PHẦN MỞ ĐẦU

1. Tính cấp thiết của luận án

"Giấu thông tin" (Steganography) là kỹ thuật giấu thông tin quan trọng vào đối tượng khác. Nó đã có lịch sử phát triển từ hàng nghìn năm và trải qua nhiều thời kỳ biến động của xã hội loài người, ngày nay khi kỹ thuật số bùng nổ, con người cũng "số hoá" lĩnh vực đó phục vụ cho cuộc sống hiện đại.

Về nguyên lý, giấu tin trong dữ liệu đa phương tiện hay trong dữ liệu ảnh số không khác gì nhiều, nhưng do giấu tin trong ảnh dễ thực hiện hơn, giấu được nhiều thông tin hơn, và cũng là đối tượng số được sử dụng khá phổ biến trên Internet hiện nay, nên kỹ thuật giấu tin trong ảnh chiếm tỉ lệ nhiều nhất trong các loại dữ liệu đa phương tiện [32]. Thông tin có thể được giấu trên miền không gian hoặc trên miền biến đổi như biến đổi tần số (cosine, wavelet, fourier rời rạc) hay biến đổi sai phân (difference image).

Kỹ thuật giấu tin trong ảnh đa số là phương pháp giấu trên bit có ít ý nghĩa nhất LSB (Least Significant Bit) của điểm ảnh hoặc của các hệ số biến đổi (biến đổi cosine rời rạc, wavelet rời rạc, sai phân – image difference,…). Ngoài ra còn có một số phương pháp giấu khác theo cách thức có sự thay đổi nhỏ trên ảnh theo hình thức chèn nhiễu SS (Spread Spectrum), điều chỉnh hệ số lượng tử QIM (Quantization index modulation)...

Giống như trong Mật mã, Thám mã (Cryptanalysis) là kỹ thuật đối lập nhưng song song tồn tại và phát triển cùng với sự phát triển của kỹ thuật mật mã, nhằm giải mã các "bản mã" thu được để hiểu rõ nội dung ban đầu của bản mã, thì phát hiện ảnh có giấu tin (Image Steganalysis) là kỹ thuật đối lập với Image Steganography nhằm dò tìm ảnh số nào đó có giấu thông tin hay không.

Việc nghiên cứu Steganalysis ngoài ý nghĩa khoa học còn có hai ý nghĩa thực tiễn, đó là: Thứ nhất, nhằm phục vụ đắc lực cho lĩnh vực an toàn thông tin; Thứ hai, nhằm nâng cấp và thúc đẩy sự phát triển của kỹ thuật giấu tin trong ảnh. Với hai mục đích nêu trên dẫn đến hai hướng nghiên cứu khác nhau. Hướng thứ nhất, cố gắng xây dựng thuật toán phát hiện mù (blind steganalysis) cho ảnh có giấu tin sử dụng kỹ thuật giấu bất kỳ. Hướng thứ hai, dựa vào kỹ thuật giấu tin nào đó đã biết, có thể xây dựng được thuật toán phát hiện phù hợp (phát hiện có ràng buộc – constraint steganalysis).

Đã có nhiều công trình nghiên cứu công bố trên thế giới thành công theo hai hướng này. Tuy nhiên, các kỹ thuật giấu tin ra đời sau ngày càng tinh xảo hơn đòi hỏi các nhà phát hiện ảnh giấu tin không ngừng tìm ra phương pháp phát hiện phù hợp bắt kịp với xu hướng phát triển của kỹ thuật giấu. Đặc biệt với tốc độ phát triển nhanh chóng của Internet thì nhu cầu trao đổi thông tin bằng ảnh ngày càng lớn mạnh, do đó để đảm bảo an toàn an ninh, quốc phòng hay nhằm hỗ trợ nâng cấp, cải tiến kỹ thuật giấu nào đó an toàn hơn đang là bài toán cấp thiết đặt ra cho các nhà nghiên cứu trong lĩnh vực an toàn thông tin hiện nay.

