ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA

NGUYỄN THANH TUẤN

NÂNG CAO HIỆU QUẢ KỸ THUẬT WATERMARKING THIẾU THÔNG TIN TIÊN NGHIỆM CHO ẢNH Y TẾ VÀ ẢNH ĐA KÊNH

Ngành: Kỹ thuật viễn thông
Mã số ngành: 62520208

TÓM TẮT LUẬN ÁN TIẾN SĨ

TP. HỒ CHÍ MINH - NĂM 2023

Công trình được hoàn thành tại **Trường Đại học Bách Khoa – ĐHQG-HCM**

Người hướng dẫn: GS. TS. LÊ TIẾN THƯỜNG

Phản biện độc lập:
Phản biện độc lập:

Phản biện:
Phản biện:
Phản biện:

Luận án sẽ được bảo vệ trước Hội đồng đánh giá luận án họp tại
.....
.....
vào lúc giờ ngày tháng năm

Có thể tìm hiểu luận án tại thư viện:

- Thư viện Trường Đại học Bách Khoa – ĐHQG-HCM
- Thư viện Đại học Quốc gia Tp.HCM
- Thư viện Khoa học Tổng hợp Tp.HCM

CHƯƠNG 1 GIỚI THIỆU

1.1 Mở đầu

Một cách tổng quát, watermarking là kỹ thuật nhúng và trích thông tin vào dữ liệu đa phương tiện. Kỹ thuật watermarking bắt đầu nhận được sự quan tâm từ những năm đầu thập niên 1990, và phát triển nhanh chóng trong nhiều lĩnh vực như bảo vệ bản quyền [5], xác nhận dấu vân tay, chống sao chép, giám sát quảng bá, xác thực dữ liệu, giấu dữ liệu, tạo danh mục, vv. [6, 7]. Mặc dù có nhiều phương pháp watermarking với những ưu điểm khác nhau nhưng bản thân mỗi phương pháp vẫn còn tồn tại một số hạn chế nhất định [8, 9].

Nhìn chung có thể chia phương pháp watermarking ra làm hai loại là có đầy đủ thông tin tiên nghiệm (tường minh) và thiếu thông tin tiên nghiệm (mù). Phần lớn các giải pháp đã công bố cho kết quả tốt với watermarking tường minh nhưng lại bị giới hạn trong phạm vi ứng dụng thực tế do yêu cầu phải có dữ liệu gốc trong quá trình trích thông tin [10]. Ngược lại, các kỹ thuật watermarking thiếu thông tin tiên nghiệm (không cần dữ liệu gốc hoặc đầy đủ các thông số nhúng khi trích thông tin) có phạm vi ứng dụng rộng rãi hơn nhưng cũng đặt ra nhiều thách thức hơn trong việc trích thông tin chính xác trước các loại tấn công khác nhau [11-14]. Mặt khác, trong trường hợp watermarking ảnh, nhiều tác giả chỉ tập trung cải tiến các giải thuật cho một loại ảnh cụ thể, phần lớn là ảnh xám đơn kênh thông thường [15]. Số lượng các nghiên cứu cho các loại ảnh y tế và ảnh đa kênh vẫn còn giới hạn và thách thức [16-19]. Bên cạnh đó, các thông số trong các giải thuật này chủ yếu được lựa chọn dựa trên thực nghiệm mà thiếu các phân tích đánh giá tối ưu. Ngoài ra, nhiều tác giả cũng không xem xét ảnh hưởng của sai số làm tròn và giới hạn của bộ giả ngẫu nhiên trong thực tế đến độ chính xác của hệ thống watermarking ảnh, đặc biệt là khi thực hiện ở các miền biến đổi. Thêm vào đó, nhiều tác giả không xem xét tính bền vững trước đầy đủ các loại tấn công khác nhau hay tính bảo mật khi thực hiện trích thông tin.

Xuất phát từ các thách thức khoa học và nhu cầu ứng dụng rộng rãi, luận án tập trung nghiên cứu kỹ thuật watermarking ảnh thiếu thông tin tiên nghiệm (mù),

nghĩa là quá trình trích thông tin chỉ dựa vào ảnh nhúng mà không cần ảnh gốc hoặc đầy đủ các thông số nhúng (ngoại trừ khóa bảo mật). Các ứng dụng khảo sát chủ yếu với các ảnh chuyên dụng như ảnh y tế từ nhiều phương thức tạo ảnh khác nhau bao gồm chụp cắt lớp vi tính (CT), cộng hưởng từ (MRI), X quang (XR), siêu âm (US) ở cả hai định dạng thông thường và đặc thù DICOM, và ảnh đa kênh (ví dụ như ảnh màu). Do đó, luận án không những mang tính mới với thách thức khoa học cao, phù hợp với xu hướng học thuật thế giới mà còn mang tính cấp thiết do đáp ứng nhiều nhu cầu thực tiễn trong việc đẩy mạnh áp dụng các tiến bộ khoa học kỹ thuật vào công cuộc chuyển đổi số đang diễn ra mạnh mẽ trên mọi lĩnh vực, đặc biệt là ngành y tế tại Việt Nam.

1.2 Tổng quan tình hình nghiên cứu

Những nghiên cứu đầu tiên về watermarking ảnh thực hiện trực tiếp ở miền không gian dựa trên các phương pháp điều chỉnh giá trị mức xám. Kỹ thuật thay thế bit trọng số thấp LSB (Least Significant Bit) được đề xuất bởi Tirkel, Schyndel và các cộng sự [55, 56] bằng cách nhúng watermark là chuỗi ngẫu nhiên nhị phân vào LSB còn lại của ảnh sau nén histogram mức xám 7-bit và dùng bộ so sánh chuỗi bit để phát hiện watermak. Một số tác giả khác thực hiện nhúng trích thông tin nhị phân trực tiếp trong các mặt phẳng LSB của ảnh [57-59].

Cox và cộng sự [10] là những người đầu tiên khai thác lý thuyết truyền thông trải phổ (Spread Spectrum) để xây dựng giải thuật watermarking. Kỹ thuật này khá bền vững nhưng không thực sự hữu ích trong thực tế vì đòi hỏi phải có ảnh gốc và thời gian tính toán lâu. Các tác giả khác cũng dùng khái niệm trải phổ nhưng theo cách thức không cần dữ liệu gốc trong quá trình khôi phục [11-14, 60]. Ngoài ra, kỹ thuật trải phổ dùng trong watermarking có thể thực hiện trực tiếp ở miền không gian hay các miền biến đổi khác như DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), vv. [61-65]. Tuy nhiên, bản thân tín hiệu đem nhúng cũng được xem như là nhiễu nên có thể gây ra sai số đáng kể ở quá trình trích. Vì vậy, một số phương pháp trải phổ cải tiến hoặc điều chỉnh đã được nghiên cứu để khắc phục phần nào các hạn chế trong phương pháp trải phổ truyền thống [44, 45].

Trong phần lớn trường hợp, việc mở rộng cho dữ liệu đa kênh như ảnh màu, ảnh siêu phổ, vv. được thực hiện bằng cách nhúng watermark trực tiếp vào một thành phần đặc biệt nào đó của dữ liệu bao phủ, chẳng hạn như kênh màu xanh dương trong không gian màu RGB, thành phần độ sáng trong không gian màu YUV, hoặc xử lý riêng mỗi thành phần mà không xem xét tương quan giữa chúng [66-68]. Trái lại, Piva và cộng sự [16] khai thác tương quan chéo của các kênh màu RGB bằng cách thiết kế một bộ phát hiện dựa trên tương quan kết hợp trung bình để tổng hợp thông tin thu được từ tất cả ba kênh màu, từ đó chất lượng thực hiện của hệ thống được cải thiện. Tuy nhiên, nó đòi hỏi dữ liệu gốc tại bộ phát hiện. Không như thế, Barni và cộng sự [17] sử dụng biến đổi DCT để giảm tương quan giữa các kênh màu. Đặc biệt, Barni và cộng sự [18] cùng Hajjaji và cộng sự [19] khai thác đặc tính giải tương quan hoàn hảo của biến đổi KLT (Karhunen-Loeve Transform) để nhúng watermark. Không may, một hạn chế của biến đổi KLT là nó phụ thuộc vào đặc tính thống kê của dữ liệu gốc. Vì vậy, các kết quả trong các bài báo [18, 19] chỉ đúng với điều kiện giả sử khác biệt giữa ma trận hiệp phương sai của ảnh nhúng và ảnh gốc là không đáng kể.

