỏi thuật toán phức tạp và thời gian xử lý tăng, đặc biệt với ảnh độ phân giải cao, tạo thách thức về hiệu suất tính toán.
3. Rủi ro bảo mật: Nhúng thủy vân vào vùng ảnh nổi bật tăng khả năng thủy vân bị phát hiện và loại bỏ bởi kẻ tấn công, do sự chú ý cao đến các vùng này.
4. Ảnh hưởng chất lượng hình ảnh: Mặc dù giảm thiểu tác động thị giác, nhưng thực hiện không đúng cách có thể ảnh hưởng tiêu cực đến chất lượng hình ảnh tổng thể, đặc biệt khi dung lượng thủy vân lớn.

5. Tính khái quát không đồng nhất: Độ nổi bật thị giác biến đổi theo bối cảnh và cá nhân người xem, khiến vị trí nhúng thủy vân không tối ưu cho mọi trường hợp.

6. Giảm độ bền: Thủy vân nhúng trong vùng nổi bật dễ bị ảnh hưởng bởi các biến đổi như cắt, nén hoặc thay đổi kích thước, do đó sự biến đổi trong thông tin thị giác có thể làm mất hoặc làm hỏng thông tin thủy vân.

### 1.2.2. Thủy vân thuận nghịch

Thủy vân thuận nghịch [43] là một phương pháp thủy vân số cho phép nhúng dữ liệu vào trong tài liệu mà không làm mất thông tin gốc, đồng thời có khả năng hoàn toàn phục hồi lại tài liệu ban đầu sau khi dữ liệu thủy vân được trích xuất. Kỹ thuật này sử dụng các phương pháp như mở rộng khác biệt, ánh xạ giá trị điểm ảnh hoặc biến đổi dựa trên dải tần để đạt được sự cân bằng giữa tính bảo mật và khả năng phục hồi dữ liệu. Thủy vân thuận nghịch được ứng dụng trong nhiều lĩnh vực như bảo vệ quyền sở hữu trí tuệ, y tế điện tử và bảo mật dữ liệu, nơi mà việc giữ nguyên tính toàn vẹn của dữ liệu là cực kỳ quan trọng.

**Thủy vân trong miền RGB**

Các phương pháp hiện tại cho thủy vân thuận nghịch bao gồm việc kiểm tra các mức xám qua biểu đồ của ảnh gốc. Một số nghiên cứu đã được trình bày trong tài liệu về việc quan sát mức pixel cao nhất và thấp nhất trong biểu đồ ảnh. Việc ẩn dữ liệu vào ảnh gốc có thể bao gồm việc dịch chuyển biểu đồ [44]. Có thể nhận thấy rằng phương pháp dựa trên dịch chuyển biểu đồ gặp phải các vấn đề về tràn và thiếu dữ liệu do việc đổi vòng các mức pixel. Các kỹ thuật dịch chuyển biểu đồ khác đã được khám phá để giải quyết vấn đề tràn hoặc thiếu bằng cách áp dụng dịch chuyển biểu đồ lên ảnh chênh lệch giữa ảnh gốc đã được chỉnh sửa và bản dự đoán của nó [45]. Phương pháp của luận án bắt đầu từ việc kiểm tra biểu đồ nhưng không áp dụng dịch chuyển biểu đồ để ẩn thông tin.

Ngoài ra, vị trí để ẩn dữ liệu trong thủy vân thuận nghịch có thể được xác định bởi lỗi nội suy [46] là sự khác biệt giữa giá trị pixel nội suy và giá trị pixel tương ứng. Trong phương pháp của luận án, vị trí ẩn dữ liệu được đề xuất dựa trên việc phân tích từng pixel với các hàng xóm cục bộ của nó. Gần đây, các kỹ thuật giấu tin số (steganography) đã được sử dụng ngày càng nhiều [47] để thực

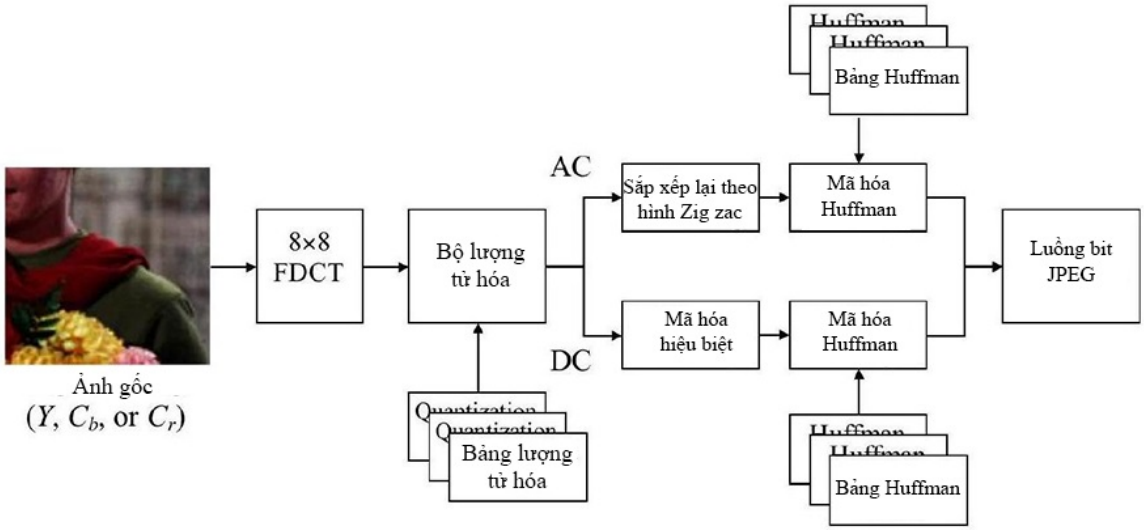
hiện thủy vân cho hình ảnh. Phương pháp như vậy áp dụng bit quan trọng nhất (MSB) [48] để đánh giá lỗi dự đoán và sau đó ẩn dữ liệu. Trong phương pháp của luận án, việc chuyển đổi hình ảnh xám sang hình ảnh nhị phân là bước tiền xử lý cho phép thực hiện xói mòn hình học [49] để tìm vị trí ẩn dữ liệu. Sử dụng nhận thức thị giác để thực hiện sự thay đổi bằng cách thêm dữ liệu một cách không thể nhận biết là một phương pháp khác cho thủy vân thuận nghịch [50]. Tại đây, luận án trình bày một phương pháp thay thế để ẩn dữ liệu với sự khác biệt thấp giữa ảnh gốc và ảnh đã được thủy vân.

Cho đến gần đây, các phương pháp thủy vân thuận nghịch được thiết kế để đạt được nhiều mục tiêu bao gồm khả năng đảo ngược, tính vô hình và khả năng chống tấn công [51]. Tất nhiên, khả năng đảo ngược là yêu cầu chính cho thủy vân thuận nghịch. Tuy nhiên, sẽ không có sự kiểm soát nào đối với ảnh gốc và dữ liệu bí mật nếu chúng có thể được phát hiện bởi bên thứ ba mà không cần biết khóa nhúng. Ví dụ, bằng cách kiểm tra tất cả các kết hợp có thể của hai giá trị xám được sử dụng làm khóa cho việc nhúng/trích xuất dữ liệu trong một phương pháp dịch chuyển biểu đồ, ảnh gốc và dữ liệu bí mật có thể được phát hiện hoàn toàn. Sau đó, dữ liệu giả có thể được nhúng vào ảnh gốc đã khôi phục bằng cách sử dụng cùng một phương pháp dịch chuyển biểu đồ, tạo ra một ảnh đã thủy vân giả mạo. Để mở rộng khả năng áp dụng thủy vân thuận nghịch cho nội dung số thực, việc cần thiết là phải có thể tăng cường bảo mật [52] để bảo vệ cả ảnh gốc và dữ liệu bí mật. Nhằm đạt được bối cảnh đầy đủ cho tất cả các pixel, một phương pháp đề xuất tạo ra bốn ảnh bối cảnh phụ và sau đó sử dụng chúng như bối cảnh của thủy vân [53].

Luận án đề xuất một thuật toán sử dụng yếu tố cấu trúc cho thủy vân thuận nghịch với sự quan tâm đặc biệt đến bảo mật chống lại các cuộc tấn công phát hiện. Ngoài khả năng phục hồi ảnh gốc và dữ liệu bí mật, phương pháp của luận án duy trì độ phức tạp phát hiện cao, phụ thuộc vào việc lựa chọn mã khóa và yếu tố cấu trúc.

**Thủy vân trong miền DCT**

Tổng quan về thuật toán JPEG được thể hiện trong hình 1.5. Thông thường, có ba bước được bao gồm trong thuật toán, đó là biến đổi Fourier rời rạc (Discrete fourier transform - DCT), lượng tử hóa và bộ mã hóa entropy. Trước hết, hình ảnh gốc được chia thành các khối không chồng lấn kích thước $8 \times 8$, sau đó được đưa vào hàm biến đổi DCT 2D (FDCT). Các bảng DCT thu được được lượng tử hóa bằng các bảng lượng tử hóa. Cuối cùng, các hệ số lượng




***Hình 1.5:*** *Thuật toán JPEG*

tử hóa được áp dụng bằng cách sử dụng các bảng Huffman để tạo mã entropy. Mỗi thành phần của thành phần độ sáng và các thành phần màu sắc được gọi là $Y$ và thành phần ($C_r$, $C_b$). Để nén các thành phần của hình ảnh JPEG, mỗi thành phần được lượng tử hóa bằng cách sử dụng bảng lượng tử hóa tương ứng, được gọi là $Q_y$, $Q_{cr}$ và $Q_{cb}$. Các hệ số lượng tử hóa tác động trực tiếp vào chất lượng của hình ảnh JPEG. Do đó, để làm giảm thiểu thêm sự méo dạng của hình ảnh JPEG, luận án nghiên cứu tác động của quá trình lượng tử hóa lên các hệ số DCT để tạo chiến lược lựa chọn các hệ số lượng tử hóa cho việc nhúng thông tin.

Thuật toán RDH được áp dụng trên hình ảnh JPEG khá khó khăn để thực hiện do miền thông tin nén ít hơn cho việc nhúng. Một số thuật toán RDH đã được đề xuất cho hình ảnh JPEG, tuy nhiên nó có một số điểm yếu trên miền JPEG.

Một vấn đề đầu tiên là giới hạn của miền thông tin có thể được nhúng. Như kết quả của cuộc khảo sát trong bài viết [54], thông tin bí mật có thể được nhúng trong miền DCT và luồng mã hóa Huffman của hình ảnh JPEG. Miền nhúng thông tin cũng cần được chọn cẩn thận để đạt được chất lượng cao của hình ảnh JPEG nhúng thông tin.

Vấn đề thứ hai là chất lượng dễ vỡ của hình ảnh JPEG. Điều này có nghĩa là chất lượng của hình ảnh JPEG rất nhạy cảm với việc điều chỉnh số lượng hệ số DCT. Do đó, việc lựa chọn các hệ số DCT cần được xem xét cẩn thận để nhúng thông tin.

Ba loại được biết đến rất rõ là các phương pháp nối thêm mã nén không mất dữ liệu [55], mở rộng khác biệt [56] và dịch chuyển biểu đồ tần số [44]. Những thuật toán này thường được áp dụng trên hình ảnh xám hoặc hình ảnh màu. Gần đây, sự kết hợp của các phương pháp RDH cũng được xem xét để đạt hiệu suất cao hơn như lỗi dự đoán (PEs) được đề xuất trong các bài viết [57, 58, 59].

Hầu hết các thuật toán RDH được đề xuất dễ dàng trên dữ liệu hình ảnh, bao gồm cả hình ảnh xám [60, 61, 62]. Trong các hình ảnh dựa trên màu sắc, các thành phần độ sáng, thành phần tương phản màu sắc và kênh RGB được sử dụng để kiểm soát miền màu sắc để ẩn các thông tin kỹ thuật số bí mật có dung lượng lớn [63, 64, 65]. Tuy nhiên, các phương pháp RDH dựa trên màu sắc dẫn đến việc hủy hoại hình ảnh màu sắc một cách không thể đảo ngược. Điều này có nghĩa là không thể khôi phục hình ảnh mà không gây mất mát trong một số trường hợp. Do đó, các phương pháp RDH cho hình ảnh cần phải chọn các đặc điểm mạnh mẽ, các khu vực phù hợp để nhúng thông tin số bí mật.

Một vấn đề khác của các phương pháp RDH cho hình ảnh là chi phí tính toán của thuật toán khôi phục [12, 13]. Điều này làm cho chúng khó áp dụng trong các ứng dụng thực tế. Do đó, chỉ trong các ứng dụng như hình ảnh y khoa, hình ảnh quân sự, trong đó sự biến dạng không mong muốn, các phương pháp RDH có thể được áp dụng.

Dựa trên những giải thích trên, luận án kết luận rằng thuật toán RDH rất quan trọng cho các ứng dụng thực tế, đặc biệt là cho hình ảnh JPEG.

#### *1.2.2.1. Công trình "Robust reversible image watermarking scheme based on spread spectrum" [66]*

Công trình "Robust reversible image watermarking scheme based on spread spectrum" [66] giới thiệu một phương pháp thủy vân số thuận nghịch (reversible) mạnh mẽ, sử dụng mã phổ phân tán (spread-spectrum) thích ứng để nhúng bit thủy vân vào ảnh gốc. Phương pháp này cân nhắc giữa độ mạnh của việc chống lại các cuộc tấn công và khả năng phục hồi ảnh gốc mà không làm mất dữ liệu. Một ưu điểm lớn là khả năng phục hồi ảnh gốc ngay cả khi ảnh có thủy vân bị tấn công, dù chỉ có thể phục hồi một phần. Tuy nhiên, phương pháp còn phụ thuộc vào việc ước lượng chính xác biên độ nhúng, điều này có thể trở nên phức tạp trong trường hợp ảnh bị biến dạng do tấn công.

#### *1.2.2.2. Công trình "Reversible data hiding in JPEG document images based on zero coefficients embedding" [67]*

Công trình "Reversible data hiding in JPEG document images based on zero coefficients embedding" [67] tập trung vào việc cải thiện chất lượng hình ảnh và dung lượng nhúng thông qua việc chèn dữ liệu vào các hệ số DCT bằng 0 của ảnh JPEG. Điều này khác biệt so với các phương pháp trước đây chủ yếu sử dụng các hệ số DCT khác 0 và 1 để nhúng dữ liệu, dẫn đến việc giảm chất lượng hình ảnh. Phương pháp được đề xuất sử dụng một chiến lược chọn lựa hệ số 0 tối ưu để giảm thiểu sự biến dạng hình ảnh và tăng cường dung lượng nhúng. Ưu điểm chính là khả năng cung cấp dung lượng nhúng cao hơn và chất lượng hình ảnh tốt hơn so với các phương pháp trước đây. Tuy nhiên, một nhược điểm có thể thấy là sự phức tạp trong việc tính toán và chọn lọc hệ số 0 để nhúng dữ liệu cũng như việc cần phải ghi lại thông tin dịch chuyển như một phần thông tin phụ trợ nhỏ có thể làm tăng kích thước tệp tin.

#### *1.2.2.3. Công trình "Reversible data hiding for JPEG images with minimum additive distortion" [68]*

Công trình "Reversible data hiding for JPEG images with minimum additive distortion" [68] đề xuất một phương pháp mới cho việc ẩn dữ liệu thuận nghịch trong ảnh JPEG bằng cách giảm thiểu sự biến dạng cộng gộp. Phương pháp này tính toán chi phí của mỗi khối DCT và tần số DCT, sau đó kết hợp chúng để tối thiểu hóa sự biến dạng. Sử dụng chiến lược dịch chuyển histogram hai chiều cải tiến, phương pháp giảm thiểu số lần sửa đổi không hợp lệ của hệ số DCT. Kết quả thử nghiệm cho thấy phương pháp này vượt trội so với các phương pháp ẩn dữ liệu khả nghịch JPEG hiện có, về chất lượng hình ảnh và mức độ tăng kích thước tệp tin nhỏ hơn. Tuy nhiên, một nhược điểm có thể nhận ra là phương pháp có thể phức tạp về mặt tính toán khi kết hợp nhiều hàm chi phí và sử dụng chiến lược dịch chuyển histogram hai chiều, điều này có thể ảnh hưởng đến hiệu quả xử lý đối với ảnh có kích thước lớn hoặc khi cần áp dụng trong thời gian thực.

#### *1.2.2.4. Công trình "Dual-jpeg-image reversible data hiding" [69]*

Công trình "Dual-jpeg-image reversible data hiding" [69] đề xuất một phương pháp ẩn dữ liệu khả nghịch trên ảnh JPEG dùng chiến lược ảnh đôi.

Phương pháp này tận dụng các hệ số DCT không bằng không, không gây ra sự biến dạng thêm do các sửa đổi không hợp lệ và giảm thiểu sự mở rộng kích thước tệp. Một phương pháp phân bổ động được đề xuất để phân bổ khả năng nhúng sao cho gây ra ít sự biến dạng nhất. Hệ số DCT không bằng không được nhúng linh hoạt với số bit dữ liệu bí mật khác nhau, cải thiện đáng kể khả năng nhúng. Kết quả thử nghiệm chứng minh hiệu quả của phương pháp với khả năng nhúng cao và chất lượng hình ảnh thỏa đáng trong khi kiểm soát sự mở rộng kích thước tệp. Nhược điểm là phương pháp trong công trình có thể phức tạp về mặt tính toán do cần xử lý hai ảnh cùng một lúc và đòi hỏi sự chính xác cao trong việc phục hồi dữ liệu và ảnh gốc.

#### *1.2.2.5. Một số hạn chế còn tồn tại*

Thủy vân thuận nghịch (Reversible Watermarking) trong lĩnh vực ảnh số mang lại khả năng nhúng thông tin vào ảnh mà sau đó có thể hoàn toàn loại bỏ thông tin nhúng để trả lại ảnh gốc mà không có sự mất mát dữ liệu nào. Tuy nhiên, dù có nhiều ưu điểm, kỹ thuật này vẫn gặp phải một số hạn chế còn tồn tại:

1. Hạn chế về dung lượng nhúng: Khả năng nhúng thông tin có hạn. Đối với thủy vân thuận nghịch, việc duy trì tính nguyên vẹn của ảnh gốc hạn chế lượng thông tin có thể được nhúng. Điều này làm cho việc truyền tải thông tin có kích thước lớn trở nên khó khăn.

2. Ảnh hưởng đến chất lượng hình ảnh: Mặc dù thủy vân thuận nghịch cho phép khôi phục lại ảnh gốc, quá trình nhúng và trích xuất thông tin có thể tạo ra biến đổi nhỏ trên ảnh được nhúng thủy vân, đặc biệt nếu lượng thông tin nhúng lớn.

3. Độ phức tạp tính toán cao: Việc thiết kế và thực hiện các thuật toán thủy vân thuận nghịch thường phức tạp hơn so với thủy vân không thuận nghịch do yêu cầu khôi phục ảnh gốc mà không làm mất mát dữ liệu.

4. Khả năng phát hiện và loại bỏ: Trong một số trường hợp, việc nhúng thông tin thuận nghịch có thể làm tăng khả năng phát hiện của thủy vân, do các điểm đặc biệt trong quá trình nhúng có thể tạo ra các mẫu nhận dạng. Điều này có thể dẫn đến việc loại bỏ dễ dàng hơn bởi những người không mong muốn.

5. Bảo mật: Mặc dù khả năng khôi phục ảnh gốc là một ưu điểm lớn, nhưng nó cũng đặt ra vấn đề về bảo mật. Thông tin nhúng có thể dễ dàng bị trích xuất và sử dụng không đúng mục đích nếu không được bảo vệ đúng cách.

6. Tương thích và tính linh hoạt: Các thuật toán thủy vân thuận nghịch đôi khi gặp khó khăn trong việc áp dụng cho một loạt các định dạng ảnh số hoặc cần phải được thiết kế cụ thể cho từng loại ảnh, làm giảm tính linh hoạt và tương thích trong thực tế.

### 1.3. Kết luận

Luận án tập trung vào việc phát triển các giải pháp mới trong lĩnh vực thủy vân số với trọng tâm là khắc phục những hạn chế của việc áp dụng độ nổi bật trong ảnh số và thủy vân thuận nghịch. Luận án giới thiệu phương pháp thủy vân bằng cách học không nổi bật (WLNS), giúp giảm sự phụ thuộc vào mô hình độ nổi bật, cải thiện đáng kể bảo mật và giảm thiểu ảnh hưởng đến chất lượng hình ảnh. Về thủy vân thuận nghịch, các phương pháp mới sử dụng miền DCT và yếu tố cấu trúc giúp tối ưu hóa dung lượng nhúng, tăng cường bảo mật và giảm độ phức tạp tính toán, từ đó nâng cao hiệu suất và tính linh hoạt. Các thí nghiệm thực hiện đã chứng minh rằng các phương pháp đề xuất không chỉ tăng khả năng nhúng mà còn cải thiện chất lượng hình ảnh và giảm thiểu rủi ro bảo mật, tạo tiền đề cho ứng dụng rộng rãi hơn trong lĩnh vực thủy vân số.

# CHƯƠNG 2. PHÂN TÍCH ẢNH HƯỞNG ĐỘ NỔI BẬT CỦA ẢNH TRONG THỦY VÂN SỐ

## 2.1. Giới thiệu

Chương 2 của luận án tập trung vào việc phát triển và đề xuất các phương pháp thủy vân số tiên tiến, đặc biệt là trong bối cảnh xử lý ảnh số. Những hạn chế như sự phụ thuộc quá mức vào mô hình độ nổi bật, độ phức tạp tính toán cao và rủi ro bảo mật vẫn chưa được giải quyết một cách toàn diện. Vì vậy, các giải pháp được đề xuất trong chương này nhằm khắc phục những vấn đề này bằng cách giảm thiểu sự phụ thuộc vào các mô hình hiện có, tối ưu hóa quy trình tính toán và tăng cường bảo mật cho các phương pháp thủy vân số. Mục tiêu chính là cải thiện hiệu suất tổng thể của các hệ thống thủy vân, đảm bảo tính ổn định và bền vững trong các môi trường có nhiều tác động tiêu cực như nén dữ liệu, chỉnh sửa và các dạng tấn công khác.

Trong trường hợp đối tượng nhúng là hình ảnh, việc theo dõi một số lượng lớn các loại hình ảnh và loại thông tin được nhúng vào (có thể là văn bản hoặc hình ảnh) là đặc biệt quan trọng. Khi xem xét sự chú ý hình ảnh trong nhận thức con người thông qua các mô hình độ nổi bật [63], có thể thấy rằng bản đồ độ nổi bật [70, 71, 72, 73] có thể được sử dụng cho thủy vân số. Mục đích của chương này là điều chỉnh một số mô hình về độ nổi bật để sử dụng các khu vực không nổi bật cho thủy vân thông qua học máy để nâng cao tính tin cậy của thủy vân. Phương pháp này gọi là phương pháp thủy vân bằng cách học vùng không nổi bật (Watermark by Learning Non Saliency - WLNS) được mô tả và trình bày. Các đóng góp quan trọng của chương này bao gồm:

- Phát triển phương pháp thủy vân bằng cách học vùng không nổi bật (Watermark by Learning Non Saliency - WLNS):

  - Xác định vùng không nổi bật: Phương pháp này sử dụng các mô hình độ nổi bật để xác định và học các vùng không nổi bật trong ảnh. Việc này giúp nhúng thông tin vào những vùng ít được chú ý, tăng cường tính vô hình của thủy vân.

  - Áp dụng học máy để chọn vùng nhúng: Sử dụng Support Vector Machine

(SVM) để phân loại và chọn các vùng không nổi bật phù hợp nhất để nhúng thủy vân, đảm bảo giảm thiểu sự thay đổi về độ nổi bật của các vùng này sau khi nhúng.

- Thử nghiệm và đánh giá:

  - Khả năng chống tấn công: Các thử nghiệm trên dữ liệu hình ảnh cho thấy phương pháp WLNS có khả năng chống lại các loại tấn công phổ biến như nén, cắt xén và thêm nhiễu mà không làm giảm đáng kể chất lượng thị giác của ảnh.

  - Tính bền vững: Phương pháp này chứng minh tính bền vững đáng kể đối với một số mô hình độ nổi bật trong khi chỉ gây mất mát nhỏ về tính chính xác.

- Kiểm tra và xác thực với các mô hình độ nổi bật khác nhau:

  Khái niệm về thủy vân không nổi bật đã được kiểm tra và xác thực với các mô hình độ nổi bật và phương pháp mã hóa khác nhau, cho thấy tính khả thi và hiệu quả của phương pháp này trong việc bảo vệ quyền sở hữu trí tuệ và xác thực nguồn gốc của hình ảnh.

## 2.2. Thủy vân dựa trên đặc trưng không nổi bật của ảnh số

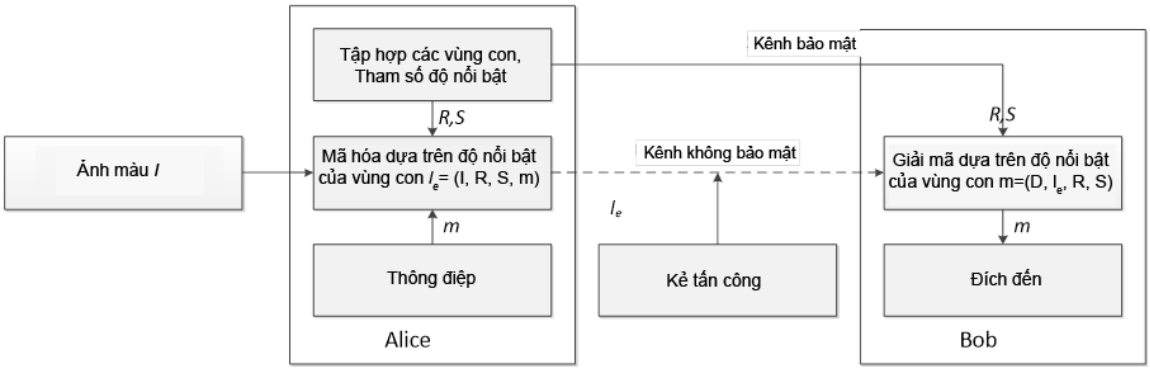
### 2.2.1. Phương pháp dựa trên học vùng không nổi bật

Phương pháp này yêu cầu việc phát hiện độ nổi bật và lựa chọn phân vùng con để bảo mật thông điệp ẩn trong quá trình nhúng thủy vân. Luận án sử dụng một ảnh màu và một thông điệp $m$ mà luận án muốn nhúng vào một khu vực của ảnh. Phương pháp phát hiện độ nổi bật $S$ có các tham số cho phép ước tính bản đồ nổi bật $I^s$ bằng cách sử dụng công thức (2.1) và đặc trưng của nó $s$ bằng (2.2) đối với việc xác định một phân vùng con mà luận án muốn ẩn một thông điệp:

$$(I, S) = \xrightarrow{\text{phát hiện độ nổi bật}} I^s \tag{2.1}$$

$$I^s \xrightarrow{\text{phát hiện đặc trưng}} s \tag{2.2}$$

Luận án sử dụng một tập hợp các phân vùng con đã xác định trước $R$ để cho phép dễ dàng chọn một phân vùng con $u$ để nhúng thông điệp. Công việc được




***Hình 2.1:*** *Phương pháp nhúng thủy vân cho ảnh I trong quá trình truyền thông giữa người gửi (Alice) và người nhận (Bob) bằng cách sử dụng các đặc trưng nổi bật với một kênh bảo mật để trao đổi các khóa riêng tư R, S.*

ghi lại bằng công thức:

$$I_e = E(I, R, S, m) \tag{2.3}$$

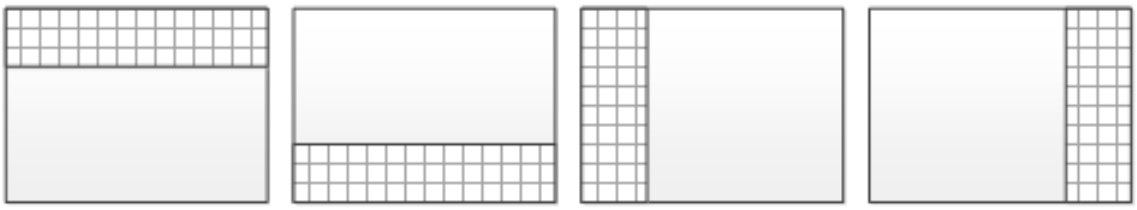
Trong đó $I_e$ là ảnh đã nhúng thủy vân. Do đó, luận án có thể thấy mô hình phát hiện độ nổi bật với các tham số của nó $S$ và tập hợp phân vùng con đã xác định trước $R$ như các khóa riêng tư được chuyển từ người gửi (Alice) tới người nhận (Bob) qua kênh bảo mật, trong khi ảnh đã nhúng thủy vân $I_e$ được gửi qua kênh không bảo mật (hình 2.1). Khi mô hình phát hiện độ nổi bật với các tham số $S$ của nó và tập hợp phân vùng con đã xác định trước $R$ được chia sẻ một cách an toàn, người nhận Bob áp dụng mô hình phát hiện độ nổi bật cho ảnh đã nhúng thủy vân bằng mô hình độ nổi bật $S$ để nhận được bản đồ độ nổi bật $I_e$ và đặc trưng $e$ của nó, có thể khác với đặc trưng nổi bật $s$ của ảnh gốc $I$. Bằng cách sử dụng tập hợp phân vùng con đã xác định trước $R$ trong việc phân tích bản đồ độ nổi bật để có đặc trưng nổi bật $e$, một phân vùng con $r$ được tính toán và thông điệp $m$ được giải mã từ phân vùng con đó:

$$(I_e, S) = \xrightarrow{\text{phát hiện độ nổi bật}} I_e^s \tag{2.4}$$

$$I_e^s \xrightarrow{\text{phát hiện đặc trưng}} e \tag{2.5}$$

Hình 2.1 trình bày khái niệm về việc ẩn tin bằng thủy vân dựa trên độ nổi bật, bao gồm đặc trưng nổi bật của ảnh mang $s$, vùng con đã chọn $u$ của ảnh, đặc trưng nổi bật của ảnh đã được nhúng thủy vân $e$ và vùng con đã chọn $r$ của ảnh đã được nhúng thủy vân. Rõ ràng, phương pháp này được xác minh khi các vùng con của ảnh đã được nhúng thủy vân được xác định chính xác để


***Hình 2.2:*** *Phương pháp nhúng thủy vân dựa trên độ nổi bật, s - đặc trưng nổi bật, u - vùng con đã được chọn, e - đặc trưng nổi bật của ảnh đã được nhúng thủy vân, và r - vùng con đã được chọn của ảnh đã được nhúng thủy vân.*



***Hình 2.3:*** *Các vị trí biến đổi của vùng con trong ảnh, bao phủ $\frac{1}{4}$ diện tích của ảnh.*

khôi phục lại thông điệp đã được mã hóa.