2. Mục tiêu và phạm vi nghiên cứu

Từ các vấn đề nêu trên, luận án này tập trung nghiên cứu cải tiến và đề xuất một số kỹ thuật phát hiện ảnh có giấu tin theo hai hướng chính:

- Thứ nhất, đưa ra kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian và miền tần số.
- Thứ hai, đưa ra một số kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin với kỹ thuật giấu biết trước.

Đối tượng ảnh nghiên cứu là các ảnh dạng BITMAP như các định dạng: JPG, GIF, PNG, TIF, BMP.

3. Những đóng góp của luận án

Những đóng góp chính của luận án là đưa ra kỹ thuật phát hiện ảnh có giấu tin theo hai bài toán:

Bài toán 1: Kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB :

- Của miền không gian với bốn phương pháp đề xuất sau: phương pháp phân tích độ lệch chuẩn, phương pháp thống kê χ^2 một bậc tự do (χ_1^2), phương pháp phân tích tỉ lệ xám, phương pháp ước lượng số bit thông tin giấu trên LSB của miền không gian bằng lý thuyết trùng khớp.
- Của miền tần số bằng phương pháp phân tích tỉ lệ xám.

Bài toán 2: Kỹ thuật phát hiện có ràng buộc cho ảnh giấu tin sử dụng kỹ thuật giấu đã biết gồm kỹ thuật: IWH trên hệ số wavelet, DIH trên hệ số sai phân, HKC trên miền không gian, RVH trên miền không gian với hai pha ngang dọc.

Tiến hành thử nghiệm trên những tập dữ liệu có số lượng ảnh lớn để so sánh kỹ thuật đề xuất với các kỹ thuật phát hiện khác.

4.Tổ chức luận án

Luận án gồm ba chương trong đó:

Chương 1 giới thiệu tổng quan về giấu tin trong ảnh, phát hiện ảnh có giấu tin và các nghiên cứu liên quan.

Chương 2 trình bày kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB.

Chương 3 trình bày kỹ thuật phát hiện có ràng buộc.

Phần cuối cùng là phần **kết luận chung** và **phụ lục**:

Phụ lục giới thiệu chương trình đề mô với hai mô đun chính: Mô đun giấu tin và mô đun phát hiện ảnh giấu tin phục vụ các thử nghiệm trong luận án.

Chương 1. GIẤU TIN TRONG ẢNH, PHÁT HIỆN ẢNH CÓ GIẤU TIN VÀ CÁC NGHIÊN CỨU LIÊN QUAN

1.1. GIẤU TIN TRONG ẢNH VÀ NGHIÊN CỨU LIÊN QUAN

1.1.1. Khái niệm

1.1.2. Phương pháp giấu tin và nghiên cứu liên quan

Phương pháp giấu trên LSB là phương pháp thay thế các bit thông tin vào các bit LSB của điểm ảnh [16, 17, 19, 50, 51, 53 - 55, 65, 67, 69, 75, 77, 91, 100]. Trong một điểm ảnh của ảnh 8-bit màu thì bit cuối cùng (bit thứ 8) gọi là bit LSB. Do vậy khi thay đổi giá trị của bit này (từ "0" sang "1" hay từ "1" sang "0") không làm ảnh hưởng nhiều đến chất lượng trực quan của ảnh. Thông tin có thể giấu trên LSB của các hệ số biến đổi cosine, wavelet, ...

Ngoài phương pháp giấu trên LSB còn có một số phương pháp giấu tin khác theo hình thức chèn nhiễu SS [3, 4, 26, 27, 32, 60], điều chỉnh hệ số lượng tử hóa QIM [5, 23, 42, 65, 79], kỹ thuật giấu thuận nghịch (đòi hỏi yêu cầu sau khi tách thông tin chúng ta còn có thể khôi phục lại ảnh gốc ban đầu) mở ra một hướng mới trong lĩnh vực giấu tin với một loạt các kỹ thuật giấu tin thuận nghịch được công bố [21, 24, 25, 35, 41, 45, 48, 49, 52, 53, 58, 90, 91, 93, 98, 99].