Trong những năm gần đây, một trong những lĩnh vực cực kì khó khăn của watermarking là các giải thuật watermaking bền vững trước các sái dạng hình học vẫn không ngừng phát triển [68, 69]. Có nhiều phương pháp khác nhau đã được đề xuất như nhúng dựa trên mẫu tham chiếu, nhúng miền bất biến RST (Rotation, Shifting, and Translation), watermark tự đồng bộ hay đồng bộ dựa trên đặc trưng [70-77]. Có nhiều đặc trưng khác nhau được sử dụng như góc Harris, wavelet Mexican Hat, phát hiện Harris-Laplace, các mo-ment [78-80] và gần đây là biến đổi SIFT (Scale-Invariant Feature Transform) [38-43, 81-84]. Ý tưởng chính của biến đổi SIFT là trích xuất các đặc trưng ổn định trong không gian tỉ lệ. Dựa trên SIFT, Nikolaidis [81] dùng tất cả đặc trưng để nhúng watermark vì thế vấn đề đồng bộ được bảo toàn. Tuy nhiên, số lượng lớn các vùng nhúng theo đòi hỏi của giải thuật làm suy giảm chất lượng của ảnh nhúng. Ngoài ra, không phải tất cả các đặc trưng đều hữu ích cho quá trình nhúng và trích. Do đó, Guo, Li và Pan [82] chỉ lựa chọn vài đặc trưng bền vững để nhúng thông tin dùng giải

thuật lượng tử chẵn lẻ và đã chứng tỏ hiệu quả so với các phương pháp trước đó. Tuy nhiên, theo phương pháp này thì thông tin gốc đòi hỏi ở quá trình trích và chỉ dùng trong ứng dụng kiểm chứng watermark. Ngoài ra, do dùng cùng giải thuật lựa chọn vùng nhúng bền vững ở quá trình nhúng và trích nên có thể dẫn đến mất đồng bộ trong quá trình trích. Mặt khác, một số tác giả cải thiện độ bền vững bằng cách dùng thêm đặc trưng hướng hoặc cải tiến biến đổi SIFT. Tuy nhiên, họ cần biết trước các mô tả gốc của các đặc trưng nhúng trong quá trình trích [77, 78]. Ngược lại, một số bài báo nghiên cứu thực hiện watermarking thiếu thông tin tiên nghiệm dùng biến đổi SIFT lại không xem xét tính bền vững trước các tấn công đồng bộ như xoay ảnh và co giãn ảnh [83, 84].

Đặc biệt, trước sự phát triển của các thiết bị chẩn đoán hình ảnh và sự bùng nổ của Internet, một số kỹ thuật watermarking trong ảnh y tế khác nhau bắt đầu được quan tâm nghiên cứu để đáp ứng các yêu cầu đặc thù riêng của ngành y tế [85-91]. Thông thường, một ảnh y tế thường được chẩn đoán trước khi lưu trữ lâu dài vì vậy phần nội dung quan trọng có ý nghĩa trong ảnh được gọi là ROI (Region of Interest) đã được xác định và vùng còn lại không có ý nghĩa được gọi là RONI (Region of Non-Interest). Do đó một hướng tiếp cận của watermarking cho ảnh y tế là nhúng trích watermark trong vùng ROI/RONI cho các yêu cầu ứng dụng khác nhau. Tuy nhiên, các phương pháp này thường yêu cầu thông tin đi kèm để xác định vùng ROI/RONI khi trích watermark [92-102]. Một hướng tiếp cận thứ hai là sử dụng watermarking khả đảo, theo đó thực hiện nhúng watermark vào ảnh gốc theo cách thức có thể đảo ngược nghĩa là khi watermark được trích thì ảnh gốc cũng được khôi phục chính xác hoàn toàn [103-105]. Một hướng tiếp cận khác sử dụng rộng rãi hơn của watermarking với ảnh y tế là khai thác các phương pháp watermarking ảnh thông thường với yêu cầu tối thiểu méo dạng để đảm bảo chất lượng trong chẩn đoán y tế [106-112].

1.3 Mục tiêu và nhiệm vụ

Mục tiêu của luận án là đưa ra các mô hình xác suất và lời giải tối ưu của các giải pháp đề xuất nâng cao hiệu quả kỹ thuật watermarking thiếu thông tin tiên nghiệm (mù) cho ảnh y tế và ảnh đa kênh ở miền không gian cũng như các miền

biến đổi phù hợp với mỗi yêu cầu ứng dụng cụ thể. Các giải pháp đề xuất được phân tích có thể áp dụng cho cả hai trường hợp watermarking một bit và nhiều bit. Các kết quả lý thuyết được kiểm chứng thông qua mô phỏng và ứng dụng thực tiễn. Các kết quả được thực hiện với nhiều loại ảnh phổ biến cũng như đặc thù và xem xét các loại tấn công khác nhau. Bên cạnh việc đánh giá tính cảm thụ và tính bền vững, luận án còn bổ sung đánh giá độ tin cậy và tăng cường tính năng bảo mật để phù hợp với các yêu cầu đặc thù trong lĩnh vực y tế.

Để thực hiện mục tiêu trên, trước tiên, luận án tiến hành phân tích sơ đồ tổng quát của hệ thống watermarking dựa trên nền tảng lý thuyết truyền thông và khảo sát các thông số dùng trong nghiên cứu đánh giá hiệu quả của các kỹ thuật watermarking tiêu biểu với dữ liệu ảnh số. Bên cạnh đó, luận án kết hợp phân tích lý thuyết dựa trên các mô hình xác suất thống kê để đưa ra lời giải tối ưu đồng thời tiến hành khảo sát thực nghiệm với các cơ sở dữ liệu và môi trường ứng dụng cụ thể để so sánh đánh giá ưu khuyết điểm của các phương pháp watermarking khác nhau làm cơ sở cho các giải pháp nâng cao hiệu quả của kỹ thuật watermarking thiếu thông tin tiên nghiệm cho ảnh y tế và ảnh đa kênh.

1.4 Những đóng góp chính

Luận án góp phần làm phong phú hơn về lý luận watermarking bằng các phân tích đánh giá chi tiết mang tính tổng quát về một số hệ thống watermarking điển hình thế hệ thứ nhất bền vững trước các tấn công không đồng bộ như nén ảnh (JPEG, JPEG2000), lọc ảnh (tuyến tính, phi tuyến), nhiễu ảnh (Gaussian, muối tiêu) và thế hệ thứ hai bền vững trước các tấn công đồng bộ như cắt ảnh, xoay ảnh, co giãn ảnh, siêu phân giải dùng trí tuệ nhân tạo [20]. Ngoài ra, luận án còn mở ra khả năng thực hiện các ứng dụng thực tiễn với hiệu quả chất lượng cao thông qua các kết quả thu được từ các cải tiến đề xuất. Chính vì vậy, xuyên suốt luận án là sự kết hợp giữa phân tích lý thuyết tổng quát và kết quả ứng dụng cụ thể đối với một số cải tiến đột phá nhằm nâng cao hiệu quả kỹ thuật watermarking dựa trên các giải thuật tiêu biểu. Các đề xuất cải tiến tập trung vào ba nội dung.

Nội dung đầu tiên của luận án tập trung đề xuất hai giải pháp hiệu quả DICOM_LSB_AES và DICOM_LSB_AES_RONI cho việc nhúng trích thông tin trong ảnh y tế đặc thù DICOM (The Digital Image and Communication in Medicine) nhằm tăng cường tính bảo mật trong lĩnh vực y tế từ xa.

Ở nội dung nghiên cứu thứ hai, luận án đề xuất các giải pháp watermarking bền vững mang tính đột phá dựa trên đặc tính tự đồng bộ và tương quan giữa các watermark trích để khôi phục vùng nhúng và thông tin nhúng sử dụng biến đổi SIFT khi không có ảnh gốc đồng thời vẫn tăng cường tính bảo mật cao. Ngoài các loại tấn công xử lý ảnh thông thường bao gồm cả hai loại đồng bộ và không đồng bộ, tính bền vững của các giải pháp đề xuất cũng được phân tích đánh giá với loại tấn công siêu phân giải dùng trí tuệ nhân tạo dựa trên mô hình kiến trúc mạng học sâu RRDN (Residual-in-Residual Dense Network). Bên cạnh giải pháp watermaking một bit Q_SIFT, các kết quả được xem xét mở rộng cho cả trường hợp nhiều bit thông tin qua việc phân tích đánh giá hai giải pháp nhúng theo hình quạt FSQ_SIFT và hình nửa vành khuyên HRSQ_SIFT. Với mỗi giải pháp, luận án đều bổ sung tính bảo mật kép bằng cách khai thác các thông số của đặc trưng SIFT qua giải pháp SQ_SIFT và khóa bí mật.