*2.2.1.1. Đặc trưng nổi bật*

Như được thể hiện trong hình 2.1, một tập hợp các khu vực con $R$ được định nghĩa trước để nhúng thông điệp vào một trong các khu vực con này. Tập hợp này được thiết kế một cách bí mật để mã hóa và giải mã. Một ví dụ đơn giản về tập hợp này bao gồm bốn vị trí của hình chữ nhật, nằm dọc theo biên của hình ảnh và bao phủ $\frac{1}{4}$ diện tích hình ảnh, xem hình 2.3. Một tập hợp các khu vực con như vậy được thiết kế với kỳ vọng rằng các khu vực nổi bật thường được phân bổ bên trong hình ảnh và các khu vực không nổi bật thường được thấy dọc theo biên.

Cho trước một bản đồ nổi bật của ảnh $I^s$, trong đó mức độ nổi bật nằm trong đoạn $[0, 1]$, mặt nổi bật cho mỗi điểm ảnh 0, 1 có thể được tạo ra bằng cách so sánh đơn giản với một ngưỡng $\lambda$, theo mặc định $\lambda = 0,5$. Lưu ý rằng một phép toán hình thái học như *imerode* là hiệu quả để áp dụng cho mặt nổi bật để loại bỏ các đối tượng nhỏ và hiển thị các khu vực nổi bật bằng các khu vực lớn. Khi đã tìm thấy mặt nổi bật, khoảng cách nhỏ nhất từ các đối tượng nổi bật đến viền khung ảnh có thể được ước tính để hiển thị một khu vực không nổi bật dọc theo viền khung ảnh dưới dạng hình chữ nhật. Đặc trưng nổi bật của ảnh được chỉ định bằng tỷ lệ diện tích của hình chữ nhật $v_i$ trên diện tích của toàn bộ ảnh bằng công thức (2.6). Như vậy, các vùng con được đề cập ở trên với ví dụ trong hình 2.3 có thể được sắp xếp theo thứ tự các khu vực của

hình chữ nhật $v_i$ bằng công thức (2.7).

$$s \propto \overrightarrow{v}^s = \{v_i/v_I\}_{i=1}^k, v_I - \text{area of image} \tag{2.6}$$

$$u \propto sortarg(s) = sortarg(\overrightarrow{v}^s) \tag{2.7}$$

Các chỉ số của các vùng con $u$ cho thấy mức độ thích hợp để ẩn thông tin không nhìn thấy vì chúng tương ứng với các vùng không nổi bật dọc theo viền ảnh. Do đó, các vùng con được xác định trước với các chỉ số được sắp xếp được biểu diễn bằng

$$\Omega_{u_j} = \{x, y, w, h\}, \Omega_{u_j} \subset \Omega \tag{2.8}$$

Hiện tại, thông điệp $m$ được ẩn vào ảnh trong một vùng con, tạo ra ảnh chứa thủy vân $I_e$ bằng công thức (2.9). Để nhúng thông điệp văn bản vào ảnh, có nhiều phương pháp có sẵn có thể được thực hiện vào một vùng con. Ở đây, luận án chọn LSB [18] để nhúng văn bản vào ảnh để kiểm tra tính bền vững bằng cách so sánh thông điệp đã mã hóa với phiên bản đã khôi phục sau khi thay đổi đặc trưng nổi bật bị ảnh hưởng bởi việc mã hóa ở mức bit. Ở phía của người nhận, ảnh chứa thủy vân $I_e$ được phân tích để thu thập bản đồ nổi bật của nó và đặc trưng nổi bật liên quan $e$. Tương tự như công thức (2.6), đặc trưng $e$ được đo bằng diện tích của hình chữ nhật $v_j$ bằng công thức (2.10) và các vùng con của $I_e$ có thể có chỉ số được sắp xếp theo thứ tự diện tích của hình chữ nhật $v_j$ bằng công thức (2.11).

$$(I, m, \Omega_{u_j}) \xrightarrow{\text{mã hóa}} I_e \tag{2.9}$$

$$e \propto \overrightarrow{v}^e = \{v_j^e/v_{I_e}\}_{j=1}^k, v_I = v_I, : \text{area of image} \tag{2.10}$$

$$r \propto sortarg(e) = sortarg(\overrightarrow{v}^e) \tag{2.11}$$

Luận án sử dụng các mô tả đã được cung cấp để ước tính các đặc trưng $\{s, u, e, r\}$ có tính chất mô tả quá trình mã hóa và giải mã của thủy vân số.

#### *2.2.1.2. Xác thực thủy vân số*

Để giúp làm rõ tác động của phương pháp thủy vân số, có thể hữu ích khi nhìn vào quá trình từ góc độ xác suất Bayesian [74] và hiểu dễ dàng khía

cạnh chọn vùng con dựa trên đặc trưng về độ nổi bật bằng cách sử dụng công thức (2.12). Với $r$ và $u$ là chỉ số của vùng con, chúng có miền giá trị $\{0, 1, 2, 3\}$. Lý tưởng, vùng con $r$ nên giống với vùng con $u$, tức là $r = u$ để đảm bảo rằng thông điệp được mã hóa trong vùng con có thể được phát hiện và giải mã. Sự kiện $r = u$ được thể hiện thông qua các đặc trưng về độ nổi bật bằng công thức (2.13).

$$p(r, e, u, s) = p(r|e)p(e|u)p(u|s)p(s) \tag{2.12}$$

$$p(r = u|s) \sum_{r\in\{0,1,2,3\},e\in[0,1],u\in\{0,1,2,3\}} p(r = u|e, u, s) \tag{2.13}$$

Để tận dụng tính nhất quán của các đặc trưng bằng cách sử dụng công thức (2.12), luận án mở rộng công thức (2.13) thành công thức (2.14) đại diện cho kết quả của các nhiệm vụ nhúng thủy vân. Khi gần đến sự kiện bắt đầu ($s$) - nơi vị trí của khu vực con $u$ được xác định, luận án sử dụng công thức (2.15).

$$p(r = u|s) \propto \sum_{r\in\{0,1,2,3\},e\in[0,1],u\in\{0,1,2,3\}} p(r = u|e)p(e, u) \underbrace{p(u|s))}_{\gamma_s(u)} \tag{2.14}$$

$$p(r = u|s) \propto \sum_{r\in\{0,1,2,3\},e\in[0,1],u\in\{0,1,2,3\}} p(r = u|e)p(e, u)\gamma_s(u)) \tag{2.15}$$

Quá trình này được lặp lại cho đặc trưng $e$ của hình ảnh đã được sửa đổi bằng cách nhúng tin nhắn với chỉ số $\gamma_s(e)$ bởi (2.16). Ví dụ, việc tích luỹ cho phép luận án xây dựng một cái nhìn cuối cùng về các sự kiện phụ thuộc bằng công thức (2.17).

$$p(r = u|s) \propto \sum_{r\in\{0,1,2,3\},e\in[0,1]} p(r = u|e) \underbrace{\sum_{u\in\{0,1,2,3\}} p(e|u)\gamma_s(u))}_{\gamma_s(u)} \tag{2.16}$$

$$p(r = u|s) \equiv \sum_{r\in\{0,1,2,3\}} p(r = u|e)\gamma_u(e)) \tag{2.17}$$

Cho hình ảnh ban đầu có đặc trưng độ nổi bật $s$, xác suất của việc có cùng vị trí của khu vực con $r = u$ trước và sau quá trình thủy vân liên quan đến đặc trưng $e$. Một biểu thức tương tự áp dụng cho $r \neq u$ theo (2.18). Ở đây, luận án lấy tỷ lệ của $p(r = u|s)$ và $p(r \neq u|s)$ để biết mức độ bền vững cho một trường

hợp thủy vân với đặc trưng độ nổi bật $s$ theo (2.19).

$$p(r \neq u|s) \equiv \sum_{r\in\{0,1,2,3\}} p(r \neq u|e)\gamma_u(e)) \tag{2.18}$$

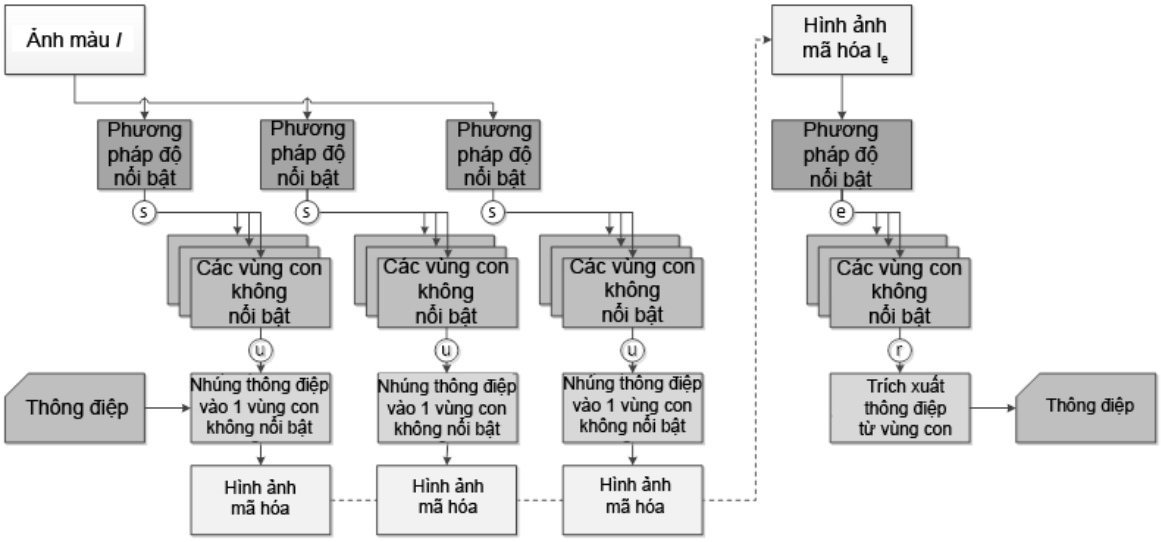
$$\frac{p(r = u|s)}{p(r \neq u|s)} \equiv \frac{\sum\limits_{r\in\{0,1,2,3\}} p(r = u|e)\gamma_u(e))}{\sum\limits_{r\in\{0,1,2,3\}} p(r \neq u|e)\gamma_u(e))} = \frac{\sum\limits_{r\in\{0,1,2,3\}} p(r = u|e)}{\sum\limits_{r\in\{0,1,2,3\}} p(r \neq u|e)} \tag{2.19}$$

Cách tạo ra bản đồ độ nổi bật thay đổi theo các phương pháp phát hiện độ nổi bật khác nhau và các phương pháp mã hóa - giải mã thông điệp trong hình ảnh cũng khác nhau. Điều này dẫn đến sự thay đổi của bản đồ độ nổi bật và đặc trưng độ nổi bật trước và sau quá trình thủy vân. Tuy nhiên, kỳ vọng cao về việc có $r = u$ cho tất cả theo (2.19) nói chung là không thực tế đối với các hình ảnh mang thủy vân $I$ khác nhau và các thông điệp văn bản biến đổi $m$ khác nhau. Nếu tồn tại ít nhất một khu vực con $r$ nào đó khiến cho $r = u$ sau quá trình thủy vân, sẽ tồn tại vị trí thích hợp của vùng con để giải mã thông điệp mặc cho đặc trưng độ nổi bật $e$ khác với $s$ theo (2.20). Bằng cách giới hạn cho điều kiện tồn tại một khu vực con $i$ thay vì tất cả các khu vực con (2.20), luận án có thể thấy kỳ vọng của việc có $r = u$ trong biểu thức (2.21), thể hiện sự phụ thuộc vào đặc trưng $e$ của hình ảnh đã được thêm thủy vân.

$$I \neq I_e \rightarrow I^s \neq I_e^s \rightarrow s \neq e, \exists i \in \{0, 1, 2, 3\}, r_i = u_i \tag{2.20}$$

$$\frac{p(r = u|s)}{p(r \neq u|s)} \equiv \frac{max_{r\in\{0,1,2,3\}} p(r = u|e)}{1 - max_{r\in\{0,1,2,3\}} p(r = u|e)} \tag{2.21}$$

Xem xét vấn đề trong phương pháp phân loại cho không gian đặc trưng $\{s\}$. Ghi $\{0, 1\}$ cho miền lớp để biểu diễn $r \neq u$ hoặc $r = u$. Như đã đề cập trong hình 2.2, để xác định khu vực con $r$ nào dành cho việc nhúng tin nhắn dựa trên $s$, đặc trưng độ nổi bật $e$ có tác động giống như một trạng thái ẩn. Cần phải áp dụng các kỹ thuật học máy để tìm hiểu tác động của trạng thái ẩn (hình 2.4). Đặc trưng $s$ được trích xuất cho mỗi hình ảnh $I$ từ cơ sở dữ liệu bằng tập hợp các mô hình phát hiện độ nổi bật để cho phép mã hóa và giải mã thủy vân. Thông điệp được nhúng vào từng khu vực con $u$ để tạo ra hình ảnh đã thêm thủy vân cụ thể $I_e$, do đó đặc trưng $e$ được trích xuất trong nhiệm vụ giải mã. Khu vực con $r$ được định nghĩa để giải mã trong khi tính bền vững được ước tính bằng cách so sánh $u$ với $r$.




***Hình 2.4:*** *Mã hóa thủy vân dựa trên mô hình phát hiện độ nổi bật*

Giả sử $\theta$ đại diện cho mô hình độ nổi bật được sử dụng để trích xuất đặc trưng độ nổi bật, hàm ước lượng xác suất $L(\theta)$ đo lường tính mạnh mẽ của mô hình độ nổi bật bằng cách tham chiếu đến dữ liệu thống kê được xuất ra trong quá trình nhúng thủy vân cho các hình ảnh $I$ từ tập dữ liệu D thông qua biểu thức (2.22). Giá trị tối đa của hàm hợp lý với quan hệ đối với $\theta$ được đánh giá bằng ước tính ML (maximum likelihood) [75] thông qua biểu thức (2.23). Bốn mô hình độ nổi bật được sử dụng để thực hiện các phương pháp mã hóa thủy vân và được kiểm tra để ước tính hàm hợp lý $L(\theta)$.

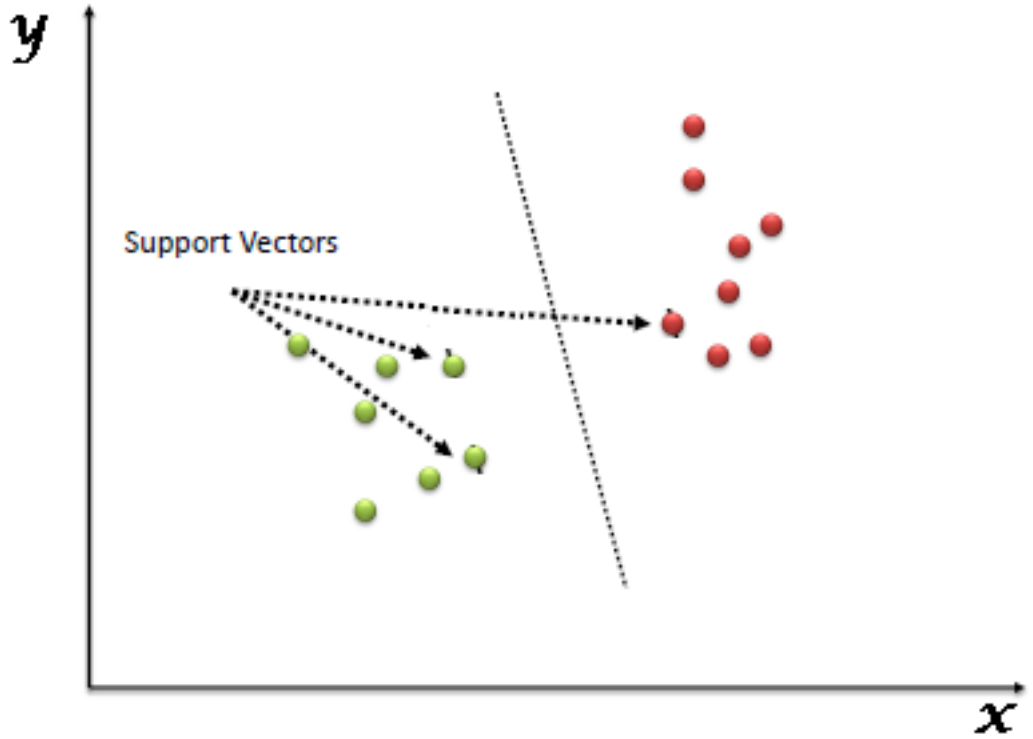
$$L(\theta) = \Pi_{I \in D} p(r(I) = u(I)|s(I)) \tag{2.22}$$

$$\widehat{\theta} = argmax_{\theta} L(\theta) \tag{2.23}$$

Ước tính ML được thực hiện thông qua mô hình học của luận án sử dụng máy vector hỗ trợ (SVM) [76]. Các đặc điểm được thu thập trong quá trình phát hiện đặc điểm bằng cách sử dụng quá trình phát hiện dựa trên độ nổi bật đã được đề cập ở trên. Quá trình học SVM được thực hiện cho các đặc điểm đã được tổng hợp để xây dựng các hàm kernel.

#### *2.2.1.3. Áp dụng phương pháp học máy SVM*

Support Vector Machine (SVM) trong hình 2.5 là một phương pháp học máy được sử dụng rộng rãi cho các bài toán phân loại và hồi quy. SVM hoạt động bằng cách tìm ra một siêu phẳng trong không gian đa chiều, có khả năng




***Hình 2.5:*** *Mô hình học máy SVM*

phân tách các điểm dữ liệu thuộc các lớp khác nhau. SVM được đánh giá cao nhờ khả năng phân loại mạnh mẽ và khả năng tổng quát hóa tốt.

SVM được luận án lựa chọn trong phương pháp này vì các lý do sau:

- Khả năng phân loại mạnh mẽ: SVM có khả năng phân loại các dữ liệu phi tuyến một cách hiệu quả nhờ vào việc sử dụng các hàm kernel.

- Độ tổng quát hóa cao: SVM thường có độ tổng quát hóa tốt, nghĩa là mô hình không chỉ hoạt động tốt trên dữ liệu huấn luyện mà còn trên dữ liệu mới.

- Khả năng xử lý dữ liệu lớn: Với các kỹ thuật như "Support Vector", SVM có thể xử lý các bộ dữ liệu lớn và phức tạp.

SVM được ứng dụng để chọn các vùng không nổi bật của ảnh để nhúng thủy vân nhằm đảm bảo tính vô hình và ổn định của thủy vân. Các bước cụ thể bao gồm:

Bước 1. Chuẩn bị dữ liệu:

- Dữ liệu đầu vào là các ảnh số cần được nhúng thủy vân.

- Các vùng con của ảnh được trích xuất để tính toán các đặc trưng độ nổi bật.

Bước 2. Trích xuất đặc trưng độ nổi bật:

Sử dụng các mô hình độ nổi bật để tính toán đặc trưng độ nổi bật của từng vùng con trong ảnh. Các mô hình này có thể bao gồm hiệp phương sai vùng, độ nổi bật thưa thớt, độ nổi bật phổ tần số, và độ nổi bật hiếm gặp.

Bước 3. Huấn luyện SVM:

- SVM được huấn luyện bằng cách sử dụng các đặc trưng độ nổi bật của các vùng con làm đầu vào.

- Nhãn của các vùng con được xác định dựa trên mức độ nổi bật: các vùng con có độ nổi bật thấp sẽ được gán nhãn là "không nổi bật", còn các vùng con có độ nổi bật cao sẽ được gán nhãn là "nổi bật".

Bước 4. Chọn vùng nhúng thủy vân:

- Sau khi huấn luyện, SVM được sử dụng để phân loại các vùng con mới trong ảnh cần nhúng thủy vân.

- Các vùng con không nổi bật nhất được chọn để nhúng thủy vân nhằm đảm bảo tính không thể nhận thấy của thủy vân.

Bước 5. Nhúng thủy vân:

Thủy vân được nhúng vào các vùng con đã được chọn bởi SVM. Quá trình nhúng thủy vân bao gồm việc điều chỉnh các giá trị điểm ảnh trong các vùng con không nổi bật này.

Bước 6. Kiểm tra và đánh giá:

- Sau khi nhúng, ảnh chứa thủy vân được kiểm tra để đảm bảo tính không thể nhận thấy và độ ổn định của thủy vân.

- Các tiêu chí đánh giá bao gồm độ chính xác (precision), độ nhớ (recall), độ đo F (F-measure) và sai số trung bình đối nghịch bình phương (MSE).

Bước 7. Trích xuất thủy vân:

- Khi cần kiểm tra tính hợp lệ, SVM được sử dụng lại để xác định các vùng con chứa thủy vân trong ảnh đã nhúng.

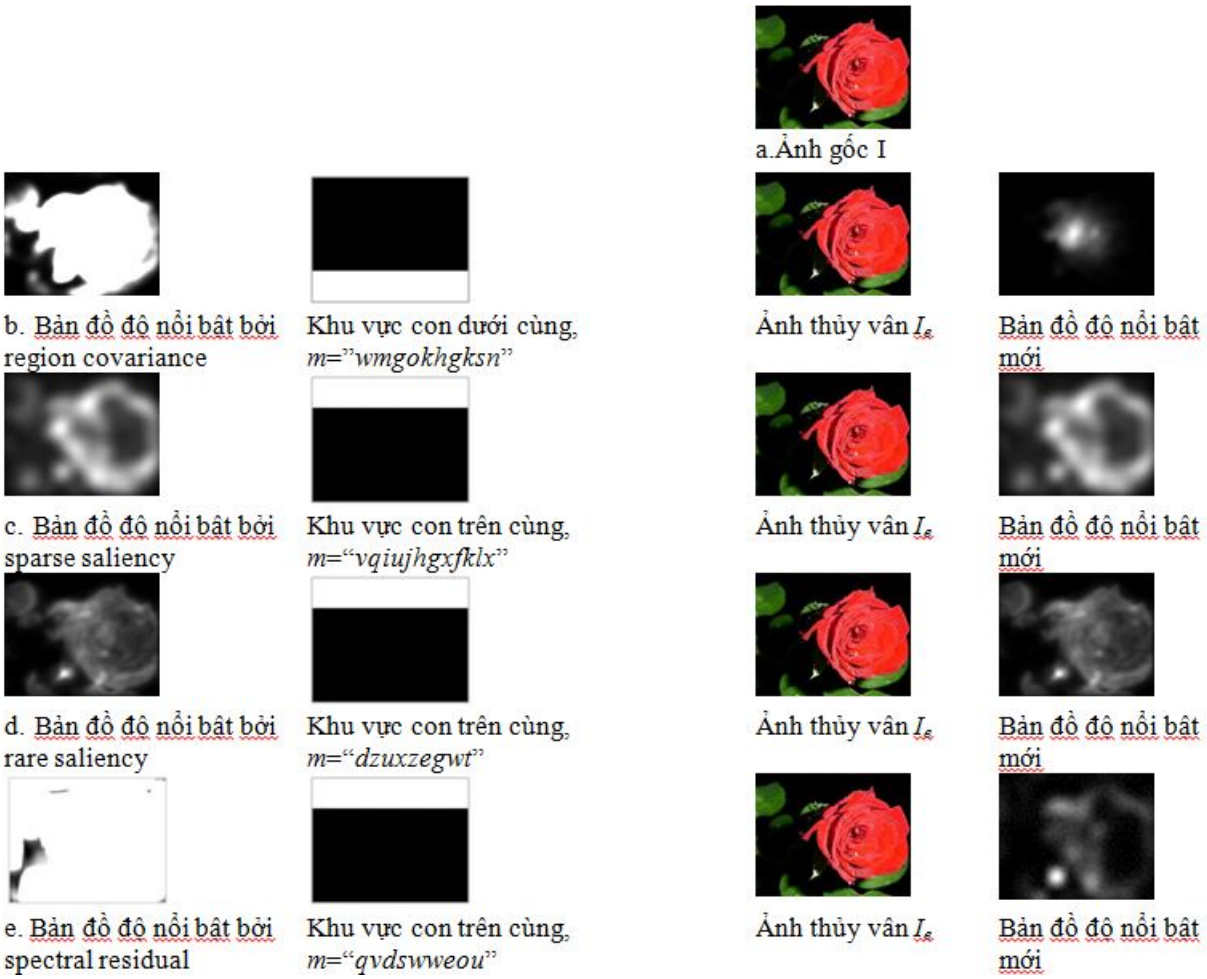
- Thủy vân được trích xuất từ các vùng này để xác thực tính nguyên vẹn và nguồn gốc của ảnh.

Phương pháp sử dụng SVM trong thủy vân số không chỉ tăng cường độ bảo mật và tính vô hình mà còn đảm bảo thủy vân vẫn ổn định dưới các biến đổi và tấn công. Bằng cách sử dụng SVM để phân loại và chọn lọc các vùng không nổi bật trong ảnh, phương pháp này đạt được hiệu quả cao trong việc bảo vệ quyền sở hữu trí tuệ và đảm bảo tính toàn vẹn của dữ liệu số.

### 2.2.2. Kết quả thực nghiệm

Nhiệm vụ xác định các khu vực cụ thể để thực hiện thủy vân số thông qua việc học đặc điểm không nổi bật đòi hỏi làm rõ tính bền vững vì hàm xác suất $L(\theta)$ theo (2.22) được kỳ vọng đạt 100% đối với một mô hình nổi bật đã chọn. Do đó, thử nghiệm của luận án đã tập trung vào việc tìm kiếm một số mô hình nổi bật thỏa mãn kỳ vọng đó. Phương pháp ban đầu của luận án cho việc học bao gồm độ nổi bật sử dụng hiệp phương sai vùng (saliency using region covariance) bởi [70], độ nổi bật thưa thớt (sparse saliency) bởi [71], độ nổi bật phổ tần số (spectral residual saliency) bởi [72] và độ nổi bật hiếm gặp (rare saliency) bởi [73].

