ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

HÀ TRỌNG THẮNG

BẢO VỆ BẢN QUYỀN ẢNH MÀU KỸ THUẬT SỐ BẰNG LƯỢC ĐỒ THỦY VÂN DỰA VÀO PHÉP BIẾN ĐỔI DFT KẾT HỢP VỚI PHÉP BIẾN ĐỔI SIFT

Chuyên ngành: Khoa học máy tính
Mã số: 60 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS TS BÙI THẾ HỒNG

Thái Nguyên, 2015

LỜI CAM ĐOAN

Tôi xin cam đoan, luận văn "***Bảo vệ bản quyền ảnh màu kỹ thuật số bằng lược đồ thủy vân dựa vào phép biến đổi DFT kết hợp với phép biến đổi SIFT***" là công trình nghiên cứu của cá nhân tôi, các nội dung nghiên cứu và trình bày trong luận văn là trung thực. Những tư liệu được sử dụng trong luận văn có nguồn gốc và trích dẫn rõ ràng, đầy đủ.

Thái Nguyên, tháng 05 năm 2015

Tác giả luận văn

Hà Trọng Thắng

LỜI CẢM ƠN

Tôi xin cảm ơn Trường Đại học Công nghệ thông tin và Truyền thông - Đại học Thái Nguyên đã tạo điều kiện thuận lợi cho tôi hoàn thành khóa học và khóa luận này.

Tôi xin gửi lời cảm ơn chân thành nhất tới PGS TS Bùi Thế Hồng. Thầy đã cho tôi những định hướng nghiên cứu, giúp đỡ tôi trong suốt thời gian hoàn thành luận văn này.

Để hoàn thành khóa học còn có công sức rất lớn của các thầy, cô đã nhiệt tình giảng dạy, trang bị cho tôi những kiến thức quý báu trong thời gian học tập tại trường.

Cảm ơn các bạn trong lớp đã nhiệt tình giúp đỡ trong suốt thời gian học tập tại trường.

Học viên

Hà Trọng Thắng

MỤC LỤC

MỞ ĐẦU

CHƯƠNG I

TỔNG QUAN VỀ THỦY VÂN SỐ

1.1 Giới thiệu về thủy vân 4
1.2 Giới thiệu về ảnh 6
1.2.1 Ảnh 6
1.2.2 Một số định dạng của ảnh 8
1.3 Những tấn công trên hệ thuỷ vân 10
1.4 Phân loại thủy vân 11
1.5 Các ứng dụng của thủy vân 13
1.6 So sánh kỹ thuật giấu tin và thủy vân trên ảnh số 15
1.7 Các phép biến đổi rời rạc 16
1.7.1 Phép biến đổi Cosine rời rạc (DCT) 16
1.7.2 Phép biến đổi sóng nhỏ rời rạc (DWT) 17
1.7.3 Phép biến đổi Fourier rời rạc (DFT) 19

CHƯƠNG II

LƯỢC ĐỒ THỦY VÂN ẢNH SỐ DỰA VÀO PHÉP BIẾN ĐỔI DFT KẾT HỢP VỚI PHÉP BIẾN ĐỔI SIFT

2.1 Bộ phát hiện góc Harris 22
2.2 Đồng bộ hóa thủy vân 25
2.3 Phép biến đổi đặc trưng bất biến tỷ lệ (SIFT) 25
2.3.1 Phát hiện cực trị 26
2.3.2 Định vị các điểm khóa 29
2.3.3 Gán hướng cho các điểm khóa 30
2.3.4 Xây dựng bộ mô tả cục bộ 31
2.4 Khôi phục ảnh 36
2.5 Lược đồ thủy vân sử dụng kết hợp DFT và SIFT 37
2.5.1 Lược đồ nhúng thủy vân 37
2.5.2 Lược đồ phát hiện thủy vân 42

CHƯƠNG III

XÂY DỰNG CHƯƠNG TRÌNH THỬ NGHIỆM

3.1 Giới thiệu 46
3.2 Thiết kế chương trình 46
3.3 Thử nghiệm chương trình 47
3.4 Đánh giá kết quả thử nghiệm 55
KẾT LUẬN 58
TÀI LIỆU THAM KHẢO 59
PHỤ LỤC 61

NHỮNG CHỮ VIẾT TẮT

Chữ viết tắt	Chữ viết đầy đủ
BMP	Bitmap
JPEG	Joint Photographic Experts Group
GIF	Graphics Interchange Format
PNG	Portable Network Graphics
DoG	Difference-of-Gaussian
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
PSNR	Peak Signal to Noise Ratio
SIFT	Scale Invariant Feature Transform

DANH MỤC BẢNG BIỂU

Bảng 3.1 Kết quả so khớp thủy vân trích xuất và thủy vân gốc ……..... 52

Bảng 3.2 Kết quả so khớp thủy vân trích xuất và thủy vân gốc……..... 55

Bảng 3.3 Tỷ số PSNR của ảnh biến đổi Affine và ảnh khôi phục……. 56

Bảng 3.4 Tỷ số PSNR của ảnh xoay 60^0 và ảnh khôi phục……..... 56

Bảng 3.5 Tổng hợp kết quả thử nghiệm……. 57

DANH MỤC HÌNH VẼ

Hình 1.1 Phân loại các kỹ thuật thuỷ vân……. 11
Hình 1.2 Ví dụ về thuỷ vân hiện, dòng chữ "Abdullah alzaid"…….. 12
Hình 1.3 Ảnh Pepper đã được nhúng thuỷ vân ẩn ở hình bên phải…….. 13
Hình 1.4 Phân loại kỹ thuật giấu tin trong ảnh…….. 15
Hình 2.1 Nguyên tắc phát hiện góc Harris…….. 24
Hình 2.2 Đồng bộ hóa dựa trên trích xuất các điểm đặc trưng…… 25
Hình 2.3 Xây dựng một thể hiện không gian tỷ lệ…….. 27
Hình 2.4 Các giá trị cực đại và cực tiểu của các ảnh DoG…….. 28
Hình 2.5 Bộ mô tả điểm khóa…….. 32
Hình 2.6 Các điểm đặc trưng được so khớp dùng biến đổi SIFT …….. 35
Hình 2.7 Khôi phục ảnh dưới các tấn công hình học khác nhau…….. 37
Hình 2.8 Lược đồ nhúng thủy vân…….. 38
Hình 2.9 Cặp điểm (x_i, y_i) và (-y_i, x_i) trên mặt phẳng DFT…… 39
Hình 2.10 Lược đồ phát hiện thủy vân…….. 43
Hình 3.1 Giao diện chính của chương trình..... 47
Hình 3.2 Trích xuất 2 ảnh con từ ảnh gốc..... 48
Hình 3.3 Giao diện chương trình demo thực nghiệm tấn công..... 49
Hình 3.4 Ảnh đã thủy vân với các điểm đặc trưng quan trọng..... 50
Hình 3.5 Ảnh biến đổi Affine với các điểm đặc trưng quan trọng..... 50
Hình 3.6 So khớp điểm đặc trưng giữa ảnh thủy vân và ảnh biến dạng..... 50
Hình 3.7 Ảnh được khôi phục…….. 51
Hình 3.8 Trích xuất 2 ảnh con từ ảnh đã khôi phục..... 51
Hình 3.9 Giao diện chương trình demo thực nghiệm tấn công..... 52
Hình 3.10 Ảnh đã thủy vân với các điểm đặc trưng quan trọng..... 53

Hình 3.11 Ảnh xoay 60^0 với các điểm đặc trưng quan trọng..... 53
Hình 3.12 So khớp điểm đặc trưng giữa ảnh thủy vân và ảnh biến dạng.... 54
Hình 3.13 Ảnh được khôi phục…….... 54
Hình 3.14 Trích xuất 2 ảnh con từ ảnh được phục hồi..... 55

MỞ ĐẦU

Trong thời đại ngày nay, cùng với sự phát triển vượt bậc của công nghệ thông tin là sự phát triển mạnh mẽ của các sản phẩm số. Các sản phẩm số này có thể là văn bản, âm thanh, hình ảnh, video, phần mềm, cơ sở dữ liệu. Đồng thời, công nghệ thông tin phát triển cũng giúp cho việc chỉnh sửa, sao chép và phân phối các sản phẩm số trở nên dễ dàng, điều này kéo theo một thực trạng là số lượng các bản sao chép bất hợp pháp của các sản phẩm số ngày một nhiều. Làm thế nào để bảo vệ bản quyền, chống sao chép, phân biệt giả mạo là một nhu cầu thiết yếu nhằm bảo vệ bản quyền và sở hữu trí tuệ cho các sản phẩm số. Một trong những kỹ thuật để giải quyết vấn đề này chính là kỹ thuật thủy vân số (Digital Watermarking).

Thủy vân là một mẩu tin được ẩn trực tiếp trong sản phẩm số. Bằng trực quan thì khó có thể phát hiện được thủy vân trong sản phẩm chứa nhưng ta có thể tách được chúng bằng các chương trình có cài đặt thuật toán thủy vân. Thủy vân tách được từ sản phẩm số chính là bằng chứng kết luận sản phẩm này là thuộc về ai hoặc sản phẩm này có bị xuyên tạc hay không.

Hiện tại đã có khá nhiều lược đồ thuỷ vân nhằm bảo vệ quyền sở hữu cho các bức ảnh kỹ thuật số thông qua các thông tin được nhúng trong ảnh, và đó như là một hình thức dán tem bản quyền. Việc lựa chọn một thuật toán thủy vân tối ưu để nó có thể tồn tại bền vững cùng với sản phẩm nhằm chống việc tẩy xóa, làm giả hay biến đổi, phá hủy thủy vân, là một yêu cầu cần phải nghiên cứu.

Để vượt qua được một trong những khó khăn trên, gần đây một số tác giả của bài báo [12] đã đưa ra ý tưởng về một lược đồ thủy vân dựa trên sự phục hồi của ảnh sử dụng phép biến đổi đặc trưng bất biến tỷ lệ (Scale Invariant Feature Transform - SIFT). Với mục đích của lược đồ này là tạo khả

năng bền vững cho thủy vân trước các cuộc tấn công xử lý tín hiệu thông thường và các cuộc tấn công biến dạng hình học, bao gồm: xoay, lật, co giãn, dịch chuyển, mở rộng, cắt xén, và một số các cuộc tấn công kết hợp.

Trong số những cuộc tấn công, biến dạng hình học đã được coi là một trong những cuộc tấn công khó khăn nhất để chống lại, do các lỗi đồng bộ hóa biến dạng hình học tạo ra. Do đó, quá trình đồng bộ hóa thủy vân là điều cần thiết cho sự bền vững của các hệ thống thủy vân.

Trong lược đồ thủy vân, quá trình đồng bộ hóa có hai điểm chính là: trích xuất các điểm đặc trưng của ảnh (lấy các điểm đặc trưng quan trọng mà bất biến với biến đổi hình học) [5] và khôi phục hình ảnh.

Bài báo trên đã mở ra một hướng mới trong việc khôi phục ảnh đã thủy vân dựa trên các điểm đặc trưng bất biến. Vì vậy để tiếp tục nghiên cứu theo hướng này, học viên đã tìm hiểu về lược đồ thủy vân có thể chịu được các biến đổi hình học bằng cách sử dụng kết hợp phép biến đổi DFT và phép biến đổi SIFT để nâng cao thêm tính bền vững của thủy vân trước các cuộc tấn công biến dạng hình học [6, 14, 16, 17]. Với lược đồ thủy vân này, thủ tục nhúng và phát hiện thủy vân đều được áp dụng trong miền biến đổi Fourier rời rạc (DFT) cho mỗi ảnh con (ảnh con là được lấy xung quanh vùng giữa của ảnh ban đầu). Để cải thiện sự bền vững của thủy vân, tất cả ảnh con mang cùng một bản sao của thủy vân.

Trước khi phát hiện thủy vân, các mô tả SIFT được sử dụng để khôi phục lại ảnh gần đúng với ảnh ban đầu. Việc phát hiện thủy vân dựa trên số lượng các bit được so khớp giữa thủy vân được trích xuất và thủy vân ban đầu trong các khối hình ảnh nhúng.

Với mục tiêu tìm hiểu về một số lược đồ thủy vân cho ảnh màu kỹ thuật số, đặc biệt là việc sử dụng lược đồ thủy vân dựa vào phép biến đổi Fourier

rời rạc DFT kết hợp với phép biến đổi đặc trưng bất biến tỷ lệ SIFT, học viên đã lựa chọn đề tài: "***Bảo vệ bản quyền ảnh màu kỹ thuật số bằng lược đồ thủy vân dựa vào phép biến đổi DFT kết hợp với phép biến đổi SIFT*** " làm nội dung nghiên cứu cho luận văn tốt nghiệp của mình.

Luận văn được chia làm 3 chương với các nội dung nghiên cứu chính:

Chương 1: *Tổng quan về thủy vân số*

Trong chương này trình bày khái quát những kiến thức cơ bản về thủy vân số, những kiểu tấn công đối với thủy vân, phân loại, ứng dụng và một số kỹ thuật thủy vân trên ảnh số. So sánh giữa kỹ thuật giấu tin và thủy vân trên ảnh số.

Chương 2: *Lược đồ thủy vân ảnh số dựa vào phép biến đổi DFT kết hợp với phép biến đổi SIFT*

Trong chương này trình bày chi tiết kỹ thuật thủy vân ảnh số dựa vào phép biến đổi Fourier rời rạc (DFT) kết hợp với phép biến đổi đặc trưng bất biến tỷ lệ (SIFT) nhằm tạo ra thủy vân bền vững trước các cuộc tấn công hình học trên ảnh số, như: xoay, lật, co giãn, dịch chuyển, mở rộng, cắt xén,…

Chương 3: *Xây dựng chương trình thử nghiệm*

Trong phần này, luận văn sẽ giới thiệu chương trình demo cho lược đồ thủy vân đã đề xuất và thử nghiệm trên một số mẫu ảnh. Sau đó đánh giá các kết quả đã đạt được sau khi thử nghiệm.

CHƯƠNG I
TỔNG QUAN VỀ THỦY VÂN SỐ

Trong chương này trình bày khái quát những kiến thức cơ bản về thủy vân số, những kiểu tấn công đối với thủy vân, phân loại, ứng dụng và một số kỹ thuật thủy vân trên ảnh số. So sánh giữa kỹ thuật giấu tin và thủy vân trên ảnh số.

1.1 Giới thiệu về thủy vân

Phương pháp thủy vân đầu tiên được thực hiện là thủy vân trên giấy. Đó là một thông tin nhỏ được nhúng chìm trong giấy để thể hiện bản gốc hoặc bản chính thức. Theo Hartung và Kutter, thủy vân trên giấy đã bắt đầu được sử dụng vào năm 1292 ở Fabriano, Italy – nơi được coi là nơi sinh của thủy vân. Sau đó, thủy vân đã nhanh chóng lan rộng trên toàn Italy và rồi trên các nước châu Âu và Mỹ. Ban đầu, thủy vân giấy được dùng với mục đích xác định nhãn hàng và nhà máy sản xuất. Sau này được sử dụng để xác định định dạng, chất lượng và độ dài, ngày tháng của sản phẩm. Đến thế kỷ thứ 18, nó bắt đầu được dùng cho tiền tệ và cho đến nay thủy vân vẫn là một công cụ được dùng rộng rãi với mục đích bảo mật cho tiền tệ, chống làm tiền giả. Thuật ngữ "thủy vân" (watermarking) được đưa ra vào cuối thế 18, nó bắt nguồn từ một loại mực vô hình khi viết lên giấy và chỉ hiển thị khi nhúng giấy đó vào nước. Năm 1988, Komatsu và Tominaga đã đưa ra thuật ngữ "thủy vân số" (Digital watermarking).

Trong môi trường phân phối điện tử đang phát triển như hiện nay, việc bảo vệ bản quyền tác giả đối với các sản phẩm số trở nên rất cần thiết. Hiện tại đã có khá nhiều lược đồ thuỷ vân nhằm bảo vệ quyền sở hữu của các bức ảnh số thông qua các thông tin được nhúng trong ảnh.

Có thể chia các kỹ thuật thuỷ vân theo hai hướng tiếp cận chính:

Hướng thứ nhất dựa trên miền không gian ảnh, tức là tiến hành khảo sát tín hiệu và hệ thống rời rạc một cách trực tiếp trên miền giá trị rời rạc của các điểm ảnh gọi là trên miền biến số độc lập tự nhiên. Sau đó, tìm cách nhúng các thông tin bản quyền vào ảnh bằng cách thay đổi các giá trị điểm ảnh sao cho không ảnh hưởng nhiều đến chất lượng ảnh và đảm bảo sự bền vững của thông tin nhúng trước những tấn công có thể có đối với bức ảnh đã nhúng thuỷ vân. Điển hình cho cách tiếp cận này là phương pháp tách bit ít quan trọng nhất *LSB (Least Significant Bit*) và phương pháp sử dụng ma trận số giả ngẫu nhiên.