Nội dung thứ ba của luận án đưa ra một số điều chỉnh cải tiến khắc phục các hạn chế của phương pháp trải phổ truyền thống cho ảnh đơn kênh, từ đó đề xuất và phân tích đánh giá hiệu quả của hệ thống watermarking hợp tác mới cho ảnh đa kênh dựa trên bộ thu tuyến tính tối ưu. Với ảnh đơn kênh, các giải pháp đề xuất điều chỉnh cải tiến bao gồm MISS (Multibit Improved Spread Spectrum), MISS_DCT, MISS_DWT nhằm tăng cường tính chính xác của toàn bộ quá trình nhúng và trích xuất thông tin đồng thời nâng cao dung lượng thông tin nhúng và cải thiện chất lượng dữ liệu sau khi nhúng. Với ảnh đa kênh, luận án đề xuất giải pháp watermarking mới gọi là trải phổ hợp tác CSS (Cooperative Spread Spectrum) và khai thác biến đổi KLT với giải pháp CSS_KLT để giải tương quan giữa các thành phần tín hiệu của ảnh đa kênh. Theo đó, thông tin được cùng nhúng vào nhiều kênh ảnh và một bộ quyết định hợp tác tuyến tính toàn cục được sử dụng để khai thác tối ưu mức độ đóng góp của từng bộ phát hiện tương quan

cục bộ ở mỗi kênh. Không giống các giải pháp khác bị giới hạn bởi yêu cầu sử dụng dữ liệu gốc của biến đổi KLT, bằng việc chứng minh với điều kiện watermark trực giao thì phương pháp đề xuất có thể trích thông tin mà không cần ảnh gốc. Bên cạnh đó, các giải pháp cải tiến để loại bỏ can nhiễu giữa watermark và các kênh ảnh cũng như mở rộng watermarking nhiều bit cũng được đề xuất và phân tích, bao gồm ICSS (Improved CSS), MCSS (Multibit CSS), ICSS_KLT, MCSS_KLT. Các kết quả được phân tích lý thuyết bằng mô hình toán học đồng thời kiểm chứng qua mô phỏng và thực nghiệm với các loại ảnh y tế khác nhau.

Các kết quả nổi bật của luận án đã được công bố trong 3 bài báo tạp chí quốc tế Scopus, 1 bài báo tạp chí trong nước, 6 bài báo hội nghị quốc tế uy tín và thử nghiệm ứng dụng thực tiễn trong 6 đề tài nghiên cứu khoa học đã nghiệm thu thành công.

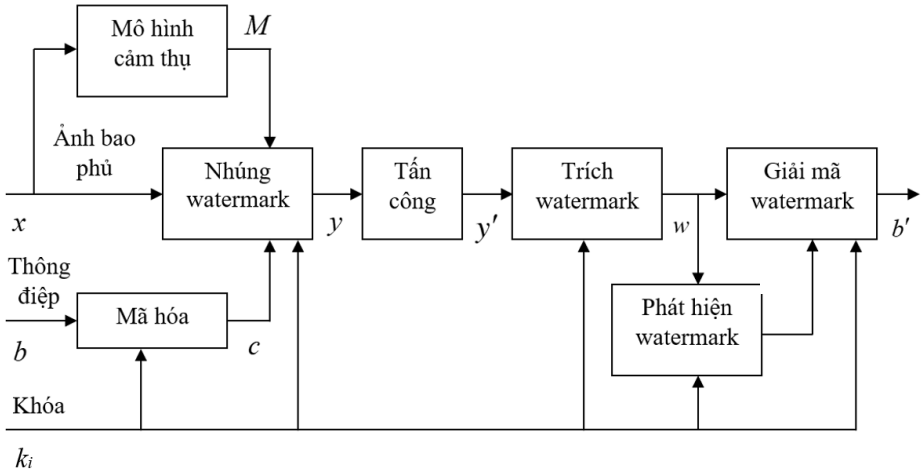
1.5 Bố cục luận án

Phần tiếp theo của luận án được bố cục như sau. Chương 2 trình bày cơ sở lý thuyết của các nội dung nghiên cứu trong luận án. Chương 3 đề xuất giải pháp watermarking dùng kỹ thuật LSB với ảnh DICOM nhằm tăng cường tính bảo mật cho ứng dụng y tế từ xa. Chương 4 đề xuất giải pháp watermarking dùng kỹ thuật lượng tử và chọn lọc đặc trưng SIFT để nâng cao tính bền vững trước các tấn công đồng bộ. Chương 5 đề xuất giải pháp watermarking trải phổ hợp tác với ảnh đa kênh sử dụng biến đổi KLT và các bộ thu tối ưu cùng các điều chỉnh cải tiến mở rộng. Chương 6 đưa ra kết luận chung và các hướng nghiên cứu tiếp theo.

CHƯƠNG 2 CƠ SỞ LÝ THUYẾT

2.1 Tổng quan hệ thống watermarking

Dựa trên nền tảng truyền thông, một hệ thống watermarking thiếu thông tin tiên nghiệm như trình bày ở Hình 2.1 có thể được xem xét gồm ba thành phần chính: nhúng thông điệp, kênh tấn công và trích thông điệp.



Hình 2.1 Hệ thống watermarking thiếu thông tin tiên nghiệm.

2.2 Các phương pháp watermarking

2.2.1 Phương pháp LSB

Phương pháp LSB là một phương pháp đơn giản và phổ biến để nhúng trích thông tin. Trong phương pháp LSB, dữ liệu thông tin được đưa về dạng bit, sau đó được thay thế vào các bit có trọng số thấp của dữ liệu bao phủ nên đảm bảo được tính cảm thụ. Trong trường hợp cần tăng dung lượng thông tin nhúng, kỹ thuật LSB có thể mở rộng cho các mặt phẳng bit có trọng số thấp liền kề.

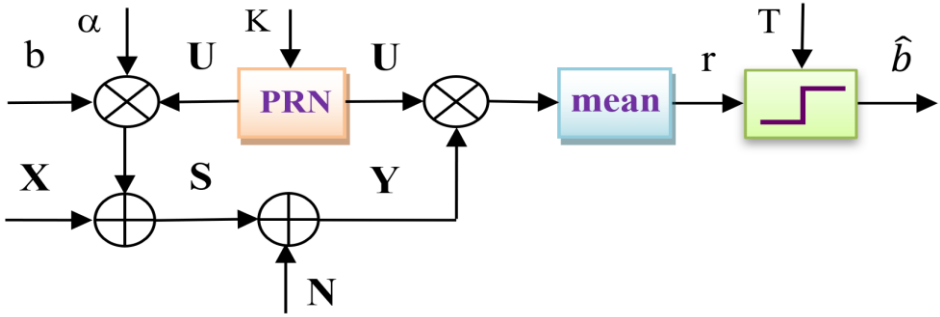
2.2.2 Phương pháp watermarking lượng tử

Để đơn giản hóa cách biểu diễn và thực hiện so với phương pháp watermarking lượng tử trong các bài báo [114-116], luận án đưa ra cách tiếp cận watermarking dùng hai bộ lượng tử tương ứng với mỗi bit thông tin 0 và 1, trong đó $Q_{0k} =$

$2k\Delta$ là các giá trị lượng tử của bộ lượng tử chẵn, $Q_{1k} = (2k+1)\Delta$ là các giá trị lượng tử của bộ lượng tử lẻ. Khi muốn nhúng một bit thông tin b vào trong giá trị điểm ảnh (pixel) s ta phải kiểm tra b là 0 hay 1 để chọn bộ lượng tử thích hợp, sau đó tìm ra giá trị lượng tử gần với s nhất bằng cách tính khoảng cách nhỏ nhất từ s đến các giá trị lượng tử. Việc trích lấy thông tin đã nhúng bằng phương pháp lượng tử hóa cũng khá dễ dàng do phía trích đã biết được bảng giá trị lượng tử, từ đó so sánh giá trị thu được s' với cả hai bộ lượng tử để trích lấy lại thông tin được nhúng từ giá trị lượng tử gần nhất. Lưu ý theo cách tiếp cận này thì trường hợp đặc biệt khi $\Delta = 1$ tương ứng với phương pháp LSB.

2.2.3 Phương pháp watermarking trải phổ

Luận án xem xét mô hình watermarking thiếu thông tin tiên nghiệm dựa trên kỹ thuật trải phổ truyền thống như Hình 2.4. Một bộ giả ngẫu nhiên PRN với khóa bí mật K tạo ra chuỗi ngẫu nhiên U, còn gọi là chuỗi watermark, như nhau ở cả quá trình nhúng và trích thông tin. Ở quá trình nhúng, chuỗi watermark U được nhúng vào ảnh gốc X theo hệ số độ mạnh nhúng α và bit thông tin b tương ứng để tạo thành ảnh nhúng S. Ở quá trình trích, giá trị trung bình của tích số giữa ảnh thu được và chuỗi watermark như đã sử dụng ở quá trình trích được tính toán (tương tự như cách tính tương quan hay tích nội trong đại số tuyến tính) và so sánh với giá trị ngưỡng để quyết định bit thông tin trích.



Hình 2.2 Mô hình watermarking trải phổ truyền thống.