Một tập dữ liệu về độ nổi bật chứa mười nghìn hình ảnh [77] được sử dụng trong các thí nghiệm học tập. Đối với tập dữ liệu này, các đối tượng nổi bật trong hình ảnh được đa dạng hóa. Một chuỗi ngẫu nhiên được tạo ra cho mỗi việc nhúng văn bản. Cơ sở dữ liệu hình ảnh được chia ngẫu nhiên thành hai tập dữ liệu: một tập dữ liệu để huấn luyện $DL$ và một tập dữ liệu để kiểm tra $DT$. Đối với mỗi mô hình độ nổi bật, quá trình đào tạo SVM được thực hiện để đạt được các kernel. Để chọn một phần vùng để ẩn thông điệp, SVM kiểm tra đặc trưng nổi bật $s$, được trích xuất từ bản đồ nổi bật của hình ảnh $I$. Một ví dụ được thể hiện trong hình 2.6(a): SVM với bản đồ nổi bật bởi phương pháp sử dụng hiệp phương sai vùng [70] đề xuất lấy phần vùng hàng đầu để ẩn một thông điệp *wmgokhgksn* dẫn đến hình ảnh mới $I_e$ và bản đồ nổi bật mới. Bản đồ này khác với bản đồ ban đầu. Lưu ý rằng thủy vân trong hình ảnh không thể nhận biết bằng mắt người. Sau khi có hai hình ảnh $I$ và $I_e$, sự khác biệt giữa chúng có thể được đo bằng độ chính xác (precision), độ nhớ (recall), độ đo $F$ (F-measure) [77] và sai số trung bình đối nghịch bình phương (MSE) [78], tổng của sự khác biệt tuyệt đối (Sum of Absolute Differences - SAD) [79], chỉ số đo lường sự tương đồng cấu trúc (SSIM) và tỷ lệ tín hiệu tối đa đến nhiễu (Peak Signal to Noise Ratio - PSNR) [80] để đánh giá sự giống nhau thay vì sự khác biệt. Nhóm đầu tiên đo đạc để học mức độ thay đổi hình ảnh bằng thủy vân số




***Hình 2.6:*** *Ví dụ về việc nhúng thủy vân bằng các mô hình độ nổi bật khác nhau*

***Bảng 2.1:*** *Tính toàn vẹn của thủy vân dựa trên đặc trưng không nổi bật (Các điểm số in đậm là tốt nhất, các điểm số in nghiêng là thứ hai)*

| Mô hình độ nổi bật | Precision | Recall | Fmeasure | rMSE |
|---|---|---|---|---|
| Covariance [70] | 0.8895 | 0.9947 | 0.9391 | 0.9638 |
| Highlighting [71] | **0.9266** | *0.9959* | **0.9573** | *0.9652* |
| Spectral [72] | 0.9154 | 0.9944 | 0.9505 | **0.9655** |
| Rare [73] | *0.9189* | **0.9965** | *0.9510* | 0.9651 |

***Bảng 2.2:*** *Đánh giá độ bền vững của bản đồ độ nổi bật và hiệu suất mã hóa thông điệp trong thủy vân số*

| A. Độ ổn định của bản đồ độ nổi bật | | | | | B. Tương ứng thông điệp | | |
|---|---|---|---|---|---|---|---|
| Mô hình độ nổi bật | Precision | Recall | Fmeasure | rMSE | *jw* distance | Thời gian mã hóa ($s$) | Thời gian giải mã ($s$) |
| Covariance [70] | 0.9365 | 0.9370 | 0.9367 | 0.9051 | 0.9017 | 0.2667 | 20.2770 |
| Highlighting [71] | **1.000** | **1.000** | **1.000** | **1.000** | **1.000** | 0.1269 | 0.1705 |
| Rare [72] | **1.000** | **1.000** | **1.000** | **1.000** | **1.000** | 0.0614 | 1.0465 |
| Spectral [73] | 0.9011 | 0.9053 | 0.9032 | 0.8545 | 0.8634 | 0.0462 | 0.1360 |

tạo ra báo cáo thống kê trong bảng 2.1.

Bảng 2.1 và bảng 2.2 trình bày kết quả đánh giá về tính vô hình và tính toàn vẹn của thủy vân số sử dụng bốn mô hình nổi bật: độ nổi bật sử dụng hiệp phương sai khu vực (Region Covariance Saliency) [70], độ nổi bật thưa (Sparse Saliency) [71], độ nổi bật tần số quang phổ (Spectral Residual Saliency) [72] và độ nổi bật hiếm (Rare Saliency) [73].

Trong bảng 2.1, các chỉ số precision, recall và f-measure được tính toán để đánh giá tính toàn vẹn của quá trình thủy vân. Kết quả cho thấy các phương pháp sử dụng độ nổi bật thưa thớt (sparse saliency) [71] và độ nổi bật hiếm (rare saliency) [73] đạt được điểm số cao nhất và thứ hai, cho thấy rằng hệ thống có khả năng nhận diện và tái tạo thông điệp nhúng một cách chính xác và hiệu quả. Điều này khẳng định rằng các khu vực nhúng thông điệp được Alice thực hiện luôn được Bob phát hiện đúng, một minh chứng quan trọng cho tính ổn định và độ tin cậy của phương pháp thủy vân số.

Bảng 2.2 trình bày kết quả đánh giá chi tiết về các yếu tố quan trọng của

thủy vân số, bao gồm tính toàn vẹn, tính vô hình, tính bền vững, và sự tương ứng thông điệp.

***Tính toàn vẹn:***

Các chỉ số precision, recall, và f-measure được tính toán để đánh giá khả năng hệ thống trong việc tái tạo và nhận diện thông điệp nhúng một cách chính xác và hiệu quả. Kết quả cho thấy các mô hình độ nổi bật thưa thớt (sparse saliency) [71] và độ nổi bật hiếm (rare saliency) [73] đạt được các điểm số cao nhất, chứng tỏ rằng những khu vực nhúng thông điệp của Alice luôn được Bob phát hiện đúng. Điều này khẳng định tính toàn vẹn của thông điệp được bảo đảm trong suốt quá trình xử lý.

***Tính vô hình:***

Chỉ số rMSE (root Mean Squared Error) được sử dụng để đánh giá mức độ sai lệch giữa hình ảnh gốc và hình ảnh đã nhúng thủy vân. Kết quả cho thấy các mô hình độ nổi bật thưa thớt (sparse saliency) [71] và độ nổi bật hiếm (rare saliency) [73] có giá trị rMSE thấp nhất, chứng tỏ rằng sự sai lệch là rất nhỏ, đảm bảo tính vô hình cao của thủy vân.

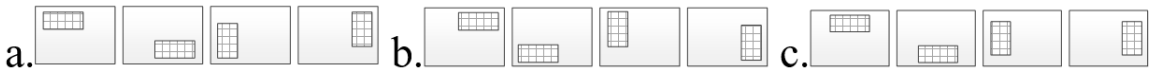
***Tính bền vững:***

Các chỉ số như MSE (Mean Squared Error), SAD (Sum of Absolute Differences), SSIM (Structural Similarity Index Measure) và PSNR (Peak Signal-to-Noise Ratio) được sử dụng để đánh giá tính bền vững của thủy vân dưới các tác động khác nhau. Kết quả cho thấy các mô hình độ nổi bật thưa thớt (sparse saliency) [71] và độ nổi bật hiếm (rare saliency) [73] đều có giá trị MSE và SAD rất thấp, SSIM đạt giá trị tối đa là 1.0 và PSNR cao nhất, chứng tỏ rằng hệ thống có khả năng giữ nguyên vẹn chất lượng hình ảnh sau khi nhúng thủy vân, đồng thời đảm bảo sự bền vững của thông điệp nhúng.

***Sự tương ứng thông điệp:***

Khoảng cách Jaro-Winkler (thước đo sự tương đồng giữa hai chuỗi ký tự) được sử dụng để đánh giá mức độ tương ứng thông điệp sau khi nhúng và tái tạo. Kết quả cho thấy các mô hình độ nổi bật thưa thớt (sparse saliency) [71] và độ nổi bật hiếm (rare saliency) [73] có điểm số Jaro-Winkler cao nhất, minh chứng cho sự tương ứng chính xác giữa thông điệp ban đầu và thông điệp được tái tạo.

Kết quả từ bảng 2.2 cho thấy tất cả các mô hình đều có hiệu suất tốt trong việc đảm bảo tính toàn vẹn, tính vô hình, tính bền vững, và sự tương ứng




***Hình 2.7:*** *Các ví dụ về sắp xếp các khu vực con với các cách căn chỉnh khác nhau: a. trái, b. phải, c. giữa*

thông điệp của thủy vân số. Đặc biệt, các mô hình độ nổi bật thưa thớt (sparse saliency) [71] và độ nổi bật hiếm (rare saliency) [73] nổi bật hơn với các điểm số tốt nhất, khẳng định rằng phương pháp thủy vân đề xuất có thể được áp dụng mạnh mẽ trong các ứng dụng thực tế.

Trong quá trình phát triển mối quan hệ giữa các đặc trưng nổi bật và việc chọn một khu vực con để ẩn thông điệp, SVM trong các kỹ thuật học máy đã được áp dụng. Độ ổn định hiệu quả của phương pháp độ nổi bật thưa thớt (sparse saliency) [71] và phương pháp độ nổi bật hiếm (rare saliency) [73] đã được thu thập từ thử nghiệm trên tập dữ liệu riêng biệt. Độ nổi bật nhạy cảm với sự thay đổi của hình ảnh thông qua việc tỉ lệ, cắt và xoay. Do đó, khả năng chống lại tấn công thủy vân dựa trên độ nổi bật rất nhạy cảm với sự thay đổi của hình ảnh chứa thủy vân. Thủy vân dựa trên văn bản thường dễ bị hỏng hơn so với thủy vân dựa trên hình ảnh vì nó yêu cầu tính đúng đắn ở mức bit cho quá trình giải mã. Kết quả là, nó có thể bị ảnh hưởng bởi các cuộc tấn công độc hại như việc thay đổi kích thước hoặc xoay hình ảnh. Để tránh vấn đề này, văn bản có thể được chuyển thành một hình ảnh nhỏ sau đó được nhúng vào một khu vực con của hình ảnh chứa thủy vân. Khả năng thiết kế một tập hợp các khu vực con để nhúng thông tin là rất lớn. Tập hợp được hiển thị trong hình 2.3 là cách đơn giản nhất với các hình chữ nhật được phân bổ dọc theo mép hình ảnh. Một phiên bản thay thế của tập hợp bao gồm việc thay đổi kích thước hình chữ nhật thành kích thước nhỏ hơn và di chuyển các hình chữ nhật vào trung tâm hình ảnh bằng một khoảng cách nhỏ bí mật (hình 2.7). Tập hợp các khu vực con được định nghĩa trước để ẩn thông tin được sử dụng như một khóa riêng tư trong quá trình thủy vân.

Bởi vì nhiệm vụ ẩn thông tin bằng một tập hợp cụ thể các khu vực con làm thay đổi biểu đồ nổi bật một cách đặc thù theo tập hợp, điều này gợi ý thực hiện việc học bằng SVM cho mỗi tập hợp các khu vực con và kiểm tra tính bền vững của thuật toán đối với cấu hình các khu vực con bằng cách sử dụng công thức (2.22) trước khi sử dụng tập hợp đó cho việc nhúng thủy vân.

## 2.3. Thủy vân dựa trên đặc trưng độ nổi bật của ảnh số

Khi ẩn thông tin vào trong một hình ảnh gốc, các loại đặc điểm hình ảnh khác nhau có thể được sử dụng như một khóa bí mật. Phương pháp thủy vân phân tích mật mã được công nhận là giải pháp cải thiện độ mạnh mẽ cho các hệ thống xác thực và chống giả mạo từ các cuộc tấn công. Công trình này đóng góp một kỹ thuật mới sử dụng các đặc điểm nổi bật để thiết lập một khóa bí mật và sau đó áp dụng khóa đó như một tham số cho cả việc nhúng và trích xuất thủy vân. Tuy nhiên, có sự thay đổi của các đặc điểm hình ảnh thông qua việc chèn thông tin trong quá trình nhúng thủy vân. Luận án đề xuất sử dụng phương pháp học cùng với các mô hình nổi bật, để đảm bảo độ mạnh mẽ trong việc trích xuất thủy vân. Ở đây, phương pháp thủy vân hình ảnh được mô tả với việc học SVM và sự hỗ trợ của một số mô hình nổi bật. Kết quả của luận án cho thấy phương pháp thủy vân phân tích mật mã đủ để đạt được tính vô hình và ổn định của thủy vân. Kết quả thực nghiệm trên một chuẩn mực chỉ ra lợi thế của phương pháp dựa trên đặc điểm nổi bật cho các ứng dụng chống giả mạo.

Do các vùng con trong hình ảnh được chú ý cao về khả năng nhìn thấy [81] được xem là các phần quan trọng của hình ảnh, chúng thường không bị loại bỏ trong quá trình chỉnh sửa hình ảnh. Do đó, việc nhúng thủy vân một cách rõ ràng vào các vùng con nổi bật là phương pháp hợp lý để tăng cường sự chú ý đến bản quyền văn bản. Hơn nữa, các khu vực hình ảnh ít được chú ý đến về khả năng nhìn thấy có tiềm năng cao để nhúng thủy vân dự kiến sẽ không thể phát hiện được. Phương pháp thứ hai thuộc về kỹ thuật ẩn tin (steganography) hỗ trợ cho giao tiếp ẩn. Giả định rằng phương pháp mã hóa trong kỹ thuật thủy vân dựa trên độ nổi bật vô hình không gây ra suy giảm chất lượng hình ảnh và do đó khu vực có dấu vết được nhúng vẫn không nổi bật thì thủy vân không thể phát hiện như mong đợi. Tuy nhiên, quá trình mã hóa làm thay đổi hình ảnh và các khu vực không nổi bật của hình ảnh đã mã hóa chắc chắn không giống hệt như hình ảnh gốc.

Biến thể lớn của các mô hình độ nổi bật trong việc phân bổ khu vực nổi bật có nghĩa là mỗi phương pháp phân tích kỹ thuật ẩn tin dựa trên độ nổi bật phải được tích hợp tương ứng với mô hình độ nổi bật để đảm bảo độ mạnh mẽ của thủy vân sau khi giải mã. Do đó, đóng góp chính của công trình này là thích ứng các đặc điểm nổi bật để thiết lập một khóa bí mật và sau đó áp dụng khóa

đó như một tham số cho cả quá trình nhúng thủy vân và trích xuất thủy vân. Luận án cũng đề xuất việc học đặc điểm nổi bật, nhận biết cách tạo khóa bí mật từ đặc điểm nổi bật và đảm bảo độ mạnh mẽ của quá trình trích xuất thủy vân, cải thiện đáng kể hiệu suất của nó.

Như đã đề cập ở trên, phương pháp chú ý thị giác có nhiều điểm tương đồng với việc trích xuất đặc điểm hình ảnh; mặc dù ưu tiên nhiều hơn cho sự chú ý thị giác và việc giải thích khu vực, nơi khu vực đó có sự quan tâm thị giác nhiều nhất. Sự chú ý thị giác như vậy đã phân đoạn các khu vực quan tâm thị giác; điều này có thể được coi là ý tưởng đáng khuyến khích nếu một khu vực của hình ảnh gốc là phù hợp cho việc nhúng thủy vân và không ảnh hưởng đến chất lượng thị giác được cảm nhận.

Luận án sẽ thảo luận một số nguyên tắc của việc ước lượng sự chú ý thị giác. Để xác định phát hiện độ nổi bật dựa trên cấu trúc dữ liệu cục bộ của hình ảnh [82], sự tương đồng của đặc điểm tại một điểm pixel quan tâm so với các điểm xung quanh của nó cần được đo lường. Trong một mục khác [71], vị trí của phần nền thưa thớt được ước lượng trên nền thưa thớt với biến đổi cosine rời rạc (DCT). Nghiên cứu cũng đã được thực hiện về đo lường tương phản cục bộ và độ hiếm toàn cầu [73] cho việc trích xuất đặc điểm. Mô tả tương phản so với các khu vực lân cận và ngoại vi được chọn một cách ngẫu nhiên, phân biệt mục tiêu và yếu tố gây xao lãng là phương pháp đánh giá độ nổi bật [83].

Tiếp theo, luận án sẽ thảo luận về một số công trình liên quan đến thủy vân số được xem là một trong những phương pháp dựa trên sự chú ý thị giác bởi vì chúng liên quan đến phương pháp tiếp cận của luận án. Vì bản đồ độ nổi bật thể hiện mức độ nổi bật, các khu vực nổi bật và không nổi bật về mặt thị giác có thể được phát hiện. Để tránh ảnh hưởng đến chất lượng thị giác được cảm nhận khi mã hóa thủy vân vào hình ảnh chủ, thủy vân có độ mạnh mẽ thấp và cao được nhúng vào các khu vực nổi bật và không nổi bật về mặt thị giác, tương ứng [84]. Phương pháp sử dụng của sóng wavelet đã được đề xuất như một công cụ cho quá trình thủy vân. Ngược lại, trong công trình này luận án giới thiệu việc học độ nổi bật thay vì sóng wavelet để chọn khu vực phù hợp cho việc nhúng thủy vân mà không ảnh hưởng đến chất lượng thị giác được cảm nhận. Trong lĩnh vực thủy vân số, có sự quan tâm đến kỹ thuật ẩn tin (steganography) để nhúng các bit thông điệp vào trong một ảnh gốc như kỹ thuật ghép khớp bit ít quan trọng nhất (LSB matching). Trong phương pháp này, việc lựa chọn nhúng hoặc trích xuất thủy vân từ điểm ảnh hình ảnh gốc là ngẫu nhiên. Trong cải

tiến của LSB bởi [85], sự thay đổi trong ảnh gốc được loại bỏ bằng cách sử dụng lựa chọn thiết lập một hàm nhị phân của hai pixel ảnh bìa thành giá trị mong muốn. Cải tiến tiếp theo bởi [86] thông qua việc tính toán ma trận điểm số để tìm ra giải pháp gần tối ưu nhất trong tất cả các thứ tự hoán vị.

Như một ứng dụng của LSB, các bit của thủy vân được cấy vào vị trí ít quan trọng nhất của ảnh [32]. Tuy nhiên, trong đề xuất của luận án, khái niệm của LSB được áp dụng để thay đổi ảnh gốc bằng thủy vân với sự hỗ trợ của độ nổi bật. Ở đây, lựa chọn việc nhúng hay trích xuất thủy vân từ pixel ảnh gốc dựa trên giá trị độ nổi bật. Từ góc độ độ nổi bật thị giác, các khu vực quan tâm (ROIs) có thể trình bày thông tin thiết yếu của ảnh. Thủy vân mạnh mẽ được sử dụng bởi [30] được nhúng vào hệ số DCT của ROIs trong khi thủy vân dễ vỡ được nhúng vào băng tần phụ thấp hoặc ảnh đã được đánh dấu thủy vân. Một phương pháp dựa trên độ nổi bật cho việc đánh dấu thủy vân được đề xuất trong luận án này, cho phép áp dụng các mô hình độ nổi bật khác nhau để ước lượng độ nổi bật. Theo cách này, thông tin phụ khu vực được đánh giá với đặc điểm dựa trên độ nổi bật với độ tin cậy cao về sự thay đổi thấp khi nhúng thủy vân.

### 2.3.1. Phương pháp dựa trên độ nổi bật để chống giả mạo

Thuật toán đánh dấu thủy vân ảnh sử dụng đặc trưng độ nổi bật (SGW) được trình bày ở đây nhằm mục đích chống giả mạo [12]. Do đó, thủy vân thường là loại dễ vỡ để bảo vệ dữ liệu. Một cách tương tự với [13], luận án sử dụng các khái niệm toán học để biểu đạt quá trình đánh dấu thủy vân. Nhiệm vụ nhúng thông tin có thể so sánh với mã hóa trong quan điểm phân tích mật mã và cụ thể được mô tả bởi hàm (2.24) ánh xạ ảnh gốc $u$, thủy vân $w$ và khóa $k$ vào ảnh đã nhúng/mã hóa $v$. Điều này có nghĩa là $k$ có thể không được bao gồm. Nhiệm vụ trích xuất thông tin, tương đương với giải mã trong lĩnh vực phân tích mật mã, được hình thành bởi hàm (2.25).

$$v = \text{encode}(u, w, \langle k \rangle) \tag{2.24}$$

$$w = \text{decode}(v, \langle u \rangle, \langle k \rangle) \tag{2.25}$$

Nhiều mô hình độ nổi bật tồn tại có thể được sử dụng như một phương tiện phát hiện đặc trưng cho ảnh gốc, sau đó khóa $k$ có thể được tạo ra từ đặc trưng đó. Nhờ đó, hàm mã hóa (2.24) có thể có khóa ẩn và hàm giải mã (2.25)

có thể ước lượng khóa từ danh sách đầu vào (2.26). Hơn nữa, chỉ có ảnh đã mã hóa $v$ được sử dụng cho hàm giải mã (2.27). Quá trình kiểm tra chống giả mạo mù cuối cùng được thể hiện bởi hàm (2.28), trả về có hoặc không nếu tồn tại thủy vân $w$ trong ảnh $v$.

$$v = \text{encode}(u, w) \tag{2.26}$$

$$w = \text{decode}(v) \tag{2.27}$$

$$b = \text{detect}(v, w), \quad b \in \{0, 1\} \tag{2.28}$$

Trong phương pháp này, một cách tiếp cận đa phụ khu vực được áp dụng. Điều này là do không gian miền của ảnh gốc tự nhiên là mặt phẳng Descartes 2D và có nhiều cách để chia không gian thành các vùng con $r_i$ để nhúng thủy vân. Do đó, đối với mỗi ảnh trong tập dữ liệu huấn luyện $L$, đặc trưng độ nổi bật có thể được tính toán cho các phụ khu vực của nó. Điều này cho phép xác định một ma trận đặc trưng độ nổi bật f bằng cách sử dụng (2.29).

$$f_i^j = \text{saliency}\left(u\left(r_i^j\right)\right), \quad i = 1, n, j \in L \tag{2.29}$$

Trong việc chia không gian ảnh thành các vùng con để ẩn thủy vân, việc chọn vị trí của các vùng con là quan trọng. Trong trường hợp đánh dấu thủy vân chống giả mạo, vùng con nên được đặt gần các biên của ảnh nơi thường quan sát thấy không có độ nổi bật. Cách sắp xếp đơn giản bao gồm bốn hình chữ nhật nhỏ (n=4) có các cạnh dài tiếp giáp với các cạnh của ảnh. Với các phiên bản khác nhau bằng cách mã hóa thủy vân trong vùng con $r_i$, luận án muốn xác định một vùng con nơi đặc trưng độ nổi bật thay đổi ít nhất khi nhúng thủy vân. Sau khi áp dụng mô hình độ nổi bật cho mỗi khu vực, trước và sau khi mã hóa, sự biến đổi có thể được ước lượng bằng (2.30). Tại thời điểm đó, một vùng con có liên quan đến sự biến đổi nhỏ nhất được nêu bằng cách chỉ ra chỉ số của nó (2.31).

$$d_i^j = \left\| \text{saliency}\left(u\left(r_i^j\right)\right) - \text{saliency}\left(v\left(r_i^j\right)\right) \right\|, i = 1, n \tag{2.30}$$

$$i_*^j = \text{argmin}_i \, d_i^j \tag{2.31}$$

Sau khi đã xác định chỉ số của vùng con (2.32) như một phân lớp, luận án tiếp tục quá trình huấn luyện tập dữ liệu từ (2.27) để thu được kernel $K$. Với

mục đích này, có thể áp dụng nhiều phương pháp học máy. Trong phạm vi của luận án này, máy vector hỗ trợ (SVM) [48] được chọn để thực hiện bởi vì khả năng của nó trong việc phân loại phi tuyến một cách hiệu quả, bằng cách ánh xạ ngầm các đầu vào vào không gian đặc trưng đa chiều (2.32).

$$K = \text{training}\left(f^{j}_{i=1:n}, i^{j}_{*}\right), j \in L \tag{2.32}$$

Ở giai đoạn kiểm tra, luận án có ma trận dữ liệu $f$ (2.33) với các hàng trong đó] mỗi hàng chứa đặc trưng độ nổi bật của vùng con từ các ảnh kiểm tra $T$. Kernel $K$ đã học mang lại lợi ích để ước lượng một vùng con nơi đặc trưng độ nổi bật có thể thay đổi ít nhất khi nhúng thủy vân (2.34). Chỉ số của vùng con đóng vai trò như một khóa bí mật cho việc đánh dấu thủy vân ở cả hai giai đoạn mã hóa và giải mã.

$$f^{k}_{i} = \text{saliency}\left(u\left(r_i\right)\right), i = 1, n, k \in T \tag{2.33}$$

$$i^{j}_{*} = \text{test}\left(f^{j}_{i=1:n}, K\right), j \in T \tag{2.34}$$

Ma trận đặc trưng dựa trên mô hình độ nổi bật ước lượng sự chú ý thị giác cho không gian ảnh gốc (2.26). Tại đây, luận án áp dụng bốn phương pháp phát hiện độ nổi bật. Mô hình đầu tiên sử dụng sự giống nhau của một pixel $x$ với môi trường xung quanh $y$ để ước lượng độ nổi bật bằng cách sử dụng độ đo SR (Self-Resemblance) [82] bởi (2.35). Lưu ý rằng sự tương đồng cosine được sử dụng cho việc tính toán SR.

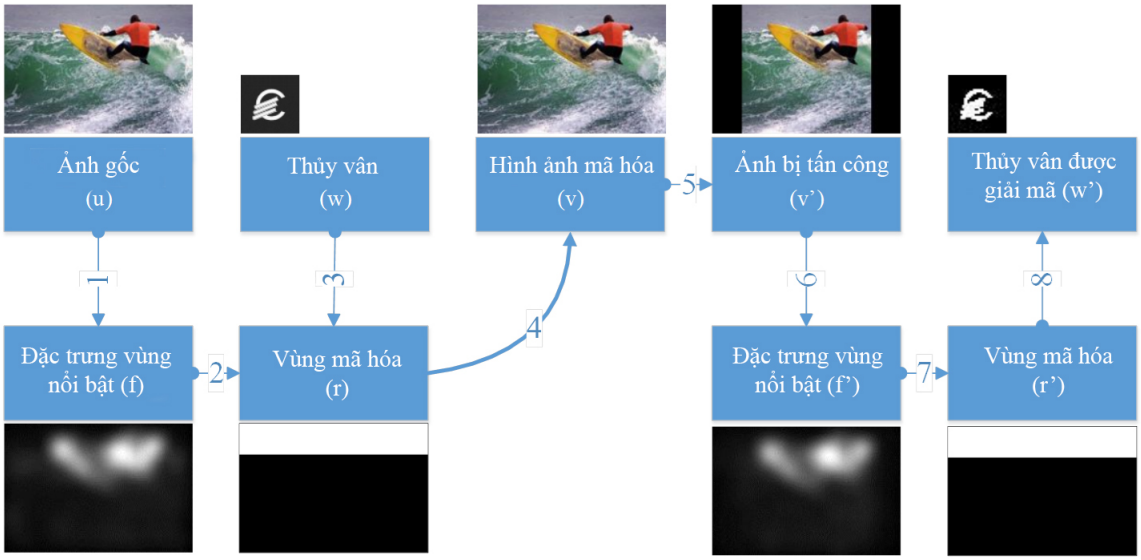
$$\text{saliency}^{SR}(u(x)) = \frac{1}{\sum_y \exp\left(\frac{-1+d_{\text{cosine}}((u(x),u(y))}{\sigma^2}\right)} \tag{2.35}$$

Trong trường hợp sử dụng độ đo SSM (Sparse Signal Mixing), độ nổi bật được ước lượng dựa trên vị trí không gian của một nền trước rời rạc ẩn trong một nền sau rời rạc về mặt quang phổ [71] bởi (2.36,2.37) với giả định rằng nền của ảnh được hỗ trợ rời rạc trong cơ sở của biến đổi cosine rời rạc (Discrete Cosine Transform, DCT) và $g$ là một kernel Gaussian.

$$\ddot{u} = iDCT(\text{sign}(DCT(u))) \tag{2.36}$$

$$\text{saliency}^{SSM}(x) = g * (\ddot{u} \circ \ddot{u}) \tag{2.37}$$

Phân tích từ cơ sở cho thấy việc so sánh các đặc trưng sáng và màu sắc ở




***Hình 2.8:*** *Quy trình đánh dấu thủy vân với các đặc trưng độ nổi bật bằng thuật toán SGW*

cấp độ thấp tạo ra các đặc trưng ở cấp độ trung bình như hướng của ảnh [73]. Tiếp theo, việc lượng tử hóa sự hiếm gặp qua các tỷ lệ khác nhau được thực hiện dựa trên xác suất xuất hiện của các điểm ảnh để ước lượng độ nổi bật, với giả định rằng các đặc trưng có độ tương phản cao một cách cục bộ và hiếm gặp một cách toàn cục là nổi bật (2.38).

Ở đây, $c$ là tỷ lệ và $o_k$ là giá trị xuất hiện của điểm ảnh $u(x)$ tại tỷ lệ thứ $k$ hoặc cấp độ độ phân giải.

$$\text{saliency}^{RARE}(x) = -\log\left(\frac{1}{c\|u(x)\|}\sum_{k=1}^{c} o_k\right) \tag{2.38}$$

Sau thành công của phân tích thành phần chính (PCA) [87], việc ước lượng độ nổi bật thị giác được dựa vào PCA để phân biệt giữa các đối tượng thị giác và các phần gây phân tâm [83]. Ở đây, việc chiếu các bức ảnh lên các không gian con khác nhau cho phép đánh giá độ tương phản trung bình giữa các điểm ảnh lân cận được chọn một cách ngẫu nhiên cho mỗi đoạn ảnh. Tiếp theo, quá trình học để lựa chọn và kết hợp các không gian con dẫn đến việc tìm kiếm giải pháp tối ưu về trọng số (2.39) và ước lượng độ nổi bật (2.40), trong đó $\phi$ là độ tương phản ngẫu nhiên (RC) cho một đoạn ảnh, $K$ là tập dữ liệu ảnh huấn luyện, $T$ và $D$ là các tập hợp các mục tiêu và yếu tố gây phân tâm cho ảnh $u$.

$$w^* = \min_w \sum_K \sum_T \sum_D \exp\left(w^T\phi(D) - w^T\phi(T)\right) \tag{2.39}$$

$$\text{saliency}^{RC}(x) = w^{*}\phi(u) \tag{2.40}$$

Để quản lý độ phức tạp của kỹ thuật ẩn tin, luận án này áp dụng thuật toán biến đổi Arnold [88] cho việc mã hóa thủy vân ban đầu thông qua công thức (2.41). Tiếp theo, bằng cách áp dụng khái niệm của LSB, thủy vân được kết hợp với LSB cùng với kênh màu xanh của vùng $r_{i*}$ dưới sự hướng dẫn của đặc trưng độ nổi bật $f$ thông qua công thức (2.42).

$$\text{cw}_A = \text{Arnold}(w) \tag{2.41}$$

$$v = \text{mixing}_{LSB}\left(w_A, u\left(r_{i*}\right), f\left(r_{i*}\right)\right) \tag{2.42}$$

Quy trình giải mã được khởi đầu bằng cách phát hiện thủy vân $w_A$ từ khu vực đã mã hóa trong kênh màu xanh của hình ảnh $v$ sử dụng công thức (2.43) với LSB và dựa vào đặc trưng độ nổi bật. Cuối cùng, phép biến đổi Arnold đảo ngược sẽ trích xuất ra thủy vân $w$ từ $w_A$.