Hướng thứ hai là sử dụng các phương pháp khảo sát gián tiếp khác thông qua các kỹ thuật biến đổi. Các kỹ thuật biến đổi này làm nhiệm vụ chuyển miền biến số độc lập sang các miền khác và như vậy tín hiệu và hệ thống rời rạc sẽ được biểu diễn trong các miền mới với các biến số mới. Phương pháp biến đổi này cũng giống như phương pháp đổi biến trong phép tính tích phân hay phương pháp đổi hệ tọa độ trong giải tích của toán phổ thông quen thuộc. Sau đó, tìm cách nhúng thuỷ vân vào ảnh bằng cách thay đổi các hệ số biến đổi trong những miền thích hợp để đảm bảo chất lượng ảnh và sự bền vững của thuỷ vân sau khi nhúng.

Phương pháp khảo sát gián tiếp sẽ làm đơn giản rất nhiều các công việc mà chúng ta gặp phải khi dùng phương pháp khảo sát trực tiếp trong miền biến số độc lập tự nhiên. Có nhiều phép biến đổi cho dữ liệu ảnh trong đó có một số phương pháp biến đổi được sử dụng rất phổ biến như: Phép biến đổi cosine rời rạc (Discrete Cosine Transform - DCT), phép biến đổi sóng nhỏ rời rạc (Discrete Wavelet Transform - DWT) và phép biến đổi Fourier rời rạc (Discrete Fourier Transform - DFT).

1.2 Giới thiệu về ảnh

1.2.1 Ảnh

Là một tập hợp hữu hạn các điểm ảnh kề nhau. Ảnh thường được biểu diễn bằng một ma trận hai chiều, mỗi phần tử của ma trận tương ứng với một điểm ảnh.

+ *Ảnh nhị phân (đen trắng)*: là ảnh có giá trị mức xám của các điểm ảnh được biểu diễn bằng 1 bit (giá trị 0 hoặc 1).

Ví dụ về biểu diễn ảnh nhị phân:

0	1	1	0
1	0	1	0
0	1	1	1
1	1	0	1

+ *Ảnh xám*: Giá trị mức xám của các điểm ảnh được biểu diễn bằng 1 byte (8 bit) (1 byte biểu diễn: $2^8 = 256$ mức, có giá trị từ 0 đến 255)

Ví dụ về biểu diễn ảnh xám:

0	6	15	0
125	17	79	5
0	88	198	17
1	253	19	11

+ *Ảnh màu*: thông thường, ảnh màu được tạo nên từ 3 ảnh xám đối với màu nền đỏ (RED), xanh lá cây (GREEN), xanh nước biển (BLUE). Tất cả các màu trong tự nhiên đều có thể được tổng hợp từ 3 thành phần màu trên

theo các tỷ lệ khác nhau. Người ta thường dùng 3 byte để mô tả mức màu, khi đó các giá trị màu: $2^{8*3} = 2^{24} \approx 16,7$ triệu màu.

Ví dụ về biểu diễn ảnh màu:

Ma trận biểu diễn mức xám của thành phần RED:

0	6	215	0
25	17	179	5
0	88	18	17
10	253	19	7

Ma trận biểu diễn mức xám của thành phần GREEN:

0	6	15	0
12	0	79	5
0	188	19	170
1	53	19	1

Ma trận biểu diễn mức xám của thành phần BLUE:

0	16	15	0
125	0	179	5
0	26	55	17
1	0	1	68

1.2.2 Một số định dạng của ảnh

+ *Ảnh BMP (Bitmap)*: Là định dạng được phát triển bởi Microsoft Corporation, được lưu trữ dưới dạng độc lập thiết bị cho phép Windows hiển thị dữ liệu không phụ thuộc vào khung chỉ định màu trên bất kì phần cứng nào. Tên mở rộng mặc định của một tập tin ảnh Bitmap là .BMP.

Cấu trúc của mỗi tập tin ảnh BMP gồm bốn phần:

∗ Bitmap Header (14 bytes): giúp nhận dạng tập tin bitmap.

∗ Bitmap Information (40 bytes): lưu một số thông tin giúp hiển thị ảnh.

∗ Palette màu - Bảng màu của ảnh: định nghĩa các màu sẽ được sử dụng trong ảnh.

∗ BitmapData - Dữ liệu ảnh: là phần chứa giá trị màu của điểm ảnh (pixel) trong BMP. Các dòng ảnh được lưu từ dưới lên trên, các điểm ảnh được lưu từ trái sang phải. Giá trị của mỗi điểm ảnh là một chỉ số trỏ tới phần tử màu tương ứng của Palette màu.

Thuộc tính BitCount (số bit cho một điểm ảnh - bit per pixel) của thành phần Bitmap Information cho biết số bit (có thể là 1, 4, 8, 16, 24) dành cho mỗi điểm ảnh và số lượng màu lớn nhất của ảnh. BitCount càng lớn thì ảnh càng có nhiều màu, và càng rõ nét hơn. Cụ thể các giá trị như sau:

- 1: Bitmap là ảnh đen trắng, mỗi bit biểu diễn một điểm ảnh. Nếu bit mang giá trị 0 thì điểm ảnh là đen, bit mang gía trị 1 điểm ảnh là điểm trắng.
- 4: Bitmap là ảnh 16 màu.
- 8: Bitmap là ảnh 256 màu.
- 16: Bitmap là ảnh high color (2^{16} = 65.536 màu).

- 24: Bitmap là ảnh true color ($2^{24} \approx 16$ triệu màu), có chất lượng hình ảnh trung thực nhất.

Chiều cao (height) và chiều rộng (width) của ảnh tính bằng điểm ảnh (pixel).

Đặc điểm nổi bật nhất của định dạng BMP là tốc độ vẽ và tốc độ xử lý nhanh, tập tin hình ảnh thường không được nén bằng bất kỳ thuật toán nào. Do đó, một hình ảnh lưu dưới dạng BMP thường có kích cỡ rất lớn, gấp nhiều lần so với các ảnh được nén (chẳng hạn JPEG, GIF hay PNG).

+ *Ảnh JPEG (Joint Photographic Experts Group)*: Đây là một định dạng ảnh được hỗ trợ bởi nhiều trình duyệt Web. Ảnh JPEG được phát triển để nén dung lượng và lưu trữ ảnh chụp, và được sử dụng tốt nhất cho đồ họa có nhiều màu sắc, ví dụ như là ảnh chụp được scan. File ảnh JPEG là ảnh Bitmap đã được nén lại.

+ *Ảnh GIF (Graphics Interchange Format)*: Được phát triển dành cho những ảnh có tính chất thay đổi. Nó được sử dụng tốt nhất cho đồ họa có ít hơn 256 màu, ví dụ như là ảnh hoạt hình hoặc là những bức vẽ với nhiều đường thẳng. File ảnh GIF là những ảnh Bitmap được nén lại.

Có hai sự khác nhau cơ bản giữa ảnh GIF và ảnh JPEG:

- Ảnh GIF nén lại theo cách dữ nguyên toàn bộ dữ liệu ảnh trong khi ảnh JPEG nén lại nhưng làm mất một số dữ liệu trong ảnh.
- Ảnh GIF bị giới hạn bởi số màu nhiều nhất là 256 trong khi ảnh JPEG không giới hạn số màu mà chúng sử dụng.

+ *Ảnh PNG (Portable Network Graphics)*: Là một dạng hình ảnh sử dụng phương pháp nén dữ liệu mới - không làm mất đi dữ liệu gốc. PNG được tạo ra nhằm cải thiện và thay thế định dạng ảnh GIF. PNG nén tốt hơn và có nhiều tính năng kỹ thuật hay hơn GIF. Tất cả tính năng của GIF, trừ nén hoạt hình, đều được hỗ trợ bởi PNG.

1.3 Những tấn công trên hệ thuỷ vân

Phương pháp thuỷ vân cần chống lại được một số phép xử lý ảnh thông thường và một số tấn công có chủ đích. Cho đến nay vẫn chưa có một hệ thống thuỷ vân hoàn hảo và cũng không rõ ràng việc liệu có tồn tại hay không một hệ thống thuỷ vân an toàn tuyệt đối. Vì vậy, trong thực tế thì thuỷ vân phải cân nhắc giữa bền vững với các thuộc tính khác như lượng thông tin giấu, tính ẩn… Dựa vào yêu cầu của ứng dụng mà sẽ ảnh hưởng đến phương pháp thuỷ vân. Dựa vào những biến đổi có chủ đích hay không có chủ đích đối với hệ thuỷ vân mà ta có thể phân biệt thành hai nhóm tấn công sau: một là các biến đổi được xem như là các nhiễu đối với dữ liệu, hai là làm mất tính đồng bộ để không thể lấy tin ra được.

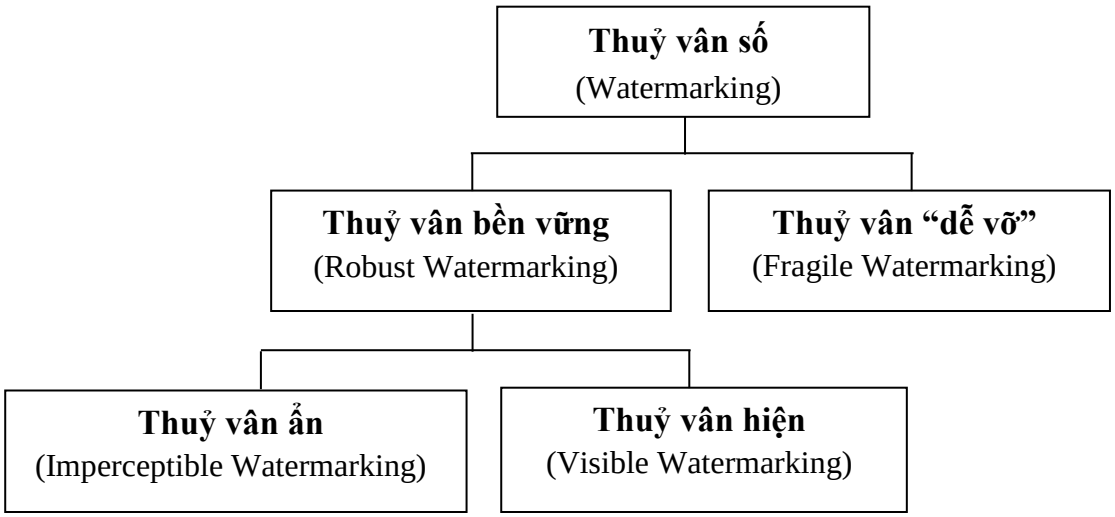
Dưới đây là một vài phép thay đổi trên ảnh số:

- Biến đổi tín hiệu: làm sắc nét, thay đổi độ tương phản, màu, gamma…
- Nhiễu cộng, nhiễu nhân…
- Lọc tuyến tính
- Nén mất thông tin
- Biến đổi affine cục bộ hoặc toàn cục
- Giảm dữ liệu: cropping, sửa histogram
- Chuyển mã (gif $\rightarrow$ jpeg)
- Chuyển đổi tương tự - số
- Thuỷ vân nhiều lần

Nguyên tắc cơ bản của phương pháp thuỷ vân là đảm bảo đủ tính bền vững sao cho các tấn công sẽ làm cho giá trị thương mại của ảnh gốc bị ảnh hưởng.

1.4 Phân loại thủy vân

Ứng dụng của thủy vân là rất lớn, mỗi ứng dụng lại có những yêu cầu riêng và tính chất riêng, do đó các kỹ thuật thuỷ vân cũng có những tính năng khác biệt tương ứng:



Hình 1.1 Phân loại các kỹ thuật thuỷ vân

Các kỹ thuật thuỷ vân trên *hình 1.1* được phân biệt nhau bởi những đặc trưng, tính chất của từng kỹ thuật và ứng dụng những kỹ thuật đó. Thuỷ vân "dễ vỡ" (fragile) là kỹ thuật nhúng thuỷ vân vào trong ảnh sao cho khi phân phối sản phẩm trong môi trường mở nếu có bất cứ một phép biến đổi nào làm thay đổi đối tượng sản phẩm gốc thì thuỷ vân đã được giấu trong đối tượng sẽ không còn nguyên vẹn như trước khi giấu nữa (dễ vỡ). Các kỹ thuật thuỷ vân có tính chất này được sử dụng trong các ứng dụng nhận thực thông tin (authentication) và phát hiện xuyên tạc thông tin (tamper detection). Rất dễ hiểu vì sao những ứng dụng này cần đến kỹ thuật thuỷ vân dễ vỡ. Ví dụ như để bảo vệ chống xuyên tạc một ảnh nào đó ta nhúng một thuỷ vân vào trong ảnh và sau đó phân phối, quảng bá ảnh đó. Khi cần kiểm tra lại ảnh ta sử dụng hệ thống đọc thủy vân. Nếu không đọc được thuỷ vân hoặc thuỷ vân đã bị sai lệch nhiều so với thuỷ vân ban đầu đã nhúng vào ảnh thì có nghĩa là có thể ảnh đó đã bị thay đổi. Ngược lại, với kỹ thuật thuỷ vân dễ vỡ là kỹ thuật thuỷ

vân bền vững (robust). Các kỹ thuật thuỷ vân bền vững thường được sử dụng trong các ứng dụng bảo vệ bản quyền. Trong những ứng dụng đó, thuỷ vân đóng vai trò là thông tin sở hữu của người chủ hợp pháp. Thuỷ vân được nhúng trong sản phẩm như một hình thức dán tem bản quyền. Trong trường hợp như thế, thuỷ vân phải tồn tại bền vững cùng với sản phẩm nhằm chống việc tẩy xoá, làm giả hay biến đổi phá huỷ thuỷ vân. Một yêu cầu lí tưởng đối với thuỷ vân bền vững là nếu muốn loại bỏ thuỷ vân thì cách duy nhất là phá huỷ sản phẩm.

Thuỷ vân bền vững lại được chia thành hai loại là thuỷ vân ẩn và thuỷ vân hiện. Thuỷ vân hiện là loại thuỷ vân được hiện ngay trên sản phẩm và người dùng có thể nhìn thấy được giống như các biểu tượng kênh chương trình trên Tivi mà chúng ta thường thấy. Các thuỷ vân hiện trên ảnh thường dưới dạng chìm, mờ hoặc trong suốt để không gây ảnh hưởng đến chất lượng ảnh gốc. Đối với thuỷ vân hiện, thông tin bản quyền hiển thị ngay trên sản phẩm.

Hình 1.2 Ví dụ về thuỷ vân hiện, dòng chữ "Abdullah alzaid"

Hình 1.3 Ảnh Pepper đã được nhúng thuỷ vân ẩn là hình bên phải

Còn đối với thuỷ vân ẩn thì cũng giống như giấu tin, bằng mắt thường không thể nhìn thấy thuỷ vân. Trong vấn đề bảo vệ bản quyền, thuỷ vân ẩn mang tính "bất ngờ" hơn trong việc phát hiện sản phẩm bị đánh cắp. Trong trường hợp này, người chủ sở hữu hợp pháp sẽ chỉ ra bằng chứng là thuỷ vân đã được nhúng trong sản phẩm bị đánh cắp.

1.5 Các ứng dụng của thủy vân

a) Bảo vệ bản quyền tác giả

Đây là ứng dụng cơ bản nhất của kỹ thuật thuỷ vân số, một dạng của phương pháp giấu tin. Một thông tin nào đó mang ý nghĩa quyền sở hữu tác giả sẽ được nhúng vào trong các sản phẩm kỹ thuật số trước khi đưa vào lưu thông, phân phối. Thuỷ vân này chỉ một mình người chủ sở hữu hợp pháp các sản phẩm đó có và được dùng làm minh chứng cho bản quyền sản phẩm. Giả sử có một thành phẩm dữ liệu dạng đa phương tiện như ảnh, âm thanh, video và cần được lưu thông trên mạng. Để bảo vệ các sản phẩm chống lại các hành vi lấy cắp hoặc làm nhái cần phải có một kỹ thuật để "dán tem bản quyền" vào sản phẩm này. Việc dán tem hay chính là việc nhúng thuỷ vân cần phải đảm bảo không để lại một ảnh hưởng lớn nào đến chất lượng cảm nhận của sản phẩm. Yêu cầu kỹ thuật đối với ứng dụng này là thuỷ vân phải tồn tại bền vững cùng với sản phẩm, muốn bỏ thuỷ vân này mà không được phép của người chủ sở hữu thì chỉ còn cách là phá huỷ sản phẩm.

b) Nhận thực thông tin và phát hiện xuyên tạc thông tin

Một tập các thông tin sẽ được giấu trong sản phẩm. Sau đó, các thông tin này sẽ được sử dụng để nhận biết xem sản phẩm gốc có bị thay đổi hay không. Trong trường hợp này, các thuỷ vân thường có dạng ẩn để không bị phát hiện và nếu có bị lộ thì cũng khó làm giả và cũng dễ nhận ra những chỗ đã bị xuyên tạc. Trong các ứng dụng thực tế, người ta mong muốn tìm được vị trí bị xuyên tạc cũng như phân biệt được các thay đổi (ví dụ như phân biệt xem một đối tượng đa phương tiện chứa thông tin giấu đã bị thay đổi, xuyên tạc nội dung hay là chỉ bị nén mất dữ liệu). Yêu cầu chung đối với ứng dụng này là khả năng giấu thông tin cao và thuỷ vân không cần bền vững.