CHƯƠNG 3 NÂNG CAO HIỆU QUẢ KỸ THUẬT WATERMARKING LSB ỨNG DỤNG CHO ẢNH Y TẾ DICOM

3.1 Các vấn đề bảo mật với ảnh DICOM

DICOM là một hệ thống tiêu chuẩn công nghiệp được phát triển nhằm đáp ứng nhu cầu của các nhà sản xuất cũng như người sử dụng trong việc kết nối, lưu trữ, trao đổi, in ấn ảnh y tế. Một tập tin DICOM (phần mở rộng .dcm) ngoài dữ liệu hình ảnh, còn chứa cả những thông tin khác như thông tin về bệnh nhân, về phương thức kỹ thuật tạo ra bức ảnh, vv. Trong khi đó, hạn chế của phần lớn các trình xem ảnh DICOM hiện nay đều thiếu tính bảo mật khiến cho các thông tin cá nhân có nguy cơ bị xâm phạm trong quá trình lưu trữ và truyền nhận, nhất là trong môi trường Internet. Để giải quyết vấn đề trên, một số tác giả khai thác kỹ thuật mã hóa mật mã, trong đó phổ biến là mật mã AES (Advanced Encryption Standard) tiên tiến đến thời điểm hiện tại. Ở Việt Nam, thuật toán AES đã được công bố thành tiêu chuẩn quốc gia TCVN 7816:2007. Tuy nhiên, việc áp dụng mã hóa AES cho toàn bộ tập tin DICOM là không hiệu quả do kích thước rất lớn. Trong khi đó, việc chỉ mã hóa mật mã AES cho các trường dữ liệu liên quan đến thông tin cá nhân không hoàn toàn thành công do cú pháp quy định cho các trường dữ liệu liên quan đến thông tin cá nhân của ảnh DICOM phải ở định dạng chuỗi ký tự.

3.2 Giải pháp đề xuất DICOM_LSB_AES

Với đặc trưng ảnh DICOM thường sử dụng hơn 8 bit so với các định dạng ảnh xám (đơn sắc) phổ biến, có thể hỗ trợ lên đến 16 bit để đạt chất lượng hiển thị cao cho chẩn đoán thì việc nghiên cứu hoàn thiện kỹ thuật watermarking LSB cho ảnh DICOM mang lại hiệu quả rõ rệt về mặt cảm thụ. Ngoài ra, phương pháp này còn có thuận lợi là đơn giản trong thực hiện nhúng và trích thông tin do có thể thực hiện trực tiếp trong miền không gian. Tuy nhiên, thông tin cá nhân đã nhúng trong ảnh DICOM luôn có thể được truy xuất nếu xác định được vị trí nhúng bằng cách trích lại các bit có trọng số thấp của dữ liệu nhúng nên độ bảo mật của phương pháp này rất thấp. Vì vậy, trước tiên luận án đề xuất giải pháp kết hợp kỹ thuật mã hóa và kỹ thuật mật mã để nhúng trích thông tin cá nhân

trong ảnh y tế đặc thù DICOM, gọi là DICOM_LSB_AES nhằm tăng cường tính bảo mật hỗ trợ cho ứng dụng y tế từ xa.

Quá trình nhúng thông tin của giải pháp đề xuất DICOM_LSB_AES được thực hiện qua các bước sau:

- Bước 1: Mã hóa nhị phân chuỗi thông tin cá nhân theo đúng định dạng cấu trúc dữ liệu chuẩn DICOM.
- Bước 2: Mã hóa mật mã AES chuỗi nhị phân dùng 1 từ mã bí mật.
- Bước 3: Chèn dữ liệu sau mã hóa mật mã vào các mặt phẳng bit trọng số thấp LSB của ảnh gốc. Sau khi thu được ảnh nhúng, toàn bộ các trường dữ liệu liên quan đến thông tin cá nhân sẽ được xóa bỏ khỏi tập tin DICOM.

Quá trình trích thông tin của giải pháp đề xuất DICOM_LSB_AES được thực hiện ngược lại với các bước sau:

- Bước 1: Trích dữ liệu từ các mặt phẳng bit trọng số thấp LSB của ảnh nhúng.
- Bước 2: Giải mã hóa mật mã AES chuỗi nhị phân trích với từ mã bí mật ban đầu.
- Bước 3: Giải mã hóa nhị phân chuỗi bit thu được sau giải mã hóa mật mã theo đúng định dạng cấu trúc dữ liệu chuẩn DICOM.

Qua các kết quả khảo sát có thể rút ra kết luận giới hạn dưới của giá trị PSNR để chất lượng ảnh nhúng không thể cảm thụ là khoảng 37 dB, tương ứng nhúng tối đa 3 mặt phẳng LSB với ảnh xám có độ sâu 8 bit. So sánh với giải thuật trong bài báo [52] thì kết quả của giải pháp đề xuất hoàn toàn tương đồng khi có thể nhúng tối đa 98304 byte thông tin cá nhân vào 3 mặt phẳng LSB của ảnh xám kích thước 512x512. Tuy nhiên, không như các tác giả trong bài báo trên khi áp dụng cho ảnh tự nhiên với độ bảo mật rất thấp do chỉ dùng kỹ thuật đảo bit trong khi giải pháp đề xuất thực hiện cho ảnh y tế DICOM có tăng cường tính năng bảo mật đáp ứng yêu cầu thực tiễn của y tế từ xa.

Với các ảnh y tế DICOM có độ sâu bit lớn hơn 8 thì có thể nhúng nhiều hơn 3 mặt phẳng LSB mà vẫn đảm bảo chất lượng của ảnh nhúng. Bảng 3.4 trình bày kết quả phân tích lý thuyết của MSE và PSNR trong trường hợp nhúng tối đa toàn bộ các điểm ảnh khi thay đổi số lượng mặt phẳng LSB nhúng cho các ảnh có độ sâu bit khác nhau. Qua đó, số lượng tối đa mặt phẳng LSB có thể nhúng cũng được xác định tương ứng với độ sâu bit của ảnh gốc để đảm bảo chất lượng của ảnh nhúng.

Bảng 3.1 Giá trị lý thuyết của MSE và PSNR.

Embedded LSB planes	**PSNR (dB) Bit depth of original image**				**MSE**
	8	10	12	16	
1	51.14	63.21	75.26	99.34	0.5
2	44.15	56.22	68.27	92.35	2.5
3	37.92	49.99	62.03	86.12	10.5
4		43.91	55.96	80.05	42.5
5		37.66	49.93	74.01	170.5
6			43.90	67.99	682.5
7			37.88	61.97	2730.5
8				55.95	10922.5
9				49.93	43690.5
10				43.90	174762.5
11				37.88	699050.5

3.3 Giải pháp đề xuất DICOM_LSB_AES_RONI

Dựa trên đặc tính ảnh y tế thường có vùng nội dung quan tâm ROI (Region Of Interest) và không quan tâm RONI (Region Of Non-Interest) có vai trò ý nghĩa khác nhau trong việc chẩn đoán, luận án tiếp tục đề xuất giải pháp DICOM_LSB_AES_RONI nhúng trích thông tin trong vùng RONI được tạo ra từ đa giác khoanh vùng ROI/RONI một cách tự động hoặc có thể hiệu chỉnh bởi bác sĩ chẩn đoán nhằm tăng cường độ tin cậy của quá trình chẩn đoán.

Quá trình nhúng thông tin trong giải pháp đề xuất DICOM_LSB_AES_RONI được thực hiện qua 5 bước sau:

- Bước 1: Mã hóa nhị phân chuỗi thông tin cá nhân theo đúng định dạng cấu trúc dữ liệu chuẩn DICOM.
- Bước 2: Mã hóa mật mã AES chuỗi nhị phân dùng 1 từ mã bí mật.
- Bước 3: Lựa chọn đa giác khoanh vùng ROI/RONI.
- Bước 4: Chèn dữ liệu sau mã hóa mật mã vào các mặt phẳng bit trọng số thấp LSB của vùng RONI của ảnh gốc, ngoại trừ tại các biên ảnh. Sau khi thu được ảnh nhúng, toàn bộ các trường dữ liệu liên quan đến thông tin cá nhân sẽ được xóa bỏ khỏi tập tin DICOM.
- Bước 5: Chèn các thông số cần thiết cho quá trình trích như chiều dài dữ liệu sau mật mã, vị trí các đỉnh đa giác khoanh vùng ROI/RONI ở định dạng mã hóa nhị phân vào các mặt phẳng bit trọng số thấp LSB tại các biên ảnh.