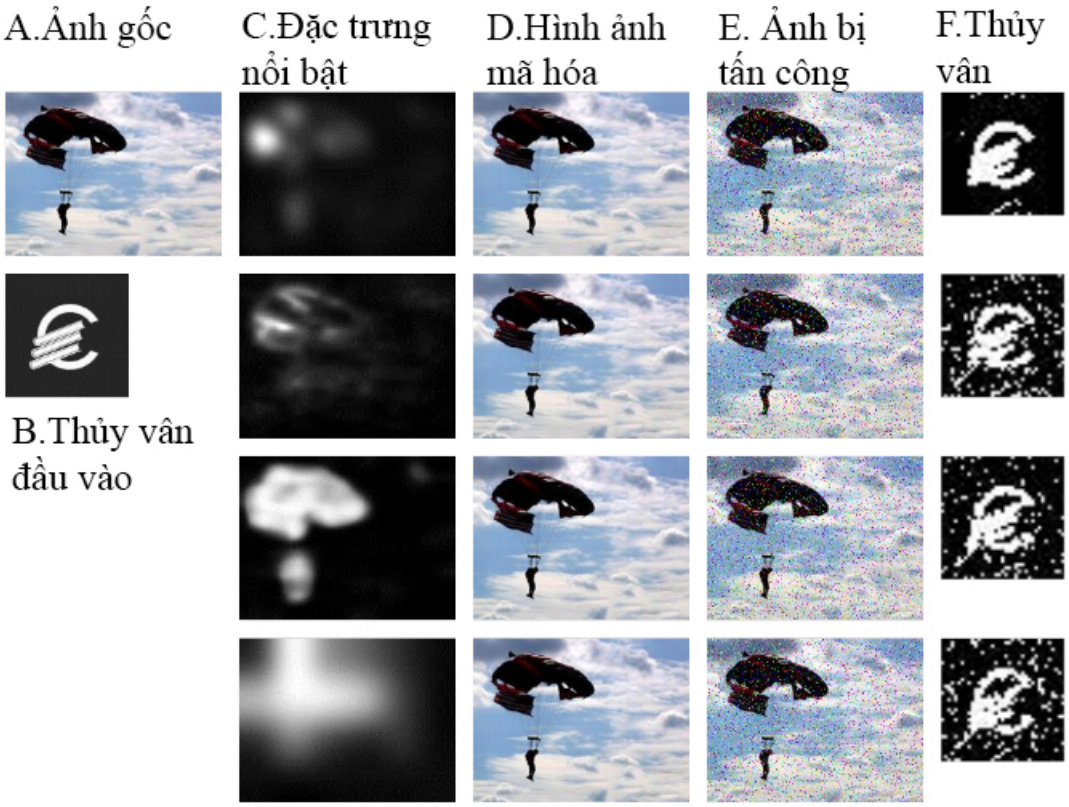
$$\text{w}_A = \text{detect}_{LSB}(v(r_{i*}), f(r_{i*})) \tag{2.43}$$

$$w = i\,\text{Arnold}\left(w_A\right) \tag{2.44}$$

Luận án đã nghiên cứu làm thế nào tìm ra đặc trưng ảnh từ các mô hình độ nổi bật khác nhau (2.29-2.31), không phụ thuộc vào phương pháp ước lượng của chúng như SR [82], SSM [71], RARE [73] và RC [83], có thể được áp dụng cho các tác vụ mã hóa và giải mã thủy vân. Hình 2.8 mô tả quá trình đánh dấu thủy vân cho một ví dụ về ảnh gốc $u$. Sau khi đánh giá độ nổi bật cho ảnh, đặc trưng độ nổi bật $f$ cho từng vùng con được định nghĩa. Tại đây, kernel SVM giúp chọn lọc một vùng con $r$ được định vị ở phần trên của ảnh. Vì thủy vân $w$ được nhúng, phiên bản mới của ảnh gốc $v$ có sự khác biệt nhỏ so với phiên bản ban đầu của nó. Thêm vào đó, ảnh có thể bị tấn công, chẳng hạn như bằng cách cắt bớt. Một khi đặc trưng độ nổi bật $f'$ cho ảnh $v'$ được phát hiện, kernel SVM một lần nữa chỉ ra vùng con $r'$ mà thủy vân được nhúng vào. Do đó, thủy vân $w'$ có thể được giải mã.

### 2.3.2. Kết quả thực nghiệm

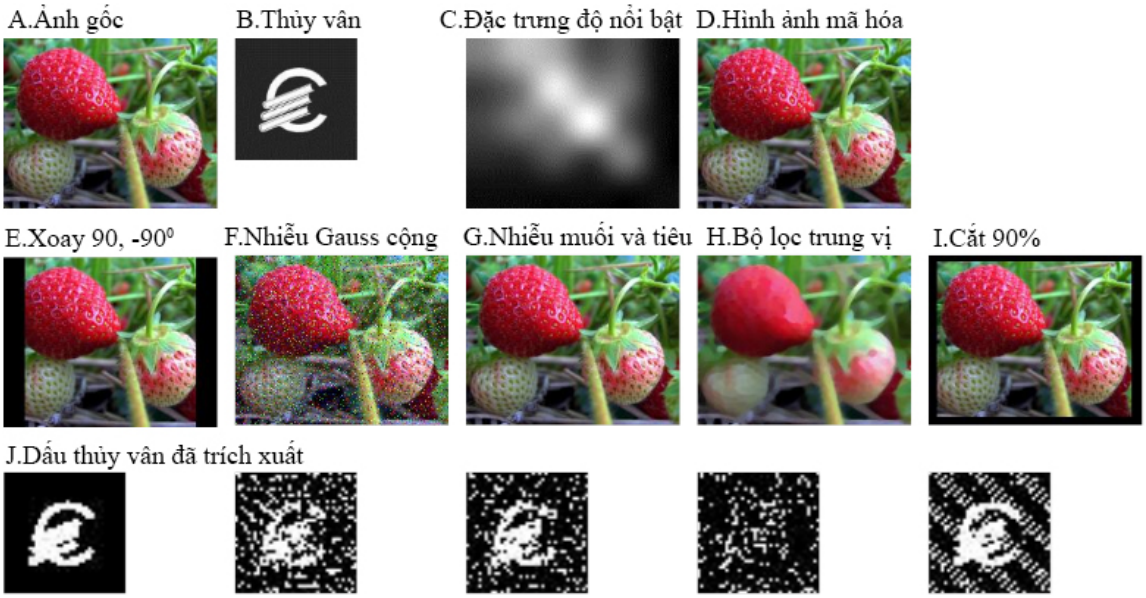
Phần này bàn về tính ổn định của phương pháp được mô tả kèm theo một số mô hình độ nổi bật nhất định. Luận án đã thử nghiệm phương pháp trên bộ




***Hình 2.9:*** *Nhúng một logo đen trắng vào ảnh 112691.jpg từ MSRA10K, áp dụng bốn mô hình độ nổi bật: SR [82] ở hàng đầu tiên, SSM [71] - hàng thứ hai, RARE [73] - hàng thứ ba và RC [83] - hàng thứ tư.*

dữ liệu đối tượng nổi bật MSRA10K [89] gồm 10.000 hình ảnh thực tế. Bộ dữ liệu được chia một cách ngẫu nhiên thành bộ huấn luyện và bộ kiểm tra. Bằng cách tiến hành thí nghiệm với bốn mô hình độ nổi bật, luận án so sánh hiệu năng sử dụng các kernel được sinh ra bởi máy vector hỗ trợ (SVM). Ngoài ra, bài kiểm tra tấn công bao gồm các loại tấn công đa dạng như phóng to/thu nhỏ, xoay, nhiễu Gauss cộng, nhiễu muối và tiêu, cân bằng histogram, lọc trung vị, và cắt ảnh.

Hình 2.9 mô tả một ví dụ về việc nhúng một logo màu đen trắng vào ảnh có tên là 112691.jpg từ MSRA10K, sử dụng bốn mô hình độ nổi bật SR [82], SSM [71], RARE [73] và RC [83] (hình 2.9C). Như kỳ vọng, việc tấn công bằng nhiễu Gauss cộng đã làm cho ảnh gốc chứa mã bị nhiễu (hình 2.9E). Các hình ảnh chứa dấu thủy vân được giải mã từ bốn trường hợp bị suy giảm ở các mức độ khác nhau do tấn công nhiễu và các đặc điểm độ nổi bật được hướng dẫn (hình 2.9F). Một ví dụ về các cuộc tấn công được thể hiện trong hình 2.9 và 2.10. Đối với một hình ảnh gốc (A) và dấu thủy vân (B), hình ảnh được mã hóa (D) được tạo ra dưới sự hỗ trợ của đặc điểm độ nổi bật (C).




***Hình 2.10:*** *Nhúng một logo đen trắng vào ảnh 113516.jpg từ MSRA10K, áp dụng bốn mô hình độ nổi bật: SR [82] ở hàng đầu tiên, SSM [71] - hàng thứ hai, RARE [73] - hàng thứ ba và RC [83] - hàng thứ tư.*

Sau đó, ảnh sẽ chịu các tấn công như xoay 90°, -90° (F), áp dụng nhiễu Gauss cộng (F), nhiễu muối và tiêu (G), lọc trung vị (H) và cắt bớt 90% (I). Dấu thủy vân được trích rút từ các ảnh sau khi bị tấn công cho thấy mức độ suy giảm khác nhau (J). Có thể nhận thấy, sự suy giảm do xoay 90°, -90° (F) là không đáng kể, trong khi đó sự suy giảm nặng nề được gây ra bởi bộ lọc trung vị. Các cuộc tấn công khác cũng gây ra sự suy giảm đáng kể nhưng vẫn giữ lại được phần lớn dấu thủy vân.

Luận án đã kiểm tra tính vô hình của thủy vân bằng cách so sánh từng cặp ảnh gốc và ảnh đã mã hóa, đánh giá dựa trên các độ đo về Recall, Rrecision, F-measure [90], tổng của các khác biệt tuyệt đối (SAD) [91], độ tương đồng cấu trúc (SSIM) [92], sai số bình phương trung bình (MSE) [79] và PSNR [93]. Do các thủy vân đã giải mã bị suy giảm bởi các cuộc tấn công, chúng được so sánh với phiên bản ban đầu để làm nổi bật tính dễ bị tổn thương của thủy vân.

Bảng 2.3 cung cấp một cái nhìn tổng quan về tính vô hình và tính toàn vẹn của thủy vân trong các mô hình nổi bật SR, SSM, RARE, và RC. Các chỉ số được báo cáo trong bảng bao gồm độ chính xác, Recall, F-measure (F1-score), MSE (Mean Squared Error), SAD (Sum of Absolute Differences), SSIM (Structural Similarity Index Measure), và PSNR (Peak Signal-to-Noise Ratio).

Cả bốn mô hình đều đạt được độ chính xác và Recall cao (0.99) và F-measure gần như tuyệt đối (99.99), cho thấy khả năng duy trì tính toàn vẹn của

***Bảng 2.3:*** *Tính vô hình và tính toàn vẹn của thủy vân*

| Độ nổi bật | Độ chính xác | Recall | Fmeasure | MSE | SAD | SSIM | PSNR |
|---|---|---|---|---|---|---|---|
| SR | 0.99 | 0.99 | 99.99 | 0.0002 | 0.0002 | 1.0 | **97.57** |
| SSM | 0.99 | 0.99 | 99.99 | **0.0001** | **0.0001** | 1.0 | 97.56 |
| RARE | 0.99 | 0.99 | 99.99 | **0.0001** | **0.0001** | 1.0 | 97.56 |
| RC | 0.99 | 0.99 | 99.99 | 0.0002 | 0.0002 | 1.0 | 97.34 |

thủy vân rất tốt. Các giá trị này phản ánh rằng hệ thống có khả năng cao trong việc nhận diện và khôi phục thủy vân, đồng thời giảm thiểu lỗi khi nhúng và truy xuất thông tin.

Về tính vô hình, các chỉ số MSE và SAD của các mô hình SSM và RARE thấp nhất (0.0001) cho thấy mức độ sai lệch giữa hình ảnh gốc và hình ảnh đã nhúng thủy vân là rất nhỏ, đảm bảo rằng chất lượng hình ảnh gốc hầu như không bị ảnh hưởng. Mô hình SR và RC có giá trị MSE và SAD cao hơn một chút (0.0002) nhưng vẫn ở mức rất thấp, điều này đảm bảo rằng sự biến dạng hình ảnh là không đáng kể sau khi nhúng thủy vân.

Cả bốn mô hình đều đạt SSIM tối đa là 1.0, chứng minh sự tương đồng cấu trúc giữa hình ảnh gốc và hình ảnh sau khi nhúng thủy vân là hoàn hảo. PSNR của các mô hình SR, SSM, RARE, và RC lần lượt là 97.57, 97.56, 97.56 và 97.34, cho thấy rằng chất lượng hình ảnh sau khi nhúng thủy vân vẫn giữ được độ trung thực cao.

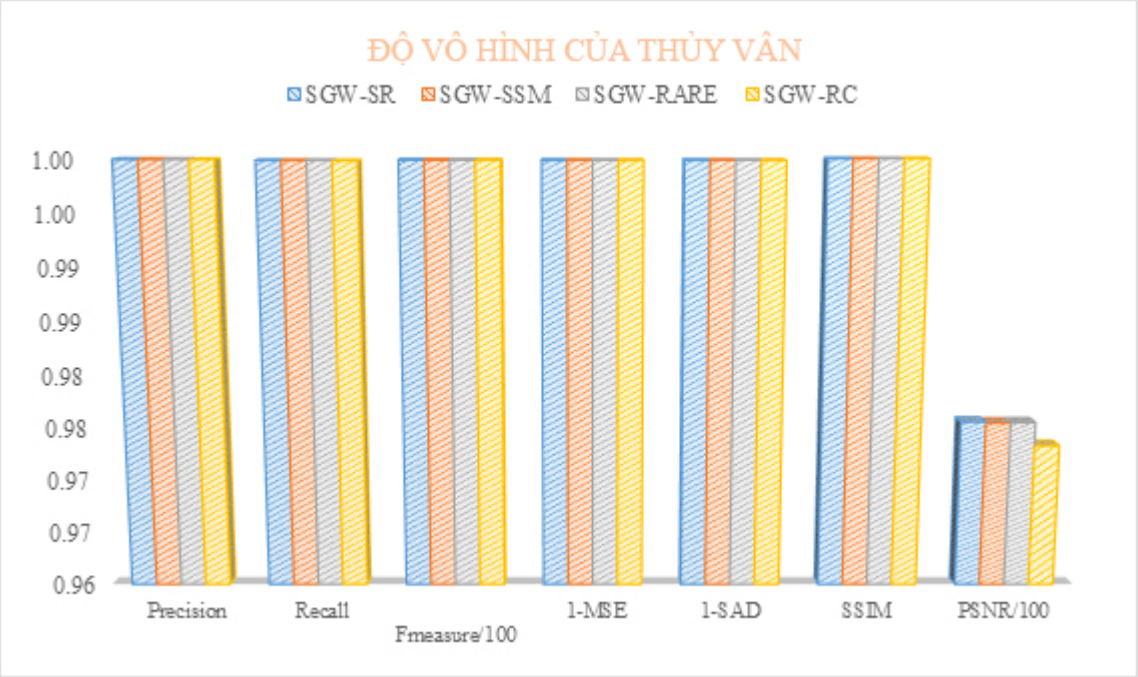
Nhìn chung, bảng 2.3 cho thấy rằng cả bốn mô hình nổi bật không chỉ tối ưu về mặt giữ nguyên chất lượng hình ảnh (tính vô hình) mà còn đảm bảo duy trì độ tin cậy và tính toàn vẹn của thủy vân khi phải đối mặt với các tấn công và biến đổi hình ảnh. Mô hình SSM và RARE đặc biệt nổi bật với các chỉ số MSE và SAD thấp nhất, trong khi tất cả các mô hình đều duy trì được SSIM và PSNR ở mức rất cao, thể hiện hiệu suất vượt trội của phương pháp đề xuất.

Đây là một lợi thế của phương pháp dựa trên nổi bật được đề xuất do việc chọn vùng không nổi bật để ẩn thủy vân và thực tế là việc nhúng thông tin không làm thay đổi quá lớn các đặc điểm nổi bật. Lưu ý rằng luận án đã quan sát sự suy giảm thủy vân do chính việc nhúng thủy vân. Đặc điểm nổi bật bị thay đổi sau khi mã hóa và sau đó quá trình giải mã mù sử dụng đặc điểm nổi bật của hình ảnh đã mã hóa để trích xuất thủy vân.

Để đo lường độ ổn định của thủy vân, việc so sánh thủy vân ban đầu với

***Bảng 2.4:*** *Đánh giá hiệu suất và độ bền vững của các phương pháp thủy vân*

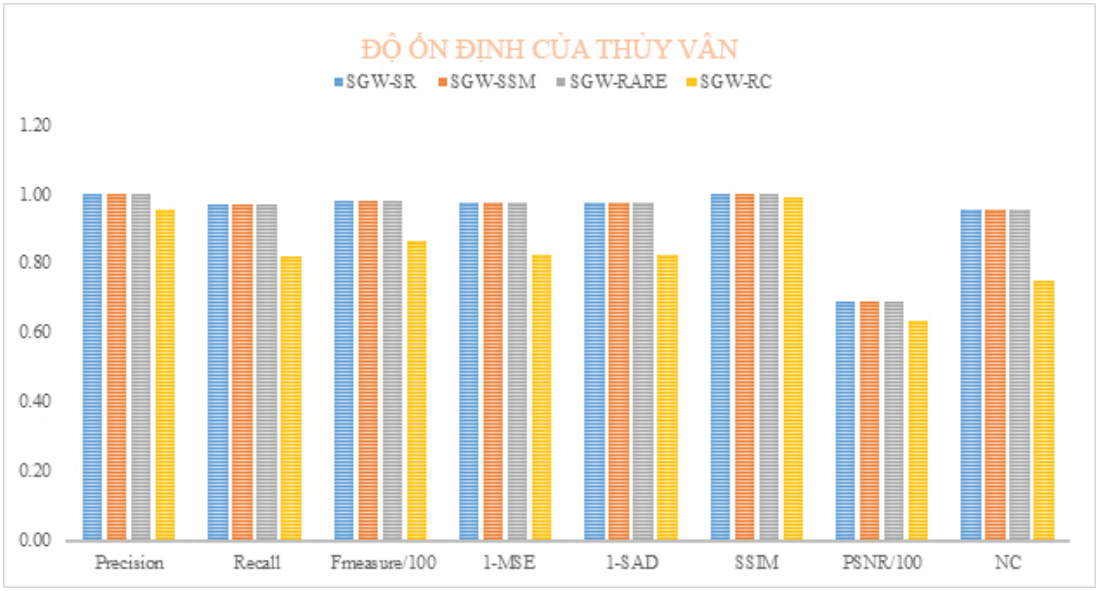
| Phương pháp | Precision | Recall | Fmeasure | MSE | SAD | SSIM | PSNR | NC |
|---|---|---|---|---|---|---|---|---|
| SR | **0.99** | **0.96** | **97.90** | 0.02 | **0.02** | 0.99 | **68.91** | **0.95** |
| SSM | **0.99** | **0.96** | 97.89 | 0.02 | **0.02** | 0.99 | **68.91** | **0.95** |
| RARE | **0.99** | **0.96** | 97.88 | 0.02 | 0.02 | 0.99 | **68.91** | **0.95** |
| RC | 0.95 | 0.81 | 86.26 | **0.17** | 0.17 | **0.98** | 63.37 | 0.75 |
| LSB [86] | | | | | | | 54.32 | |
| LSB [85] | | | | | | | 52.43 | |




***Hình 2.11:*** *Tính vô hình của thủy vân*

thủy vân được trích xuất có thể được đánh giá thông qua các chỉ số chất lượng bao gồm Precision, Recall, F-measure, SAD, SSIM, MSE, PSNR và tương quan chéo chuẩn hóa (NC) [94]. Bảng 2.4 cung cấp một cái nhìn tổng quan về chất lượng của quá trình mã hóa thủy vân đối với bốn mô hình nổi bật: SR, SSM, RARE và RC.

Phân tích chi tiết bảng 2.4 cho thấy rằng ba mô hình SR [82], SSM [71], RARE [73] đạt được kết quả xuất sắc với các chỉ số Precision, PSNR và NC cao nhất. Điều này cho thấy rằng các phương pháp này có khả năng giữ lại thông tin thủy vân một cách chính xác và ổn định, đồng thời đảm bảo chất lượng hình ảnh cao sau khi mã hóa. Cụ thể, các giá trị Precision và Recall đều đạt 0.99, chỉ




***Hình 2.12:*** *Độ ổn định của thủy vân*

số PSNR đạt 68.91 và tương quan chéo chuẩn hóa (NC) đạt 0.95, cho thấy tính vô hình và độ ổn định của thủy vân được duy trì tốt.

Phương pháp RC mặc dù không đạt được kết quả tốt nhất về Precision và NC nhưng lại nổi trội hơn với các chỉ số MSE và SSIM tốt nhất với các giá trị lần lượt là 0.17 và 0.98. Điều này cho thấy phương pháp RC có khả năng khôi phục hình ảnh gốc một cách chính xác hơn trong một số trường hợp.

Các điểm số PSNR của các phương pháp khác như LSB [85] và [86] được đưa vào để tham khảo, mặc dù dữ liệu thử nghiệm của họ chỉ bao gồm bốn hình ảnh khác biệt so với bộ dữ liệu 5000 hình ảnh trong nghiên cứu này.

Qua bảng này, có thể thấy rằng mô hình SR, SSM, và RARE đạt kết quả tốt nhất về độ ổn định và chất lượng của thủy vân, trong khi phương pháp RC có ưu thế về MSE và SSIM. Các phương pháp khác như LSB chỉ được sử dụng để tham khảo vì khác biệt về dữ liệu thử nghiệm.

Trong quá trình đánh giá độ ổn định của thủy vân trước các cuộc tấn công, luận án đã khảo sát một loạt các loại tấn công cụ thể được mô tả chi tiết trong cột đầu tiên của bảng 2.5. Mỗi mô hình độ nổi bật cung cấp giá trị PSNR trung bình cho các thử nghiệm tấn công được thể hiện trong các cột 2-5. Hình 2.13 chỉ ra rằng phương pháp đề xuất của luận án có tính bền vững mạnh mẽ trước tấn công xoay 90°, -90° nhưng kết quả vẫn chưa cao trước tấn công bằng cân bằng histogram và xoay 45°, -45°.

Kết quả này cho thấy phương pháp SR, SSM và RARE có khả năng duy

***Bảng 2.5:*** *Đánh giá độ bền vững của thủy vân trước các cuộc tấn công dựa trên chỉ số PSNR*

| PSNR | SR | SSM | RARE | RC | ROI [30] | LSB [32] |
|---|---|---|---|---|---|---|
| Co giãn 0.8 | 51.65 | **51.66** | 51.65 | 51.41 | | |
| Co giãn 1.2 | 52.85 | **52.87** | 52.85 | 52.05 | | |
| Xoay 30°, −30° | **51.85** | 51.84 | **51.85** | 51.55 | | |
| Xoay 45°, −45° | 51.71 | 51.70 | **51.71** | 51.43 | | |
| Xoay 90°, −90° | 64.37 | **64.49** | 64.37 | 59.85 | | |
| Nhiễu Gauss cộng | **51.98** | 51.97 | 51.96 | 51.76 | | 25.05 |
| Nhiễu muối và tiêu | 54.58 | 54.58 | 54.58 | **54.62** | | 32.43 |
| Cân bằng Histogram | **51.47** | **51.47** | **51.47** | 51.45 | | |
| Bộ lọc trung vị | **53.80** | **53.80** | **53.80** | 52.89 | 28.63 | |
| Cắt 0.9 | **53.38** | **53.38** | **53.38** | 52.57 | | |

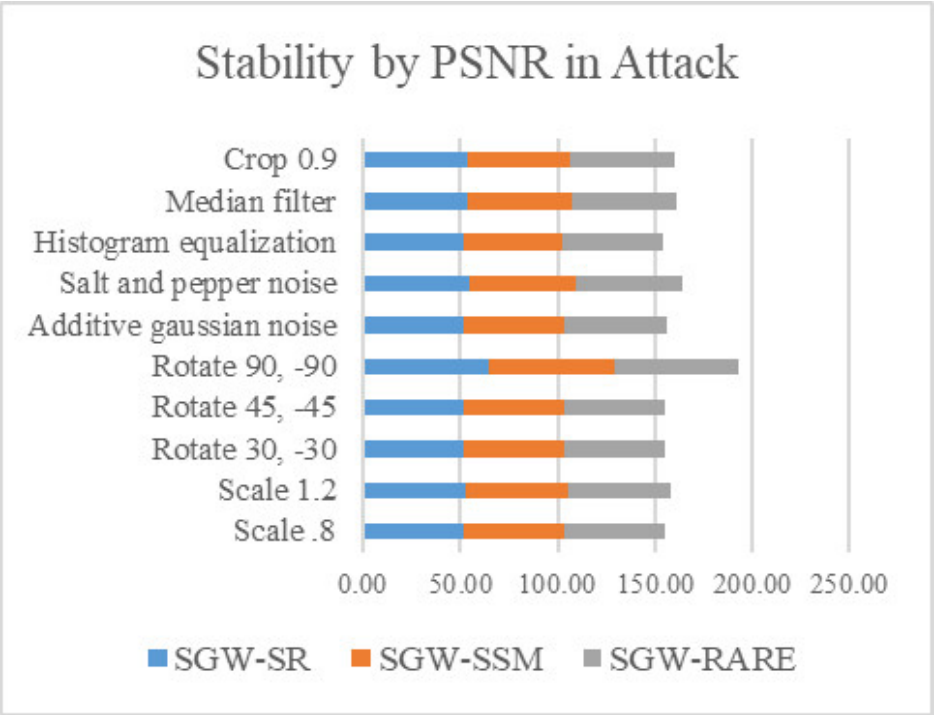
trì chất lượng hình ảnh rất tốt khi bị tấn công bằng các loại tấn công khác nhau với giá trị PSNR cao nhất cho các thử nghiệm tấn công xoay 90°, -90°, đạt từ 64.37 đến 64.49. Phương pháp RC cũng cho thấy khả năng duy trì chất lượng hình ảnh tốt nhưng không bằng các phương pháp khác, đặc biệt khi bị tấn công bằng xoay 90°, -90°.

Kết quả tấn công bằng nhiễu Gauss cộng và nhiễu muối và tiêu cho thấy các phương pháp này có khả năng chống lại các loại nhiễu tốt với giá trị PSNR cao từ 51.96 đến 54.62. Phương pháp RC đạt PSNR cao nhất khi bị tấn công bằng nhiễu muối và tiêu đạt 54.62, chứng tỏ khả năng chống lại loại nhiễu này tốt hơn.

Tuy nhiên, kết quả PSNR cho thấy phương pháp đề xuất vẫn chưa đạt hiệu suất cao nhất khi đối mặt với tấn công bằng cân bằng histogram và xoay 45°, -45° với các giá trị PSNR thấp hơn so với các phương pháp khác.

Đáng chú ý, kết quả của các phương pháp khác đối với PSNR với các loại tấn công tương tự được tham khảo trong các cột 6 và 7. Tuy nhiên, những kết quả này đến từ bộ dữ liệu khác nhau. Bộ dữ liệu được kiểm tra bởi phương pháp ROI [30] bao gồm ba ảnh gốc và một thủy vân và bốn ảnh khác được sử dụng cho bài kiểm tra trong LSB [32]. Hai cột bên phải của bảng 2.5 chỉ được sử dụng để tham khảo, giúp làm rõ sự khác biệt về dữ liệu thử nghiệm giữa các phương pháp.