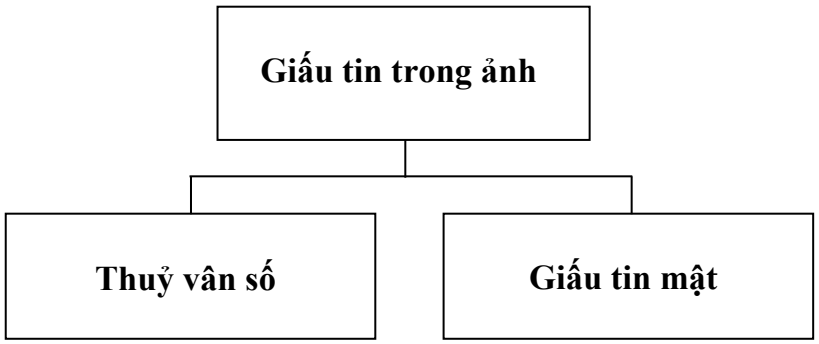
c) Lăn tay hoặc dán nhãn

Thuỷ vân trong những ứng dụng này được sử dụng để nhận diện người gửi hay người nhận của một thông tin nào đó. Ví dụ như các vân khác nhau sẽ được nhúng vào các bản copy khác nhau của thông tin gốc trước khi chuyển cho nhiều người. Với những ứng dụng loại này thì yêu cầu cơ bản chính là đảm bảo độ an toàn cao cho các thuỷ vân không bị xoá hoặc thay đổi trong quá trình phân phối.

d) Kiểm soát sao chép

Các thuỷ vân trong những trường hợp này được sử dụng để kiểm soát sao chép không hợp lệ đối với các sản phẩm kỹ thuật số. Các thiết bị phát hiện ra thuỷ vân thường được gắn sẵn vào trong các hệ thống đọc/ghi. Ví dụ như hệ thống quản lí sao chép DVD đã được ứng dụng ở Nhật. Các ứng dụng loại này cũng yêu cầu thuỷ vân phải được bảo đảm an toàn và cũng sử dụng phương pháp phát hiện thuỷ vân đã giấu mà không cần thông tin gốc.

1.6 So sánh kỹ thuật giấu tin và thủy vân trên ảnh số



Hình 1.4 Phân loại kỹ thuật giấu tin trong ảnh

Độ an toàn và bảo mật thông tin của kỹ thuật giấu tin được thể hiện ở hai khía cạnh. Một là bảo vệ cho dữ liệu đem giấu và hai là bảo vệ cho chính đối tượng được sử dụng để giấu tin. Ứng với hai khía cạnh đó có hai hướng kỹ thuật rõ ràng đó là giấu tin mật và thuỷ vân số.

Đối với giấu tin mật (steganography), dữ liệu nhúng là những thông điệp mật cần trao đổi giữa người gửi và người nhận. Việc nhúng thông điệp mật vào những bức ảnh sẽ tránh được sự chú ý của các đối thủ. Để đảm bảo sự an toàn, trong ứng dụng thường mã hóa thông điệp mật trước khi nhúng vào ảnh và sử dụng các hệ mật mã khóa công khai để trao đổi khóa bí mật của lược đồ giấu tin.

Với thuỷ vân số là kỹ thuật giấu tin nhắm đến những ứng dụng bảo đảm an toàn dữ liệu cho đối tượng được sử dụng để giấu tin như: bảo vệ bản quyền, chống xuyên tạc, nhận thực thông tin, điều khiển sao chép v.v…

Xét về tính chất, thủy vân giống giấu tin ở chỗ cả hai hướng này đều tìm cách nhúng thông tin mật vào một môi trường, nên hệ thuỷ vân số trên ảnh cũng là một hệ giấu tin và có một số đặc điểm chung, như:

- Phương tiện chứa là ảnh hai chiều tĩnh,

- Thuỷ vân trên ảnh tác động lên dữ liệu ảnh nhưng không làm thay đổi kích thước ảnh,
- Kỹ thuật giấu phụ thuộc vào tính chất của hệ thống thị giác con người,
- Khi giải tin có thể cần ảnh gốc.

Nhưng về bản chất thì thủy vân và giấu tin có những nét khác ở một số điểm sau:

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

1.7 Các phép biến đổi rời rạc

1.7.1 Phép biến đổi Cosine rời rạc (DCT)

Phép biến đổi Cosine rời rạc (Discrete Cosine Transform - DCT) do Ahmed và các đồng nghiệp của ông đưa ra vào năm 1974. Từ đó cho đến nay, nó được sử dụng rất phổ biến trong nhiều kỹ thuật xử lí ảnh số. Phép biến đổi Cosine rời rạc gồm: biến đổi thuận (DCT) và biến đổi ngược (IDCT). Biến đổi thuận dùng để chuyển dữ liệu từ miền không gian sang miền tần số, biến đổi ngược chuyển dữ liệu từ miền tần số về miền không gian. Trong các kỹ thuật thuỷ vân ảnh dựa trên phép biến đổi dữ liệu ảnh sang miền tần số thì phép

biến đổi DCT được sử dụng nhiều nhất. Bởi phép biến đổi DCT đã được dùng trong dạng chuẩn ảnh JPEG.

Trong lĩnh vực xử lý ảnh số, biến đổi DCT 2 chiều có dạng như sau:

$$Y_{ij} = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_i\alpha_j\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}X_{uv}Cos\frac{(2u+1)i\pi}{2M}Cos\frac{(2v+1)j\pi}{2N}$$

Với: Y_{ij} là giá trị tại vị trí hàng i, cột j của ma trận DCT.

X_{uv} là giá trị tại hàng u, cột v của ma trận ảnh gốc X.

M,N là kích thước của ảnh gốc (M hàng, N cột).

$$\alpha_i = \begin{cases} \frac{1}{\sqrt{2}} : i = 0 \\ 1 : i = 1,2,...,M-1 \end{cases} \qquad \alpha_j = \begin{cases} \frac{1}{\sqrt{2}} : j = 0 \\ 1 : j = 1,2,...,N-1 \end{cases}$$

Và biến đổi ngược của nó là:

$$X_{ij} = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha_u\alpha_v Y_{uv}Cos\frac{(2i+1)u\pi}{2M}Cos\frac{(2j+1)v\pi}{2N}$$

1.7.2 Phép biến đổi sóng nhỏ rời rạc (DWT)

Đây là phép biến đổi mới nhất được áp dụng cho ảnh số. Ý tưởng của phép biến đổi sóng nhỏ rời rạc (Discrete Wavelet Transform - DWT) cho tín hiệu một chiều như sau: Tín hiệu được chia thành 2 phần, phần tần số cao và phần tần số thấp. Hầu hết năng lượng được tập trung ở phần góc cạnh hoặc có kết cấu và thuộc thành phần có tần số cao. Thành phần tần số có thể được phân tích tiếp thành hai phần có tần số cao và thấp. Với các bài toán nén và thuỷ vân thì ta chỉ cần áp dụng không quá năm lần bước phân chia trên. Ngoài ra, từ các hệ số DWT, ta có thể tạo lại ảnh ban đầu bằng quá trình DWT ngược (IDWT).

Ta có thể mô tả bằng toán học DWT và IDWT như sau. Đặt:

$$H(\omega) = \sum_k h_k e^{-jkw}, \qquad và \qquad G(\omega) = \sum_k g_k e^{-jkw}$$

là lọc thông thấp và lọc thông cao tương ứng, mà thoả mãn một vài điều kiện cho việc tái xây dựng ảnh ban đầu. Một tín hiệu F(n) có thể được phân tích đệ quy như sau:

$$f_{j-1}^{low}(k) = \sum_n h_{n-2k} f_j(n) \quad \text{và} \quad f_{j-1}^{high}(k) = \sum_n g_{n-2k} f_j(n)$$

với j = J+1, J, …, J_0 với $f_{J+1}(k) = F(j)$, $k \in Z$. J+1 là chỉ số mức phân giải cao còn J_0 là chỉ số mức phân giải thấp. Các hệ số

$$f_{J_0}^{low}(k),\ f_{J_0}^{high}(k),\ f_{J_0+1}^{low}(k) \ldots,\ f_J^{high}(k)$$

được gọi là các hệ số của tín hiệu F(n), với $f_{J_0}^{low}(k)$ là phần phân giải nhỏ nhất (xấp xỉ) của F(n) và $f_J^{high}(k)$ là phần chi tiết của F(n) tại các dải tần khác nhau. Tín hiệu ban đầu F(n) có thể được xây dựng lại từ các hệ số DWT bằng cách đệ quy như sau:

$$f_j^{low}(n) = \sum_k h_{n-2k} \cdot f_{j-1}^{k} + \sum_k g_{n-2k} \cdot f_{j-1}^{high}(k)$$

Để đảm bảo quan hệ giữa DWT và IDWT, thì H(ω) và G(ω) phải thoả điều kiện trực giao sau: $|H(\omega)|^2 + |G(\omega)|^2 = 1$.

Biến đổi DWT và IDWT cho mảng hai chiều M×N có thể được định nghĩa tương tự bằng cách thực hiện các biến đổi một chiều DWT và IDWT cho mỗi chiều tương ứng.

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

- Biến đổi sóng là một mô tả đa độ phân giải của ảnh. Quá trình giải mã có thể được xử lý tuần tự từ độ phân giải thấp cho đến độ phân giải cao.

- Biến đổi DWT gần gũi với hệ thống thị giác người hơn biến đổi DCT. Vì vậy, có thể nén với tỉ lệ cao bằng DWT mà sự biến đổi ảnh khó nhận thấy hơn nếu dùng DCT với tỉ lệ tương tự.
- Biến đổi sóng nhỏ tạo ra một cấu trúc được gọi là biểu diễn tỉ lệ-không gian (scale-space representation). Trong biểu diễn này, các tín hiệu tần số cao được xác định chính xác trong miền điểm ảnh (pixel domain), còn các tín hiệu tần số thấp được xác định chính xác trong miền tần số.

1.7.3 Phép biến đổi Fourier rời rạc (DFT)

Phép biến đổi Fourier rời rạc (Discrete Fourier Transform - DFT) là một công cụ toán học được dùng để chuyển cách biểu diễn tín hiệu và hệ thống rời rạc sang miền tần số rời rạc. Thực chất của cách biểu diễn này là lấy từng điểm rời rạc trên vòng tròn đơn vị trong mặt phẳng Z để biểu diễn. Việc biểu diễn trong miền tần số rời rạc đặc biệt hiệu quả khi xuất hiện các thuật toán tính nhanh DFT, thường được gọi là phép biến đổi Fourier nhanh FFT (Fast Fourier Transform).

Định nghĩa biến đổi Fourier rời rạc cho tín hiệu hai chiều (ảnh số)

Tổng quát, phép biến đổi Fourier rời rạc của một ảnh M × N: {u(m,n)} được định nghĩa như sau:

$$v(k,l) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} u(m,n) w_N^{km} w_N^{ln} \qquad \textit{Với} \quad 0 <= l, k <= N-1$$

Biến đổi ngược:

$$u(m,n) = \frac{1}{N}\sum_{k=0}^{N-1}\sum_{l=0}^{N-1} v(k,l) w_N^{-km} w_N^{-ln} \qquad \textit{Với} \quad 0 <= m, n <= N-1$$

ở đây, $W_N^{(km+\ln)}$ là ma trận ảnh cơ sở.

Ta biết rằng, phép biến đổi Fourier rời rạc (DFT) được phát triển dựa trên biến đổi Fourier (Fourier Transform - FT) cho ảnh số (vì ảnh số chỉ là một phần của tín hiệu số), biến đổi DFT tính các giá trị của biến đổi Fourier (FT) cho một tập các giá trị trong không gian tần số được cách đều. Biến đổi Fourier (FT) biểu diễn ảnh liên tục trong không gian 2 chiều được định nghĩa:

- Biến đổi thuận: $F(u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)e^{-2\pi i(xu+yv)}dxdy$
  u, v biểu diễn tần số.
- Biến đổi ngược: $f(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} F(u,v)e^{2\pi i(xu+yv)}dudv$

Theo công thức Ơle: $e^{j\propto} = \cos(\propto) + j\sin(\propto)$

Do vậy:

$$W_N^{(km+\ln)} = e^{-j2\pi(km+ln)/N}$$
$$= \cos(2\pi(km+ln)/N) - j\sin(2\pi(km+ln)/N)$$

Như vậy, các hàm cơ sở trong ma trận ảnh cơ sở của biến đổi Fourier là các hàm cosine và hàm sine. Theo tính toán trên, ta thấy biến đổi Fourier biểu diễn ảnh trong không gian mới theo các hàm sine và cosine.

Biến đổi Fourier đóng vai trò quan trọng trong phân tích các đặc trưng của ảnh, trong nén ảnh và trong việc cải thiện chất lượng của một ảnh khi khôi phục lại.

CHƯƠNG II
LƯỢC ĐỒ THỦY VÂN ẢNH SỐ DỰA VÀO PHÉP BIẾN ĐỔI DFT KẾT HỢP VỚI PHÉP BIẾN ĐỔI SIFT

Trong chương này trình bày chi tiết kỹ thuật thủy vân số dựa vào phép biến đổi Fourier rời rạc (DFT) kết hợp với phép biến đổi đặc trưng bất biến tỷ lệ (SIFT) nhằm tạo ra thủy vân bền vững trước các cuộc tấn công hình học trên ảnh số, như: xoay, lật, co giãn, dịch chuyển, mở rộng, cắt xén,…

Thủy vân là một phương pháp hiệu quả để bảo vệ bản quyền cho ảnh số. Trong số những cuộc tấn công đối với thủy vân, biến dạng hình học đã được coi là một trong những cuộc tấn công khó khăn nhất để chống lại, do các lỗi đồng bộ hóa biến dạng hình học tạo ra.

Trong những năm gần đây, một số phương pháp thủy vân có khả năng chịu được các biến dạng hình học đã được đề xuất. Các lược đồ có thể được tạm phân loại là dựa trên mẫu, dựa trên miền biến đổi bất biến, và dựa trên thời điểm.

Trong luận văn này, giới thiệu một lược đồ thủy vân trên ảnh màu kỹ thuật số dựa vào phép biến đổi Fourier rời rạc (DFT) kết hợp với phép biến đổi đặc trưng bất biến tỷ lệ (SIFT) nhằm cải thiện sự bền vững của thủy vân để chống lại biến dạng hình học. Lược đồ này tách các điểm đặc trưng nổi bật mà bất biến với biến đổi hình học để đồng bộ hóa thủy vân.

Bas et al. [7] đã đề xuất một lược đồ thủy vân dựa trên nội dung, trong đó sử dụng bộ phát hiện góc Harris để trích xuất điểm đặc trưng nổi bật và sau đó lập nên một tập hợp các hình tam giác rời nhau thông qua Delaunay tessellation, và cuối cùng thủy vân được nhúng sử dụng sơ đồ phụ cổ điển DFT và phát hiện thủy vân sử dụng thuộc tính tương quan trong những hình

tam giác. Sự bền vững của các lược đồ thủy vân phụ thuộc vào khả năng của các bộ phát hiện Harris, do đó số lượng các điểm đặc trưng phụ thuộc vào kết cấu của ảnh [9].

Xiaojun Qi et al. [9] đề xuất một kết cấu ảnh dựa trên bộ phát hiện góc Harris thích ứng cho các điểm đặc trưng số phù hợp và phân phối đồng nhất, bất kể hình ảnh kết cấu cao, trung bình hoặc thấp. Và sử dụng thiết lập của các hình tam giác được tạo ra bởi Delaunay tessellation để các yếu tố biến đổi ước lượng, chẳng hạn như yếu tố dịch, yếu tố luân chuyển và yếu tố nhân rộng. Ba yếu tố giống hệt nhau được sử dụng để khôi phục lại hình ảnh mẫu thử, hiệu suất là chấp nhận được.

2.1 Bộ phát hiện góc Harris

Bộ phát hiện góc Harris (*Harris corner detector*) hoặc một thuật ngữ tổng quát hơn là phát hiện điểm quan tâm (*interest point detection*) là một hướng tiếp cận được sử dụng trong các hệ thống thị giác máy tính để trích chọn các loại đặc trưng và suy luận ra các nội dung của một ảnh.

Một góc được xác định bởi nơi giao nhau của hai cạnh. Một góc cũng có thể được xác định như một điểm có hai hướng khác nhau trong một vùng cục bộ của điểm đó. Một điểm quan tâm là một điểm trong một ảnh mà điểm này có vị trí được xác định tốt và có thể được phát hiện nhanh chóng. Điều này có nghĩa là một điểm quan tâm có thể là một góc nhưng cũng có thể là một điểm đơn có giá trị cường độ cực đại hoặc cực tiểu cục bộ, các điểm kết thúc của đường thẳng hoặc một điểm trên một đường cong mà ở đó độ cong là tối đa cục bộ. Trên thực tế, hầu hết các phương pháp phát hiện góc phát hiện các điểm hơn là các góc nói riêng.