1.1.3. Phương pháp đánh giá độ an toàn của một lược đồ giấu tin

Chúng ta đưa ra một vài ký hiệu sẽ được sử dụng xuyên suốt luận án này. Ký hiệu $\boldsymbol{\mathcal{C}}$ là tập tất cả các ảnh gốc C, $\boldsymbol{\mathcal{M}}$ là tập các thông tin mật M, $\boldsymbol{\mathcal{K}}$ là tập các khóa K giấu tin, $\boldsymbol{\mathcal{S}}$ là tập tất cả các ảnh stego S (ảnh có giấu tin). Một lược đồ giấu tin (thuật toán) là một cặp (S_E, S_X), với S_E: $\boldsymbol{\mathcal{C}} \times \boldsymbol{\mathcal{M}} \times \boldsymbol{\mathcal{K}} \rightarrow \boldsymbol{\mathcal{S}}$ là hàm nhúng thông tin, $S_X : \boldsymbol{\mathcal{S}} \times \boldsymbol{\mathcal{K}} \rightarrow \boldsymbol{\mathcal{M}}$ là hàm tách thông tin. Hàm nhúng S_E tạo ra một đối tượng $S \in \boldsymbol{\mathcal{S}}$ từ mỗi $C \in \boldsymbol{\mathcal{C}}$, $M \in \boldsymbol{\mathcal{M}}$ và $K \in \boldsymbol{\mathcal{K}}$, hàm tách S_X tách tin M từ S bằng khóa K.

Giả sử P_C hàm phân bố xác xuất của $C \in \boldsymbol{\mathcal{C}}$. Nếu khóa $K \in \boldsymbol{\mathcal{K}}$ và $M \in \boldsymbol{\mathcal{M}}$ được chọn ngẫu nhiên thì lược đồ giấu tin (S_E, S_X) cùng với hàm phân bố xác suất P_C sẽ được hàm phân bố xác suất P_S tương ứng của $S \in \boldsymbol{\mathcal{S}}$. Khi đó theo khái niệm về giấu tin an toàn của Cachin [15] ta có định nghĩa sau:

Định nghĩa 1.1 [15]– Một lược đồ (thuật toán) giấu tin được gọi là an toàn nếu sai phân Kullback – Leibler giữa hàm mật độ xác suất của P_C và P_S theo (1.1) bằng 0:

$$D_{KL}(P_C \,||\, P_S) = \sum_{C \in \mathcal{C}} P_C(C) log \frac{P_C(C)}{P_S(C)} \qquad (1.1)$$

Khi $D_{KL}(P_C \,||\, P_S) < \varepsilon$ thì lược đồ giấu tin có độ an toàn ε (ε - secure), trong đó ε là một số thực dương đủ nhỏ tùy ý cho trước.

Đây là khái niệm đứng từ quan điểm lý thuyết, rất khó thực hiện trong thực tế vì không gian ảnh là quá lớn (vô hạn). Mặt khác, một lược đồ giấu tin để đảm bảo $D_{KL}(P_C \,||\, P_S) = 0$ là không thể vì điều này có nghĩa không thay đổi gì trên ảnh gốc, tức là $P_C = P_S$ (theo bổ đề cơ bản trong Lý thuyết thông tin). Vì vậy, người ta thường giấu sao cho đạt độ an toàn ε - secure đảm bảo thay đổi trên ảnh nhỏ nhất mà mắt người khó có thể cảm nhận.

1.2. PHÁT HIỆN ẢNH GIẤU TIN VÀ CÁC NGHIÊN CỨU LIÊN QUAN

1.2.1. Khái niệm

Phát hiện ảnh giấu tin (image steganalysis) là kỹ thuật phát hiện sự tồn tại của thông tin được giấu trong ảnh số nào đó [27].