Quá trình trích thông tin trong giải pháp đề xuất DICOM_LSB_AES_RONI được thực hiện ngược lại với các bước sau:

- Bước 1: Trích dữ liệu từ các mặt phẳng bit trọng số thấp LSB tại các biên của ảnh nhúng và giải mã để xác định chiều dài dữ liệu sau mật mã và vị trí các đỉnh đa giác khoanh vùng ROI/RONI.
- Bước 2: Trích dữ liệu từ các mặt phẳng bit trọng số thấp LSB của vùng RONI trong ảnh nhúng.
- Bước 3: Giải mã hóa mật mã AES chuỗi nhị phân trích với từ mã bí mật ban đầu.
- Bước 4: Giải mã hóa nhị phân chuỗi bit thu được sau giải mã hóa mật mã theo đúng định dạng cấu trúc dữ liệu chuẩn DICOM.

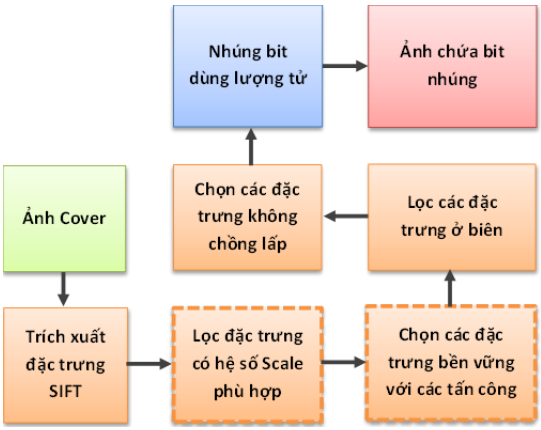
3.4 Kết quả thử nghiệm ứng dụng thực tiễn

Dựa trên các kết quả nghiên cứu, luận án đã xây dựng và thử nghiệm phần mềm khai thác dữ liệu ảnh DICOM có tăng cường tính bảo mật hỗ trợ cho ứng dụng y tế từ xa dựa trên hai giải pháp đề xuất tại một số bệnh viện. Kết quả thử nghiệm cho thấy cả hai giải pháp DICOM_LSB_AES và DICOM_LSB_AES_RONI có thể được sử dụng rộng rãi trong các hệ thống xử lý ảnh DICOM, nhất là những ứng dụng có hạn chế về khả năng xử lý.

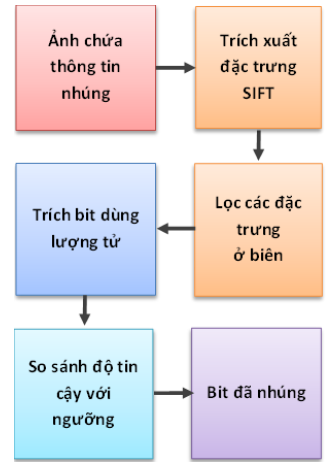
CHƯƠNG 4 NÂNG CAO HIỆU QUẢ KỸ THUẬT WATERMARKING LƯỢNG TỬ VÀ BIẾN ĐỔI SIFT TRƯỚC CÁC TẤN CÔNG ĐỒNG BỘ

4.1 Giải pháp đề xuất watermarking một bit Q_SIFT

Hình 4.1 và Hình 4.9 trình bày giải thuật nhúng và trích một bit thông tin Q_SIFT.



Hình 4.1 Giải thuật nhúng Q_SIFT.



Hình 4.2 Giải thuật trích Q_SIFT.

Theo đó, các đặc trưng SIFT được đưa qua các bước chọn lọc phù hợp để tăng tính bền vững và hiệu quả trước khi thực hiện nhúng thông tin. Để tăng cường độ chính xác của việc trích thông tin khi các đặc trưng trích có thay đổi nhỏ, luận án nhúng cùng thông tin theo kỹ thuật lượng tử chẵn lẻ vào các vùng tròn theo tọa độ và hệ số scale của các đặc trưng như trong công thức 4.1:

$$(x - t_1)^2 + (y - t_2)^2 = (k\sigma)^2 \quad (4.1)$$

Khi đó, bit thông tin trích tương ứng được xác định dựa trên số lượng lớn hơn của loại bit giải lượng tử theo công thức (4.2):

$$b' = \begin{cases} 0, & NUM_0 \geq NUM_1 \\ 1, & NUM_0 < NUM_1 \end{cases} \quad (4.2)$$

trong đó NUM_0 và NUM_1 lần lượt là tổng số bit 0 và bit 1 sau giải lượng tử.

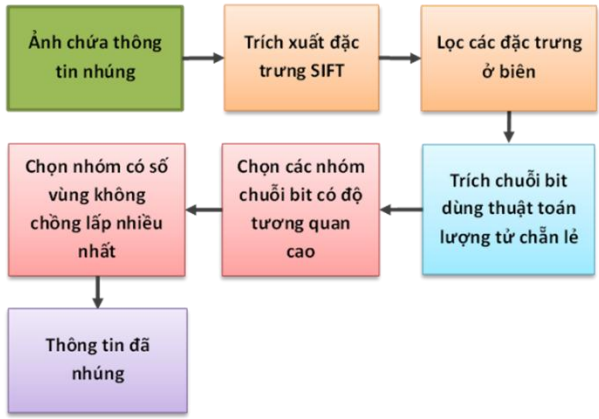
Bởi lẽ quá trích trích thông tin không dùng ảnh gốc hoặc thông tin của các đặc trưng ban đầu thế nên các đặc trưng thu thường sẽ khác với các đặc trưng đã

nhúng thông tin. Ngoài ra, chưa kể ảnh hưởng của các tấn công làm sai lệch đặc trưng nhúng ban đầu nên không thể lựa chọn các đặc trưng như ở quá trình nhúng. Lúc này, thông số độ tin cậy được đề xuất tính toán và so sánh với ngưỡng để quyết định bit thông tin tương ứng với vùng nhúng ban đầu. Ở cấp độ bit, độ tin cậy được xác định dựa trên các bit sau giải lượng tử ở mỗi vùng trích theo công thức sau:

$$R_{Qb} = \frac{\max\{NUM_0, NUM_1\}}{NUM_0 + NUM_1} \quad (4.3)$$

4.2 Các giải pháp đề xuất watermarking nhiều bit HRSMQ_SIFT và FSMQ_SIFT

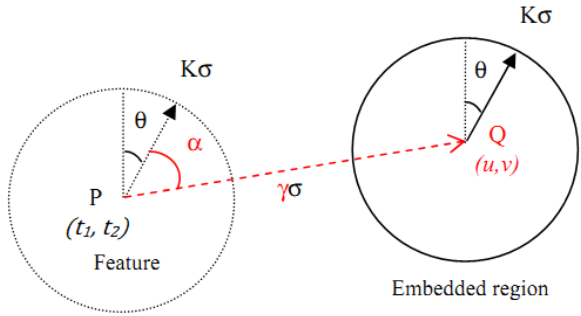
Các giải pháp đề xuất nhúng nhiều bit thông tin tương tự như giải pháp nhúng một bit thông tin Q_SIFT, chỉ khác ở bước cuối cùng thực hiện nhúng chuỗi bit thông tin vào các phần nửa vành khuyên (HRSMQ_SIFT) hoặc các phần hình quạt (FSMQ_SIFT) của mỗi vùng tròn nhúng không chồng lấp. Hình 4.12 trình bày giải thuật trích nhiều bit thông tin cho cả hai trường hợp đề xuất. Theo đó, có sự khác biệt so với giải thuật trích một bit thông tin ở bước mở rộng trích chuỗi bit theo các phần nửa vành khuyên (HRSMQ_SIFT) hoặc các phần hình quạt (FSMQ_SIFT) và khai thác tương quan giữa các vùng thông tin trích để trích chọn các vùng nhúng không chồng lấp ban đầu.



Hình 4.3 Giải thuật trích nhiều bit thông tin (HRSMQ_SIFT và FSMQ_SIFT).

4.3 Giải pháp đề xuất SQ_SIFT tăng cường tính bảo mật

Ngoài ra, luận án cũng đề xuất thêm giải pháp tăng cường bảo mật SQ_SIFT (Secure Q_SIFT) bằng cách thay đổi vị trí vùng nhúng dựa trên các đặc trưng và khóa bí mật như minh họa ở Hình 4.13. Khóa bí mật sẽ tạo ra cặp thông số (α, γ) và vị trí nhúng sẽ thay đổi đến vị trí mới Q(u,v) từ vị trí đặc trưng ban đầu P(t_1,t_2) bằng pháp xoay góc α so với hệ số góc θ của đặc trưng SIFT và tịnh tiến $\gamma\sigma$ theo hệ số scale σ của đặc trưng SIFT. Nhờ vậy, ngoài việc tăng cường tính bảo mật, các đặc trưng khi trích ít bị ảnh hưởng do vùng nhúng thông tin không thực hiện trực tiếp tại vị trí các đặc trưng.



Hình 4.4 Thay đổi vị trí vùng nhúng dựa trên các đặc trưng và khóa bí mật.