Phương pháp phát hiện góc Harris là một phương pháp phát hiện điểm quan tâm phổ biến vì nó bất biến đối với phép xoay, thay đổi độ sáng và tạp

nhiễu ảnh. Phương pháp này dựa trên hàm tương quan tự động cục bộ của một tín hiệu; ở đó hàm tương quan tự động cục bộ đo các thay đổi cục bộ của tín hiệu với các phần ảnh được dịch chuyển một lượng nhỏ theo các hướng khác nhau.

Cho trước sự dịch chuyển ($\triangle x$, $\triangle y$) và một điểm (x, y), hàm tương quan tự động được định nghĩa như sau:

$$c(x,y) = \sum_{\mathrm{w}} [I(x_i, y_i) - I(x_i + \Delta x, y_i + \Delta y)]^2 \qquad (2.1)$$

trong đó $I(x_i, y_i)$ biểu thị hàm ảnh và (x_i, y_i) là các điểm trong cửa sổ W đặt ở vị trí (x, y). Ảnh được dịch chuyển được xấp xỉ bởi phép khai triển Taylor được lượt bớt thành các hạng thức bậc nhất:

$$I(x_i + \Delta x, y_i + \Delta y)] \approx I(x_i, y_i) + [I_x(x_i, y_i) I_y(x_i, y_i)] \begin{bmatrix} \Delta_x \\ \Delta_y \end{bmatrix} \qquad (2.2)$$

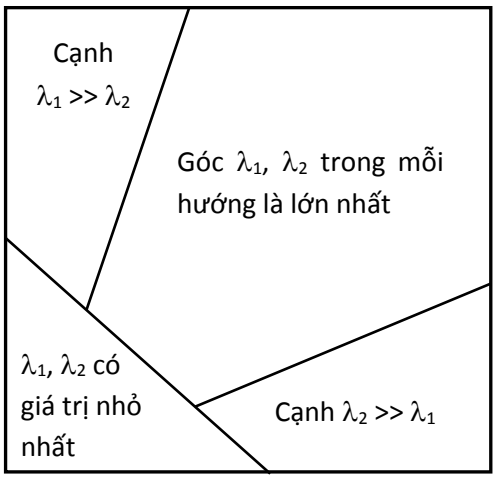
Ở đây, $I_x(x_i, y_i)$ và $I_y(x_i, y_i)$ biểu thị các đạo hàm từng phần tương ứng theo x và y. Thế công thức (2.2) vào (2.1), ta được:

$$\begin{aligned}
c(x,y) &= \textstyle\sum_{\mathrm{w}} [I(x_i, y_i) - I(x_i + \Delta x, y_i + \Delta y)]^2 \\
&= \textstyle\sum_{\mathrm{w}} \left(I(x_i, y_i) - I(x_i, y_i) - [I_x(x_i, y_i) I_y(x_i, y_i)] \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} \right)^2 \\
&= \sum_{\mathrm{w}} \left(-[I_x(x_i, y_i) I_y(x_i, y_i)] \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} \right)^2 \\
&= \sum_{\mathrm{w}} \left([I_x(x_i, y_i) I_y(x_i, y_i)] \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} \right)^2 \\
&= [\Delta x \quad \Delta y] \begin{bmatrix} \sum_{\mathrm{w}} (I_x(x_i, y_i))^2 & \sum_{\mathrm{w}} I_x(x_i, y_i) I_y(x_i, y_i) \\ \sum_{\mathrm{w}} I_x(x_i, y_i) I_y(x_i, y_i) & \sum_{\mathrm{w}} (I_x(x_i, y_i))^2 \end{bmatrix} \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} \\
&= [\Delta x \quad \Delta y] \, c(x,y) \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix}
\end{aligned}$$

Ở đây, ma trận $C(x,y)$ bắt giữ cấu trúc cường độ của một vùng lân cận cục bộ quanh điểm (x, y). Lấy λ_1, λ_2 là các giá trị riêng của ma trận $C(x, y)$. Các giá trị riêng này tạo nên một sự mô tả bất biến đối với phép xoay. Có 3 trường hợp cần được xét:

1. Nếu cả λ_1, λ_2 đều nhỏ, để hàm tương quan tự động cục bộ không thay đổi (tức là ít thay đổi tại $C(x, y)$ theo bất kỳ hướng nào) thì vùng ảnh nằm trong cửa sổ gần như không thay đổi về cường độ. Tức là trong trường hợp này, không có điểm quan tâm nào được tìm thấy tại điểm ảnh (x, y).
2. Nếu một giá trị riêng là lớn và một giá trị riêng là nhỏ, thì chỉ có các dịch chuyển cục bộ theo một hướng (dọc theo đỉnh đó) gây nên sự thay đổi nhỏ ở $C(x, y)$ và thay đổi đáng kể ở hướng trực giao, điều này biểu thị cho một cạnh.
3. Nếu cả hai giá trị riêng đều lớn, thì các sự dịch chuyển theo bất kỳ hướng nào cũng sẽ đưa đến kết quả là làm tăng đáng kể; điều này biểu thị cho một góc.

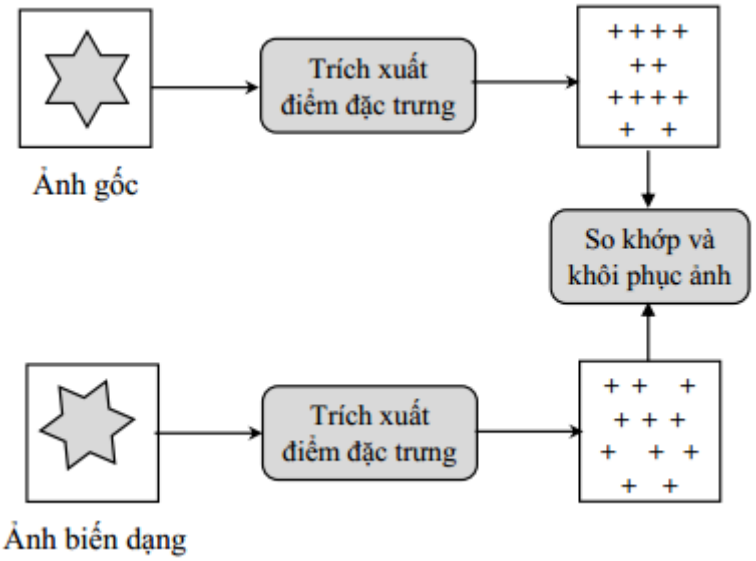
Thuật toán này phát hiện được nhanh chóng các điểm quan tâm trong ảnh.



Hình 2.1 Nguyên tắc phát hiện góc Harris

2.2 Đồng bộ hóa thủy vân

Biến dạng hình học có thể làm ảnh hưởng đáng kể việc thực hiện phát hiện thủy vân vì lỗi đồng bộ hóa. Vì vậy, để giảm tác động của lỗi đồng bộ hóa, đồng bộ hóa thủy vân là điều cần thiết cho lược đồ thủy vân. Trong lược đồ thủy vân được đề xuất, quá trình này có hai điểm chính là: trích xuất các điểm đặc trưng và khôi phục hình ảnh. Quá trình đồng bộ hóa thủy vân hoàn toàn tự động. Luận văn sẽ giới thiệu chi tiết cả hai ở phần sau.



Hình 2.2 Đồng bộ hóa dựa trên trích xuất các điểm đặc trưng

2.3 Phép biến đổi đặc trưng bất biến tỷ lệ (SIFT)

Phép biến đổi đặc trưng bất biến tỷ lệ (Scale Invariant Feature Transform - SIFT) được đề xuất bởi David Lowe [8] và đã chứng minh rằng các điểm trích xuất là bất biến với các biến đổi dịch hình ảnh, xoay, co giãn và chiếu. Ý tưởng chính của SIFT là trích xuất các đặc trưng ổn định trong không gian tỷ lệ. Đây là một trong những phương pháp hiệu quả để trích chọn các điểm bất biến từ các ảnh được dùng để thực hiện so khớp tin cậy giữa các tầm nhìn khác nhau của cùng một đối tượng hoặc quang cảnh. Phương pháp này biến đổi dữ liệu ảnh thành các tọa độ bất biến tỷ lệ có liên quan tới các đặc

trưng cục bộ. Thuật toán gồm 4 giai đoạn chính là: phát hiện các cực trị trong không gian tỷ lệ, định vị chính xác điểm khóa, gán hướng cho các điểm khóa, xây dựng đặc trưng.

2.3.1 Phát hiện cực trị

Giai đoạn đầu tiên của phát hiện điểm khóa là tìm ra các vị trí và các tỷ lệ có thể được gán lặp đi lặp lại dưới các tầm nhìn khác nhau của cùng một đối tượng. Việc phát hiện các vị trí bất biến khi có sự thay đổi tỷ lệ của ảnh có thể được thực hiện bằng việc tìm kiếm các đặc trưng ổn định qua tất cả các tỷ lệ có thể, sử dụng một hàm liên tục tỷ lệ được hiểu như không gian tỷ lệ.

Dùng hàm Gaussian làm hàm nhân của không gian tỷ lệ. Vì vậy, không gian tỷ lệ của một ảnh được xác định bởi hàm $L(x, y, \sigma)$, hàm này được tạo ra từ phép cuộn Gaussian biến thiên tỷ lệ, $G(x, y, \sigma)$, với ảnh đầu vào $I(x, y)$:

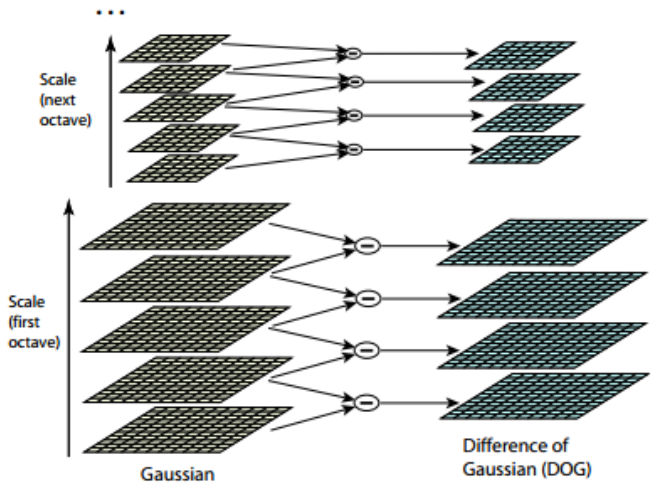
$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y)$$

trong đó * là phép toán cuộn theo x và y, và:

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2}$$

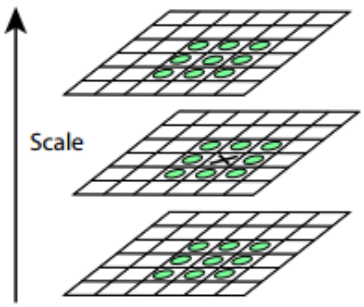
Để phát hiện hiệu quả các vị trí điểm khóa ổn định trong không gian tỷ lệ, ta sử dụng các cực trị không gian tỷ lệ trong hàm *Difference-of-Gaussian (DoG)* được cuộn với ảnh đó, $D(x, y, \sigma)$, hàm này có thể được tính từ sự chênh lệch giữa hai tỷ lệ lân cận được phân biệt bởi thừa số k:

$$\begin{aligned} D(x, y, \sigma) &= \big(G(x, y, k\sigma) - G(x, y, \sigma)\big) * I(x, y) \\ &= L(x, y, k\sigma) - L(x, y, \sigma) \end{aligned} \tag{2.3}$$



Hình 2.3 Xây dựng một thể hiện không gian tỷ lệ

Hình 2.3 thể hiện một phương pháp hiệu quả cho việc xây dựng hàm $D(x, y, \sigma)$. Ảnh ban đầu được cuộn theo kiểu gia tăng với các hàm Gaussian để tạo ra các ảnh được phân biệt bởi thừa số k trong không gian tỷ lệ, được xếp thành chồng ở cột bên trái. Ta chia mỗi quãng của không gian tỷ lệ (nghĩa là gấp đôi σ) thành s khoảng (s là số nguyên), vì vậy $k = 2^{1/s}$. Chúng ta phải tạo ra $s + 3$ ảnh trong chồng các ảnh bị làm mờ cho mỗi quãng, để việc phát hiện cực trị cuối cùng bao phủ trọn vẹn một quãng. Các tỷ lệ ảnh gần kề được trừ với nhau để tạo ra các ảnh *Difference-of-Gaussian* được thể hiện ở hình bên phải. Một khi một quãng trọn vẹn được xử lý, chúng ta tái lấy mẫu ảnh Gaussian gấp đôi giá trị ban đầu σ và việc xử lý được lặp lại.



Hình 2.4 Các giá trị cực đại và cực tiểu của các ảnh DoG được tìm thấy bằng việc so sánh một điểm ảnh (đánh dấu X) với 26 láng giềng trong các vùng 3×3 ở các mức hiện thời và các mức gần kề (được đánh dấu O).

Để tìm giá trị cực đại và cực tiểu địa phương của hàm $D(x, y, \sigma)$, mỗi điểm mẫu được so sánh với 8 láng giềng trong ảnh hiện thời và 9 láng giềng trong tỷ lệ ở trên và ở dưới (*Hình 2.4*). Nó được chọn chỉ khi lớn hơn tất cả các láng giềng này hoặc nhỏ hơn tất cả chúng. Chi phí của sự kiểm tra này là khá nhỏ vì trên thực tế hầu hết các điểm mẫu sẽ bị loại bỏ sau vài lần kiểm tra đầu tiên.

**** Tần số lấy mẫu theo tỷ lệ***:

Sự xác định thực nghiệm của tần số lấy mẫu làm tăng tối đa tính ổn định của các cực trị. Để xác định tần số lấy mẫu người ta sử dụng một bộ sưu tập gồm 32 ảnh thực gồm nhiều loại khác nhau, bao gồm các cảnh ngoài trời, các mặt người, các bức ảnh trên không và các ảnh kỹ nghệ. Sau đó mỗi ảnh phải chịu một dãy các phép biến đổi, bao gồm phép xoay, thay đổi tỷ lệ, thay đổi độ sáng và độ tương phản, và thêm tạp nhiễu ảnh. Bởi vì các thay đổi này là không tự nhiên, nên có thể dự đoán chính xác nơi mà mỗi đặc trưng trong ảnh gốc sẽ xuất hiện trong ảnh đã biến đổi, chú ý đến phép đo tính lặp lại và độ chính xác vị trí đối với mỗi đặc trưng. Kết quả là, khả năng lặp lại cao nhất được đạt đến khi lấy mẫu 3 tỷ lệ cho mỗi quãng.

Thực nghiệm cho thấy khả năng lặp lại của các điểm khóa không tăng khi nhiều tỷ lệ hơn được lấy mẫu. Lý do là vì có nhiều cực trị địa phương hơn được phát hiện, nhưng tính trung bình các cực trị này ít ổn định và vì vậy ít có khả năng được phát hiện trong ảnh đã bị biến đổi. Số lượng các điểm khóa tăng lên cùng với việc lấy mẫu tăng của các tỷ lệ và tổng số lượng các so khớp chính xác cũng tăng. Vì sự thành công của việc nhận dạng đối tượng thường phụ thuộc nhiều vào số lượng các điểm khóa được so khớp chính xác, chứ không phải tỷ lệ phần trăm so khớp chính xác của chúng, nên đối với nhiều

ứng dụng, sẽ tối ưu hơn khi sử dụng một lượng lớn các mẫu tỷ lệ. Tuy nhiên, chi phí tính toán cũng tăng cùng với số lượng này, vì vậy qua thực nghiệm chúng ta chỉ cần chọn 3 mẫu tỷ lệ trên mỗi quãng.

Tóm lại, các thí nghiệm cho thấy rằng hàm *Difference-of-Gaussian* của không gian tỷ lệ có một lượng lớn các cực trị và sẽ tốn nhiều chi phí để phát hiện tất cả chúng. May thay, chúng ta có thể phát hiện được một tập con ổn định và hữu ích nhất thậm chí khi việc lấy mẫu tỷ lệ trở nên không được tốt.

2.3.2 Định vị các điểm khóa

Một khi một điểm khóa ứng cử được tìm thấy bằng việc so sánh một điểm ảnh với các láng giềng của nó, thì bước tiếp theo là thực hiện điều chỉnh chi tiết với dữ liệu lân cận cho vị trí, tỷ lệ, và tỷ lệ của các độ cong chủ yếu. Thông tin này cho phép loại bỏ các điểm có độ tương phản thấp hoặc được định vị kém dọc biên.