1.2.2. Phương pháp phát hiện ảnh có giấu tin

Phát hiện ảnh giấu tin có thể định nghĩa như một bài toán phân loại dựa trên kiểm định giả thuyết thống kê. Điều này phụ thuộc vào hiểu biết của chúng ta về lược đồ giấu tin, do đó phát hiện ảnh giấu tin được phát biểu: hoặc như bài toán kiểm định giả thuyết đơn (simple hypothesis); hoặc như bài toán kiểm giả thuyết phức hợp (composite hypothesis).

Nếu chúng ta không có thông tin gì về lược đồ giấu tin thì phương pháp phát hiện gọi là phát hiện mù (blind steganalysis), bài toán phân loại có thể phát biểu dựa trên kiểm định giả thuyết phức hợp sau:

H_0: X được rút ra từ hàm phân bố xác suất là P_S

H_1: X không được rút ra từ hàm phân bố xác suất P_S

Với X là mẫu dữ liệu ảnh được xét.

Trong trường hợp biết trước thông tin về lược đồ giấu tin thì phương pháp phát hiện gọi là phát hiện có ràng buộc (constraint steganalysis). Giả sử chúng ta biết được phân bố xác suất của P_C, lược đồ giấu tin (S_E, S_X) và phân bố của thông tin M, chúng ta có thể tính được P_S. Từ đó chúng ta có thể đưa ra phương pháp phát hiện theo bài toán phân loại dựa trên kiểm định giả thuyết đơn sau:

H_0: X có phân bố xác suất là P_S

H_1: X có phân bố xác suất là P_C

Để giải quyết bài toán kiểm định giả thuyết thống kê này, chúng ta cần tìm ra được miền điều kiện hoặc đặc trưng nào đó để có thể phân loại sao cho tỉ lệ lỗi xảy ra là nhỏ nhất.

Rõ ràng có nhiều cách chia như vậy. Nhưng vấn đề là bằng cách chia bất kỳ đều dẫn đến hai sai số theo thống kê gọi là sai số loại I (type I error) với xác suất α ($0 < \alpha < 1$) (khẳng định sai) và sai số loại II (type II error) (phủ định sai) với xác suất β ($0 < \beta < 1$).

1.2.3. Nghiên cứu liên quan và hướng phát triển của luận án

Các phương pháp nghiên cứu của Steganalysis tập trung vào hai hướng chính như đã nêu trên:

- Hướng thứ nhất cố gắng xây dựng phát hiện mù cho kỹ thuật giấu bất kỳ.
- Hướng thứ hai tìm cách phát hiện ảnh stego khi biết kỹ thuật giấu tin

Trong luận án này đi sâu vào nghiên cứu kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB và phát hiện có ràng buộc cho một số kỹ thuật giấu biết trước.

1.3. PHƯƠNG PHÁP THỰC NGHIỆM VÀ ĐÁNH GIÁ

1.3.1. Tiêu chuẩn đánh giá

Phát hiện ảnh có giấu tin thực chất là bài toán phân lớp tập ảnh bất kỳ vào hai tập con là tập ảnh gốc và tập ảnh có giấu tin. Với phân lớp này, nhà phân tích thường sử dụng các độ đo đánh giá: độ chính xác P (precision), độ bao phủ R (recall) và độ trung bình điều hòa F (f-measure) áp dụng cho kỹ thuật phát hiện đề xuất để có thể đánh giá khách quan, hiệu quả và độ tin cậy của kỹ thuật.

1.3.2. Nguồn dữ liệu ảnh thử nghiệm

Một vấn đề quan trọng trong luận án chính là việc chuẩn bị các tập dữ liệu ảnh để thực hiện các thực nghiệm liên quan. Nguồn dữ liệu được chọn phải đảm bảo các yêu cầu sau: Có độ tin cậy nhất định, được công bố bởi các tổ chức có uy tín, có số lượng ảnh tương đối lớn, nội dung ảnh đa dạng.