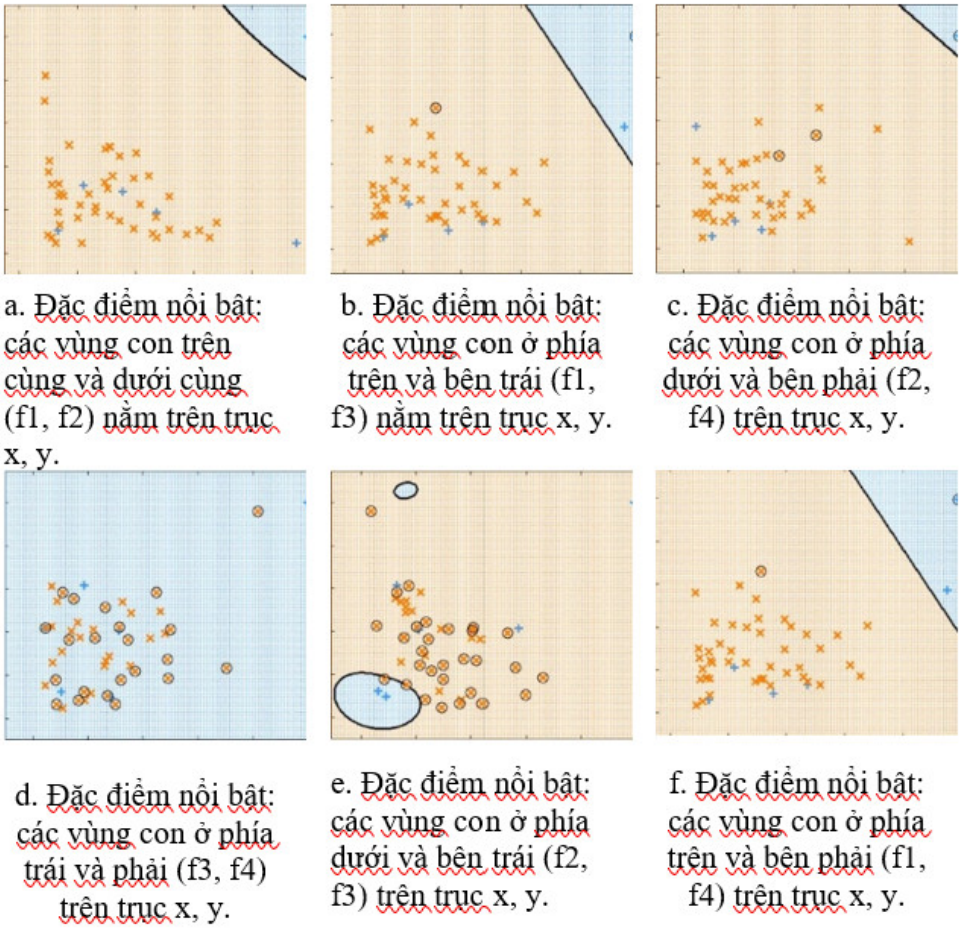
Trong khuôn khổ của luận án này, các thử nghiệm đã được thực hiện để xây dựng kernel cho từng mô hình độ nổi bật và mỗi vùng con cụ thể. Độ bền




***Hình 2.13:*** *Độ ổn định của thủy vân trước các cuộc tấn công*

vững của các đặc điểm độ nổi bật được làm rõ thông qua cấu trúc của kernel được tạo ra. Hình 2.14 cung cấp các ví dụ về kernel được hình thành từ quá trình liên kết học với các đặc điểm nổi bật hiếm gặp RARE [73] và quá trình chọn lọc vùng con ưu tiên cho việc nhúng thủy vân. Quá trình đào tạo SVM diễn ra trong một không gian có 4 chiều, phản ánh 4 vùng con trong vector đặc điểm độ nổi bật của ảnh gốc. Để minh họa trên một không gian 2 chiều, luận án này mô tả mối quan hệ giữa các cặp vùng con và quyết định lựa chọn vùng con hàng đầu. Hình 2.14a thể hiện diện tích phần trăm của vùng con hàng đầu qua trục ngang và diện tích phần trăm của vùng con phía dưới qua trục dọc. Các điểm có dấu hiệu màu xanh là mẫu cho lớp "go", tức là chọn lựa vùng con hàng đầu với kỳ vọng sự thay đổi không đáng kể về đặc điểm nổi bật của vùng này sau khi nhúng thủy vân. Các điểm màu vàng là mẫu cho lớp "no-go" với kỳ vọng sự thay đổi đáng kể của đặc điểm nổi bật.

Đường viền màu đen trong hình 2.14a minh họa kernel thu được qua đào tạo, hiển thị không gian phân loại. Sự xuất hiện của các đường viền hỗ trợ quyết định chọn một vùng con cho thủy vân. Xem xét mối quan hệ giữa vùng con hàng đầu và bên trái đối với phân loại, hình 2.14b trình bày các mẫu khác và đường viền. Điều này tương tự cho trường hợp vùng con hàng đầu và bên phải trong Hình 2.14f. Qua hình 2.14d, màu xanh chiếm phần lớn không gian cho quyết




***Hình 2.14:*** *Các kernel học được sử dụng để chọn vùng con dựa trên đặc điểm nổi bật. Các điểm có dấu hiệu màu xanh là mẫu cho lớp "chọn" để chọn vùng con phía trên với kỳ vọng sự thay đổi không đáng kể về đặc điểm nổi bật cho vùng con này sau khi nhúng thủy vân. Các điểm có dấu hiệu màu vàng là mẫu cho lớp "không chọn" với kỳ vọng sự thay đổi đáng kể về đặc điểm nổi bật sau khi nhúng thủy vân.*

định "go" trong khi chỉ một không gian nhỏ trong hình 2.14c được che phủ bởi màu sắc. Ít nhất ba vùng con tròn trong Hình 2.14e được dành riêng cho quyết định "go".

Luận án đã giới thiệu phương pháp đánh dấu thủy vân bằng cách học hỏi từ các vùng không nổi bật, với sự chứng minh về độ ổn định đối với hai mô hình độ nổi bật liên quan. Do quá trình lựa chọn vùng con thích hợp được thực hiện thông qua tìm kiếm trong một tập hợp các vùng con được xác định trước, độ phức tạp tính toán của phương pháp tỷ lệ với số lượng vùng con của ảnh gốc.

Trong phương pháp của luận án, việc phát hiện độ nổi bật và nhúng thông điệp được áp dụng, và hiệu suất tính toán của chúng đóng vai trò trung tâm trong việc ước lượng công thức tính toán O: $O = O_s + O_w$, nơi $O_s$ và $O_w$ là độ

phức tạp tính toán của mô hình độ nổi bật và phương pháp nhúng thông điệp. Đặt $m$ là kích thước của ảnh, $n$ là kích thước của vùng con. Lưu ý rằng việc phát hiện độ nổi bật được thực hiện cho toàn bộ ảnh trong khi nhúng thông điệp chỉ áp dụng cho một vùng con.

Dựa trên mô tả của tự tương đồng [82], độ nổi bật thưa [71], độ nổi bật hiếm [73] và nhúng ảnh bằng độ tương phản ngẫu nhiên [83], tất cả các phương pháp này đều có độ phức tạp tuyến tính với kích thước ảnh đầu vào $O_f = O(m)$, $O_w = O(n)$, với $m \geq n$. Do đó, $O(m)$ là độ phức tạp tính toán cho thuật toán được đề xuất bởi mô hình độ nổi bật và phương pháp nhúng ảnh đã chọn: $O = O(m) + O(n) \leq O(\max(m, n))$.

## 2.4. Kết luận

Trong chương 2, luận án đã giới thiệu và đánh giá hai phương pháp thủy vân ảnh mới, mỗi phương pháp đều tận dụng các đặc điểm độ nổi bật khác nhau và áp dụng học máy để nâng cao khả năng bảo mật và ổn định của thủy vân.

Đóng góp chính cụ thể của chương 2 bao gồm:

1. Phương pháp thủy vân sử dụng vùng không nổi bật:

- Xác định và sử dụng vùng không nổi bật: Phương pháp này tập trung vào việc tìm kiếm và sử dụng các vùng không nổi bật để nhúng thủy vân, nhằm tăng cường độ không thể nhận biết của thông điệp được nhúng. Việc này giúp giảm thiểu sự thay đổi của các vùng không nổi bật khi nhúng thông tin.

- Áp dụng học máy: Sử dụng Support Vector Machine (SVM) để chọn chính xác các vùng không nổi bật cho quá trình nhúng và giải mã, đảm bảo tính bảo mật và ổn định của thủy vân. Điều này giúp giải quyết hiệu quả vấn đề phát sinh do sự thay đổi của bản đồ độ nổi bật trong quá trình nhúng.

2. Phương pháp thủy vân sử dụng đặc trưng độ nổi bật để thiết lập khóa bí mật:

- Thiết lập khóa bí mật từ đặc trưng độ nổi bật: Sử dụng các đặc điểm nổi bật để thiết lập khóa bí mật, sau đó áp dụng khóa này làm tham số cho cả quá trình nhúng và trích xuất thủy vân. Cách tiếp cận này không chỉ tăng cường bảo mật thông qua việc học đặc trưng độ nổi bật mà còn đảm bảo tính ổn định của thủy vân.

- Kết quả thực nghiệm: Các thử nghiệm trên cơ sở dữ liệu chuẩn chỉ ra rằng phương pháp này có thể cải thiện đáng kể khả năng chống giả mạo và bảo mật thông tin nhúng. Phương pháp dựa trên đặc trưng độ nổi bật đã chứng minh lợi thế cho các ứng dụng chống giả mạo.

Kết quả của chương này không chỉ cung cấp cái nhìn sâu sắc về cách thức tận dụng độ nổi bật và học máy trong việc thiết kế các phương pháp thủy vân ảnh mới mà còn đề xuất hướng tiếp cận hiệu quả cho việc cải thiện độ bảo mật và ổn định của thủy vân trong bối cảnh số ngày càng phức tạp. Các đóng góp quan trọng bao gồm:

- Phát triển phương pháp thủy vân mới sử dụng các vùng không nổi bật để tăng tính tàng hình và bảo mật.
- Thử nghiệm và đánh giá phương pháp trên các dữ liệu hình ảnh thử nghiệm,

cho thấy tính bền vững đáng kể đối với một số mô hình độ nổi bật trong khi gây mất mát nhỏ về tính chính xác.

- Đề xuất và kiểm tra khái niệm thủy vân không nổi bật với các mô hình độ nổi bật và phương pháp mã hóa khác nhau, chứng minh tính khả thi và hiệu quả của phương pháp này trong việc bảo vệ quyền sở hữu trí tuệ và chống giả mạo.

Với những đóng góp này, luận án đã làm rõ tiềm năng của các kỹ thuật thủy vân dựa trên đặc trưng độ nổi bật và không nổi bật trong việc nâng cao tính bảo mật và hiệu quả của các phương pháp thủy vân số trong các ứng dụng thực tế.

# CHƯƠNG 3. PHÁT TRIỂN KỸ THUẬT THỦY VÂN ĐẢM BẢO TÍNH TOÀN VẸN CỦA ẢNH GỐC

## 3.1. Giới thiệu

Chương 3 của luận án phát triển các phương pháp nhằm khắc phục những hạn chế liên quan đến độ phức tạp tính toán và nguy cơ ảnh hưởng đến chất lượng hình ảnh. Các kỹ thuật được đề xuất trong chương 3 không chỉ giúp giảm thiểu độ phức tạp tính toán mà còn nâng cao tính bền vững và vô hình của thủy vân, từ đó trực tiếp giải quyết những thách thức về tăng độ phức tạp tính toán và ảnh hưởng đến chất lượng hình ảnh.

Hậu quả của việc chèn thông tin vào nội dung số là việc phá hủy một phần thông tin trong tác phẩm gốc. Mục tiêu cho phép khôi phục hoàn toàn thông tin của tác phẩm gốc đưa ra một dạng thủy vân đặc biệt, được gọi là thủy vân thuận nghịch (Reversible data hiding - RDH) [95]. Trong phạm vi nghiên cứu của luận án này, tác phẩm gốc và thông tin được ẩn đi là các hình ảnh xám.

Trong tài liệu, các kỹ thuật ẩn dữ liệu có khả năng đảo ngược là một giải pháp cho phép người dùng ẩn một lượng thông tin bí mật vào nội dung đa phương tiện của họ để tạo ra nội dung nhúng. Trong các giải pháp này, cả nội dung gốc ban đầu và thông tin bí mật có thể được khôi phục bằng cách sử dụng nội dung đã nhúng mà không gây ra sự biến dạng. Do đó, những kỹ thuật quan trọng này thường được áp dụng trong hình ảnh y học, hình ảnh quân sự và pháp y vì hình ảnh gốc không thể được điều chỉnh hoặc hỏng hóc sau khi trích xuất thông tin bí mật [19, 55].

Để áp dụng các phương pháp RDH vào các ứng dụng thực tế, một số nghiên cứu viên đã đề xuất các thuật toán RDH cho hình ảnh JPEG (Joint Photographic Experts Group). Phương pháp RDH trong hình ảnh JPEG có ích cho tính toàn vẹn hình ảnh, xác thực hình ảnh và quyền riêng tư hình ảnh. Việc áp dụng RDH cho hình ảnh JPEG cần xem xét các vấn đề sau đây: (1) Khả năng lưu trữ thông tin ẩn hạn chế; (2) Chất lượng hình ảnh JPEG thấp hơn so với hình ảnh chưa nén; (3) Kích thước hình ảnh JPEG đã nhúng có thể tăng lên so với hình ảnh ban đầu. Chính vì vậy, RDH cho hình ảnh JPEG là một thách thức so với RDH cho hình ảnh chưa nén.

***Bảng 3.1:*** *Ưu, nhược điểm của 3 thuật toán ẩn dữ liệu phổ biến*

| | Ưu điểm | Nhược điểm |
|---|---|---|
| Thuật toán mã phân tán [66] | - Khả năng bền vững cao, khó phá hủy.<br>- Có thể áp dụng cho nhiều loại tín hiệu khác nhau.<br>- Hỗ trợ giảm nhiễu và mức lỗi bằng cách sử dụng các kỹ thuật mã hóa kênh.<br>- Không cần giải mã để xác định các bit ẩn. | - Yêu cầu băng thông rộng để truyền tải tín hiệu tăng dần.<br>- Cần sử dụng phương pháp đồng bộ hóa để xác định khoảng cách giữa tín hiệu gốc và tín hiệu ảnh.<br>- Có thể phát hiện khi bị tấn công bằng các phương pháp phân tích phổ biến. |
| Thuật toán RDH [68, 67] | - Giảm thiểu sự thay đổi dữ liệu gốc, giúp bảo toàn chất lượng hình ảnh ban đầu.<br>- Không cần giải mã để xác định các bit ẩn.<br>- Khả năng bền vững cao, khó phá hủy. | - Hiệu quả chỉ hoạt động với các tệp hình ảnh JPEG có kích thước lớn hơn hoặc bằng kích thước của dữ liệu cần ẩn.<br>-Ẩn thông tin có thể làm giảm chất lượng của tệp hình ảnh gốc.<br>-Không chống lại các cuộc tấn công giải mã. |
| Thuật toán DCT [69] | - Cung cấp nén dữ liệu, giúp tiết kiệm năng lượng trong quá trình lưu trữ.<br>- Có thể áp dụng cho nhiều loại hình ảnh và tệp dữ liệu khác nhau.<br>- Thân thiện với người dùng, dễ sử dụng và triển khai. | - Không thể chứa lượng lớn dữ liệu.<br>- Các thuật toán ẩn thông tin sử dụng DCT có thể bị phát hiện bằng cách so sánh các khối DCT giữa tệp gốc và tệp ẩn. |

Nói chung, các thuật toán ẩn dữ liệu đã trở thành một công cụ quan trọng trong việc bảo vệ thông tin. Dưới đây là một phân tích về ưu điểm và nhược điểm liên quan đến ba thuật toán phổ biến được sử dụng cho việc ẩn dữ liệu: thuật toán mã phân tán, thuật toán RDH và thuật toán biến đổi DCT cho hình ảnh JPEG.

Những thuật toán ở trên cho thấy mỗi thuật toán có ưu điểm và nhược điểm riêng, tuy nhiên, RDH có thể được sử dụng để bảo vệ thông tin bên trong các nội dung số.

Trong phần này, luận án tập trung vào việc đề xuất thuật toán RDH cho hình ảnh JPEG bằng cách sử dụng sự kết hợp giữa nhiều bảng lượng tử từ JPEG theo phương pháp chéo. Dựa trên phương pháp của Tian [56], luận án cải thiện chất lượng của hình ảnh JPEG sau khi nhúng thông tin. Nhiều bảng lượng tử

của JPEG được khảo sát để áp dụng cho thủy vân thuận nghịch. Trong phương pháp của luận án, hiệu quả của từng bảng lượng tử cho từng thành phần từ thuật toán JPEG được khảo sát để chọn các hệ số DCT phù hợp áp dụng cho phương pháp RDH được đề xuất. Luận án giả định rằng chủ yếu tần suất cao của các hệ số DCT khác không ảnh hưởng đến chất lượng của hình ảnh JPEG đã nhúng. Do đó, nếu khu vực hệ số DCT ít hiệu quả hơn được chọn, có thể tăng dung lượng nhúng và sau đó duy trì chất lượng của hình ảnh JPEG.

Trong chương này, hai phương pháp thủy vân thuận nghịch sau sẽ được trình bày:

- Phương pháp bằng yếu tố cấu trúc
- Phương pháp bằng DCT

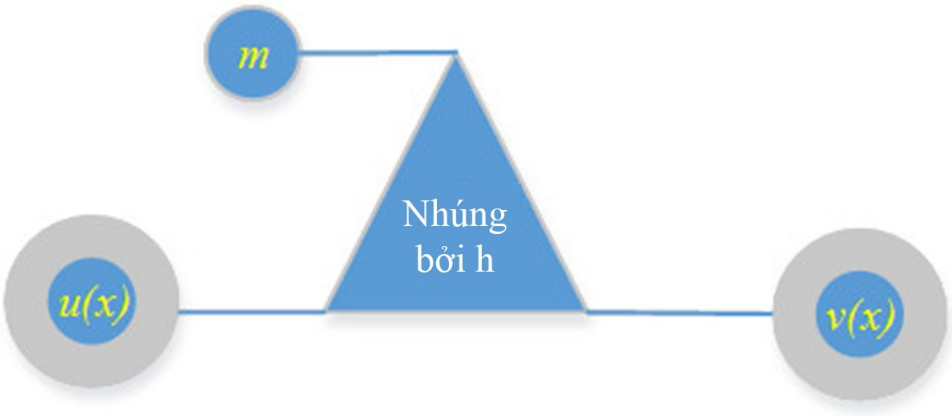
## 3.2. Phương pháp sử dụng yếu tố cấu trúc

Trong nghiên cứu này, yếu tố cấu trúc đã được sử dụng cho thủy vân số với khả năng đảo ngược của hình ảnh gốc. Cụ thể, trong một hình ảnh xám, nó xác định cách một pixel có thể được sử dụng để ẩn thông tin và giá trị xám của một pixel cần thay đổi bao nhiêu để ẩn thông tin bí mật. Mối quan hệ giữa dấu thủy vân $m$ và hình ảnh gốc $u(x)$ trên mặt phẳng hình ảnh và hình ảnh đã thủy vân $v(x)$ cần phải có tính nhất quán để có thể phục hồi cả hình ảnh gốc và dấu thủy vân từ hình ảnh đã thủy vân.

### 3.2.1. Yếu tố cấu trúc

Xem xét yếu tố cấu trúc $h$ [96] biểu thị đặc điểm cục bộ của một pixel vì các pixel lân cận được kiểm tra. Tuy nhiên, trong phương pháp của luận án, khi được thủy vân, yếu tố cấu trúc tiết lộ các pixel nơi thông tin được ẩn giấu. Trong hình 3.1 có một viền xám lớn xung quanh pixel $x$ để minh họa các pixel lân cận của pixel đó.

Giả sử chúng ta có hình ảnh gốc $u$ là một bức ảnh chụp chân dung. Quá trình nhúng thủy vân diễn ra như sau: Đầu tiên, xác định yếu tố cấu trúc $h$ bằng cách xác định các vùng không nổi bật trong hình ảnh gốc $u$, chẳng hạn như nền phía sau hoặc các khu vực đồng màu như quần áo ít chi tiết. Tiếp theo, sử dụng yếu tố cấu trúc $h$ để nhúng thông tin thủy vân $m$ vào các vùng không nổi bật này. Quá trình này đảm bảo rằng thông tin được nhúng sẽ khó bị phát




***Hình 3.1:*** *Yếu tố cấu trúc h được sử dụng để nhúng thông tin m vào hình ảnh gốc u, tạo ra hình ảnh đã được thủy vân v.*

hiện bằng mắt thường. Kết quả là hình ảnh đã được thủy vân $v$, trong đó thông tin thủy vân $m$ được nhúng vào các vùng không nổi bật của hình ảnh, đảm bảo tính vô hình và tính bền vững của thông tin được nhúng.

Để thuận tiện, luận án biểu diễn một hình ảnh xám gốc bằng một hàm số nguyên (1) và dấu thủy vân – bằng một hàm nhị phân. Yếu tố cấu trúc $h$ được mô tả bằng một ma trận nhị phân 2D. Ngoài ra, dấu thủy vân được nhúng vào hình ảnh gốc $u(x)$ với yếu tố cấu trúc $h$ theo công thức (3.1)-(3.3).

$$u(x) : D \to N, D \subset N^2 \tag{3.1}$$

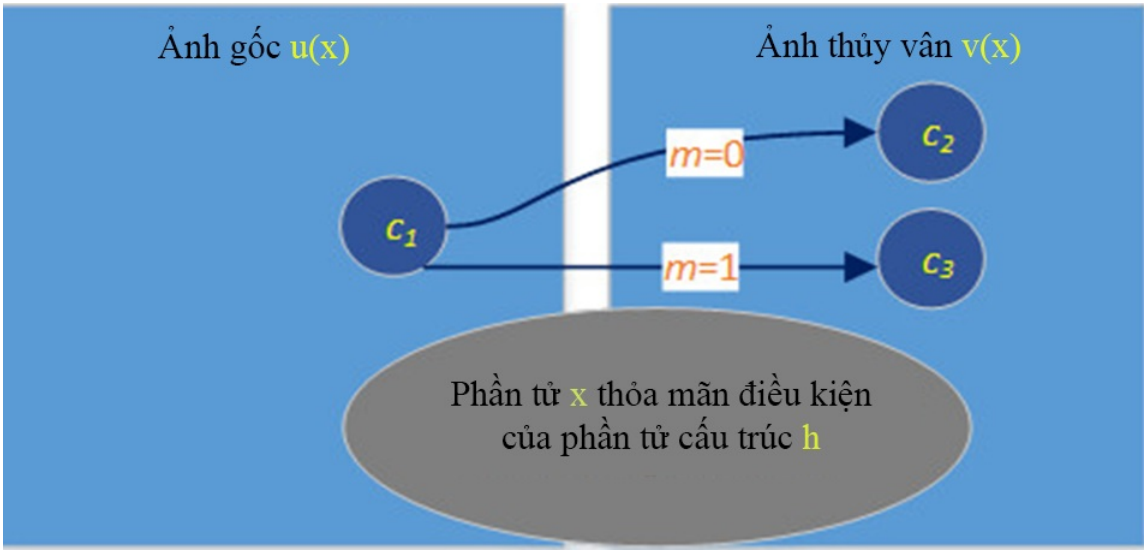
$$m(x) : D_m \to [0, 1], D_m \subset D \tag{3.2}$$

$$v(x) := \text{embed}(u(x), m(x), h), x \in D \tag{3.3}$$

Một cách để ẩn giá trị nhị phân của dấu thủy vân là thay đổi giá trị xám $c_1$ của một pixel trong hình ảnh gốc thành $c_2$ hoặc $c_3$ tùy thuộc vào giá trị của dấu thủy vân là không hoặc một. Từ quan điểm này, luận án nhận thấy rằng các pixel chứa các giá trị xám $c_1$, $c_2$ và $c_3$ là các giá trị mã cần được xem xét đặc biệt trong quá trình thủy vân, đặc biệt là khi tìm kiếm các vị trí để nhúng (3.4).

$$t(x) = (u == c_1) \,\|(u == c_2)\|\, (u == c_3) \tag{3.4}$$

Với yếu tố cấu trúc $h$, xói mòn hình học theo công thức (3.5) và lọc theo giá trị xám $c_1$ có thể trích xuất một bản đồ vị trí của các pixel (3.6), được sử




***Hình 3.2:*** *Hình ảnh đã thủy vân $v(x)$ được xử lý theo cách tương tự như bộ lọc*

dụng để nhúng thông tin (3.5).

$$e(x) = \text{imerode}(t, h) \tag{3.5}$$

$$D_m = \{x, (e(x)\&\,(u == c_1)) == 1\} \tag{3.6}$$

Giả sử các giá trị xám $c_1$, $c_2$ và $c_3$ được xác định trước bởi một nhiệm vụ, sẽ được mô tả sau, giá trị xám $c_1$ trong các pixel của bản đồ $D_m$ được chỉnh sửa tương ứng với các giá trị nhị phân của dấu thủy vân theo công thức (3.7).

$$v(x) = \left\{ c_2, m(x) = 0; c_3, m(x) = 1;\ x \in D_m \right. \tag{3.7}$$

Hình 3.2 minh họa quá trình nhúng với yếu tố cấu trúc $h$. Lưu ý rằng nhiệm vụ phục hồi (3.8) phải khôi phục đầy đủ hình ảnh gốc $u(x)$ và dấu thủy vân $m$ từ hình ảnh đã thủy vân $v(x)$ với sự hỗ trợ của yếu tố cấu trúc $h$.

$$[u(x), m] := \text{recover}(v(x), h) \tag{3.8}$$

Để phát hiện các pixel quan trọng, ban đầu luận án sử dụng bộ lọc (3.9) áp dụng cho hình ảnh đã thủy vân $v(x)$ theo cách tương tự như bộ lọc (3.4), đã được áp dụng cho hình ảnh gốc $u(x)$.

Xói mòn hình học [49] bằng yếu tố cấu trúc h và các bộ lọc của các giá trị mã $c_1$, $c_2$, $c_3$ tạo nên bản đồ các pixel $D'_m$ chứa các giá trị nhúng của dấu thủy vân theo công thức (3.9), (3.10).

$$t'(x) = (v == c_1) \,\|(v == c_2)\|\, (v == c_3) \tag{3.9}$$

$$e'(x) = \text{imerode}\left(t', h\right) \tag{3.10}$$

$$D'_m = \left\{x, \left(e'(x)\&\left(v == c_2 \| v == c_3\right)\right) == 1\right\} \tag{3.11}$$

Khi bản đồ $D'_m$ được tìm thấy, dấu thủy vân được thu thập bằng cách trích xuất các pixel đã nhúng và thay đổi các giá trị xám $c_1$, $c_2$ thành giá trị không và một tương ứng của chúng (3.12). Một sự chỉnh sửa của hình ảnh đã thủy vân $v(x)$ được ước lượng từ các pixel tương ứng, và hình ảnh gốc được khôi phục (3.13).

$$m'(x) = \begin{cases} 0, v(x) = c_2 \\ 1, v(x) = c_3 \end{cases}, x \in D'_m \tag{3.12}$$

$$u'(x) = \begin{cases} c_1, v(x) = c_2 \\ c_1, v(x) = c_3 \\ v(x), \text{ otherwise} \end{cases}, x \in D'_m \tag{3.13}$$

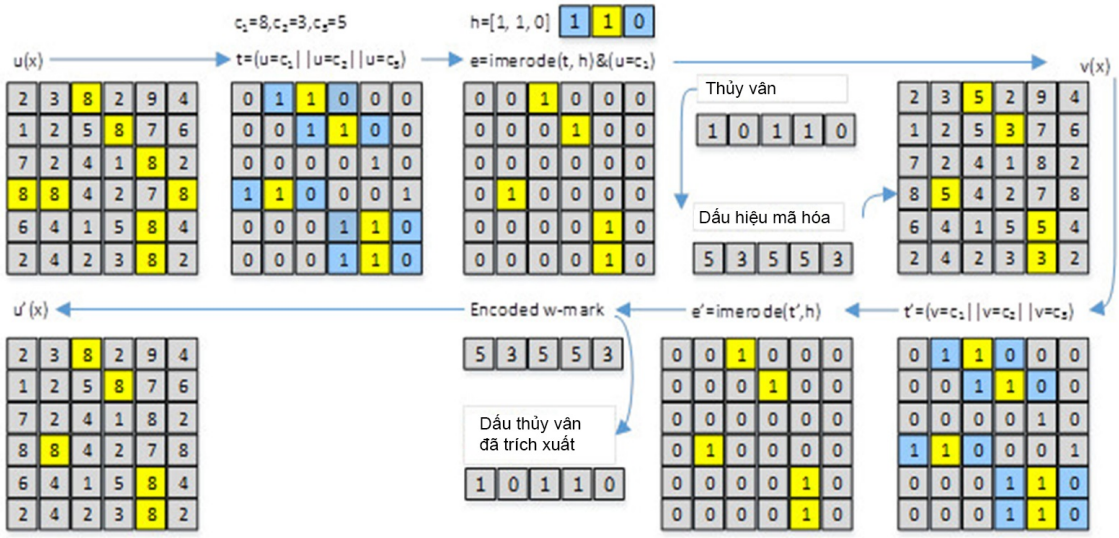
Để khả năng nhúng thông tin được coi là có thể đạt được, luận án kỳ vọng rằng số lượng pixel trong bản đồ $D_m$ do yếu tố cấu trúc $h$ và các giá trị mã $c_1$, $c_2$, $c_3$ cung cấp phải lớn hơn kích thước của dấu thủy vân một cách rõ ràng theo công thức (3.14).

$$\text{count}\left(D_m\right) \geq \text{count}(m) \tag{3.14}$$

Trong hình ảnh gốc, tồn tại một số lượng pixel có giá trị xám của $c_2$, $c_3$ là các giá trị mục tiêu của nhiệm vụ thủy vân. Các pixel tương ứng trong hình ảnh đã thủy vân có thể bị hiểu nhầm là nơi chứa thông tin ẩn và điều này dẫn đến thất bại trong việc khôi phục lại thủy vân và hình ảnh gốc. Cụ thể, xói mòn hình học với các yếu tố cấu trúc được đề xuất sử dụng trong công trình này để tránh vấn đề này. Điều kiện (3.15) cho phép lựa chọn một yếu tố cấu trúc và các giá trị mã $c_1$, $c_2$, $c_3$ bằng cách kiểm tra xem không có pixel nào với các giá trị xám $c_2$, $c_3$ xuất hiện khi lọc với các yếu tố được chọn.

$$\text{count}\left(e\&\left(u == c_2\right)\right) == 0 \, \text{count}\left(e\&\left(u == c_3\right)\right) == 0 \tag{3.15}$$

Để quản lý tính vô hình của thủy vân, khoảng cách giữa các giá trị trước




***Hình 3.3:*** *Yếu tố cấu trúc $h$ được sử dụng để nhúng thông tin của dấu thủy vân $m$ vào hình ảnh gốc $u$, tạo ra hình ảnh đã được thủy vân $v$*

và sau khi thủy vân phải nhỏ nhất có thể:

$$d = \sum_{i=2,3} |c_1 - c_i| \to \min \tag{3.16}$$

### 3.2.2. Thuật toán

Các yếu tố cấu trúc được tạo ra và sử dụng trong các thuật toán sau đây phù hợp cho việc nhúng và trích xuất thủy vân cũng như khôi phục hình ảnh gốc.