Thực thi ban đầu của hướng tiếp cận này đã định vị một cách đơn giản các điểm khóa ở vị trí và tỷ lệ của điểm mẫu trung tâm. Tuy nhiên, gần đây người ta sử dụng một phương pháp khác đó là làm phù hợp một hàm bậc hai 3D cho các điểm mẫu địa phương để xác định vị trí nội suy của điểm cực đại, và các thử nghiệm đã cho thấy rằng phương pháp này mang lại sự cải tiến đáng kể cho việc so khớp và độ ổn định. Phương pháp này sử dụng phép khai triển Taylor (tối đa là dạng bậc hai) của hàm không gian tỷ lệ, $D(x, y, \sigma)$, được thay đổi để ảnh gốc ở vị trí điểm mẫu:

$$D(\mathrm{x}) = D + \frac{\partial D^T}{\partial \mathrm{x}}\mathrm{x} + \frac{1}{2}\mathrm{x}^T\frac{\partial^2 D}{\partial x^2}\mathrm{x} \qquad (2.4)$$

Trong đó, D và các đạo hàm của nó được định giá ở điểm mẫu đó và $\mathrm{x} = (x, y, \sigma)^T$ là *offset* từ điểm này. Vị trí của cực trị, $\hat{\mathrm{x}}$, được xác định bằng việc lấy đạo hàm theo x và thiết lập nó bằng 0, ta thu được:

$$\hat{\mathrm{x}} = -\frac{\partial^2 D^{-1}}{\partial \mathrm{x}^2}\frac{\partial D}{\partial \mathrm{x}} \qquad (2.5)$$

Theo đề xuất của Brown thì ma trận Hessian và đạo hàm của *D* được xấp xỉ bằng việc sử dụng các độ chênh lệch giữa các điểm mẫu lân cận. Nếu *offset* $\hat{\mathrm{x}}$ lớn hơn 0.5 ở bất kỳ chiều nào, thì có nghĩa là cực trị đó nằm gần với một điểm mẫu khác hơn. Trong trường hợp này, điểm mẫu được thay đổi và thực hiện phép nội suy thay cho điểm đó. *Offset* cuối cùng $\hat{\mathrm{x}}$ được cộng thêm về hướng vị trí điểm mẫu của nó để có được sự ước lượng nội suy cho vị trí của cực trị đó.

Giá trị hàm ở cực trị, $D(\hat{\mathrm{x}})$, có ích cho việc loại bỏ các cực trị không ổn định có độ tương phản thấp. Có thể đạt được điều này bằng việc thế phương trình (2.5) vào (2.4), ta được:

$$D(\hat{\mathrm{x}}) = D + \frac{1}{2}\frac{\partial D^T}{\partial \mathrm{x}}\hat{\mathrm{x}}$$

Thông qua các thí nghiệm người ta nhận thấy rằng, tất cả các cực trị có giá trị $|D(\hat{\mathrm{x}})|$ nhỏ hơn 0.03 đều được loại bỏ.

2.3.3 Gán hướng cho các điểm khóa

Bằng việc gán một hướng thích hợp cho mỗi điểm khóa dựa trên các đặc tính ảnh cục bộ, bộ mô tả điểm khóa được trình bày ở phần sau có liên quan tới hướng này và vì vậy đạt được sự bất biến đối với phép xoay ảnh.

Để gán một hướng cục bộ cho mỗi điểm khóa ta sử dụng hướng gradient của ảnh. Tỷ lệ của điểm khóa được dùng để lựa chọn ảnh được làm trơn Gaussian, *L*, với tỷ lệ gần nhất, để thực hiện tất cả các tính toán theo kiểu bất biến tỷ lệ. Đối với mỗi mẫu ảnh, $L(x, y)$, ở tỷ lệ này, cường độ gradient, $m(x, y)$, và hướng, $\theta(x, y)$, được tính toán trước sử dụng độ chênh lệch điểm ảnh:

$$m(x,y) = \sqrt{\big(L(x+1,y) - L(x-1,y)\big)^2 + \big(L(x,y+1) - L(x,y-1)\big)^2}$$

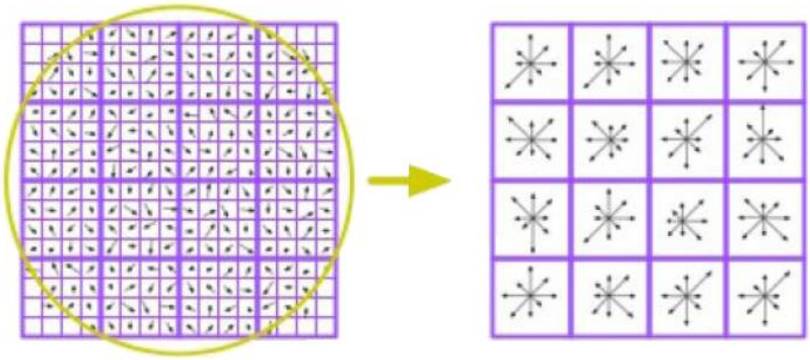
$$\theta(x,y) = \tan^{-1}\Big(\big(L(x,y+1) - L(x,y-1)\big)/\big(L(x+1,y) - L(x-1,y)\big)\Big)$$

Một biểu đồ hướng được thiết lập từ các hướng gradient của các điểm mẫu trong phạm vi một vùng lân cận xung quanh điểm khóa. Biểu đồ hướng có 36 bin bao phủ 360 độ của tất cả các hướng. Mỗi mẫu được thêm vào biểu đồ được gán trọng số bởi độ lớn gradient của nó và bởi một cửa sổ hình tròn Gaussian với σ gấp 1.5 lần tỷ lệ của điểm khóa đó.

Các đỉnh trong biểu đồ hướng tương ứng với các hướng bao quát các gradient cục bộ. Dựa vào biểu đồ hướng ta có thể xác định được đỉnh cao nhất trong biểu đồ và khi đó bất kỳ đỉnh cục bộ nào khác nằm trong phạm vi 80% so với đỉnh cao nhất đều được dùng để tạo ra một điểm khóa với cùng hướng đó. Vì vậy, đối với các vị trí có nhiều đỉnh có cường độ tương tự nhau, thì sẽ có nhiều điểm khóa được tạo ra ở cùng vị trí và tỷ lệ đó nhưng các hướng thì khác nhau. Chỉ có khoảng 15% điểm được gán nhiều hướng, nhưng những điểm này góp phần đáng kể cho tính ổn định của việc so khớp. Cuối cùng, một đường parabol được làm phù hợp với 3 giá trị của biểu đồ gần với mỗi đỉnh nhất để nội suy vị trí của đỉnh đó để mang lại độ chính xác tốt hơn.

2.3.4 Xây dựng bộ mô tả cục bộ

Các thao tác ở trên đã gán vị trí, tỷ lệ và hướng cho mối điểm khóa. Các tham số này áp đặt cho hệ tọa độ 2D cục bộ để mô tả một vùng ảnh cục bộ. Bước tiếp theo là tính toán một bộ mô tả cho vùng ảnh cục bộ đó để có thể bất biến đối với các thay đổi còn lại như thay đổi độ sáng hoặc điểm nhìn 3D.



Gradients ảnh Bộ mô tả điểm khóa

Hình 2.5 Bộ mô tả điểm khóa

Hình 2.5 minh họa cho việc tính toán bộ mô tả điểm khóa được tạo ra bằng cách: đầu tiên tính toán độ lớn và hướng gradient ở mỗi điểm mẫu trong một vùng xung quanh vị trí điểm khóa, như hình bên trái. Các hướng này được gán trọng số bởi một cửa sổ Gaussian, được biểu thị bởi đường tròn phủ ngoài. Sau đó các mẫu này được gom lại thành các biểu đồ hướng tóm tắt nội dung trên 4 x 4 vùng con, được thể hiện ở hình phải, với chiều dài mỗi mũi tên tương đương với tổng các cường độ gradient gần với hướng đó trong phạm vi của vùng đó. Các bộ mô tả điểm khóa là các đạo hàm Gaussian được tính trong một vùng lân cận cục bộ xung quanh các điểm khóa. Để đạt đến sự bất biến về hướng, thì các tọa độ của bộ mô tả và các hướng gradient bị quay có liên quan tới hướng của điểm khóa. Sự bất biến đối với các biến đổi về cường độ affine được đạt đến bằng việc chia các đạo hàm bậc cao hơn thành các đạo hàm bậc nhất. Để thuận tiện trong việc tính toán bộ mô tả, các gradient phải được tính trước cho tất cả các mức của hình chóp. Các gradient này được minh họa bởi các mũi tên nhỏ ở mỗi vị trí mẫu ở hình bên trái của *hình 2.5*.

Hàm gán trọng số Gaussian với σ bằng một nửa chiều rộng của cửa sổ bộ mô tả được dùng để gán một trọng số cho cường độ của mỗi điểm mẫu. Điều này được minh họa bằng một cửa sổ hình tròn thể hiện ở hình bên trái

của *hình 2.5*. Mục đích của cửa sổ Gaussian này là tránh các thay đổi đột ngột trong bộ mô tả khi có các thay đổi nhỏ ở vị trí của cửa sổ và ít quan tâm đến các gradient ở xa vị trí trung tâm của bộ mô tả.

Hình bên phải của *hình 2.5* thể hiện bộ mô tả điểm khóa. Nó chú ý đến sự thay đổi đáng kể ở các vị trí gradient bằng việc tạo ra các biểu đồ hướng trên 4×4 vùng mẫu. Hình này thể hiện 8 hướng cho mỗi biểu đồ, với chiều dài của mỗi mũi tên tương ứng với độ lớn của mỗi mục (*entry*) của biểu đồ.

Bộ mô tả được tạo nên từ một vectơ chứa các giá trị của tất cả các *entry* của biểu đồ hướng, tương ứng với các chiều dài của các mũi tên ở hình bên phải của *hình 2.5*. Hình này thể hiện một mảng 4×4 các biểu đồ với 8 bin hướng. Do đó, một vectơ đặc trưng có 4×4×8 =128 phần tử để mô tả cho mỗi điểm khóa.

Như vậy, chúng ta thu được các bộ mô tả với số chiều hữu hạn biểu diễn các đặc trưng được trích chọn từ các điểm bất biến.

**** Loại bỏ các đáp ứng biên:***

Đối với tính ổn định, không đủ để loại bỏ các điểm khóa có độ tương phản thấp. Dù vị trí dọc theo biên được xác định tồi nhưng hàm *Difference-of-Gaussian* vẫn có một đáp ứng mạnh dọc theo các biên và vì vậy không ổn định khi có các lượng nhỏ tạp nhiễu.

Đỉnh được xác định tồi trong hàm *Difference-of-Gaussian* sẽ có một độ cong lớn chủ yếu ngang qua biên ngoại trừ độ cong nhỏ ở hướng trực giao. Các độ cong chủ yếu có thể được tính từ ma trận Hessian 2×2, H, được tính ở vị trí và tỷ lệ của điểm khóa:

$$\mathrm{H} = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \qquad (2.6)$$

Các đạo hàm được ước lượng bằng việc lấy các độ chênh lệch giữa các điểm mẫu láng giềng.

Các giá trị riêng của ma trận H tương ứng với các độ cong chủ yếu của *D*. Lấy α là giá trị riêng với cường độ lớn nhất và β là giá trị riêng với cường độ nhỏ hơn. Khi đó, ta có thể tính tổng các giá trị riêng từ dấu vết của H và tích của chúng được tính từ giá trị của định thức:

$$\mathrm{Tr(H)} = D_{xx} + D_{yy} = \alpha + \beta$$

$$\mathrm{Det(H)} = D_{xx}D_{yy} - \left(D_{xy}\right)^2 = \alpha\beta$$

Trong trường hợp không chắc xảy ra đó là định thức có giá trị âm, các độ cong có các dấu hiệu khác nhau vì vậy điểm bị loại bỏ không phải là một cực trị. Lấy r là tỷ lệ giữa giá trị riêng có cường độ lớn nhất và giá trị riêng có cường độ nhỏ hơn, để $\alpha = r\beta$. Khi đó,

$$\frac{\mathrm{Tr(H)}^2}{\mathrm{Det(H)}} = \frac{(\alpha+\beta)^2}{\alpha\beta} = \frac{(r\beta+\beta)^2}{r\beta^2} = \frac{(r+1)^2}{r}$$

Biểu thức $(r + 1)^2/r$ nhận giá trị cực tiểu khi hai giá trị riêng bằng nhau và nó tăng cùng với r. Vì vậy, để kiểm tra xem tỷ lệ của các độ cong chủ yếu có ở dưới một ngưỡng r nào đó không, ta chỉ cần kiểm tra:

$$\frac{\mathrm{Tr(H)}^2}{\mathrm{Det(H)}} < \frac{(r+1)^2}{r}$$

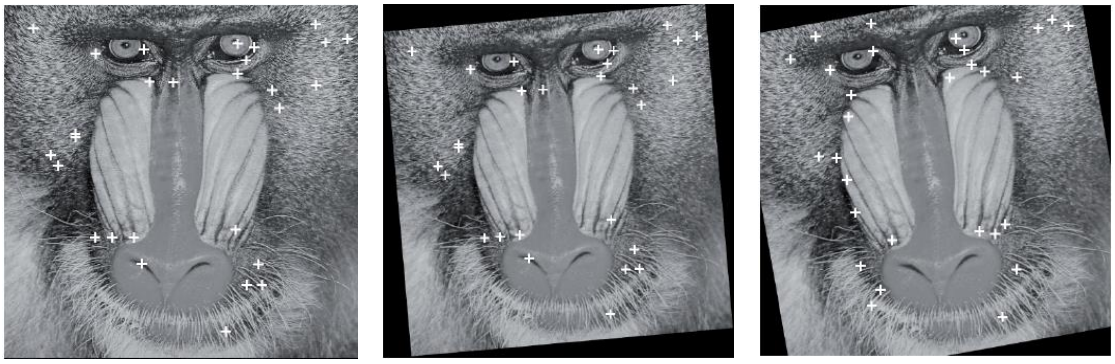
Các thí nghiệm cho thấy sử dụng giá trị $r = 10$, sẽ loại bỏ được các điểm khóa có tỷ lệ giữa các độ cong chủ yếu lớn hơn 10.

Các mô tả đặc trưng SIFT bao gồm vị trí điểm khóa, tỷ lệ và hướng. Các thuộc tính này được lưu cho so khớp điểm khóa và phục hồi hình ảnh trong lược đồ thủy vân.

Tuy nhiên, các đặc trưng từ các mô tả SIFT không hợp trực tiếp với thủy vân, mà dựa theo số lượng và sự phân bố của các đặc trưng tùy thuộc vào nội dung và kết cấu ảnh [9]. Hơn nữa, phục hồi ảnh cần thêm sự so khớp các đặc trưng ổn định trong lược đồ thủy vân. Vì vậy, cần điều chỉnh số lượng các đặc trưng, loại bỏ những đặc trưng hình ảnh dễ bị tấn công. Thông thường, sử dụng đơn vị đo khoảng cách Euclide để so khớp một điểm đặc trưng giữa ảnh gốc với ảnh bị biến dạng. Giả sử các đặc trưng được mô tả thành các vectơ trong không gian Euclide R^n thì khoảng cách giữa hai đặc trưng P = (p_1, p_2,..,p_n) và Q = (q_1, q_2,..,q_n) được định nghĩa như sau:

$$\sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots + (p_n - q_n)^2} = \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2}$$

Nếu tỷ lệ của khoảng cách gần nhất và gần thứ hai là ít hơn một ngưỡng, thì sự so khớp là thành công. Giảm ngưỡng này, ta thu được số lượng ít hơn và nhiều điểm đặc trưng ổn định hơn, nó tốt hơn cho khôi phục ảnh của lược đồ. Sau việc này, ta có được tập các điểm được so khớp *Ω1*. Tuy nhiên vẫn còn vài điểm không được so khớp còn tồn tại, trong phần "Khôi phục ảnh" sẽ giới thiệu cách để loại bỏ các điểm này.



***(a)** ảnh baboon* ***(b)** xoay 5^0* ***(c)** xoay 10^0 và cắt xén*

Hình 2.6 Các điểm đặc trưng được so khớp dùng biến đổi SIFT

Hình 2.6 cho thấy các điểm được so khớp giữa ảnh gốc và ảnh xoay, xoay-cắt xén, ta có thể thấy rằng các điểm khóa SIFT là được so khớp chính xác.

2.4 Khôi phục ảnh

Trước khi thực hiện bước phát hiện thủy vân, các mô tả SIFT được sử dụng để khôi phục lại hình ảnh gần đúng của hình ảnh ban đầu. Một biến đổi tuyến tính bao gồm xoay, mở rộng, dịch, v.v… có thể được viết bằng cách sử dụng phối hợp đồng nhất [13] như:

$$\begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = A \begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} \qquad (2.7)$$

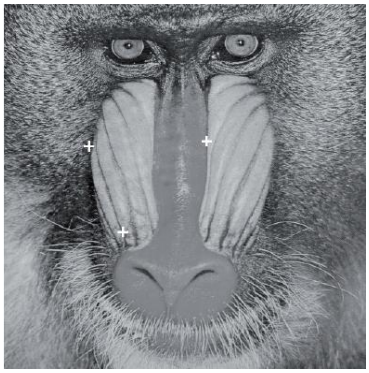
Để thực hiện ma trận *A*, ta chọn ba cặp điểm so khớp giữa ảnh được thủy vân và ảnh bị biến dạng. Để giảm tác động của các điểm không so khớp trên phục hồi ảnh, trước hết chúng ta loại bỏ những điểm đó bằng cách so sánh các giá trị của ma trận *A* mà nó thu được từ mỗi ba cặp điểm so khớp trong tập $\Omega 1$.

Bởi vì hầu hết các điểm được so khớp trong tập $\Omega 1$ là chính xác, chúng ta có thể tìm thấy những điểm không được so khớp và loại bỏ chúng để thu được tập $\Omega 2$ (là tập mà tất cả các điểm so khớp đều chính xác).