4.4 Các kết quả mô phỏng và thử nghiệm

Luận án khảo sát độ tin cậy của phương pháp SS và lượng tử đề xuất (Q_SIFT) cho trường hợp nhúng một bit thông tin trước các loại tấn công khác nhau như trình bày trong Bảng 4.4. Nhìn chung, phương pháp đề xuất Q_SIFT cho độ tin cậy vượt trội so với phương pháp SS trước các tấn công đồng bộ, trong khi kém hiệu quả trước các tấn công nhiễu.

Bảng 4.1 Bảng đánh giá độ tin cậy trước các tấn công với nhúng một bit.

Tấn công	SS	Q_SIFT
Nhiễu Gaussian (0, 0.01)	0.9448	0.5297
Nhiễu muối tiêu (0.02)	0.9594	NA
Nén JPEG (100)	0.9685	1
Nén JPEG (75)	0.6335	0.6932

Nén JPEG2000	0.9615	1
Xoay 90º	0.5324	1
Xoay 1º	0.5292	1
Xoay 15º	0.5276	1
Xoay 30º	0.5273	1
Xoay 45º	0.5280	1
Cắt xén 10%	NA	1
Cắt xén 20%	NA	1
Co giãn 0.5 lần	NA	0.6927
Co giãn 0.8 lần	NA	0.8086
Co giãn 0.9 lần	NA	0.8007
Co giãn 1.5 lần	NA	0.8630
Co giãn 2 lần	NA	0.9069
Siêu phân giải AI 2 lần	NA	0.8631

Tiếp theo, luận án đánh giá độ chính xác và độ tin cậy trung bình của giải thuật đề xuất cho trường hợp nhúng 64 bit thông tin với hai phương pháp phân chia vùng nhúng theo hình nửa vành khuyên và hình quạt với kết quả trong Bảng 4.5. Các cột Acc trình bày độ chính xác của chuỗi bit thông tin trích sau cùng. Các cột N cho biết số vùng trích tương quan cao dùng trong trích thông tin. Các cột Re tương ứng với độ tin cậy trung bình của thông tin trích. Nó được tính cho mỗi vùng nhúng với mỗi bit thông tin.

Bảng 4.2 Bảng đánh giá hiệu năng của hai giải pháp trước các tấn công với nhúng nhiều bit.

Tấn công	**HRSMQ_SIFT**			**FSMQ_SIFT**		
	Acc	**N**	**Re**	**Acc**	**N**	**Re**
Không	1	4	0.9221	1	5	0.9736
Nhiễu Gaussian (0, 0.01)	NA	0	NA	NA	0	NA
Nhiễu muối tiêu (0.02)	NA	0	NA	NA	0	NA
Nén JPEG (100)	1	3	0.9668	1	5	0.9651
Nén JPEG (90)	1	3	0.7724	1	5	0.7562
Nén JPEG (75)	0.9844	3	0.7072	1	5	0.6900
Nén JPEG (50)	NA	0	NA	1	5	0.6534
Nén JPEG2000	1	3	0.9537	1	5	0.9550
Xoay 180º	1	2	0.8833	0.9219	4	0.8558

Xoay 1º	1	4	0.9006	1	5	0.9117
Xoay 5º	1	3	0.9368	1	4	0.9173
Xoay 10º	0.9844	2	0.8943	1	5	0.9077
Xoay 15º	0.7344	3	0.8682	1	3	0.9277
Xoay 30º	0.9844	3	0.9006	1	3	0.9173
Xoay 45º	0.7813	2	0.8761	1	4	0.9136
Cắt xén 10%	1	2	0.9611	1	4	0.9687
Cắt xén 20%	1	2	0.9614	1	4	0.8975
Co giãn 0.5 lần	0.9063	2	0.7267	1	3	0.7304
Co giãn 0.8 lần	1	3	0.7753	1	5	0.7723
Co giãn 0.9 lần	0.6406	2	0.7754	1	4	0.7822
Co giãn 1.5 lần	0.9844	3	0.8084	1	5	0.8075
Co giãn 2 lần	0.9844	3	0.8099	1	5	0.8221
Siêu phân giải AI 2 lần	0.6875	2	0.7157	1	4	0.7215
Xoay 5º và Co giãn 0.8 lần	NA	0	NA	1	5	0.7571
Xoay 5º và Co giãn 1.5 lần	1	2	0.8053	1	5	0.7692
Xoay 10º và Co giãn 0.8 lần	1	2	0.7922	1	5	0.7516
Xoay 10º và Co giãn 1.5 lần	1	3	0.8147	1	5	0.7839
Xoay 45º và Co giãn 0.5 lần	NA	0	NA	1	4	0.7159
Xoay 45º và Co giãn 2 lần	1	3	0.8104	1	4	0.8215

CHƯƠNG 5 NÂNG CAO HIỆU QUẢ KỸ THUẬT WATERMARKING TRẢI PHỔ ỨNG DỤNG CHO ẢNH ĐA KÊNH

5.1 Các giải pháp watermarking trải phổ điều chỉnh cải tiến cho ảnh đơn kênh

Trước tiên, luận án đưa ra giải pháp điều chỉnh cải tiến MISS (Multibit Improved Spread Spectrum) nhằm tăng cường độ tin cậy của toàn bộ quá trình nhúng và trích thông tin cho ảnh đơn kênh đồng thời nâng cao dung lượng thông tin nhúng và cải thiện chất lượng ảnh nhúng. Giả sử $\{U_i\}_{i=[1...B]}$ là các chuỗi watermarrk ngẫu nhiên chuẩn hóa trung bình 0 với chỉ hai giá trị ± 1 tương ứng với B bit thông tin $\{b_i\}$. Ảnh sau khi nhúng S của giải pháp đề xuất MISS được tạo thành từ ảnh gốc X với hệ số độ mạnh watermark α được xác định theo công thức sau:

$$S = X + \sum_{i=1}^{B} \left(b_i \alpha - E[(X - \bar{X}).U_i] \right) U_i . \quad (5.1)$$

Trong trường hợp lý tưởng không có tấn công, giá trị tương quan của bộ trích trong phương pháp đề xuất MISS ứng với từng bit thông tin có dạng:

$$r_i = E[(Y - \bar{Y}).U_i] = \alpha b_i - \sum_{k \neq i} E[X.U_i] E[U_k.U_i]. \quad (5.4)$$

Từ kết quả (5.4) có thể thấy rằng giải pháp đề xuất đạt được độ tin cậy 100% khi và chỉ khi điều kiện $E[U_k.U_i] = 0 \ \forall k \neq i$ thỏa mãn. Điều này có thể thực hiện được khi sử dụng ma trận Hadamard để thiết kế các chuỗi watermark trực giao.

Ngoài ra, sự kết hợp MISS với biến đổi DCT hoặc DWT cho ra các giải pháp MISS_DCT và MISS_DWT cũng được so sánh đánh giá. Kết quả cho với hầu hết các tấn công đồng bộ đặc thù trong xử lý ảnh thì giải pháp MISS_DWT có tính bền vững hơn so với MISS_DCT.

5.2 Các giải pháp watermarking trải phổ hợp tác cho ảnh đa kênh

5.2.1 Giải pháp watermarking trải phổ hợp tác CSS

Với mô hình trải phổ hợp tác đề xuất gọi là CSS (Cooperative Spread Spectrum), chuỗi watermark U được cộng với từng kênh ảnh gốc X_i thông qua bit thông tin b và hệ số độ mạnh nhúng α_i để cho ra các kênh ảnh nhúng tương ứng S_i. Để cho phép các bộ phát hiện cục bộ có thể hợp tác, một bộ phát hiện tuyến tính toàn cục

được sử dụng với các hệ số trọng số thể hiện tỉ lệ đóng góp của từng kênh vào quyết định thông tin trích sau cùng. Giả sử các kênh ảnh gốc và nhiễu có phân bố Gaussian: $X_i \sim N(0, \sigma_{xi}^2)$ và $N_i \sim N(0, \sigma_{ni}^2)$. Khi đó, xác suất lỗi bit của hệ thống CSS được xác định như sau:

$$p = \frac{1}{2} erfc\left(\frac{|m_{rc}|}{\sqrt{2}\sigma_{rc}}\right) = \frac{1}{2} erfc\left(\frac{\sum_{i=1}^{m} \omega_i \alpha_i}{\sqrt{2}\sqrt{\sum_{i=1}^{m}(\omega_i^2 \sigma_{ri}^2)}}\right) \quad (5.15)$$

Thay vì sử dụng bộ tương quan toàn cục trung bình, vector trọng số $w = [w_1, w_2, \ldots w_m]^T$ được lựa chọn tối ưu để tối thiểu xác suất lỗi bit theo công thức (5.21).

$$p_{opt} = \frac{1}{2} erfc\left(\frac{1}{\sqrt{2}} \sqrt{\sum_{i=1}^{m} \frac{\alpha_i^2}{\sigma_{r_i}^2}}\right) \quad (5.21)$$