Để đánh giá độ phức tạp của thuật toán 1 ("Reversible Hiding by Structuring Element (RHSE)"), từng thủ tục cụ thể sẽ được phân tích và sau đó tổng hợp độ phức tạp tổng thể của thuật toán.

Thủ tục $createElements(u, l, l\_w)$ thực hiện việc tạo phần tử cấu trúc $h$ và các giá trị xám $c_1, c_2, c_3$. Đầu tiên, tính histogram $g$ của ảnh $u$ với độ phức tạp $O(n)$, với $n$ là số lượng pixel của ảnh. Sau đó, sắp xếp các giá trị để chọn ra các giá trị tối ưu $c_1, c_2, c_3$ với độ phức tạp $O(n \log n)$. Lựa chọn phần tử $c_1, c_2, c_3$ có độ phức tạp $O(1)$. Như vậy, tổng độ phức tạp của thủ tục này là $O(n \log n)$.

Thủ tục $allocateHidingSpace(u, h, l\_w)$ phân bổ không gian trong ảnh $u$ để ẩn dấu thông tin dựa trên phần tử $h$. Thủ tục này thường yêu cầu duyệt qua các pixel của ảnh để xác định vị trí ẩn dấu, với độ phức tạp là $O(n)$.

Thủ tục $hideMark(u, h, c\_1, c\_2, c\_3)$ thực hiện quá trình ẩn dấu thông

**ALGORITHM 1.** Reversible Hiding by Structuring Element (RHSE)

**Input:** Host image $u$, mark length $l_m$, element length $l$

**Output:** Reversible hiding image $v$, element $h$, gray values $c_1, c_2, c_3$

```
1  start
2    [h, c1, c2, c3] = createElements(u, l, lm);
3    Dm = allocateHidingSpace(u, h, c1);
4    v = hideMark (u, m, h, c1, c2, c3, Dm );
5  end
6  [h, c1, c2, c3] =function createElements(u, l, lm)
7  start
8    g = histogram(u);
9    o = sort(g);
10   c1s = o(g > l);
11   for each h, length(h) < l
12     for i =1: 255
13       for each c1 ∈ c1s;
14         for each pair c2, c3 ∈ c23
15           order by (|c1 − c2| + |c1 − c3|)
16           if checkConditions(u, h, lm);
17             break;
18         end
19       end
20     end
21   end
22 end
```

***Hình 3.4:*** *Ẩn dữ liệu có khả năng đảo ngược bằng yếu tố cấu trúc (RHSE)*

tin vào trong ảnh $u$ dựa trên phần tử $h$ và các giá trị $c_1, c_2, c_3$. Thủ tục này có độ phức tạp là $O(n)$ do cần duyệt qua các pixel và áp dụng các biến đổi để ẩn dấu.

Tổng hợp lại:

- Bước tạo phần tử và lựa chọn giá trị $c_1, c_2, c_3$ có độ phức tạp $O(n \log n)$.

- Bước phân bổ không gian và ẩn dấu thông tin có độ phức tạp lần lượt là $O(n)$.

Vì vậy, độ phức tạp tổng thể của thuật toán 1 là $O(n \log n)$, do bước sắp xếp trong thủ tục *createElements* chi phối. Các bước còn lại có độ phức tạp tuyến tính $O(n)$, không ảnh hưởng lớn đến tổng thể thuật toán. Điều này có nghĩa là khi kích thước ảnh tăng, thời gian thực hiện thuật toán sẽ tăng theo hàm $n \log n$, trong đó $n$ là số lượng pixel của ảnh.

Hàm *createElements* trong thuật toán đầu tiên thiết kế các yếu tố cấu trúc cho một hình ảnh gốc, xem xét các hạn chế và yêu cầu tối ưu về tính vô hình của thủy vân. Sử dụng biểu đồ [97] của hình ảnh gốc, luận án cho thấy rằng các giá trị xám có phân phối thấp trong biểu đồ có khả năng thỏa mãn hạn chế bằng cách kiểm tra giá trị xám theo một trật tự.

Do đó, dòng mã #14 giải quyết hạn chế cho các giá trị $c_2$, $c_3$, trong khi

dòng mã #10 và #13 đề cập đến hạn chế cho các giá trị $c_1$. Yêu cầu tối ưu được thực hiện bởi các dòng mã #14 và #15. Cụ thể, không gian ẩn trong hình ảnh gốc được xác định trong dòng mã #3 sử dụng các yếu tố cấu trúc từ dòng mã #2. Tại đây, trong dòng mã #4, một dấu thủy vân được nhúng vào không gian ẩn của hình ảnh gốc.

Khi luận án cho phép yếu tố cấu trúc $h$ lựa chọn các vị trí để ẩn một dấu thủy vân và chọn các giá trị mã $c_1$, $c_2$, $c_3$, chúng đóng vai trò là khóa để trích xuất dấu thủy vân và khôi phục hình ảnh gốc bằng thuật toán thứ hai.

Để đánh giá độ phức tạp của thuật toán 2 ("Reversible Extract Host Image and Watermark by Structuring Element (RESE)"), luận án xem xét các bước chính của thuật toán và tổng hợp độ phức tạp tổng thể.

Thuật toán bắt đầu bằng việc phân bổ không gian ẩn dấu bằng thủ tục $allocateHidingSpace(v, h, c\_1, c\_2, c\_3)$, tương tự như trong thuật toán 1, có độ phức tạp là $O(n)$ với $n$ là số lượng pixel của ảnh.

Sau đó, thuật toán thực hiện việc duyệt qua từng pixel của ảnh ẩn dấu $v$ để khôi phục lại ảnh chủ $u$ và thủy vân $m$. Việc kiểm tra và xử lý mỗi pixel để xác định giá trị của $m(i)$ và $u(i)$ dựa trên các điều kiện liên quan đến giá trị xám $c\_1, c\_2, c\_3$ có độ phức tạp tuyến tính $O(n)$ vì tất cả các phép toán này chỉ liên quan đến việc duyệt qua các pixel của ảnh.

Tổng hợp lại, cả quá trình của thuật toán 2 bao gồm hai bước chính: phân bổ không gian và duyệt qua các pixel để khôi phục thông tin. Cả hai bước này đều có độ phức tạp là $O(n)$, do đó độ phức tạp tổng thể của thuật toán 2 cũng là $O(n)$.

Điều này có nghĩa là thời gian thực hiện của thuật toán tăng tuyến tính với số lượng pixel của ảnh, tức là khi kích thước ảnh tăng lên, thời gian thực hiện thuật toán sẽ tăng theo hàm $n$, trong đó $n$ là số lượng pixel của ảnh.

Luận án có thể tính toán không gian ẩn bằng dòng mã #2. Sau đó, dấu thủy vân được xác định bằng cách so sánh không gian ẩn $D_e$ của hình ảnh đã thủy vân v với các giá trị xám $c_2$, $c_3$ bằng các dòng mã #5-6. Ngoài ra, hình ảnh gốc trong không gian ẩn $D'_m$ được khôi phục bằng cách thay đổi từ các giá trị $c_2$, $c_3$ sang giá trị $c_1$. Hình 3.3 cho thấy cách các yếu tố cấu trúc hoạt động trong các thuật toán được mô tả bởi luận án.

Hãy xem xét một hình ảnh gốc $u$ với các phần tử 6*6 pixel để ẩn một thông điệp nhị phân 5 bit. Giả sử hàm createElements của thuật toán thứ nhất trả về yếu tố cấu trúc $h$=[1,1,0] và các giá trị mã $c_1$=8, $c_2$=3, $c_3$=5. Các pixel

**ALGORITHM 2.** Reversible extract host image and watermark by structuring element (RESE)

**Input:** Watermarked image $v$, element $h$,
gray values $c_1, c_2, c_3$
**Output:** Reversible host image $u$, watermark $m$.

```
start
  D'_m = allocateHidingSpace(v, h, c1, c2, c3);
  u = v;
  for x ∈ D'_m
    m(v == c2) = 0;
    m(v ==) = 1;
    u(v == c2) = c1;
    u(v == c3) = c1;
  end
end
```

***Hình 3.5:*** *Trích xuất hình ảnh gốc và thủy vân thuận nghịch bằng yếu tố cấu trúc (RESE)*

màu vàng trong hình ảnh gốc $u$ thể hiện các pixel có giá trị xám là 8, trong khi các pixel màu vàng trong hình ảnh $t$ thể hiện vị trí của yếu tố cấu trúc $h$ mà trả về 1 bởi xói mòn hình học. Không gian ẩn $D_m$ được minh họa trong hình ảnh $e$ bằng các dấu màu vàng.

Giả sử thủy vân là $m$=[1,0,1,1,0]. Phiên bản được mã hóa của nó bởi các giá trị mã $c_1$=8, $c_2$=3, $c_3$=5 sẽ là [5,3,5,5,3] và hình ảnh đã thủy vân $v$ được hiển thị ở góc trên bên phải của hình 3.3.

Bây giờ luận án có hình ảnh đã thủy vân $v$ và khóa là yếu tố cấu trúc và các giá trị mã. Bằng cách áp dụng (3.9) và xói mòn hình học (3.10), hình ảnh $t'$ và hình ảnh $e'$ được tính toán. Tại đây, các pixel màu vàng trong hình ảnh $e'$ minh họa không gian ẩn $D'_m$. Các giá trị xám của hình ảnh $v$ tại vị trí của không gian $D'_m$ là [5,3,5,5,3] có thể được giải mã bởi $c_2$=3, $c_3$=5 thành dấu thủy vân $m'$=[1,0,1,1,0]. Các giá trị xám [5,3,5,5,3] của hình ảnh $v$ bây giờ được thay thế bằng $c_1$=8 và hình ảnh gốc được khôi phục trong không gian $D'_m$ với các giá trị [8,8,8,8,8]. Cuối cùng, hình ảnh gốc $u'$ được hiển thị ở góc dưới bên trái của hình 3.3 với các pixel màu vàng đã được khôi phục.

### 3.2.3. Các chỉ số đánh giá hiệu suất

Một trong những mối quan tâm lớn nhất đối với thủy vân là việc chèn thông tin vào hình ảnh mà không ảnh hưởng đáng kể đến chất lượng hình ảnh. Sự khác biệt giữa hình ảnh gốc $u$ và hình ảnh $v$ đã được thủy vân cung cấp thước đo về tính vô hình của thủy vân. Điều này có thể được ước lượng bởi tỉ

số tín hiệu so với nhiễu cực đại (PSNR) [98] theo công thức (3.18) dựa trên sai số bình phương trung bình (MSE) [90] theo công thức (3.17):

$$\mathrm{MSE}(u,v) = \frac{1}{\mathrm{count}(x)} \sum_{x} (u(x) - v(x))^2 \tag{3.17}$$

$$\text{imperceptibility } = \mathrm{PSNR(u,v)} = 10 \log_{10} \frac{(2^n - 1)^2}{\sqrt{\mathrm{MSE(u,v)}}} \tag{3.18}$$

Quay lại với dấu thủy vân, phiên bản gốc $m$ và phiên bản được trích xuất $m'$, luận án tính $\mathrm{PSNR}\,(m, m')$ để ước lượng độ ổn định của dấu thủy vân (3.19). Để đánh giá khả năng đảo ngược của hình ảnh gốc, luận án so sánh hình ảnh gốc và phiên bản được khôi phục từ hình ảnh đã thủy vân bằng $\mathrm{PSN}\,R\,(u, u')$ (3.20). Lưu ý rằng $\mathrm{MSE}(u,u) = 0$, và PSNR trả về vô cực (inf) $\mathrm{PSNR}(u,u) = \infty$ khi hai hình ảnh giống nhau.

$$\text{stability } = \mathrm{PSNR}\left(\mathrm{m}, \mathrm{m}'\right) \tag{3.19}$$

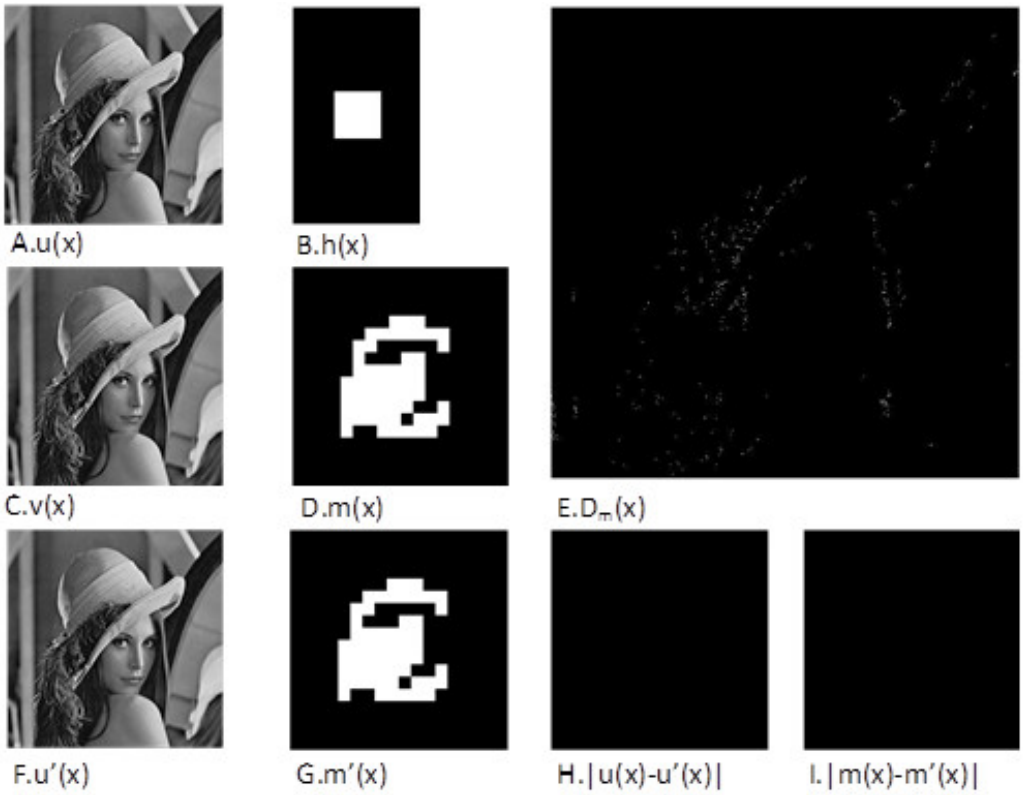
$$\text{reversibility } = \mathrm{PSNR}\left(\mathrm{u}, \mathrm{u}'\right) \tag{3.20}$$

### 3.2.4. Kết quả thực nghiệm

Trong quá trình đánh giá hiệu suất của các thuật toán, các chỉ số trên đã được xem xét trong thí nghiệm. Mỗi hình ảnh thử nghiệm được phân tích với thuật toán để tìm dung lượng ẩn thông tin. Luận án chọn chiều rộng và chiều cao của yếu tố cấu trúc trong khoảng từ 3-5 pixel, tạo ra kích thước nhỏ để giữ hiệu suất tốt cho xói mòn hình học. Đối với một hình ảnh "lena" (512 × 512 pixel), yếu tố cấu trúc của nó (3 × 5 pixel) được phát hiện bởi thuật toán và hiển thị trong hình 3.6B. Không gian ẩn $D_m$ dựa trên các yếu tố được minh họa trong hình 3.6E, nơi các pixel trắng đánh dấu vị trí để ẩn.

Giả sử thủy vân là một logo nhị phân (hình 3.6D), luận án ẩn thủy vân vào hình ảnh "lena" tạo ra một hình ảnh đã thủy vân (hình 3.6C). Việc triển khai yếu tố cấu trúc trên hình ảnh đã thủy vân đã cho phép trích xuất logo (hình 3.6G) và khôi phục hình ảnh gốc (hình 3.6F). So sánh bằng hình 3.6H và hình 3.6I cho thấy đủ khả năng đảo ngược cho cả hình ảnh gốc và thông tin ẩn.

Điểm yếu của thủy vân có thể là khả năng bị nhận ra sự thay đổi hình ảnh gốc do việc ẩn thêm thông tin. Bằng cách thay đổi kích thước của thông tin ẩn, tính vô hình có thể bị thay đổi đáng kể như được thể hiện trong bảng 3.2.




***Hình 3.6:*** *Ví dụ về thủy vân: A. Hình ảnh gốc u; B. Yếu tố cấu trúc h; C. Hình ảnh đã thủy vân v; D. Dấu thủy vân m; E. Không gian ẩn $D_m$; F. Hình ảnh gốc đã khôi phục u′; G. Dấu thủy vân đã trích xuất m′; H. Sự khác biệt giữa hình ảnh gốc u và hình ảnh đã khôi phục u′; I. Sự khác biệt giữa mặt nạ m và dấu thủy vân đã trích xuất m′*

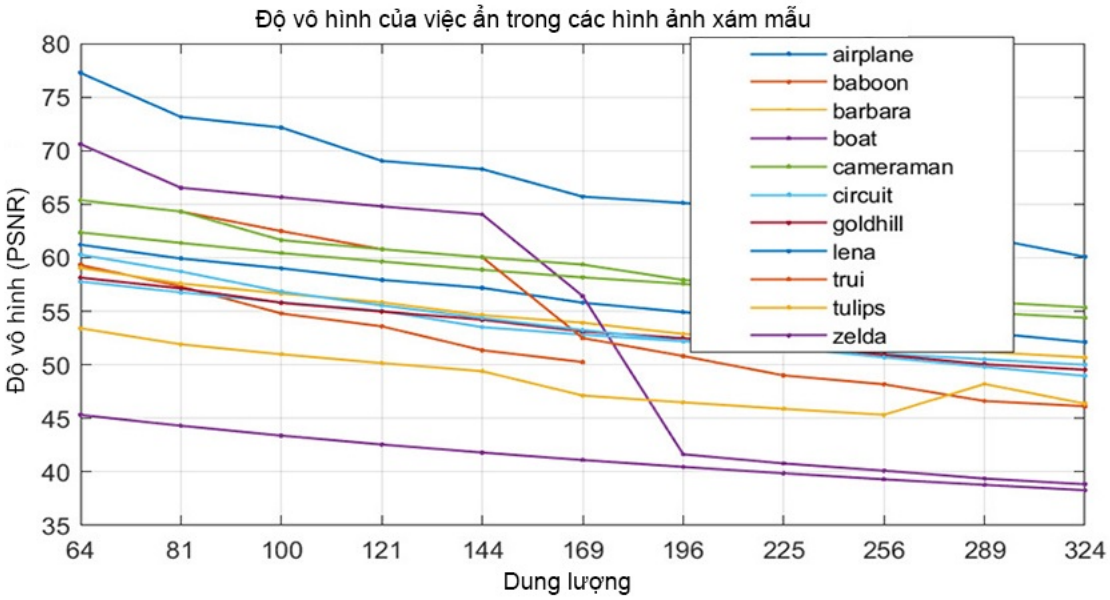
***Bảng 3.2:*** *Hiệu suất của thuật toán đối với hình ảnh Lena*

| **Dung lượng nhúng (bit)** | **Tính vô hình** | **Tính ổn định** | **Tính đảo ngược** | **Thời gian nhúng (s)** | **Thời gian trích xuất (s)** |
|---|---|---|---|---|---|
| 64 | 77.25 | 100 | 100 | 0.49 | 0.33 |
| 81 | 73.14 | 100 | 100 | 0.57 | 0.39 |
| 100 | 72.15 | 100 | 100 | 0.49 | 0.33 |
| 121 | 69.04 | 100 | 100 | 0.57 | 0.39 |
| 144 | 68.27 | 100 | 100 | 0.42 | 0.33 |
| 169 | 65.70 | 100 | 100 | 0.54 | 0.37 |
| 196 | 65.11 | 100 | 100 | 0.57 | 0.39 |
| 225 | 64.50 | 100 | 100 | 0.48 | 0.37 |
| 256 | 63.93 | 100 | 100 | 0.42 | 0.36 |
| 289 | 61.91 | 100 | 100 | 0.49 | 0.32 |
| 324 | 60.08 | 100 | 100 | 0.56 | 0.39 |

Khi kích thước của logo thay đổi từ 64 ($8 \times 8$ pixel) sang 324 ($18 \times 18$ pixel), tính vô hình giảm từ 77.25 xuống 60.08. Điều này cho thấy rằng việc tăng kích thước của thông tin nhúng làm giảm đáng kể tính vô hình của hình ảnh, khiến sự hiện diện của thủy vân dễ bị nhận ra hơn. Tuy nhiên, đáng chú ý là độ ổn định và khả năng đảo ngược vẫn duy trì ở mức 100% với giá trị PSNR đạt $\infty$, điều này có nghĩa là không có sự mất mát thông tin hoặc thay đổi nào về chất lượng hình ảnh. Điều này đảm bảo rằng cả hình ảnh gốc $u$ và thủy vân ẩn $m$ có thể được phục hồi hoàn toàn mà không bị suy giảm chất lượng.

Phân tích bảng 3.2 cho thấy rằng mặc dù kích thước của thông tin nhúng có thể ảnh hưởng đến tính vô hình, phương pháp vẫn duy trì độ ổn định và khả năng đảo ngược tuyệt đối. Đây là một ưu điểm quan trọng, đảm bảo rằng thông tin có thể được nhúng và sau đó khôi phục lại hoàn toàn mà không gây ra bất kỳ tổn thất nào về chất lượng hình ảnh. Từ kết quả này, có thể kết luận rằng việc nhúng thủy vân, dù làm giảm tính vô hình khi kích thước thông tin tăng lên, vẫn đảm bảo sự toàn vẹn và phục hồi hoàn toàn của hình ảnh.

Thời gian nhúng phụ thuộc vào kích thước của hình ảnh gốc, trong khi thời gian trích xuất phụ thuộc vào kích thước của thông tin ẩn (dung lượng). Dung lượng ẩn được đo bằng pixel được phát hiện và do đó được báo cáo cho các hình ảnh thử nghiệm như được hiển thị trong bảng 3.3. Hình ảnh "airplane.png" cung cấp không gian ẩn của 10,496 pixel, chiếm 4% tổng không gian hình ảnh. Tính vô hình cũng được gọi là tải trọng thể hiện mức độ thay đổi bị ảnh hưởng bởi việc nhúng thủy vân.



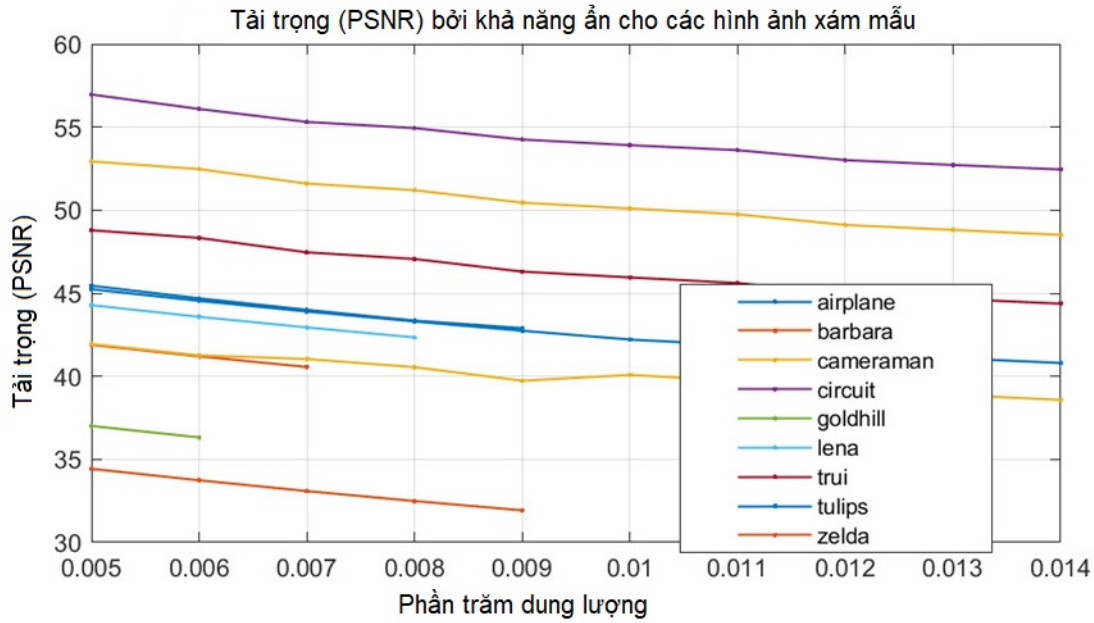

***Hình 3.7:*** *Tính vô hình dựa trên dung lượng ẩn cho các hình ảnh xám mẫu*

Các thí nghiệm được thực hiện với các hình ảnh xám bao gồm "airplane", "baboon", "barbara", "boat", "cameraman", "circuit", "goldhill", "lena", "trui", "tulips" và "zelda". Hình 3.7 trình bày điểm số về tính vô hình của phương pháp trong luận án đối với những hình ảnh này theo khả năng biến đổi. Năm cột cuối của bảng 3.3 cho thấy điểm trung bình về tính vô hình cho phương pháp của luận án và các phương pháp khác.

***Bảng 3.3:*** *Kích thước và dung lượng của các hình ảnh thử nghiệm*

| Ảnh | Độ rộng | Chiều cao | Dung lượng | PSNR | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | Kết quả | [44] | [46] | [50] | [99] |
| airplane | 512 | 512 | 10496 | 56.2 | 48.3 | 48.9 | | |
| baboon | 512 | 512 | 174 | 54.4 | 48.2 | 48.4 | | 48.6 |
| barbara | 512 | 512 | 1966 | 54.2 | | | | 49.1 |
| boat | 512 | 512 | 449 | 53.5 | | | | 48.9 |
| cameraman | 256 | 256 | 1685 | 58.5 | | | | |
| circuit | 272 | 272 | 1883 | 53.4 | | | | |
| goldhill | 512 | 512 | 1690 | 53.5 | | | | 49.0 |
| lena | 512 | 512 | 2258 | 67.4 | 48.2 | 48.8 | 46.9 | |
| trui | 256 | 256 | 1361 | 55.1 | 48.2 | | | 48.9 |
| tulips | 512 | 512 | 3573 | 48.7 | | 48.5 | | |
| zelda | 512 | 512 | 2588 | 41.4 | | | | |

Kết quả từ bảng 3.3 cho thấy rằng dung lượng ẩn của các hình ảnh khác nhau biến đổi từ 174 pixel cho hình ảnh "baboon" đến 10496 pixel cho hình ảnh




***Hình 3.8:*** *Tải trọng (PSNR) theo dung lượng ẩn cho các hình ảnh xám mẫu*

"airplane". Điểm số tính vô hình (PSNR) của phương pháp được đề xuất cho các hình ảnh này dao động từ 41.4 đến 67.4, cho thấy mức độ thay đổi về chất lượng hình ảnh do việc nhúng thủy vân. Cụ thể, hình ảnh "lena" đạt PSNR cao nhất là 67.4, trong khi hình ảnh "zelda" có PSNR thấp nhất là 41.4.