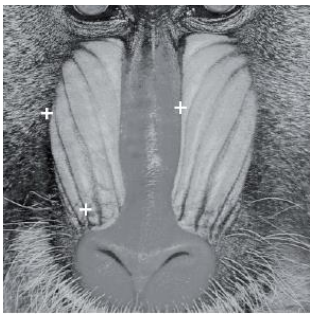
***a (1)** ảnh pepper*

***a (2)** xoay 90^0*

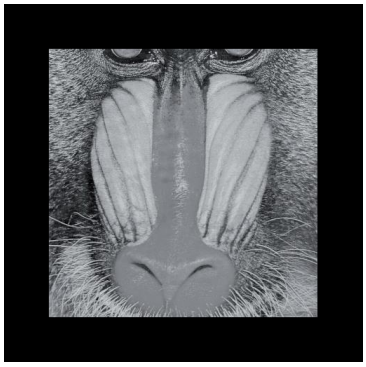
***a (3)** ảnh được khôi phục*



***b (1)** ảnh baboon*



***b (2)** cắt xén 5%*



***b (3)** ảnh được khôi phục*

Hình 2.7 Khôi phục ảnh dưới các tấn công hình học khác nhau.

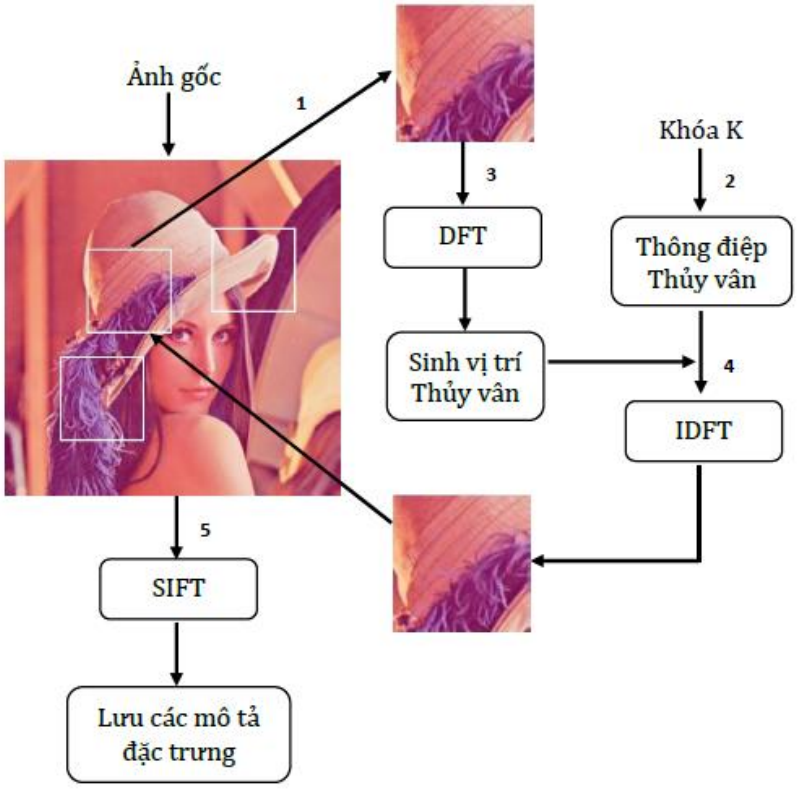
Hình 2.7 cho thấy việc thực hiện khôi phục lại ảnh dưới các biến dạng hình học khác nhau bằng cách sử dụng phương pháp này. *Hình 2.7* ***a (1)***, và ***b (1)*** là ảnh gốc và các điểm đặc trưng được lựa chọn để phục hồi ảnh. *Hình 2.7* ***a (2)***, ***b (2)*** đã được xoay (90 độ), cắt xén (5%), tương ứng. *Hình 2.7* ***a (3)***, ***b (3)*** hiển thị ảnh được khôi phục. Quá trình khôi phục ảnh được tự động mà không cần can thiệp thủ công.

2.5 Lược đồ thủy vân sử dụng kết hợp DFT và SIFT

Lược đồ thủy vân đề xuất được thiết kế để bảo vệ bản quyền cho các bức ảnh màu kỹ thuật số. Mỗi ảnh con được xem như kênh truyền thông độc lập. Để cải thiện sự bền vững của thủy vân, tất cả ảnh con mang cùng một bản sao của thủy vân. Nhúng và phát hiện thủy vân đều được áp dụng trong miền biến đổi DFT trên ảnh con.

2.5.1 Lược đồ nhúng thủy vân

Trong lược đồ nhúng thủy vân đề xuất, thủy vân được nhúng vào nhiều hơn một ảnh con ở vùng giữa của ảnh gốc. Các thủ tục nhúng thủy vân được hiển thị trong *hình 2.8* và được trình bày chi tiết từng bước như sau:



Hình 2.8 Lược đồ nhúng thủy vân

Bước 1:

Trước tiên, chúng ta chọn hai hoặc ba ảnh con *Img* xung quanh vùng trung tâm của ảnh gốc và kích thước của ảnh con được xác định bởi chiều dài của chuỗi thủy vân.

Thường kích thước của ảnh con được chọn là 128 × 128 trong khi kích thước ảnh gốc là 512 × 512, và độ dài của chuỗi thủy vân có thể nhiều hơn một trăm bit.

Bước 2:

Tạo một chuỗi ngẫu nhiên $W = \{ w_i \mid i = 1, 2, 3, ..., N \}$, như là thủy vân số, được tạo ra bởi một khóa bí mật K, w_i thuộc về tập $\{0, 1\}$, và N là độ dài của chuỗi thủy vân. Sau đó, dùng mã sửa lỗi Hamming (7, 4) để tạo ra một chuỗi bit thủy vân sửa lỗi W', có chiều dài sẽ dài hơn 7/4 lần so với chuỗi ban đầu.

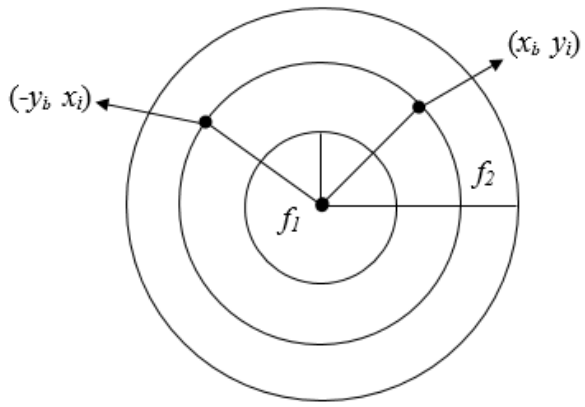
**** Mã sửa lỗi:***

Mã sửa lỗi Hamming (7, 4) được sử dụng trong lược đồ là một cơ chế phát hiện lỗi để sửa lỗi bit đơn nhằm giảm bớt sự sai lệch bit thủy vân trong những biến đổi làm biến dạng hình học có chủ ý hay vô ý.

Ví dụ, với chuỗi thủy vân 8-bit được chia thành hai chuỗi con 4-bit. Mã Hamming thực hiện lần lượt thêm vào mỗi chuỗi con 3 bit kiểm tra lỗi (7, 4) để tạo ra mã sửa lỗi bit đơn của chính nó. Khi truyền dữ liệu 4-bit luôn mang lại nhiều rủi ro sai lệch hơn so với truyền 7 bit mã sửa lỗi, khả năng sửa lỗi đảm bảo chất lượng tín hiệu tốt hơn ở người nhận và một tỷ lệ thu hồi cao hơn trong việc phát hiện thủy vân. Do đó, nó làm tăng khả năng toàn vẹn của chuỗi bit thủy vân trích xuất được.

Bước 3:

Với mỗi ảnh con *Img* thu được trong *bước 1*: Trước hết, cần áp dụng DFT để có được ảnh *FImg* và quang phổ biên độ F_k, sau đó sử dụng hàm băm một chiều [9] để sinh ra các vị trí nhúng an toàn trong các tần số giữa ($f_1 \leq f \leq f_2$) mà ở góc phần tư đầu tiên của *FImg*. Ở đây, ta chọn $f_1 = 5\% \times S$ (S là kích thước của *FImg*), $f_2 = 15\% \times S$. Tiếp theo, cần chọn một vị trí nhúng (x_i, y_i) và một vị trí khác $(-y_i, x_i)$ đó là góc 90° cách từ điểm (x_i, y_i) để nhúng 1 bit thủy vân. Cả hai đều ở nửa trên mặt phẳng DFT.



Hình 2.9 Cặp điểm (x_i, y_i) và $(-y_i, x_i)$ trên mặt phẳng DFT

Một bit thủy vân được nhúng vào như sau:

a) Tính toán sự chênh lệch biên độ ΔT giữa (x_i, y_i) và $(-y_i, x_i)$, sử dụng công thức:

$$\Delta T = F_k(x_i, y_i) - F_k(-y_i, x_i).$$

b) Sửa đổi phổ biên độ của vị trí, quy tắc là khi bit thủy vân là 0, tạo sự chênh lệch ΔT sao cho $\Delta T \leq -T$; khi bit thủy vân được nhúng là 1, tạo sự chênh lệch ΔT sao cho $\Delta T \geq T$, trong đó T là một giá trị ngưỡng. Trong lược đồ này, giá trị của T được xác định bằng phổ biên độ của vị trí nhúng, $T = 0.4 \times G \times (F_k(x_i, y_i) + F_k(-y_i, x_i))$, trong đó G là hệ số cường độ nhúng. Để giữ sự cân bằng của thủy vân ẩn bền vững, G có một khoảng giá trị là (0.25, 0.35). Thuật toán cụ thể như sau:

If the watermark bit w_i is 0 then
  If $\Delta T > -T$ then
  $F_k'(x_i, y_i) = F_k(x_i, y_i) - (T - \Delta T)/2$
  $F_k'(-y_i, x_i) = F_k(-y_i, x_i) + (T - \Delta T)/2$
  End
Else
  If $\Delta T < T$ then
  $F_k'(x_i, y_i) = F_k(x_i, y_i) + (T - \Delta T)/2$
  $F_k'(-y_i, x_i) = F_k(-y_i, x_i) - (T - \Delta T)/2$
  End
End

Trong đó $F_k(x_i, y_i)$, $F_k(-y_i, x_i)$ là độ lớn ban đầu. $F'_k(x_i, y_i)$, $F'_k(-y_i, x_i)$ là độ lớn mới tại (x_i, y_i), $(-y_i, x_i)$. Ngoài ra, các điểm đối xứng ở nửa dưới mặt phẳng DFT cũng phải được thay đổi với cùng giá trị chính xác.

**** Sinh vị trí nhúng thủy vân:***

Một biến thể của hàm băm một chiều được sử dụng trong lược đồ để tạo ra các vị trí nhúng an toàn trong tần số giữa miền DFT. Sáu bước để tạo ra các vị trí này như sau:

1. Lưu tất cả các vị trí tần số giữa vào vector *V*.

2. Chọn ngẫu nhiên hai số nguyên tố lớn *p* và *q*, và tính toán khóa bí mật $n = p \times q$.

3. Thu được *Y* bằng cách sử dụng thủ tục mã hóa:

$$X = m^K \bmod n \; ; \quad Y = X^2 \bmod n;$$

trong đó, *m* là số serial đăng ký của ảnh gốc và *K* là khóa bí mật thứ hai.

4. Tính toán một chỉ mục *l* bởi:

$$Y = Y^2 \bmod n; \; l = (Y \bmod n) \bmod length(V);$$

5. Chọn mục thứ *l* trong *V* là vị trí nhúng và loại bỏ nó từ *V* nên không có bản sao các vị trí nào trùng nhau.

6. Lặp lại các bước 4 đến 5 cho đến khi tổng số các vị trí nhúng là đạt.

Những vị trí nhúng an toàn cao có thể dễ dàng được thực hiện lại bởi cùng khóa bí mật *n* và *K*. Trong khi đó, việc sinh các vị trí nhúng này là không khả thi nếu không biết *n* và *K*. Để đảm bảo những kẻ tấn công không thể tìm ra các vị trí nhúng thủy vân bằng cách so sánh một vài bản sao thủy vân, các khóa bí mật khác nhau được sử dụng để sinh ra các vị trí nhúng cho mỗi ảnh con.

Bước 4:

Áp dụng IDFT (DFT ngược) *FImg* để có được những ảnh con thủy vân *Img* và thay thế ảnh con gốc *Img*.

Bước 5:

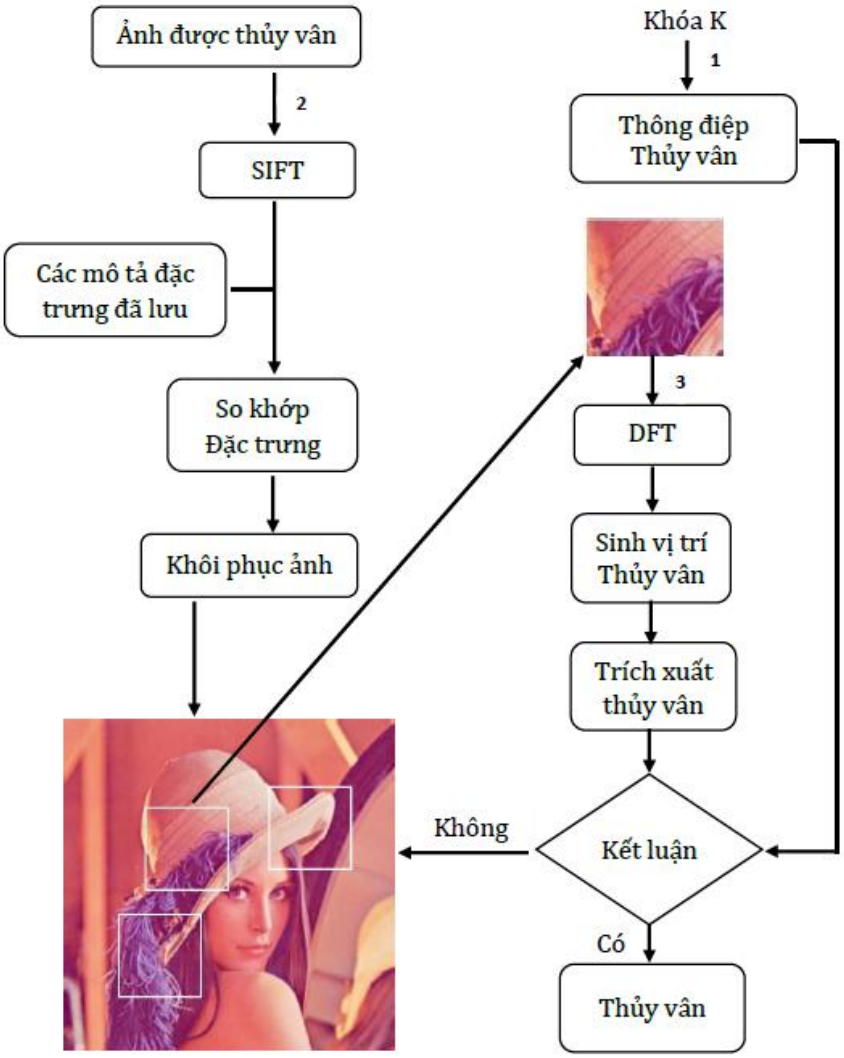
Sau khi tất cả các bit thủy vân được nhúng, chúng ta áp dụng SIFT để tìm những điểm đặc trưng quan trọng trong ảnh được thủy vân và lưu những

điểm đặc trưng này để phục hồi hình ảnh. Để giảm thiểu lỗi của so khớp đặc trưng, ta chọn các điểm đặc trưng giữa ảnh được thủy vân và ảnh bị biến dạng. Thêm nữa, hai tỷ lệ tần số giữa f_1 và f_2, khóa bí mật n, K sinh vị trí nhúng thủy vân cũng sẽ được lưu. Mặc dù có một số điểm đặc trưng quan trọng và các thông số khóa khác được lưu, nhưng dung lượng là rất nhỏ so với dung lượng lưu ảnh ban đầu.

2.5.2 Lược đồ phát hiện thủy vân

Trong lược đồ phát hiện thủy vân, nếu thủy vân được phát hiện trong một ảnh con *Img*, thì ta có thể khẳng định thủy vân là có tồn tại trong ảnh. Bộ phát hiện thủy vân không cần ảnh gốc, mà chỉ cần các thông tin đó được lưu trong quá trình nhúng thủy vân.

Lược đồ phát hiện thủy vân được hiển thị trong *hình 2.10* và các bước thực hiện như sau:



Hình 2.10 Lược đồ phát hiện thủy vân

Bước 1:

Chuỗi thủy vân ban đầu $W = \{ w_i \mid i = 1, 2, 3, ..., N \}$ được sinh ra tùy thuộc vào khóa K bí mật đã được lưu.

Bước 2:

Áp dụng SIFT để thu được các điểm đặc trưng quan trọng của ảnh bị biến dạng và thu được các điểm so khớp giữa ảnh bị biến dạng và ảnh được thủy vân. Sau đó chúng ta khôi phục lại ảnh gần đúng với ảnh gốc bằng cách sử dụng phương pháp khôi phục ảnh.