5.2.2 Giải pháp cải tiến loại bỏ can nhiễu ICSS

Quá trình nhúng ở mô hình đề xuất CSS được cải tiến thành ICSS (Improved CSS) công thức (5.41) để loại bỏ hoàn toàn ảnh hưởng của can nhiễu.

$$S_i^{imp} = X_i + b.\alpha_i.U - E[X_i.U].U \quad (5.41)$$

5.2.3 Giải pháp mở rộng watermarking nhiều bit MCSS

Quá trình watermarking trải phổ hợp tác đề xuất có thể được mở rộng cho nhiều bit thông tin $\{b_1, b_2, \ldots, b_B\}$ với giải pháp MCSS (Multibit CSS) bằng cách sử dụng các chuỗi watermark trực giao, nghĩa là $E[U_i.U_j]=0$, như công thức (5.43).

$$S_i = X_i + \sum_{k=1}^{B} b_k.\alpha_{ik}.U_k \quad (5.43)$$

5.2.4 Giải pháp watermarking trải phổ hợp tác sử dụng biến đổi KLT

Trong mô hình watermarking trải phổ hợp tác dùng KLT, gọi là CSS_KLT, quá trình nhúng trước tiên thực hiện giải tương quan hoàn toàn vector ảnh đa kênh $X = [X_1, X_2, \ldots, X_m]^T$ bằng biến đổi KLT. Kế đến, một khóa bí mật K được sử dụng bởi bộ giả ngẫu nhiên PRN để tạo ra các chuỗi trực giao $U = [U_1, U_2, \ldots, U_m]^T$ với trung bình 0 và chỉ hai giá trị ±1. Đây cũng chính là điểm khác biệt của giải pháp CSS_KLT so với mô hình trải phổ hợp tác CSS đề xuất ban đầu dùng duy

nhất chuỗi watermark U cho tất cả các kênh. Điều kiện trực giao được phân tích chứng minh để đảm bảo khả năng khôi phục hoàn hảo. Mỗi chuỗi U_i sau đó được cộng với các thành phần ảnh riêng $\tilde{X}_i$ tương ứng với bit thông tin b (cũng chỉ hai giá trị ±1) và hệ số độ mạnh α_i. Sau cùng, biến đổi KLT ngược được áp dụng để cho ra ảnh nhúng S. Ở quá trình trích của giải pháp CSS_KLT, biến đổi KLT được sử dụng lại với ảnh thu Y và mỗi thành phần ảnh riêng thu được đưa đến các bộ tương quan cục bộ tương tự như giải pháp CSS.

5.2.5 Giải pháp cải tiến loại bỏ can nhiễu ICSS_KLT

Để loại bỏ hoàn toàn các can nhiễu giữa các kênh ảnh với watermark, quá trình nhúng được cải tiến qua giải pháp ICSS_KLT (Improved CSS_KLT) như sau:

$$\tilde{S}_i = \tilde{X}_i + bW_i = \tilde{X}_i + b\alpha_i U_i - E[\tilde{X}_i . U_i].U_i \qquad (5.57)$$

5.2.6 Giải pháp mở rộng watermarking nhiều bit MCSS_KLT

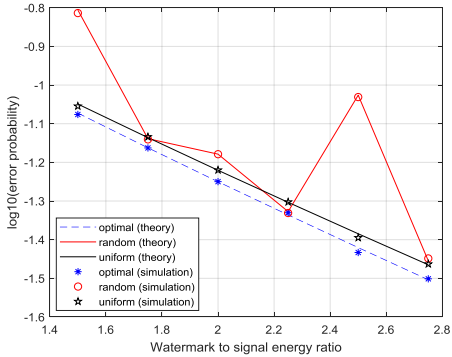
Mô hình watermarking trải phổ hợp tác dùng KLT có thể được mở rộng cho nhiều bit thông tin $\{b_1, b_2, \ldots, b_B\}$ qua giải pháp MCSS_KLT (Multibit CSS_KLT) bằng cách sử dụng tập chuỗi watermark trực giao như công thức (5.59).

$$\tilde{S}_i = \tilde{X}_i + \sum_{k=1}^{B} b_k . \alpha_{ik} . U_{ik} \qquad (5.59)$$

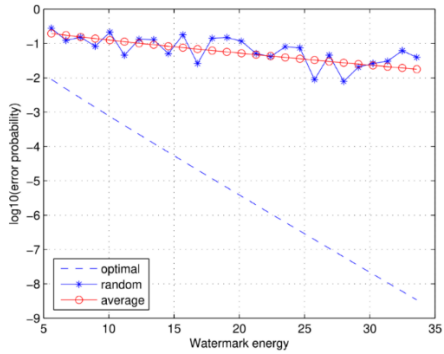
5.3 Các kết quả mô phỏng và thử nghiệm

Hình 5.14 trình bày kết quả mô phỏng ba loại bộ thu tương quan trung bình, tối ưu và ngẫu nhiên với các mức tỉ số năng lượng watermark trên tín hiệu khác nhau của mô hình hợp tác 2 kênh (m=2) trong trường hợp có nhiễu cộng Gaussian có công suất khác nhau ở mỗi kênh. Kết quả cho thấy các điểm mô phỏng hoàn toàn thích ứng với các đường giá trị từ phân tích lý thuyết. Ngoài ra, kết quả ở Hình 5.14 cũng cho thấy bộ thu tương quan tối ưu cho xác suất lỗi thấp nhất.

Hình 5.16 trình bày xác suất lỗi trong trường hợp sử dụng KLT với tỉ số năng lượng giữa các thành phần ảnh riêng là 50:10:1. Kết quả cho thấy trong trường hợp tỉ số năng lượng này có chênh lệch lớn thì bộ tương quan tối ưu cho xác suất lỗi cải thiện đáng kể so với bộ tương quan trung bình hoặc ngẫu nhiên.

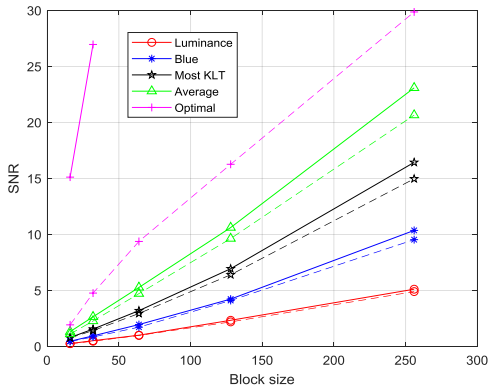


Hình 5.1 Kiểm chứng 2 kênh.



Hình 5.2 Kiểm chứng 50:10:11.

Kết quả thực hiện của mô hình watermarking trải phổ hợp tác đề xuất được so sánh với các kỹ thuật nhúng đơn kênh trước đây như kênh màu xanh dương [60], kênh độ chói [51], hay chỉ kênh ảnh thành phần KLT lớn nhất. Từ Hình 5.19 có thể nhận thấy sơ đồ đề xuất cho kết quả tốt hơn các phương pháp chỉ dùng một bộ phát hiện tương quan trong cả hai trường hợp không tấn công (đường liền) và nhiễu cộng Gaussian (đường đứt). Hình 5.19 cũng chỉ ra rằng kích thước khối càng lớn, độ cải thiện của xác suất lỗi của sơ đồ đề xuất càng tăng khi so sánh với các phương pháp nhúng watermark chỉ trong một kênh ảnh trong cả hai trường hợp có và không có sự hiện diện của nhiễu cộng Gaussian. Tuy nhiên, khi kích thước khối càng lớn thì càng ít bit thông tin có thể nhúng trong ảnh.



Hình 5.3 SNR theo kích thước khối.

CHƯƠNG 6 KẾT LUẬN VÀ KIẾN NGHỊ HƯỚNG NGHIÊN CỨU TIẾP THEO

6.1 Kết luận

Về mặt lý thuyết, luận án có ba nội dung mới và đóng góp nổi trội về mặt khoa học sau đây.

- Thứ nhất, luận án đề xuất hai giải pháp hiệu quả DICOM_LSB_AES và DICOM_LSB_AES_RONI bằng cách kết hợp các kỹ thuật mã hóa và mật mã AES với kỹ thuật watermarking LSB cho ảnh đặc thù DICOM để tăng cường tính bảo mật thông tin trong lưu trữ và truyền hình ảnh y tế. Các kết quả của nội dung nghiên cứu này đã được công bố trong 1 bài báo tạp chí trong nước và 4 bài báo hội nghị quốc tế.
- Thứ hai, luận án xây dựng và phân tích các thông số đánh giá hiệu quả của hai mô hình watermarking trải phổ hợp tác mới CSS và CSS_KLT cho ảnh đa kênh dựa trên kỹ thuật watermarking trải phổ truyền thống cùng các giải pháp điều chỉnh cải tiến mở rộng bao gồm MISS, MISS_DCT, MISS_DWT, ICSS, MCSS, ICSS_KLT, MCSS_KLT. Các kết quả của nội dung nghiên cứu này đã được công bố trong 1 bài báo tạp chí quốc tế Scopus và 1 bài báo hội nghị quốc tế.
- Thứ ba, luận án đề xuất các giải pháp Q_SIFT (Quantization_SIFT), HRMQ_SIFT (Half-Ring-shape-based Multibit Q_SIFT), FSMQ_SIFT (Fan-shape-based Multibit Q_SIFT), SQ_SIFT (Secure Q_SIFT) nhằm nâng cao tính bền vững trước các tấn công đồng bộ và tính bảo mật của watermarking mù bằng cách chọn lọc các đặc trưng SIFT và kỹ thuật lượng tử. Các kết quả của nội dung nghiên cứu này đã được công bố trong 1 bài báo tạp chí quốc tế Scopus và 1 bài báo hội nghị quốc tế.