So sánh với các phương pháp khác như được trình bày trong các cột từ [44], [46], [50] và [99], phương pháp của luận án đạt điểm số cao hơn trong một số trường hợp, đặc biệt là đối với hình ảnh "airplane" và "lena". Tuy nhiên, một số hình ảnh như "zelda" vẫn còn gặp khó khăn với điểm số PSNR thấp hơn so với các phương pháp khác.

Luận án đã được nghiên cứu cách thức dung lượng thông tin ẩn ảnh hưởng đến lượng dữ liệu có thể nhúng vào hình ảnh (tải trọng) một cách có ý nghĩa. Bằng cách thiết lập kích thước của thông tin ẩn từ 0.005 đến 0.014 so với kích thước tổng thể của hình ảnh gốc, luận án đã vẽ được đồ thị tải trọng, từ đó cho thấy một mối quan hệ tỉ lệ nghịch giữa kích thước thông tin ẩn và khả năng nhúng dữ liệu (tải trọng) vào hình ảnh (được minh họa qua hình 3.8).

Mục tiêu của thủy vân thuận nghịch là khôi phục cả hình ảnh gốc và thủy vân. Điểm đầu tiên là luận án có thể mang lại khả năng khôi phục toàn bộ hình ảnh gốc và thủy vân, như bảng 3.3 cho thấy 100% cho các cột về độ ổn định và khả năng đảo ngược.

Tại dòng 14 của thuật toán 1, điều kiện của $(|c_1 - c_2| + |c_1 - c_3|)$ được xem

xét để làm cho $c_2$, $c_3$ càng gần $c_1$ càng tốt, nhằm giảm thiểu tải trọng. Thực tế, yếu tố cấu trúc $h$ và các giá trị mã $c_1$, $c_2$, $c_3$ đóng vai trò như khóa bí mật để phát hiện thủy vân và khôi phục hình ảnh gốc. Đây là một giải pháp hiệu quả với một khóa gọn nhẹ vì luận án đã chọn yếu tố cấu trúc để đạt được điều này. Trong khi sử dụng phép xói mòn hình học bằng yếu tố cấu trúc $h$ trong phương pháp của luận án, các thao tác trên hình ảnh đã thủy vân bằng cách cắt, xoay, phóng to và thêm nhiễu ngăn cản việc khôi phục thủy vân và hình ảnh gốc. Do đó, việc thử nghiệm và triển khai các kịch bản thực tế mà thủy vân dễ vỡ [99] được yêu cầu là quan trọng.

Để thu được một thuật toán thủy vân thực tế, luận án cũng cần đảm bảo rằng độ phức tạp [100] để phát hiện thủy vân là cao nhằm giữ bí mật cho thủy vân. Do đó, theo các dòng mã 11-13 của thuật toán I, $256^3$ tổ hợp giá trị cho $c_1$, $c_2$, $c_3$ được xem xét. Với kích thước của yếu tố cấu trúc $h$ là một số nhị phân, tổng số các số thập phân có thể là $2^{\text{size(h)-1}}$ . Sự xói mòn hình học và các phép tính khác trên các yếu tố hình ảnh chủ $u$ yêu cầu thời gian tính toán tỷ lệ với size(u). Do đó, độ phức tạp của việc phát hiện thủy vân trong luận án này có thể được viết như sau:

$$\text{complexity } = \Theta\left(256^3 2^{\text{size(h)-1}} \text{ size } (u)\right) \tag{3.21}$$

Lưu ý rằng độ phức tạp trên là để tránh phát hiện thủy vân từ bên thứ ba. Độ phức tạp này đủ cao để bảo mật thủy vân. Thuật toán 1 sử dụng lệnh "break" trong dòng 17 để dừng tính toán ngay khi tìm thấy yếu tố cấu trúc $h$ đầu tiên. Điều này nhằm tối ưu hóa thời gian tính toán cho việc tạo ra một yếu tố cấu trúc. Tuy nhiên, bằng cách tìm kiếm tất cả các yếu tố cấu trúc có thể và chọn một với dung lượng tốt nhất, luận án đã thống kê dung lượng của mỗi hình ảnh xám trong bảng 3.3.

Như đã đề cập trước đây, yếu tố cấu trúc là chìa khóa chính được sử dụng trong giai đoạn ẩn và trích xuất. Áp dụng xói mòn hình học với yếu tố cấu trúc này tạo ra vị trí tìm kiếm để ẩn. Do đó, việc tìm kiếm với điều kiện hạn chế cho phép duy trì độ bảo mật cao nhưng dung lượng bị hạn chế. Ví dụ, một phương pháp thủy vân thuận nghịch sử dụng mức pixel tối đa và tối thiểu của biểu đồ hình ảnh để nhúng dữ liệu bí mật bằng cách dịch chuyển biểu đồ [44]. Phát hiện dữ liệu ẩn cần tìm hai giá trị xám và kiểm tra toàn bộ không gian hình ảnh. Do đó, độ phức tạp trong việc phát hiện của thuật toán là $\Theta\left(256^2 \text{ size(u)}\right)$.

Lỗi nội suy được xem xét như một sự khác biệt giữa giá trị pixel nội suy và

***Bảng 3.4:*** *Khóa cho việc trích xuất và độ phức tạp phát hiện*

| **Phương pháp** | **Chìa khóa** | **Độ phức tạp phát hiện** |
|---|---|---|
| Xác định mức pixel cực đại và cực tiểu trên histogram hình ảnh và dịch chuyển histogram [44] | 2 giá trị xám | $\Theta\left(256^2\,\mathrm{size(u)}\right)$ |
| Dịch chuyển histogram của hình ảnh hiệu biệt [101] | 3 giá trị, 2 giá trị xám | $\Theta\left(255^2\,\mathrm{size(u)}\right)$ |
| Kỹ thuật nội suy [46] | Lọc nội suy, khác | $\Theta(\mathrm{size(f)}\,\mathrm{size(u)}$ |
| Bit quan trọng nhất [48] | Hai chìa | $\Theta(\mathrm{size(key)}\,\mathrm{size(u)}$ |
| Mô hình cảm nhận thị giác [50] | Một chìa | $\Theta(\mathrm{size(key)}\,\mathrm{size(u))}$ |
| Phương pháp của chúng tôi | $c_1, c_2, c_3$ element $h$ | $\Theta\left(256^3 2^{\mathrm{size(h)-1}}\ \mathrm{size(u))}\right.$ |

giá trị pixel tương ứng đã được đề xuất làm cơ sở cho việc thủy vân thuận nghịch trong tài liệu [46]. Độ phức tạp của phương pháp này chủ yếu phụ thuộc vào kích thước bộ lọc nội suy và kích thước hình ảnh gốc: $\Theta(\mathrm{size(f)}\,\mathrm{size(u)})$. Phương pháp dịch chuyển biểu đồ được giới thiệu trong [45] nhằm áp dụng cho hình ảnh chênh lệch giữa hình ảnh gốc đã chỉnh sửa và hình ảnh dự đoán. Thông tin quan trọng để trích xuất thủy vân gồm có hai ngưỡng $T_0$, $T_1$, một số nguyên nhỏ và hai giá trị xám. Điều này chỉ ra rằng, với khu vực giá trị hạn chế của các ngưỡng và số nguyên, độ phức tạp phát hiện của thuật toán là $\Theta\left(256^2\,\mathrm{size(u)}\right)$.

Một cái nhìn hữu ích về bit quan trọng nhất (MSB) cho việc ẩn dữ liệu thuận nghịch trong hình ảnh được mã hóa được cung cấp bởi [48]. Tại đây, lỗi dự đoán được nhấn mạnh và hình ảnh mã hóa được chỉnh sửa cho phù hợp. Để ẩn thông điệp lớn, đa số các giá trị MSB trong hình ảnh được thay đổi.

Để tái tạo dữ liệu hình ảnh gốc, cần có khóa ẩn dữ liệu và khóa mã hóa. Phát hiện những khóa này cho hình ảnh gốc có thể yêu cầu một độ phức tạp là $\Theta$ (size(key)size(u)). Khi xem xét mô hình cảm nhận thị giác cho việc nhìn thấy thủy vân [50], có thể lựa chọn vị trí nhúng dữ liệu trong hình ảnh mã hóa. Phương pháp này sử dụng một khóa trong khoảng [0,1] cho việc nhúng dữ liệu. Từ đó, độ phức tạp phát hiện của phương pháp là $\Theta$ (size(key)size(u)).

Cuối cùng, bảng 3.4 tổng kết các khóa quan trọng dùng cho việc trích xuất và đánh giá độ phức tạp trong việc phát hiện của các phương pháp đã được bàn luận trước đó. Phương pháp dựa trên mô hình nhận thức thị giác [50] chỉ yêu cầu một khóa duy nhất cho thấy sự đơn giản trong quá trình trích xuất

thủy vân. Trong khi đó, phương pháp sử dụng kỹ thuật nội suy [46] yêu cầu các khóa chứa lượng thông tin lớn hơn làm tăng độ phức tạp trong việc trích xuất.

Luận án áp dụng ba giá trị màu xám và một yếu tố cấu trúc làm khóa. Điều này làm tăng độ phức tạp trong việc phát hiện do sự đa dạng của ba giá trị màu xám và yếu tố cấu trúc. Sự phức tạp này được minh chứng qua các chỉ số đo lường khả năng phát hiện thủy vân, cho thấy rằng phương pháp này đòi hỏi một lượng thông tin và tính toán nhiều hơn so với các phương pháp khác.

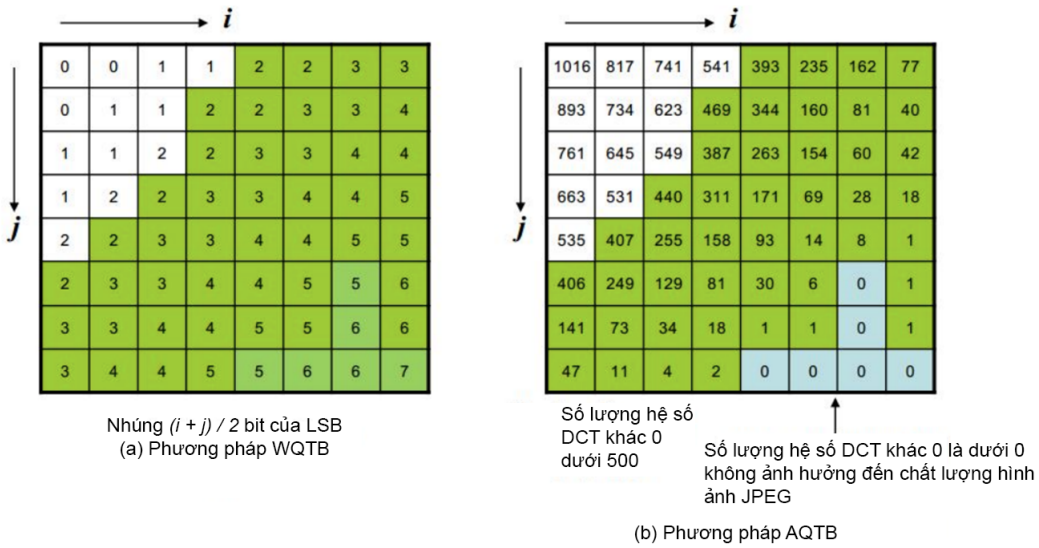
Bảng 3.4 trình bày các phương pháp khác nhau và các khóa cần thiết cho việc trích xuất thông tin thủy vân. Các phương pháp bao gồm xác định mức pixel cực đại và cực tiểu trên histogram hình ảnh và dịch chuyển histogram [44], dịch chuyển histogram của hình ảnh hiệu biệt [101], kỹ thuật nội suy [46], bit quan trọng nhất [48] và mô hình cảm nhận thị giác [50]. Phương pháp xác định mức pixel cực đại và cực tiểu trên histogram hình ảnh và dịch chuyển histogram [44] sử dụng 2 giá trị xám với độ phức tạp $\Theta(256^2 \cdot \text{size}(u))$. Phương pháp dịch chuyển histogram của hình ảnh hiệu biệt [101] sử dụng 3 giá trị và 2 giá trị xám với độ phức tạp $\Theta(255^2 \cdot \text{size}(u))$. Kỹ thuật nội suy [46] sử dụng lọc nội suy và các giá trị khác với độ phức tạp $\Theta(\text{size}(f) \cdot \text{size}(u))$. Phương pháp bit quan trọng nhất [48] sử dụng hai chìa khóa với độ phức tạp $\Theta(\text{size(key)} \cdot \text{size}(u))$. Mô hình cảm nhận thị giác [50] chỉ yêu cầu một chìa khóa với độ phức tạp $\Theta(\text{size(key)} \cdot \text{size}(u))$. Phương pháp của luận án sử dụng các khóa $c1, c2, c3$ và yếu tố $h$ với độ phức tạp $\Theta\left(256^3 2^{\text{size(h)-1 size(u))}}\right)$.

Phương pháp của luận án mặc dù phức tạp hơn nhưng lại cung cấp độ chính xác và an toàn cao hơn trong việc bảo vệ thông tin thủy vân. Điều này đặc biệt quan trọng trong các ứng dụng đòi hỏi tính bảo mật cao, nơi mà khả năng phát hiện và phục hồi thủy vân cần được đảm bảo. Bảng 3.4 cho thấy rằng việc sử dụng nhiều khóa phức tạp có thể tăng cường độ bảo mật nhưng cũng đi kèm với thách thức về độ phức tạp trong việc xử lý và trích xuất thông tin.

## 3.3. Phương pháp sử dụng miền DCT

Mục này cũng tập trung vào việc đề xuất tăng khả năng đảo ngược của phương pháp RDH bằng cách khai thác đặc điểm của hình ảnh JPEG. Luận án sử dụng bảng tỉ lệ lượng tử $Q_y$, $Q_{cb}$, $Q_{cr}$ vì mỗi bảng này được xác định bởi yếu tố chất lượng QF cụ thể.

Tác động của $Q_y, Q_{cb}, Q_{cr}$ đối với các giá trị của các hệ số DCT đang được




***Hình 3.9:*** *Số lượng hệ số DCT khác không của hình ảnh Girl*

nghiên cứu. Tổng số hệ số DCT không bằng không trong toàn bộ hình ảnh JPEG được ký hiệu là $N_z(i,j)$ được xác định. Ở đây, $(i,j)$ biểu thị tọa độ của các hệ số tỉ lệ lượng tử $Q_t(i,j)$ (với $t$ là $\vdash y, cb, cr$) trong bảng tỉ lệ lượng tử $Q_y, Q_cb, Q_{cr}$. Phần này tập trung vào việc nghiên cứu tác động của các bảng tỉ lệ lượng tử đối với hệ số độ sáng trong hình ảnh JPEG.

Luận án giả định rằng các hệ số tỉ lệ lượng tử $Q_t(i,j)$ có tác động lớn đối với số lượng lớn hệ số DCT không bằng 0 trong toàn bộ hình ảnh JPEG. Do đó, nếu thông tin bí mật $W$ được nhúng vào các hệ số tỉ lệ lượng tử $Q_t(i,j)$ có tác động ít đến các hệ số DCT của hình ảnh JPEG, luận án có thể làm tăng khả năng lưu trữ trong khi duy trì chất lượng của hình ảnh JPEG.

Để thể hiện tác động của bảng $Q_y, Q_cb, Q_{cr}$ đối với các hệ số DCT, luận án đã phân tích số lượng hệ số DCT không bằng 0 trong hình ảnh "Girl". Hình 3.9 thể hiện tần suất của các hệ số DCT không bằng 0 từ toàn bộ thành phần $Y$ của hình ảnh "Girl".

Dựa trên kết quả của hình 3.9(b), luận án xem xét rằng nếu $N_z(i,j) = 0$ thì các hệ số tỉ lệ lượng tử $Q_t(i,j)$ tương ứng không ảnh hưởng đến chất lượng của hình ảnh JPEG. Lý do là theo thuật toán của hình ảnh JPEG, các hệ số DCT không bằng 0 không có ý nghĩa trong quá trình tỉ lệ lượng tử.

Nếu $N_z(i,j) \leq T_q$ ($T_q$ là ngưỡng tiền tố) thì các hệ số tỉ lệ lượng tử $Q_t(i,j)$ tương ứng ảnh hưởng ít đến chất lượng của hình ảnh JPEG.

Dựa trên quá trình phân tích trên, luận án đề xuất phương pháp RDH mới bằng cách sử dụng việc nhúng bảng tỉ lệ lượng tử như sau:

### 3.3.1. Phương pháp nhúng sử dụng trọng số cho bảng tỉ lệ lượng tử

Miền nhúng của phương pháp đề xuất trong luận án được hiển thị theo hình 3.9(a). Trọng số của luận án cho bảng tỉ lệ lượng tử (Weights for quantization table - WQTB) tập trung vào miền tần số thấp và tần số trung bình cho việc nhúng thông thường theo phương pháp của Tian. Ngoài ra, phương pháp của luận án còn bao gồm miền của các bảng tỉ lệ lượng tử để tăng khả năng lưu trữ.

Bởi vì giá trị của các hệ số DCT từ miền tần số cao của hình ảnh JPEG gần như bằng 0, luận án quyết định nhúng $(i+j)/2$ bit vào các hệ số tỉ lệ lượng tử.

Luận án kỳ vọng rằng phương pháp nhúng áp dụng cho các hệ số tỉ lệ lượng tử của các hệ số DCT bằng 0 (miền tần số cao) sẽ không làm giảm chất lượng của hình ảnh JPEG nhiều. Điều này làm cho phương pháp của luận án có thể cải thiện khả năng lưu trữ và chất lượng.

### 3.3.2. Phương pháp nhúng sử dụng tần số của các hệ số DCT khác không

Để tránh làm giảm chất lượng của hình ảnh JPEG, luận án xem xét những yếu tố không ảnh hưởng đến chất lượng của hình ảnh đã được nhúng. Ý tưởng được thể hiện trong hình 3.9(b), luận án tính toán số lượng tất cả các hệ số DCT bằng 0 từ mỗi vị trí $(i, j)$ của các bảng lượng tử (All zero DCT coefficients from each position of quatization tables - AQTB), được gọi là $N_z(i, j)$. Sau khi xác định $N_z(i, j)$, phương pháp của luận án nhúng thông tin vào các hệ số chất lượng $Q_t(i, j)$.

Phương pháp nhúng thông tin sử dụng kỹ thuật mở rộng khác biệt (Difference Expansion - DE) [56] nhằm đảm bảo rằng thông tin có thể được nhúng một cách hồi phục mà không gây ảnh hưởng đáng kể đến chất lượng hình ảnh. Các bước chính của phương pháp này bao gồm:

1. Tính toán giá trị trung bình và khác biệt:

Với mỗi cặp giá trị pixel $(x, y)$, tính toán giá trị trung bình $\overline{a}$ và giá trị khác biệt $d$ như sau:

$$\overline{a} = \left\lfloor \frac{x+y}{2} \right\rfloor \tag{3.22}$$

$$d = x - y \tag{3.23}$$

2. Mở rộng khác biệt (Difference Expansion - DE):

Sử dụng giá trị khác biệt $d$ để tạo ra giá trị khác biệt mới $d'$ bằng cách nhúng một bit thông tin vào vị trí thấp nhất (Least Significant Bit - LSB) của $d$:

$$d' = 2d + b \tag{3.24}$$

Trong đó, $b$ là bit thông tin cần nhúng.

3. Tính toán lại giá trị pixel:

Dựa trên giá trị trung bình $\overline{a}$ và giá trị khác biệt mới $d'$, tính toán lại cặp giá trị pixel $(x', y')$ như sau:

$$x' = \overline{a} + \left\lceil \frac{d'}{2} \right\rceil \tag{3.25}$$

$$y' = \overline{a} - \left\lfloor \frac{d'}{2} \right\rfloor \tag{3.26}$$

4. Nhúng thông tin vào các hệ số lượng tử hóa $Qt(i, j)$:

- Nếu $N_z(i, j) = 0$, thay $Q_t(i, j)$ bằng 8 bit thông tin bí mật từ $W$.
- Nếu $N_z(i, j) < T_q$, nhúng bit thông tin $b$ vào $LSB$ của $Q_t(i, j)$.
- Nếu $N_z(i, j) \leq T_q$, không nhúng gì.

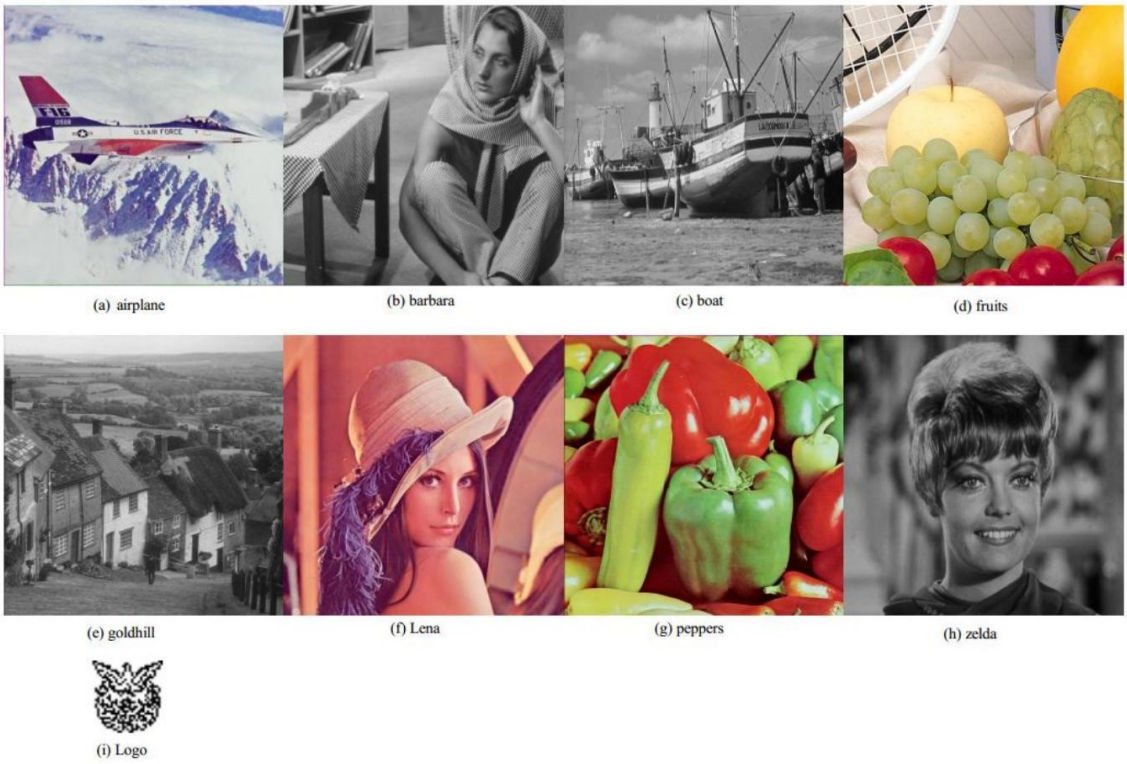
5. Bảo toàn thông tin gốc và tính toàn vẹn:

Thu thập giá trị LSB gốc của các giá trị khác biệt đã thay đổi và nhúng chúng cùng với thông tin xác thực vào trong giá trị khác biệt mới.

Phương pháp này đảm bảo rằng thông tin nhúng có thể được phục hồi hoàn toàn và chất lượng hình ảnh JPEG sau khi nhúng thông tin không bị suy giảm đáng kể.

### 3.3.3. Kết quả thực nghiệm

Hiện nay, hiệu suất của phương pháp đề xuất được đánh giá bằng cách sử dụng tám hình ảnh trong hình 3.10, mỗi hình có kích thước 512 × 512. Những hình ảnh này, gọi là "airplane", "barbara", "boat", "fruits", "goldhill", "lena",




***Hình 3.10:*** *Tám hình ảnh kiểm tra*

"peppers" và "zelda", được nén bằng công cụ IJG toolboxb với hệ số chất lượng $QF = 75$. Các bit thông điệp bí mật được trích xuất từ hình ảnh mức xám trong hình 3.10(i) có kích thước 32×32. Ngưỡng $T_q$ được đặt dựa theo kinh nghiệm là 500, được xác định dựa trên cuộc khảo sát về tần số của các hệ số DCT khác 0 bằng không được hiển thị trong 3.9(b). Ở vùng tần số thấp, số lượng các hệ số DCT khác 0 bằng không luôn lớn hơn 500. Do đó, việc nhúng thông tin vào vùng tần số thấp có thể ảnh hưởng xấu đến chất lượng của hình ảnh JPEG. Đề xuất trong tương lai là cần xác định ngưỡng $T_q$ phù hợp cho các cơ sở dữ liệu hình ảnh lớn hơn.

Luận án nhúng biểu tượng trong hình 3.10(i) vào các hình ảnh JPEG kiểm tra dựa trên thuật toán của Tian [56], sử dụng bảng lượng tử hóa (AQTB) và sử dụng bảng lượng tử hóa có trọng số (WQTB). Sau khi nhúng thông tin, luận án tính toán khả năng chứa của những thí nghiệm này và so sánh chúng với nhau.

Kết quả của phương pháp đề xuất được hiển thị trong bảng 3.5. Dựa theo so sánh trong bảng, phương pháp đề xuất của luận án đã thể hiện sự cải thiện đáng kể về khả năng chứa dữ liệu so với các phương pháp trước đây. Bảng 3.5 so sánh số bit nhúng được vào các hình ảnh JPEG khác nhau khi sử dụng phương pháp AQTB (All-zero Quantization Table Based) và WQTB (Weighted

***Bảng 3.5:*** *So sánh khả năng chứa (bits)*

| Ảnh JPEG (QF = 75) | [56] | AQTB | WQTB |
|---|---|---|---|
| airplane | 5969 | 6483 | 6385 |
| barbara | 5654 | 6266 | 6070 |
| boat | 5684 | 6296 | 6100 |
| fruits | 6384 | 6797 | 6800 |
| goldhill | 5744 | 6258 | 6160 |
| lena | 6424 | 7026 | 6840 |
| peppers | 5625 | 6194 | 6041 |
| zelda | 5918 | 6619 | 6334 |

Quantization Table Based).

Trong bảng, các giá trị số bit nhúng được vào hình ảnh như "airplane", "barbara", "boat", "fruits", "goldhill", "lena", "peppers" và "zelda" cho thấy phương pháp WQTB có khả năng chứa dữ liệu cao hơn AQTB và phương pháp trước đó [56]. Cụ thể, hình ảnh "airplane" với phương pháp AQTB có thể chứa 6483 bit, trong khi phương pháp WQTB chứa 6385 bit, cao hơn nhiều so với phương pháp cũ là 5969 bit. Tương tự, hình ảnh "lena" với phương pháp WQTB chứa 6840 bit so với 6424 bit của AQTB và 7026 bit của phương pháp cũ cho thấy sự cải thiện rõ rệt.

Điều này chứng tỏ rằng phương pháp đề xuất của luận án có hiệu suất tốt hơn trong việc tận dụng các khu vực không ảnh hưởng đến chất lượng của hình ảnh JPEG để nhúng thông tin, từ đó tăng khả năng chứa của hình ảnh. Khả năng chứa dữ liệu cao hơn đồng nghĩa với việc phương pháp này không chỉ giữ được chất lượng hình ảnh mà còn đảm bảo được tính toàn vẹn và bảo mật của thông tin nhúng. Phương pháp mới này cho phép tăng cường dung lượng nhúng mà không gây suy giảm đáng kể chất lượng hình ảnh, đặc biệt quan trọng trong các ứng dụng đòi hỏi tính bảo mật và khả năng phục hồi cao.

## 3.4. Kết luận

Trong chương 3, luận án đã đề xuất và phát triển các phương pháp thủy vân mới nhằm đảm bảo tính toàn vẹn của ảnh gốc và nâng cao hiệu quả bảo mật. Các phương pháp chính được giới thiệu bao gồm việc sử dụng yếu tố cấu trúc và ứng dụng miền tần số trong thuật toán JPEG.

Đóng góp chính của chương 3 bao gồm:

- Phương pháp thủy vân sử dụng yếu tố cấu trúc:

  - Đảm bảo khả năng phục hồi hình ảnh gốc: Sử dụng yếu tố cấu trúc để nhúng thông tin một cách an toàn và chính xác, giúp phục hồi hình ảnh gốc từ các thay đổi trong quá trình nhúng dữ liệu.

  - Tăng dung lượng nhúng dữ liệu: Yếu tố cấu trúc không chỉ đảm bảo tính an toàn mà còn tăng dung lượng nhúng dữ liệu mà không ảnh hưởng đến chất lượng của hình ảnh.

  - Duy trì độ phức tạp phát hiện cao: Tăng cường bảo mật bằng cách duy trì độ phức tạp trong việc phát hiện thông tin nhúng.

- Phương pháp sử dụng miền tần số với thuật toán JPEG:

  - Hiệu quả của các hệ số lượng tử trên bảng DCT: Khảo sát và tối ưu hóa các hệ số lượng tử trên bảng DCT để quyết định cách nhúng thông tin thủy vân, giúp tăng dung lượng và cải thiện chất lượng của hình ảnh JPEG sau khi nhúng dữ liệu.