Bước 3:

Áp dụng phép biến đổi DFT cho mỗi ảnh con và chúng ta có thể thu được phổ DFT *FImg*, phổ biên độ F'_k. Giống như thủ tục nhúng thủy vân, các hệ số DFT giữa ($f_1 \leq f \leq f_2$) được lựa chọn ở góc phần tư đầu tiên. Các vị trí nhúng thu được bằng cách sử dụng các hàm băm một chiều [9]. Với mỗi cặp vị trí được lựa chọn (x_i, y_i) và ($-y_i$, x_i) chúng ta có thể trích xuất một bit của chuỗi thủy vân sửa lỗi, được xác định bởi:

$$w'_i = \begin{cases} 1 & F'_k(x_i, y_i) \geq F'_k(-y_i, x_i) \\ 0 & F'_k(x_i, y_i) < F'_k(-y_i, x_i) \end{cases}$$

Trong đó, $F'_k(x_i, y_i)$, $F'_k(-y_i, x_i)$ là độ lớn của các hệ số tại các vị trí (x_i, y_i) và ($-y_i$, x_i). Chúng ta có thể thu được tất cả từng bit một của chuỗi thủy vân sửa lỗi.

Thủy vân lấy được sẽ được so sánh với chuỗi thủy vân sửa lỗi để xác định sự hiện diện của thủy vân. Đó là, số các bit được so khớp giữa chúng được so sánh với một ngưỡng xác định trước để xác định xem thủy vân có mặt trong hình ảnh. Ngưỡng được tính toán dựa trên khả năng cảnh báo sai mà có thể xảy ra trong việc phát hiện thủy vân. Với ảnh không được thủy vân, các bit thủy vân trích xuất được giả định là các biến ngẫu nhiên độc lập (Bernoulli trails). Đơn giản, chúng ta giả định xác suất thành công mà các so khớp bit thủy vân được trích xuất với bit thủy vân gốc là 1/2. Xác suất của *r*-bit thủy vân được trích xuất so khớp với *n*-bit thủy vân gốc được tính như sau:

$$P_r = \left(\frac{1}{2}\right)^n \left(\frac{n!}{r!\,(n-r)!}\right) \tag{2.8}$$

Xác suất cảnh báo sai $P_{falsealarm}$ được tính như sau:

$$P_{falsealarm} = \sum_{r=Th}^{n} \left(\frac{1}{2}\right)^n \left(\frac{(n - \lfloor 0.5n \rfloor)!}{(r - \lfloor 0.5n \rfloor)!\,(n-r)!}\right) \tag{2.9}$$

Trong đó, n là độ dài của chuỗi thủy vân.

r, Th là số các bit được so khớp và giá trị ngưỡng.

Từ công thức này, chúng ta có được ngưỡng xác suất cảnh báo sai là 10^{-5}, trong đó $Th = 0.75n$ và $n \geq 64$. Đó là, nếu độ dài của chuỗi thủy vân n là hơn 64 bit và số các bit được so khớp r là lớn hơn $0.75n$, ta có thể khẳng định sự hiện diện của thủy vân từ 10^{-5} là một xác suất báo sai thấp.

Trong thủ tục phát hiện, nếu một bản sao của thủy vân được phát hiện một cách chính xác trong một ảnh con được nhúng, thì có thể khẳng định sự hiện diện của thủy vân trong ảnh.

CHƯƠNG III
XÂY DỰNG CHƯƠNG TRÌNH THỬ NGHIỆM

3.1 Giới thiệu

Thủy vân là một phương pháp hữu hiệu để bảo vệ bản quyền tác giả cho ảnh kỹ thuât số. Và cũng có một số phép tấn công phổ biến nhằm loại bỏ dấu thủy vân đối với ảnh số là: nén JPEG, thêm nhiễu, lọc, xoay, cắt xén, làm mờ, thay đổi kích thước, thay đổi sáng tối, thay đổi tương phản. Trong số những cuộc tấn công đó, biến dạng hình học đã được coi là một trong những cuộc tấn công khó khăn nhất để chống lại, do các lỗi đồng bộ hóa biến dạng hình học tạo ra.

Để có khả năng chịu được các cuộc tấn công biến dạng hình học, các điểm đặc trưng so khớp được xác định bằng cách sử dụng phép biến đổi đặc trưng bất biến tỷ lệ (SIFT) để khôi phục lại ảnh nhằm giảm lỗi đồng bộ gây ra bởi các cuộc tấn công biến dạng hình học. Một lược đồ nhúng và phát hiện thủy vân tương ứng được áp dụng trong miền biến đổi Fourier rời rạc (DFT) cho mỗi ảnh con.

Kết quả có phát hiện được thủy vân hay không là dựa trên số lượng các bit được so khớp giữa thủy vân được truy xuất và thủy vân gốc trong các ảnh con này.

3.2 Thiết kế chương trình

Chương trình được mô phỏng trên Matlab 2013 với máy tính dùng bộ vi xử lý Core I3, Ram 4GB.

Giao diện của chương trình thử nghiệm được thiết kế theo các lược đồ đã trình bày trong Chương II. Sau khi cài đặt và chạy chương trình, giao diện tương ứng với mỗi quy trình như sau:

Giao diện chính của chương trình:

Gồm có 3 nút lệnh:

1. Nhúng thủy vân
2. Một số kiểu tấn công
3. Phát hiện thủy vân

Hình 3.1 Giao diện chính của chương trình

3.3 Thử nghiệm chương trình

Thử nghiệm được tiến hành trên mẫu ảnh màu Bitmap: *Zelda.bmp* có kích thước 512 × 512. Trong các mô hình thử nghiệm được thực hiện với một vài thông số cố định như: Chiều dài của chuỗi giả ngẫu nhiên là 128 bit. Khu vực nhúng trong miền DFT là một vòng với bán kính bên trong và bên ngoài là 5% và 15% kích thước của ảnh con.

Chương trình sử dụng hệ số PSNR (Peak Signal to Noise Ratio – tỷ lệ tín hiệu cực đại trên nhiễu) để đánh giá tính ẩn của thủy vân. Giá trị PSNR được tính theo công thức sau:

$$PSNR = 10\log(M255^2) / \sum_{i=1}^{M}(x_i^2 - p_i^2)$$

Trong đó, *M* là kích thước của vùng nhúng hình ảnh, và *x, p* là các mức xám của ảnh gốc và ảnh được thủy vân. Các giá trị tổng thể PSNR giữa ảnh gốc và ảnh được thủy vân là lớn hơn 40 dB. Giá trị PSNR càng lớn thể hiện sự sai khác giữa ảnh gốc và ảnh sau khi nhúng thông tin càng thấp.

Độ bền vững của thuỷ vân được tính toán dựa trên sự so sánh chuỗi thủy vân nhận được với chuỗi thủy vân sửa lỗi để xác định sự hiện diện của thủy vân. Đó là, số các bit được so khớp giữa chúng được so sánh với một ngưỡng xác định trước để xác định xem thủy vân có mặt trong hình ảnh hay không. Ngưỡng được tính toán dựa trên khả năng cảnh báo sai theo công thức (2.8) và (2.9).

Thực hiện nhúng thủy vân:

Chọn nút lệnh "1. NHUNG THUY VAN" từ chương trình chính, chương trình sẽ thực hiện các bước như sau:

Bước 1: Trích xuất 2 ảnh con từ ảnh gốc

Hình 3.2 Trích xuất 2 ảnh con từ ảnh gốc

Bước 2: Một chuỗi giả ngẫu nhiên có chiều dài 128 bit được tạo ra bởi một khóa bí mật *K* để làm chuỗi thủy vân *W*.

Bước 3: Với mỗi ảnh con thu được trong *bước 1*, áp dụng DFT để nhúng chuỗi bit thủy vân. Nếu nhúng trực tiếp chuỗi 128 bit thủy vân *W* này

thì có thể qua một vài phép biến đổi làm cho chuỗi không được toàn vẹn dẫn đến không so khớp được thủy vân hoặc tỷ lệ so khớp thấp, để khắc phục cần dùng mã sửa lỗi Hamming (7,4) để tạo ra chuỗi thủy vân sửa lỗi *W'* có độ dài 224 bit và sẽ nhúng chuỗi này vào trong các ảnh con.

Bước 4: Áp dụng IDFT (DFT ngược) để có được những ảnh con đã thủy vân và thay thế vào vị trí cũ của ảnh con trong ảnh gốc.

Mô hình thực nghiệm tấn công và phát hiện thủy vân:

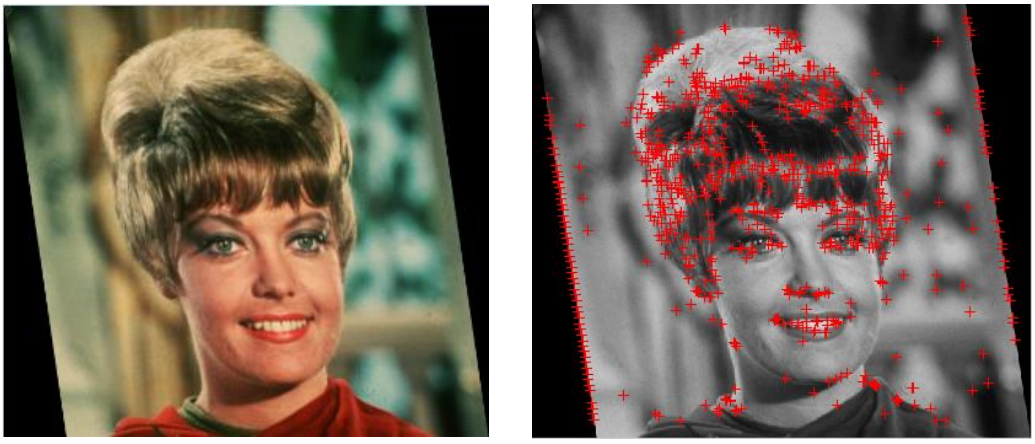
➢ ***Thực nghiệm 1*:** Thực hiện phép biến đổi Affine

Chọn nút lệnh "2. MOT SO KIEU TAN CONG" từ chương trình chính, xuất hiện giao diện của chương trình thực nghiệm tấn công như sau:

Hình 3.3 Giao diện chương trình demo thực nghiệm tấn công

Bước 1: Chọn nút lệnh "1. BIEN DOI AFFINE 15%", chương trình sẽ nạp ảnh đã thủy vân và thực hiện phép biến đổi affine với tỷ lệ là 15% kích thước của ảnh, và lưu ảnh bị biến đổi với một tên khác. Sau đó, áp dụng phép biến đổi SIFT để tìm những điểm đặc trưng quan trọng trong ảnh đã thủy vân và ảnh bị biến đổi. Tiếp đến thực hiện so khớp các điểm đặc trưng thu được của ảnh đã thủy vân và ảnh bị biến đổi để khôi phục lại ảnh.

Hình 3.4 Ảnh đã thủy vân với các điểm đặc trưng quan trọng



Hình 3.5 Ảnh biến đổi Affine với các điểm đặc trưng quan trọng

Hình 3.6 So khớp điểm đặc trưng giữa ảnh thủy vân và ảnh biến dạng

Hình 3.7 Ảnh được khôi phục

Bước 2: Chọn nút lệnh "3. PHAT HIEN THUY VAN" từ chương trình chính, chương trình sẽ thực hiện:

Trích xuất 2 ảnh con từ ảnh được phục hồi và thực hiện phép biến đổi DFT với mỗi ảnh con để thu được một chuỗi thủy vân *W''* có độ dài 224 bit và được so sánh với chuỗi thủy vân sửa lỗi ban đầu *W'* để xác định sự hiện diện của thủy vân.

Hình 3.8 Trích xuất 2 ảnh con từ ảnh đã khôi phục

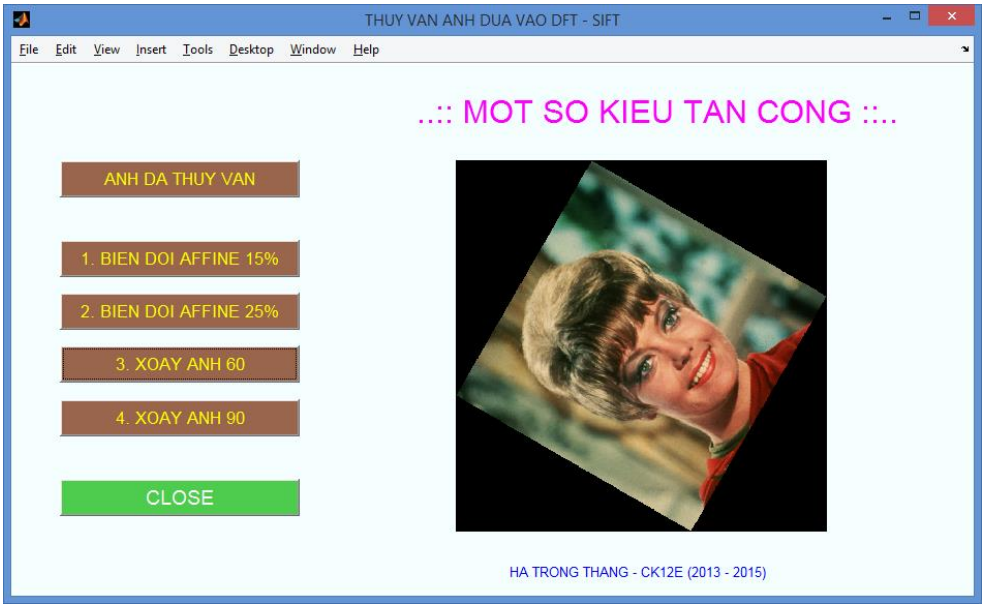
Kết quả thực nghiệm:

Ảnh trích xuất	Tỷ lệ r/n	Xác suất cảnh báo sai
Ảnh con 1	0.820	0.000061
Ảnh con 2	0.844	0.000059

Bảng 3.1 Kết quả so khớp thủy vân trích xuất và thủy vân gốc

Với bảng kết quả ở trên, ta thấy tỷ lệ so khớp của chuỗi thủy vân trích xuất được và thủy vân gốc là đạt so với các giá trị ngưỡng. Tỷ lệ so khớp *r/n* với số bit được so khớp *r* là lớn hơn 0.75*n* (*n* = 128), ta biết rằng theo cách so sánh này, tỷ số *r/n* có thể nhận các giá trị giữa 0 và 1. Khi tỷ số này càng gần 0 thì coi như hai chuỗi thủy vân không hề có quan hệ với nhau. Nếu số bit được so khớp có giá trị từ 0.75 trở lên thì có thể coi *W''* và *W'* là tương tự nhau. Xác suất cảnh báo sai thấp hơn giá trị ngưỡng 10^{-5}. Như vậy, với kết quả trên có thể khẳng định sự tồn tại của thủy vân trong ảnh.

- ***Thực nghiệm 2*:** Thực hiện phép tấn công xoay ảnh 60^0

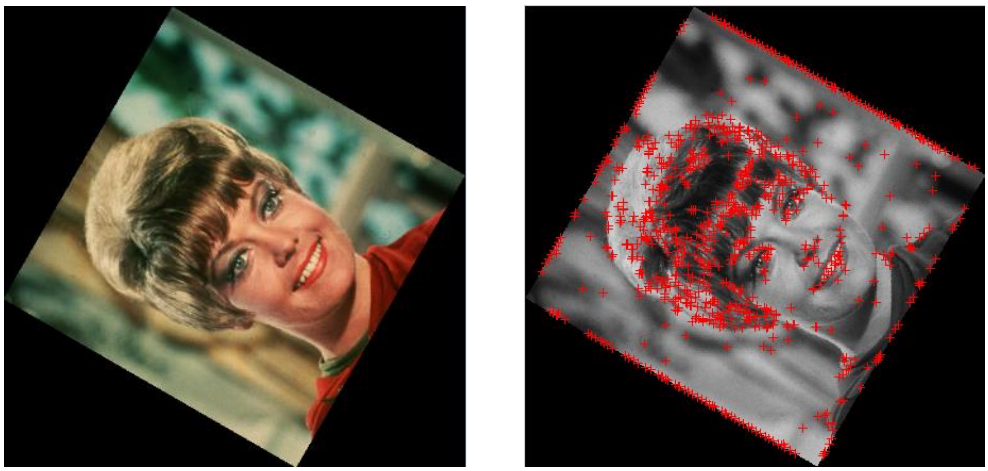


Hình 3.9 Giao diện chương trình demo thực nghiệm tấn công

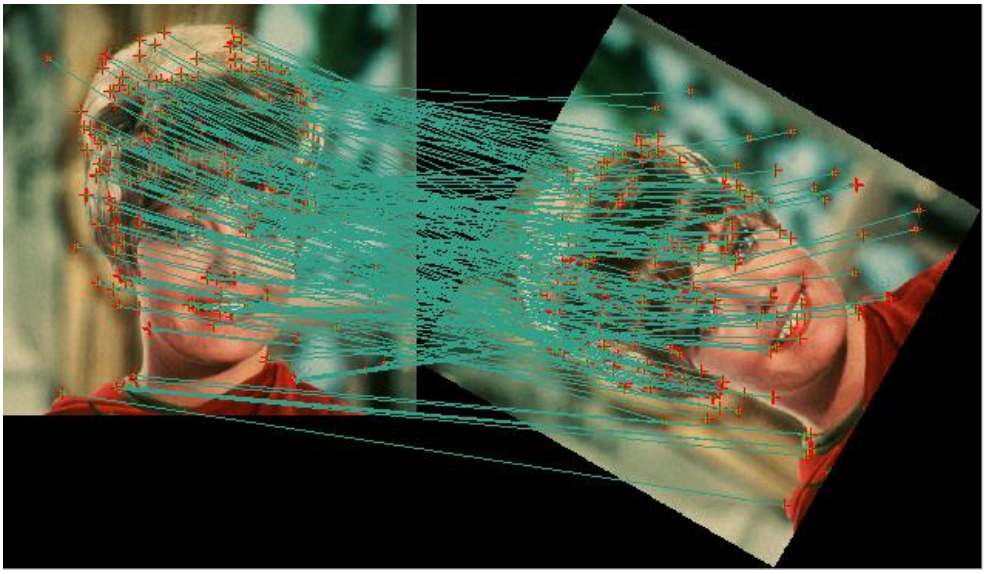
Trong giao diện chương trình demo thực nghiệm tấn công, ta chọn:

Bước 1: Chọn nút lệnh "2. XOAY ANH 60", chương trình sẽ nạp ảnh đã thủy vân và thực hiện phép xoay ảnh với góc 60 độ, và lưu ảnh bị biến đổi với một tên khác. Sau đó, áp dụng phép biến đổi SIFT để tìm những điểm đặc trưng quan trọng trong ảnh đã thủy vân và ảnh bị biến đổi. Và thực hiện so khớp các điểm đặc trưng thu được của ảnh đã thủy vân và ảnh bị biến đổi để khôi phục lại ảnh.