Để kiểm chứng tính chính xác của các giải pháp đề xuất, luận án thực hiện các phân tích dựa trên mô hình xác suất (toán học) và kiểm chứng kết quả (mô phỏng) với các loại hình ảnh khác nhau.

Về mặt thực tiễn, luận án đã thực hiện các chương trình ứng dụng để thử nghiệm các giải pháp đề xuất với dữ liệu hình ảnh y tế và môi trường thực tế tại một số

bệnh viện thông qua 2 đề tài cấp nhà nước, 2 đề tài cấp thành phố, 2 đề tài cấp trường. Tất cả các đề tài này đều đã nghiệm thu đạt yêu cầu.

6.2 Kiến nghị hướng nghiên cứu tiếp theo

Trí tuệ nhân tạo (AI) với các giải thuật học máy và các mạng nơ-ron học sâu đã ngày càng chứng tỏ được ưu thế vượt trội so với các phương pháp truyền thống trong các ứng dụng xử lý ảnh từ phát hiện, nhận dạng, phân tích, tái tạo các ảnh tự nhiên thông thường cho đến các ảnh chuyên biệt đặc thù như ảnh hồng ngoại, ảnh 3D, ảnh siêu phổ hay ảnh y tế [133-135]. Đặc điểm chung của phần lớn các ứng dụng này sử dụng mô hình học có giám sát, trong đó cần cơ sở dữ liệu ảnh mẫu tương đối lớn với dữ liệu nhãn tương ứng. Tại Việt Nam, AI được đưa vào danh mục công nghệ cao ưu tiên đầu tư phát triển từ năm 2014. Đến nay nhiều trường đại học và các tập đoàn lớn như Vingroup, FPT, Viettel, v.v. đã thành lập các trung tâm nghiên cứu mạnh về AI và bắt đầu tiến hành chia sẻ cơ sở dữ liện lớn, đặc biệt là trong lĩnh vực ảnh y tế [136]. Tuy nhiên, hiện nay cơ sở dữ liệu ảnh mẫu và dữ liệu nhãn hoàn toàn tách biệt. Điều này có thể dẫn đến những nhầm lẫn sai lệch trong quá trình thu thập hay hiệu chỉnh cơ sở dữ liệu huấn luyện cũng như gặp khó khăn trong việc xác thực hay bảo mật. Mặt khác, các mô hình học máy với trọng số đã được huấn luyện thành công sau khi công bố hay triển khai có thể bị sao chép bất hợp pháp [137].

Trong khi đó, kỹ thuật nhúng trích thông tin (watermarking) không ngừng được nghiên cứu trong suốt thời gian qua do khả năng ứng dụng và mở rộng trong nhiều lĩnh vực khác nhau [138-141]. Một trong những hướng nghiên cứu watermarking gần đây là sử dụng các mô hình học máy chuyên sâu để nâng cao hiệu quả thực hiện nhúng trích thông tin hoặc để bảo vệ bản quyền và chống sao chép các mô hình học máy [142-145]. Do đó, các kết quả của luận án có thể được tiếp tục nghiên cứu phát triển theo hướng phân tích đánh giá khả năng hoạt động của các ứng dụng xử lý ảnh dựa trên trí tuệ nhân tạo trong các trường hợp nhúng thông tin trong ảnh kiểm thử hoặc tập ảnh huấn luyện.

DANH MỤC CÔNG TRÌNH ĐÃ CÔNG BỐ

Tạp chí quốc tế

1. *Bài báo số 1.* Tuan Nguyen-Thanh, Thuong Le-Tien, "Robust Blind Medical Image Watermarking Using Quantization and SIFT with Enhanced Security," Journal of Advances in Information Technology (JAIT), 13(1): 45-52, February 2022, ISSN 1798-2340. doi: 10.12720/jait.13.1.45-52. **Indexed by Scopus**.

2. *Bài báo số 2.* Thuong Le-Tien, Tuan Nguyen-Thanh, Hanh-Phan Xuan, Giang Nguyen-Truong, and Vinh Ta-Quoc, "Deep Learning Based Approach Implemented to Image Super-Resolution," Journal of Advances in Information Technology (JAIT), 11(4): 209-216, November 2020, ISSN 1798-2340. doi: 10.12720/jait.11.4.209-216. **Indexed by Scopus**.

3. *Bài báo số 3.* Tuan Nguyen-Thanh, Thuong Le-Tien, "Study on Improved Cooperative Spread Spectrum based Robust Blind Image Watermarking," Journal of Advances in Information Technology (JAIT), 11(3): 119-127, August 2020, ISSN 1798-2340. doi: 10.12720/jait.11.3.119-127. **Indexed by Scopus**.

Tạp chí trong nước

4. *Bài* báo *số 4.* Nguyễn Chí Ngọc, Trần Quý Tường, Võ Nguyễn Thành Nhân, Nguyễn Thanh Tuấn, Trần Tùng, "Hiệu quả ứng dụng PACS-Cloud trong chẩn đoán từ xa, hội chẩn trực tuyến và quản lý thông tin tại các bệnh viện," Tạp chí Y học thực hành, vol. 1140, pp. 163-170, 2020, ISSN: 1859-1663. **(tạp chí thuộc danh mục tạp chí được tính điểm theo quy định của Hội đồng chức danh giáo sư nhà nước)**.

Kỷ yếu hội nghị quốc tế

1. *Bài báo số 5.* Tuan T. Nguyen, Ngoc C. Nguyen, Thuong T. Le, "An Efficient Solution for Robust Blind Watermarking against Geometrical Attacks with Medical Images," IEEE International Symposium on Electrical and Electronic Engineering (ISEE), pp. 114-119, 15-16 April 2021, Ho Chi Minh City - Vietnam, ISBN: 978-0-7381-3196-2. doi: 10.1109/ISEE51682.2021.9418778.

2. *Bài báo số 6*. Tuan T. Nguyen, Ngoc C. Nguyen, Thuong T. Le, "Manufacturing PACS, Online Medical Consultation System and Designing Security DICOM Web Viewer Software," IEEE International Symposium on Electrical and Electronic Engineering (ISEE), pp. 37-42, 10-12 October 2019, Ho Chi Minh City - Vietnam, ISBN: 978-1-7281-5353-7. doi: 10.1109/ISEE2.2019.8921007.

3. *Bài báo số 7.* Tuan T. Nguyen, Luan M. Tran, Ngoc C. Nguyen, Thuong T. Le, "An Efficient Solution to Secure Embedded Information in DICOM Images for Telemedicine," 7th International Conference on the Development of Biomedical Engineering in Vietnam (BME7), 2018, Ho Chi Minh City - Vietnam, IFMBE Proceedings book series (IFMBE, vol. 69), pp. 435-440, 2019, Springer, Singapore, ISBN: 978-981-13-5858-6. URL: https://doi.org/10.1007/978-981-13-5859-3_76.

4. *Bài báo số 8.* Tuan Nguyen, Binh Pham, Luan Pham, Ngoc Nguyen, Luan Tran, Thuong Le, "Design of Web based DICOM Processing Software System for Telemedicine with Mobile and Smart Television," IEEE International Conference on Advanced Computing and Applications (ACOMP), 27-29 November 2018, pp. 42-49, Ho Chi Minh City - Vietnam, ISBN: 978-1-5386-9186-1. doi: 10.1109/ACOMP.2018.00015.

5. *Bài báo số 9.* Nguyen Thanh Tuan, Nguyen Chi Ngoc, Le Tien Thuong, Tran Minh Luan, Nguyen My Qui, "Design of a DICOM Viewer Software with Enhanced Security for Telemedicine," International Symposium on Electrical and Electronics Engineering (ISEE), 2017, Ho Chi Minh City - Vietnam.

6. *Bài báo số 10.* Tuan T. Nguyen, Thuong T. Le, "A Comparative Study on Spread Spectrum Based Image Watermarking," The 11th South East Asian Technical University Consortium Symposium (SEATUC), 2017, Ho Chi Minh City - Vietnam.