  - Ứng dụng nhiều bảng lượng tử: Áp dụng nhiều bảng lượng tử trong thuật toán JPEG để tối ưu hóa quá trình nhúng thông tin, đảm bảo tính ổn định và bền vững của thông tin thủy vân.

Kết hợp hai phương pháp này, luận án đã mở ra một hướng tiếp cận mới trong việc bảo vệ quyền sở hữu trí tuệ và an ninh nội dung trong môi trường số. Phương pháp sử dụng yếu tố cấu trúc và miền tần số trong thuật toán JPEG không chỉ cải thiện khả năng bảo mật mà còn đảm bảo khả năng phục hồi dữ liệu chính xác. Các kết quả thực nghiệm đã chứng minh hiệu quả của phương pháp, thể hiện sự ưu việt so với các phương pháp truyền thống cả về dung lượng nhúng dữ liệu và chất lượng hình ảnh sau khi nhúng dữ liệu.

Những đóng góp quan trọng của chương 3 bao gồm việc phát triển và áp dụng các phương pháp thủy vân tiên tiến sử dụng yếu tố cấu trúc và miền tần số trong thuật toán JPEG. Các phương pháp này không chỉ đảm bảo tính toàn vẹn và bảo mật của ảnh gốc mà còn mở ra các hướng tiếp cận mới trong lĩnh vực thủy vân số, đáp ứng yêu cầu ngày càng cao về bảo vệ quyền sở hữu trí tuệ trong môi trường số.

# KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TRONG TƯƠNG LAI

## 1. Kết luận

Luận án này đã đạt được những đóng góp chính sau đây trong lĩnh vực thủy vân số:

**Phát triển kỹ thuật thủy vân dựa trên đặc trưng độ nổi bật của ảnh số:**

- Tăng cường tính bí mật: Phương pháp thủy vân dựa trên độ nổi bật đã tận dụng các đặc trưng thị giác để nhúng thông tin vào các vùng ít thu hút sự chú ý trong ảnh, giúp thông tin thủy vân khó bị phát hiện bằng mắt thường mà không làm giảm chất lượng thị giác của ảnh.

- Khả năng chống lại tấn công: Phương pháp này cải thiện khả năng chống lại các tấn công phổ biến như cắt, xoay và nén ảnh, đảm bảo tính bền vững của thông tin thủy vân trong các điều kiện xử lý khác nhau.

**Phát triển kỹ thuật thủy vân thuận nghịch đảm bảo tính toàn vẹn của ảnh gốc:**

- Khả năng phục hồi ảnh gốc: Kỹ thuật thủy vân thuận nghịch cho phép nhúng thông tin vào ảnh mà sau khi trích xuất, ảnh gốc có thể được phục hồi hoàn toàn, đảm bảo không có sự thay đổi nào về chất lượng hình ảnh ban đầu.

- Hiệu suất nhúng cao: Các thuật toán mới cho phép nhúng một lượng lớn dữ liệu mà không làm giảm đáng kể chất lượng thị giác của ảnh, mở rộng khả năng ứng dụng trong các lĩnh vực đòi hỏi bảo mật cao như tài liệu pháp lý và hình ảnh y tế.

**Ứng dụng thực tiễn và khả năng mở rộng:**

- Đa dạng ứng dụng: Các phương pháp thủy vân được đề xuất có thể ứng dụng trong nhiều lĩnh vực đòi hỏi bảo mật cao, như bảo vệ bản quyền cho tài liệu pháp lý, hình ảnh y tế, và các sản phẩm số khác.

- Tích hợp công nghệ tiên tiến: Nghiên cứu khả năng tích hợp các giải pháp thủy vân với công nghệ nhận dạng và phân tích ảnh tiên tiến để nâng cao hiệu quả bảo vệ quyền sở hữu trí tuệ trong môi trường số phức tạp.

***Bảng 3.6:*** *So sánh các kỹ thuật trong chương 2 và chương 3*

| **Tiêu chí** | **Thủy vân dựa trên đặc trưng độ nổi bật** | **Thủy vân thuận nghịch** |
|---|---|---|
| Tính bí mật | Cao | Trung bình |
| Khả năng chống tấn công | Cao | Cao |
| Khả năng phục hồi ảnh gốc | Không | Hoàn toàn |
| Hiệu suất nhúng | Trung bình | Cao |
| Ứng dụng thực tế | Ảnh số có yêu cầu cao về chất lượng thị giác | Ảnh số cần bảo toàn tính nguyên vẹn của ảnh gốc |
| Mức độ phức tạp tính toán | Trung bình | Cao |

Từ bảng 3.6, luận án cho thấy những ứng dụng phù hợp cho mỗi kỹ thuật như sau:

- Các kỹ thuật thủy vân dựa trên đặc trưng độ nổi bật phù hợp với các trường hợp cần bảo vệ quyền sở hữu trí tuệ mà không làm giảm chất lượng thị giác của ảnh. Phương pháp này lý tưởng cho các ứng dụng như ảnh nghệ thuật, ảnh quảng cáo, và các nội dung số yêu cầu độ chính xác cao về thị giác.

- Kỹ thuật thủy vân thuận nghịch thích hợp cho các trường hợp mà việc bảo toàn hoàn toàn ảnh gốc là rất quan trọng, như trong lĩnh vực y tế, pháp lý và các tài liệu quan trọng khác. Kỹ thuật này đảm bảo rằng sau khi thông tin được trích xuất, ảnh gốc có thể được khôi phục hoàn toàn mà không mất bất kỳ thông tin nào.

**2. Hướng nghiên cứu trong tương lai**

Hướng nghiên cứu trong tương lai sau khi hoàn thành luận án này mở ra nhiều khả năng phát triển và cải tiến cho các phương pháp thủy vân số, với mục tiêu tăng cường bảo mật, tính linh hoạt và hiệu quả ứng dụng trong các tình huống thực tế. Một số hướng có thể được khám phá bao gồm:

1. Tối ưu hóa thuật toán: Cải thiện và tối ưu hóa các thuật toán thủy vân dựa trên độ nổi bật và thuận nghịch hiện tại, nhằm giảm thời gian xử lý và tăng khả năng nhúng thông tin mà không làm mất đi chất lượng hình ảnh. Cụ thể, việc ứng dụng công nghệ học sâu và học máy trong việc tìm kiếm và xác định các vùng tối ưu cho việc nhúng thủy vân có thể mang lại hiệu quả cao.

2. Mở rộng ứng dụng: Nghiên cứu ứng dụng của thủy vân số trong các

lĩnh vực mới như video số, âm thanh số và các tài liệu đa phương tiện khác. Điều này bao gồm việc phát triển các phương pháp thủy vân đặc biệt cho từng loại dữ liệu cụ thể, với các yêu cầu bảo mật và chất lượng khác nhau.

3. Tăng cường bảo mật: Phát triển các kỹ thuật mới để tăng cường bảo mật cho thủy vân số, bao gồm việc kháng lại các cuộc tấn công phá hoại và nỗ lực giả mạo. Việc tích hợp các phương pháp mã hóa tiên tiến vào quá trình thủy vân có thể là một lĩnh vực quan trọng để khám phá.

4. Phân tích độ nổi bật cải tiến: Tiếp tục nghiên cứu và phát triển các mô hình độ nổi bật tiên tiến, tận dụng sức mạnh của AI và học sâu để chính xác hơn trong việc dự đoán và phân tích sự chú ý của người xem. Điều này giúp tối ưu hóa vị trí và kích thước của thủy vân, đồng thời duy trì tính thẩm mỹ của ảnh gốc.

5. Thích ứng với biến đổi định dạng: Nghiên cứu khả năng của thủy vân số trong việc thích ứng và bảo tồn thông tin qua các biến đổi định dạng như nén ảnh hoặc thay đổi kích thước là một lĩnh vực quan trọng khác. Phát triển các phương pháp thủy vân có khả năng duy trì tính toàn vẹn thông qua các quá trình xử lý hình ảnh là một mục tiêu đáng giá.

Những hướng nghiên cứu này không chỉ mở ra cánh cửa cho sự tiến bộ trong kỹ thuật thủy vân số mà còn hỗ trợ sự phát triển của các ứng dụng bảo mật trong thời đại số, đáp ứng nhu cầu ngày càng tăng về bảo vệ thông tin và quyền sở hữu trí tuệ.

# DANH MỤC CÔNG TRÌNH CÔNG BỐ


1. Pham Quang Huy and Ta Minh Thanh, "Cross-frequency domain for jpeg inversible watermarking using multiple quantization tables", Journal of Science and Technique-Section on Information and Communication Technology, vol. 12, no. 01, 2023, doi: 10.56651/$lqdtu.jst.v12.n1.660.ict$.

2. Pham Quang Huy and Dao Nam Anh, "A new approach to Anti-Forgery using Saliency Guided Image Watermarking", Journal of Computer Science and Cybernetics, 2024 (accepted).

3. Pham Quang Huy, Ta Minh Thanh, Le Danh Tai, Pham Van Toan, "Cross-domain using composing of selected dct coefficients strategy with quantization tables for reversible data hiding in jpeg image," in Research in Intelligent and Computing in Engineering: Select Proceedings of RICE 2020. Springer, 2021, pp. 681–693, doi: $10.1007/978-981-15-7527-3\_64$.

4. Dao Nam Anh, Pham Quang Huy, Doan Thi Huong Giang, "Steerable features for resilient image watermark", in 2019 International Conference on Multimedia Analysis and Pattern Recognition (MAPR). IEEE, 2019, pp. 1–6, doi: $10.1109/MAPR.2019.8743544$.

5. Dao Nam Anh, Pham Quang Huy, Luong Chi Mai, "Watermark by learning non-saliency", in Frontiers in Intelligent Computing: Theory and Applications: Proceedings of the 7th International Conference on FICTA (2018), Volume 1. Springer, 2020, pp. 61–72, doi: $10.1007/978-981-32-9186-7\_7$.

6. Dao Nam Anh, Pham Quang Huy, "Structuring Element for Secure Reversible Watermarking", in: 2020 International Conference on Multimedia Analysis and Pattern Recognition (MAPR), IEEE, 2020, pp. 1–6, doi: 10.1109/MAPR49794.2020.9237780.

# TÀI LIỆU THAM KHẢO


[1] Dennis WK Khong. "The historical law and economics of the first Copyright Act". In: *Erasmus L. & Econ. Rev.* 2 (2006), p. 35.

[2] Baiyang Xiao. *The intricate interplay between copyright law and technology*. 2024.

[3] Nguyễn Phương Thảo. "Bảo hộ quyền tác giả dưới tác động của Cách mạng công nghiệp 4.0". In: *Tạp chí Khoa học và Công nghệ Việt Nam* (2022).

[4] Võ Trung Hậu. "Pháp luật về bản sao kỹ thuật số". In: *Tạp chí Khoa học và Công nghệ Việt Nam* (2020).

[5] Bích Nguyễn Thị Ngọc. "Luật sở hữu trí tuệ". In: *Trường Đại học Lâm nghiệp* (2021).

[6] Trần Văn Tiến et al. "Xung đột giữa quyền tiếp cận thông tin KH&CN với bảo hộ quyền tác giả tiếp cận dưới giác độ pháp luật". In: *Bản B của Tạp chí Khoa học và Công nghệ Việt Nam* 63.10 (2021).

[7] Lionel Bently et al. *Intellectual property law*. Oxford University Press, 2022.

[8] Quốc Hội. *Luật số: 07/2022/QH15*. 2022.

[9] P Aberna and L Agilandeeswari. "Digital image and video watermarking: methodologies, attacks, applications, and future directions". In: *Multimedia Tools and Applications* 83.2 (2024), pp. 5531–5591.

[10] Mauro Barni and Stefan Katzenbeisser. "Digital watermarking". In: *Handbook of Financial Cryptography and Security*. Chapman and Hall/CRC, 2010, pp. 417–462.

[11] Mukhammad Solikhin et al. "Analisis Watermarking Menggunakan Metode Discrete Cosine Transform (DCT) dan Discrete Fourier Transform (DFT)". In: *Jurnal Sistem Cerdas* 5.3 (2022), pp. 155–170.

[12] Huy Cuong Do, Thai Hung Pham, and Minh Thanh Ta. "Reversible hiding method using secrets sharing of DNA-XNOR". In: *Journal of Science and Technique-Section on Information and Communication Technology* 11.01 (2022). DOI: 10.56651/lqdtu.jst.v11.n01.363.ict.

[13] Cao Thi Luyen, Nguyen Kim Sao, Ta Minh Thanh, et al. "An efficient reversible data hiding based on improved pixel value ordering method". In: *Journal of Computer Science and Cybernetics* 38.2 (2022), pp. 165–180. DOI: 10.15625/1813-9663/38/2/16880.

[14] LTN Giang. "Những thách thức về mặt pháp lý trong việc bảo hộ quyền tác giả trong môi trường internet". In: *Hội thảo Bảo hộ quyền tác giả trong môi trường số tại Việt Nam* (2014).

[15] Sanjay Kumar, Binod Kumar Singh, and Mohit Yadav. "A recent survey on multimedia and database watermarking". In: *Multimedia Tools and Applications* 79 (2020), pp. 20149–20197.

[16] Frank Y Shih. *Digital watermarking and steganography: fundamentals and techniques*. CRC press, 2017.

[17] Laxmanika Singh, Amit Kumar Singh, and Pradeep Kumar Singh. "Secure data hiding techniques: a survey". In: *Multimedia Tools and Applications* 79 (2020), pp. 15901–15921.

[18] IJ Cox. "Digital Watermarking and Steganography". In: *Morgan Kaufmann google schola* 2 (2007), pp. 893–914.

[19] Amrinder Singh Brar and Mandeep Kaur. "Reversible watermarking techniques for medical images with ROI-temper detection and recovery—A survey". In: *Int. J. Emerg. Technol. Adv. Eng.* 2.1 (2012), pp. 32–36. DOI: 10.1007/978-3-642-35864-7.

[20] Frank Y Shih. *Multimedia security: watermarking, steganography, and forensics*. CRC Press, 2017.

[21] Jayachandra Chilukamari. "A computational model of visual attention." PhD thesis. 2017.

[22] Laurent Itti and Christof Koch. "Computational modelling of visual attention". In: *Nature reviews neuroscience* 2.3 (2001), pp. 194–203.

[23] Chun-Hsiang Huang and Ja-Ling Wu. "Attacking visible watermarking schemes". In: *IEEE transactions on multimedia* 6.1 (2004), pp. 16–30.

[24] Deepayan Bhowmik, Matthew Oakes, and Charith Abhayaratne. "Visual attention-based image watermarking". In: *IEEE Access* 4 (2016), pp. 8002–8018.

[25] Yaqing Niu et al. "A visual saliency modulated just noticeable distortion profile for image watermarking". In: *2011 19th European Signal Processing Conference*. IEEE. 2011, pp. 2039–2043.

[26] Yaqing Niu et al. "Visual saliency's modulatory effect on just noticeable distortion profile and its application in image watermarking". In: *Signal Processing: Image Communication* 28.8 (2013), pp. 917–928.

[27] M Kivanc Mihcak et al. "Low-complexity image denoising based on statistical modeling of wavelet coefficients". In: *IEEE Signal Processing Letters* 6.12 (1999), pp. 300–303.

[28] A Watson. "DCT Quantization Matrices Optimized for Individual Images, Human Vision, Visual Processing, and Digital Display IV, vol". In: SPIE. 1993.

[29] Minwoo Sung, Xiaowei Li, and In-Kwon Lee. "Visual perception based robust watermarking with integral imaging". In: *Optik* 127.24 (2016), pp. 11828–11839.

[30] Lihua Tian et al. "An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection". In: *Signal Processing: Image Communication* 26.8-9 (2011), pp. 427–437.

[31] Chunxing Wang et al. "A novel STDM watermarking using visual saliency-based JND model". In: *Information* 8.3 (2017), p. 103.

[32] Abhishek Basu et al. "On the implementation of a saliency based digital watermarking". In: *Information Systems Design and Intelligent Applications: Proceedings of Second International Conference INDIA 2015, Volume 1*. Springer. 2015, pp. 447–455.

[33] Matthew Oakes, Deepayan Bhowmik, and Charith Abhayaratne. "Global motion compensated visual attention-based video watermarking". In: *Journal of Electronic Imaging* 25.6 (2016), pp. 061624–061624.

[34] Ahmed Gawish et al. "Robust Non-saliency guided watermarking". In: *2016 13th Conference on Computer and Robot Vision (CRV)*. IEEE. 2016, pp. 32–36.

[35] Zhengwei Zhang et al. "An improved reversible image watermarking algorithm based on difference expansion". In: *International Journal of Distributed Sensor Networks* 13.1 (2017), p. 1550147716686577.

[36] Sang-Keun Ji et al. "Robust imperceptible video watermarking for MPEG compression and DA-AD conversion using visual masking". In: *Digital-Forensics and Watermarking: 14th International Workshop, IWDW 2015, Tokyo, Japan, October 7-10, 2015, Revised Selected Papers 14*. Springer. 2016, pp. 285–298.

[37] Lihua Tian et al. "Authentication and copyright protection watermarking scheme for H. 264 based on visual saliency and secret sharing". In: *Multimedia Tools and Applications* 74 (2015), pp. 2991–3011.

[38] Frank Y Shih and Xin Zhong. "Intelligent watermarking for high-capacity low-distortion data embedding". In: *International Journal of Pattern Recognition and Artificial Intelligence* 30.05 (2016), p. 1654003.

[39] Maedeh Jamali et al. "Adaptive blind image watermarking using fuzzy inference system based on human visual perception". In: *arXiv preprint arXiv:1709.06536* (2017).

[40] Ayan Kumar Bhunia et al. "Sketch2Saliency: Learning to Detect Salient Objects from Human Drawings". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2023, pp. 2733–2743.

[41] Ahmed Khan and KokSheik Wong. "High payload watermarking based on enhanced image saliency detection". In: *Multimedia Tools and Applications* 82.10 (2023), pp. 15553–15571.

[42] Zhongjie Cui et al. "Research on region selection strategy for visible watermark embedding". In: *IETE Technical Review* 38.1 (2021), pp. 5–16.

[43] De Li et al. "A reversible watermarking for image content authentication based on wavelet transform". In: *Signal, Image and Video Processing* (2024), pp. 1–11.

[44] Zhicheng Ni et al. "Reversible data hiding". In: *IEEE Transactions on circuits and systems for video technology* 16.3 (2006), pp. 354–362. DOI: 10.1007/978-3-540-31805-7.

[45] Su-Yeon Shin, Hyang-Mi Yoo, and Jae-Won Suh. "Reversible watermarking based on histogram shifting of difference image between original and predicted images". In: *The eighth international conference on mobile ubiquitous computing, systems, services and technologies, Springer, Berlin, Heidelberg*. 2014, pp. 147–150.

[46] Lixin Luo et al. "Reversible image watermarking using interpolation technique". In: *IEEE Transactions on information forensics and security* 5.1 (2009), pp. 187–193.

[47] Jessica Fridrich, Miroslav Goljan, and David Soukal. "Searching for the stego-key". In: *Security, Steganography, and Watermarking of Multimedia Contents VI*. Vol. 5306. SPIE. 2004, pp. 70–82.

[48] Pauline Puteaux and William Puech. "High-capacity reversible data hiding in encrypted images using MSB prediction". In: *EI: Electronic Imaging*. Vol. 2017. 6. 2017, pp. 10–15.

[49] Chris Solomon and Toby Breckon. *Fundamentals of Digital Image Processing: A practical approach with examples in Matlab*. John Wiley & Sons, 2011.

[50] Yuanzhi Yao et al. "Content-adaptive reversible visible watermarking in encrypted images". In: *Signal Processing* 164 (2019), pp. 386–401.

[51] Asifullah Khan et al. "A recent survey of reversible watermarking techniques". In: *Information sciences* 279 (2014), pp. 251–272.

[52] Mauro Barni and Franco Bartolini. *Watermarking systems engineering: enabling digital assets security and other applications*. Crc Press, 2004.

[53] Ming Chen et al. "Reversible image watermarking based on full context prediction". In: *2009 16th IEEE International Conference on Image Processing (ICIP)*. IEEE. 2009, pp. 4253–4256.

[54] Ta Minh Thanh and Munetoshi Iwakiri. "A proposal of digital rights management based on incomplete cryptography using invariant Huffman code length feature". In: *Multimedia systems* 20 (2014), pp. 127–142. DOI: 10.1007/s00530-013-0327-z.

[55] Jessica Fridrich, Miroslav Goljan, and Rui Du. "Lossless data embedding for all image formats". In: *Security and watermarking of multimedia contents IV*. Vol. 4675. SPIE. 2002, pp. 572–583. DOI: 10.1117/12.465317.

[56] Jun Tian. "Reversible data embedding using a difference expansion". In: *IEEE transactions on circuits and systems for video technology* 13.8 (2003), pp. 890–896. DOI: 10.1109/TCSVT.2003.815962.

[57] Bo Ou et al. "Pairwise prediction-error expansion for efficient reversible data hiding". In: *IEEE Transactions on image processing* 22.12 (2013), pp. 5010–5021. DOI: 10.1109/TIP.2013.2281422.

[58] Bo Ou et al. "High-fidelity reversible data hiding based on geodesic path and pairwise prediction-error expansion". In: *Neurocomputing* 226 (2017), pp. 23–34. DOI: 10.1016/j.neucom.2016.11.017.

[59] Junxiang Wang et al. "Rate and distortion optimization for reversible data hiding using multiple histogram shifting". In: *IEEE transactions on cybernetics* 47.2 (2016), pp. 315–326. DOI: 10.1109/TCYB.2015.2514110.

[60] Md Asikuzzaman et al. "A blind and robust video watermarking scheme using chrominance embedding". In: *2014 International Conference on Digital Image Computing: Techniques and Applications (DICTA)*. IEEE. 2014, pp. 1–6. DOI: 10.1109/DICTA.2014.7008083.

[61] Paul Bao and Xiaohu Ma. "Image adaptive watermarking using wavelet domain singular value decomposition". In: *IEEE transactions on circuits and systems for video technology* 15.1 (2005), pp. 96–102. DOI: 10.1109/TCSVT.2004.836745.

[62] Chin-Chen Chang, Chih-Yang Lin, and Yi-Hsuan Fan. "Lossless data hiding for color images based on block truncation coding". In: *Pattern Recognition* 41.7 (2008), pp. 2347–2357. DOI: 10.1016/j.patcog.2007.12.009.

[63] Md Asikuzzaman et al. "Imperceptible and robust blind video watermarking using chrominance embedding: a set of approaches in the DT CWT domain". In: *IEEE transactions on Information Forensics and Security* 9.9 (2014), pp. 1502–1517. DOI: 10.1109/TIFS.2014.2338274.

[64] Chun-Hsien Chou and Kuo-Cheng Liu. "A perceptually tuned watermarking scheme for color images". In: *IEEE Transactions on Image Processing* 19.11 (2010), pp. 2966–2982. DOI: 10.1109/TIP.2010.2052261.

[65] Martin Kutter and Stefan Winkler. "A vision-based masking model for spread-spectrum image watermarking". In: *IEEE Transactions on Image processing* 11.1 (2002), pp. 16–25. DOI: 10.1109/83.977879.

[66] Ziquan Huang, Bingwen Feng, and Shijun Xiang. "Robust reversible image watermarking scheme based on spread spectrum". In: *Journal of Visual Communication and Image Representation* 93 (2023), p. 103808. DOI: 10.1016/j.jvcir.2023.103808.

[67] Xiaolin Yin et al. "Reversible data hiding in JPEG document images based on zero coefficients embedding". In: *Signal Processing* 206 (2023), p. 108917. DOI: 10.1109/TCSVT.2015.2473235.

[68] Fengyong Li et al. "Reversible data hiding for JPEG images with minimum additive distortion". In: *Information Sciences* 595 (2022), pp. 142–158. DOI: 10.1016/j.ins.2022.02.040.

[69] Heng Yao et al. "Dual-JPEG-image reversible data hiding". In: *Information Sciences* 563 (2021), pp. 130–149. DOI: 10.1016/j.ins.2021.02.015.

[70] Erkut Erdem and Aykut Erdem. "Visual saliency estimation by nonlinearly integrating features using region covariances". In: *Journal of vision* 13.4 (2013), pp. 11–11.

[71] Xiaodi Hou, Jonathan Harel, and Christof Koch. "Image signature: Highlighting sparse salient regions". In: *IEEE transactions on pattern analysis and machine intelligence* 34.1 (2011), pp. 194–201.

[72] Xiaodi Hou and Liqing Zhang. "Saliency detection: A spectral residual approach". In: *2007 IEEE Conference on computer vision and pattern recognition*. Ieee. 2007, pp. 1–8.

[73] Nicolas Riche et al. "Rare: A new bottom-up saliency model". In: *2012 19th IEEE International Conference on Image Processing*. IEEE. 2012, pp. 641–644.

[74] David Barber. *Bayesian reasoning and machine learning*. Cambridge University Press, 2012.

[75] J Susan Milton and Jesse C Arnold. *Schaum's outline of introduction to probability & statistics: Principles & applications for engineering & the computing sciences*. McGraw-Hill Higher Education, 1994.

[76] V Vapnik. “Invited speaker”. In: *IPMU Information Processing and Management* (2014).

[77] Ali Borji et al. “Salient object detection: A benchmark”. In: *IEEE transactions on image processing* 24.12 (2015), pp. 5706–5722.

[78] David MW Powers. “Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation”. In: *arXiv preprint arXiv:2010.16061* (2020).

[79] William E Winkler et al. “Overview of record linkage and current research directions”. In: *Bureau of the Census* 25.4 (2006), pp. 603–623.

[80] K Shivanna, SP Deva, and M Santoshkumar. *Computer Communication, Networking and Internet Security*. 2017.

[81] Laurent Itti, Christof Koch, and Ernst Niebur. “A model of saliency-based visual attention for rapid scene analysis”. In: *IEEE Transactions on pattern analysis and machine intelligence* 20.11 (1998), pp. 1254–1259.

[82] Hae Jong Seo and Peyman Milanfar. “Nonparametric bottom-up saliency detection by self-resemblance”. In: *2009 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*. IEEE. 2009, pp. 45–52.

[83] Shu Fang et al. “Learning discriminative subspaces on random contrasts for image saliency analysis”. In: *IEEE transactions on neural networks and learning systems* 28.5 (2016), pp. 1095–1108.

[84] Matthew Oakes, Deepayan Bhowmik, and Charith Abhayaratne. “Visual attention-based watermarking”. In: *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*. IEEE. 2011, pp. 2653–2656.

[85] Jarno Mielikainen. “LSB matching revisited”. In: *IEEE signal processing letters* 13.5 (2006), pp. 285–287.

[86] Huan Xu, Jianjun Wang, and Hyoung Joong Kim. “Near-optimal solution to pair-wise LSB matching via an immune programming strategy”. In: *Information Sciences* 180.8 (2010), pp. 1201–1217.

[87] Ian T Jolliffe. “Springer series in statistics”. In: *Principal component analysis* 29 (2002), p. 912.

[88] Lingling Wu et al. "Arnold transformation algorithm and anti-Arnold transformation algorithm". In: *2009 first international conference on information science and engineering*. IEEE. 2009, pp. 1164–1167.

[89] Qibin Hou et al. "Deeply supervised salient object detection with short connections". In: *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2017, pp. 3203–3212.

[90] Dennis Wackerly, William Mendenhall, and Richard L Scheaffer. *Mathematical statistics with applications*. Cengage Learning, 2014.

[91] IE Richardson. *Video Coding for Next-generation Multimedia*. 2003.

[92] Dominique Brunet, Edward R Vrscay, and Zhou Wang. "On the mathematical properties of the structural similarity index". In: *IEEE Transactions on Image Processing* 21.4 (2011), pp. 1488–1499.

[93] Nikolay Ponomarenko et al. "Modified image visual quality metrics for contrast change and mean shift accounting". In: *2011 11th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*. IEEE. 2011, pp. 305–311.

[94] François Cayre, Caroline Fontaine, and Teddy Furon. "Watermarking security: theory and practice". In: *IEEE Transactions on signal processing* 53.10 (2005), pp. 3976–3987.

[95] Chris W Honsinger et al. *Lossless recovery of an original image containing embedded data*. US Patent 6,278,791. 2001.

[96] Edward R. Dougherty. "An Introduction to Morphological Image Processing". In: *ISBN 0-8194-0845-X* (1992).

[97] Michael Freeman. *The complete guide to digital photography*. Sterling Publishing Company, Inc., 2008.

[98] Quan Huynh-Thu and Mohammed Ghanbari. "The accuracy of PSNR in predicting video quality for different video scenes and frame rates". In: *Telecommunication Systems* 49 (2012), pp. 35–48.

[99] Roberto Caldelli, Francesco Filippini, and Rudy Becarelli. "Reversible watermarking techniques: An overview and a classification". In: *EURASIP Journal on Information Security* 2010 (2010), pp. 1–19.

[100] Denise Sutherland and Mark Koltko-Rivera. *Cracking Codes and Cryptograms For Dummies*. John Wiley & Sons, 2011.