Hình 3.10 Ảnh đã thủy vân với các điểm đặc trưng quan trọng



Hình 3.11 Ảnh xoay 60^0 với các điểm đặc trưng quan trọng



Hình 3.12 So khớp điểm đặc trưng giữa ảnh thủy vân và ảnh biến dạng

Hình 3.13 Ảnh được khôi phục

Bước 2: Chọn nút lệnh "3. PHAT HIEN THUY VAN" từ chương trình chính, chương trình sẽ thực hiện:

Trích xuất 2 ảnh con từ ảnh được phục hồi và thực hiện phép biến đổi DFT với mỗi ảnh con để thu được một chuỗi thủy vân *W''* có độ dài 224 bit và được so sánh với chuỗi thủy vân sửa lỗi ban đầu *W'* để xác định sự hiện diện của thủy vân.

Ảnh khôi phục

Ảnh con 1

Ảnh con 2

Hình 3.14 Trích xuất 2 ảnh con từ ảnh được phục hồi

Kết quả thực nghiệm:

Ảnh trích xuất	Tỷ lệ r/n	Xác suất cảnh báo sai
Ảnh con 1	0.867	0.000057
Ảnh con 2	0.875	0.000057

Bảng 3.2 Kết quả so khớp thủy vân trích xuất và thủy vân gốc

Với bảng kết quả thực nghiệm ở trên, cùng với các giá trị ngưỡng như trong thực nghiệm 1, ta có thể khẳng định vẫn tồn tại thủy vân trong ảnh bị tấn công với phép biến đổi xoay ảnh 60^0.

3.4 Đánh giá kết quả thử nghiệm

Sau khi sử dụng chương trình để thực hiện thêm thực nghiệm trong từng mô hình thử nghiệm đã nêu ở trên, kết quả thu được như sau:

Chất lượng ảnh sau khi nhúng thuỷ vân và ảnh khôi phục được đánh giá thông qua giá trị của tỷ số PSNR giữa ảnh gốc *Img* và ảnh chứa thuỷ vân *FImg*.

Thời gian thực hiện tìm và so khớp các điểm đặc trưng, loại bỏ các điểm không phù hợp được thực hiện nhanh, còn thời gian khôi phục ảnh chỉ ở mức chấp nhận được.

Ảnh đã thủy vân	Biến đổi Affine 15%	Ảnh khôi phục
		
PSNR = 93.4320	PSNR = 83.8207	PSNR = 44.3822

Bảng 3.3 Tỷ số PSNR của ảnh biến đổi Affine và ảnh khôi phục

Ảnh đã thủy vân	Ảnh xoay 60^0	Ảnh khôi phục
		
PSNR = 93.4320	PSNR = 81.5721	PSNR = 42.7141

Bảng 3.4 Tỷ số PSNR của ảnh xoay 60^0 và ảnh khôi phục

Chất lượng của thuỷ vân được đánh giá thông qua tỷ lệ so khớp *r/n* giữa thuỷ vân trích xuất *W''* và thủy vân gốc *W'*, và được kiểm soát bởi xác suất cảnh báo sai khi so khớp với giá trị ngưỡng là 10^{-5}. Trong xác suất lỗi bit sử dụng thì khoảng giá trị thường được dùng để đánh giá là từ 10^{-4} (chấp nhận được) đến 10^{-9} (được xem là tốt).

Ảnh gốc sau khi nhúng thuỷ vân được biến đổi qua một số phép biến đổi ảnh, sau đó thực hiện quá trình trích xuất lại thuỷ vân, so sánh với thuỷ

vân gốc để đánh giá độ bền vững của thuỷ vân. Kết quả thể hiện qua bảng dưới đây:

STT	Phép tấn công	Ảnh con 1		Ảnh con 2	
		r/n	Xác suất cảnh báo sai	r/n	Xác suất cảnh báo sai
1	Không tấn công	1	0.000007	1	0.000006
2	Biến đổi Affine 5%	0.870	0.000076	0.870	0.000095
3	Biến đổi Affine 15%	0.820	0.000061	0.844	0.000059
4	Biến đổi Affine 25%	0.763	0.000050	0.768	0.000055
5	Xoay ảnh 30^0	0.827	0.000016	0.821	0.000010
6	Xoay ảnh 60^0	0.867	0.000057	0.875	0.000057
7	Xoay ảnh 90^0	0.952	0.000025	0.952	0.000027

Bảng 3.5 Tổng hợp kết quả thử nghiệm

Bảng 3.5 thể hiện các kết quả thực nghiệm của lược đồ thủy vân với một vài cuộc tấn công biến dạng hình học. Tương ứng là tỷ lệ giữa số các bit được so khớp *r* và chiều dài của chuỗi thủy vân *n*. Trong hầu hết các cuộc tấn công, sự tương đồng *r/n* là đủ cao để chứng minh quyền sở hữu.

Sự bền vững của lược đồ thủy vân đề xuất là dựa theo các yếu tố sau đây: Một là, sự so khớp các điểm đặc trưng chính xác để đảm bảo thực hiện tốt khôi phục ảnh. Hai là, miền DFT đảm bảo chịu được xử lý dịch ảnh và cắt ảnh mức vừa phải.

Kết quả thử nghiệm cho thấy lược đồ thủy vân đề xuất là bền vững cho một số cuộc tấn công biến dạng hình học, bao gồm: xoay, co giãn, dịch chuyển, mở rộng, cắt xén, và một số các cuộc tấn công kết hợp.

KẾT LUẬN

Trên cơ sở tìm hiểu các lược đồ thủy vân ứng dụng trong bài toán bảo vệ bản quyền với ảnh số. Một hướng nghiên cứu đã được tìm ra cho luận văn, đó là: kỹ thuật thủy vân dựa vào phép biến đổi DFT kết hợp với phép biến đổi SIFT nhằm nâng cao hơn tính bền vững của thủy vân trước các phép tấn công xử lý tín hiệu thông thường và biến dạng hình học. Trong lược đồ này, so khớp ba cặp điểm đặc trưng SIFT được sử dụng để đánh giá sự biến đổi hình học và để khôi phục lại hình ảnh gần đúng ban đầu. Thủy vân được đưa vào các hệ số tần số giữa miền DFT của ảnh. Phát hiện thủy vân cũng được thực hiện trong cùng một miền và không cần ảnh gốc ban đầu. Kết quả thử nghiệm đã chứng minh sự bền vững của lược đồ với phép xoay, mở rộng, dịch, biến đổi hình học Affine và các cuộc tấn công xử lý ảnh khác nhau. Bên cạnh đó, lược đồ thủy vân đã đề xuất cũng đáp ứng các nhu cầu của thời gian thực.

Hướng nghiên cứu tiếp theo sẽ tập trung vào việc phục hồi ảnh chống lại các cuộc tấn công biến dạng hình học cục bộ. Lược đồ cũng có thể được cải thiện hơn nữa bằng cách nâng cao hiệu suất của thuật toán nội suy hình ảnh và phục hồi hình ảnh.

Trong quá trình làm luận văn, tôi đã cố gắng rất nhiều. Tuy nhiên, do điều kiện thời gian và vốn kiến thức còn hạn chế, cộng thêm kinh nghiệm thực tế còn thiếu nên luận văn chắc chắn còn nhiều thiếu sót. Kính mong các thầy cô giáo và các bạn đồng nghiệp góp ý để luận văn được hoàn thiện hơn.

TÀI LIỆU THAM KHẢO

Tài liệu tiếng Việt

[1] Nguyễn Văn Tảo, Bùi Thế Hồng, *Nâng cao chất lượng ảnh trong kỹ thuật thuỷ vân sử dụng miền tần số giữa của phép biến đổi DCT*, Tạp chí Tin học và điều khiển học Tập 22 Số 3 Năm 2006

[2] Nguyễn Xuân Huy, Bùi Thế Hồng, Trần Quốc Dũng, *Kĩ thuật thuỷ vân số trong ứng dụng phát hiện xuyên tạc ảnh*, Báo cáo khoa học tại Hội thảo Quốc gia: Một số vấn đề chọn lọc của công nghệ thông tin, Đà Nẵng, Tháng 8/2004

[3] Lê Tiến Thường, Nguyễn Thanh Tuấn, *Giải pháp hiệu quả dùng kĩ thuật watermarking cho ứng dụng bảo vệ bản quyền ảnh số*, Tạp chí Bưu chính viễn thông, N. 14, 4/ 2005, tr. 57- 65

[4] Đỗ Năng Toàn, Phạm Việt Bình, "Giáo trình môn học - Xử lý ảnh", Đại học Thái Nguyên, tháng 11 năm 2007

[5] Đỗ Hồng Tân, Nguyễn Thị Thanh Hà, "Các định lý điểm bất động", Đại học sư phạm Hà Nội, 2003.

Tài liệu tiếng nước ngoài

[6] Navnath S. Narawade, *Robust Watermarking for Geometric attack using DFT*, IJETTCS, Volume 2, Issue 2, March - April 2013

[7] BAS, P., CHASSERY, J. M., MACQ, B. *Geometrically invariant watermarking using feature points*. IEEE Transactions on Signal Processing, 2002, vol. 11, no. 9, p. 1014-1027

[8] David G. Lowe, *Distinctive Image Features from Scale – Invariant Keypoints*, Computer Science Department University of British Columbia Vancouver, B.C., Canada, January 5, 2004

[9] QI, X. J., QI, J. *A robust content based digital image watermarking scheme*. Signal Processing, 2007, vol. 87, no. 6, p. 1264-1280.

[10] WANG, X. Y., HOU, L. M., WU, J. *A feature-based robust digital image watermarking against geometric attacks*. Image and Vision Computing, 2008, vol. 26, p. 980-989.

[11] Huming Gao, Liyuan Jia, Meiling Liu, *A Digital Watermarking Algorithm for Color Image Based on DWT*, TELKOMNIKA Indonesian Journal of Electrical Engineering, vol. 11, pp 3271-3278, 2013

[12] Haijun LUO, Xingming SUN, Hengfu YANG, Zhihua XIA, *A Robust Image Watermarking Based on Image Restoration Using SIFT*, Vol. 20, No. 2, Jun 2011

[13] Yavuz, E., Telatar, Z., *SIFT based geometric distortion correction method*, In Proceedings of 23rd International Symposium on Computer and Information Sciences (ISCIS). Istanbul (Turkey), 2008

[14] Matthieu Urvoy, Dalila Goudia, Florent Autrusseau, *Perceptual DFT Watermarking With Improved Detection and Robustness to Geometrical Distortions*. Information Forensics and Security, IEEE Transactions on (Volume: 9, Issue: 7), July 2014

[15] Ibrahim Alsonosi Nasir, Ahmed b. Abdurrman, *A Robust Color Image Watermarking Scheme Based on Image Normalization*, Proceedings of the World Congress on Engineering 2013 Vol III, July 3 - 5, 2013, London, U.K

[16] Bhalchandra D. Dhokale, Ramesh Y. Mali, *A Robust Image Watermarking Scheme Invariant to Rotation, Scaling and Translation Attack using DFT*, International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-3, Issue-5, June 2014

[17] Yanliang Ge, Jianbo Zhang, Hongbo Bi, Ying Liu, *Image Watermarking Scheme Based on Geometric Invariant Features*, Journal of Information & Computational Science 11:16 (2014) 5977–5986, November 2014

PHỤ LỤC

TRÌNH TỰ XỬ LÝ ĐỂ GIẢI QUYẾT VẤN ĐỀ BẢN QUYỀN

Nhiếp ảnh là một trong những môn nghệ thuật mà nhiều nghệ sĩ đam mê sáng tạo. Về khía cạnh pháp lý, tác phẩm nhiếp ảnh cũng là một đối tượng được pháp luật Việt Nam bảo hộ dưới hình thức bản quyền tác giả. Các nghệ sỹ khi có các tác phẩm tâm đắc, cũng có thể tiến hành đăng ký tại Cục Bản quyền tác giả Việt Nam. Việc đăng ký bản quyền tác giả sẽ tránh làm phát sinh những tranh chấp không đáng có về thời điểm sáng tạo cũng như về tác giả, chủ sở hữu của tác phẩm.

Với đặc điểm của bức ảnh được phân bố dưới dạng số là rất dễ sao chép và trao đổi, nên người sở hữu tác phẩm rất khó theo dõi các bản sao chép sản phẩm số của họ.

1. ĐĂNG KÝ BẢN QUYỀN TÁC GIẢ

Trước tiên, chủ sở hữu sẽ nhúng thủy vân số dạng ẩn, bền vững vào ảnh số giống như một hình thức "tự dán tem bản quyền". Thủy vân được sử dụng là một minh chứng cho quyền sở hữu để ngăn chặn sao chép và phân phối lậu tác phẩm.

Sau đó, tác giả làm thủ tục đăng ký bản quyền tác phẩm với cơ quan quản lý và đóng một khoản lệ phí.

Với tác phẩm đã đăng ký bản quyền thì được cơ quan nhà nước bảo hộ và có chế tài xử lý khi phát hiện ra vi phạm.

2. QUI TRÌNH XỬ LÝ VI PHẠM BẢN QUYỀN

Khi có dấu hiệu vi phạm bản quyền tác phẩm thì tuỳ theo nhu cầu và thực trạng mà chủ sở hữu áp dụng các biện pháp, phương án phù hợp.

Trước tiên, chủ sở hữu chạy chương trình để trích xuất thủy vân ra, kiểm tra tỷ lệ so khớp của thủy vân trích xuất và thủy vân gốc mà trên 75% là đủ cao để chứng minh quyền sở hữu.

Theo quy định, tác giả có tác phẩm đã đăng ký bản quyền tại cơ quan nhà nước có thẩm quyền, không có nghĩa vụ phải chứng minh quyền tác giả, quyền liên quan đã đăng ký khi có tranh chấp, trừ khi có chứng cứ ngược lại. Như vậy, tùy theo mức độ vi phạm bản quyền, chủ sở hữu có thể tiến hành xử lý vi phạm theo biện pháp dưới đây:

+ ***Biện pháp 1***: Cảnh báo vi phạm

Chủ sở hữu trực tiếp hoặc thông qua các đơn vị liên quan phát hành công văn cảnh báo vi phạm và đề nghị chấm dứt hành vi, khắc phục hậu quả.

Trong trường hợp chủ thể vi phạm không thực hiện các yêu cầu trên hoặc thực hiện không đầy đủ thì xem xét *Biện pháp 2*.

+ *Biện pháp 2*: Yêu cầu cơ quan chức năng xử lý hành vi vi phạm (biện pháp hành chính)

Theo phương án này chủ sở hữu trực tiếp soạn thảo, chuẩn bị tài liệu cần thiết và nộp yêu cầu xử lý vi phạm bản quyền cho cơ quan nhà nước có thẩm quyền.

* ***Quy định về xử phạt hành chính***:

Ngày 16/10/2013, Chính phủ đã ban hành Nghị định số 131/2013/NĐ-CP quy định xử phạt vi phạm hành chính về quyền tác giả, quyền liên quan. Nghị định có 43 điều gồm 3 điều khoản thi hành và 40 điều quy định về phạm vi, hành vi vi phạm hành chính, hình thức và mức xử phạt, biện pháp khắc phục hậu quả, thẩm quyền lập biên bản vi phạm hành chính và thẩm quyền xử phạt vi phạm hành chính về quyền tác giả, quyền liên quan. Theo đó, mức phạt tối đa trong lĩnh vực quyền tác giả, quyền liên quan quy định trong Nghị định đối với cá nhân là 250.000.000đ, đối với tổ chức là 500.000.000đ.