Tập ảnh gốc thử nghiệm: Tập ảnh gốc sử dụng chung cho các thuật toán giấu và phát hiện trong luận án gồm 2088 ảnh với các kích cỡ khác nhau trong đó: 1014 ảnh được tải về từ hai thư viện trực tuyến [103, 107] và 1074 ảnh được tạo ra từ máy ảnh kỹ thuật số và máy ảnh trên điện thoại di động. Nội dung ảnh đa dạng gồm: ảnh phong cảnh, chân dung, hoạt họa, vệ tinh, các sự kiện … đa số là ảnh 24 - bit màu được chuyển sang ảnh cấp xám bằng trình xử lý ảnh Adobe Photoshop CS 8.0 được tập ảnh thử nghiệm gồm 2088 ảnh cấp xám. Gọi tập ảnh này là $\boldsymbol{C}_0$ sẽ được sử dụng trong hầu hết các thử nghiệm của luận án.

1.3.3. Công cụ hỗ trợ và môi trường thực nghiệm

Các kỹ thuật đưa ra của luận án được cài đặt trên môi trường Matlab phiên bản R2008b (7.7.0), chạy trên máy tính cấu hình Intel (R) Core (TM) 2 Duo T.7200 2.00GHz, bộ nhớ trong 1Gb, bộ nhớ ngoài dung lượng trống khả dụng 15GB.

KẾT LUẬN CHƯƠNG 1

Chương này đưa ra bức tranh tổng quan về giấu tin trong ảnh và phát hiện ảnh giấu tin. Với mỗi phương pháp giấu sẽ hình thành nên các kỹ thuật phát hiện phù hợp thúc đẩy sự phát triển của phương pháp giấu. Việc đi sâu vào tìm hiểu các kỹ thuật phát hiện đó sẽ giúp chúng ta định hướng phát triển và cải tiến kỹ thuật giấu hiện tại hoặc đó chính là nền tảng để mở rộng cho các kỹ thuật phát hiện khác.

Chương 2. KỸ THUẬT PHÁT HIỆN MÙ CHO ẢNH GIẤU TIN TRÊN LSB

2.1. KỸ THUẬT PHÁT HIỆN MÙ TRÊN LSB CỦA MIỀN KHÔNG GIAN

2.1.1. Phát hiện bằng phân tích "độ lệch chuẩn"

2.1.1.1. Phân tích kỹ thuật giấu LSB

Khảo sát đặc trưng khác biệt giữa ảnh gốc C và ảnh S có giấu tin trên LSB. Thống kê dữ liệu của ảnh C và S được vector C^{26x10} và S^{26x10} với c_{ij}, s_{ij} ($0 \le i \le 25, 0 \le j \le 9$) là tần số của điểm ảnh C và S có giá trị bằng i*10+j. So sánh hai vector C^{26x10} và S^{26x10} phát hiện một vấn đề quan trọng đó là tổng giá trị trên từng hàng

của C^{26x10} và S^{26x10} tương ứng là không thay đổi. Chỉ có giá trị của các phần tử trong hàng đó là thay đổi. Trong ảnh C trên từng hàng của vector C^{26x10} xuất hiện nhiều điểm đột biến, tức giá trị của nó rất khác nhau. Còn với ảnh S thì các giá trị biến thiên rất gần nhau.

2.1.1.2. Phương pháp phát hiện

Để phân loại ảnh có giấu tin và không có giấu tin trên LSB trong trường hợp này ta sử dụng định lý sau:

Định lý 2.1 [108]: Cho X là đại lượng ngẫu nhiên có phân bố chuẩn $N(a,\sigma^2)$. Khi đó đại lượng ngẫu nhiên $Y= (X - a)/\sigma$ có phân bố chuẩn $N_n(0,1)$

Định lý 2.2 - Cho $X_1, X_2, ... X_n$ là đại lượng ngẫu nhiên, độc lập cùng phân bố chuẩn $N(a, \sigma^2)$. Khi đó đại lượng ngẫu nhiên $X_1 + X_2 +...+ X_n$ sẽ có phân bố chuẩn $N(na, n\sigma^2)$. (chứng minh xem trong phụ lục A).

Trong thực tế a và σ^2 chưa biết cho nên ta phải ước lượng a, σ^2. Có nhiều phương pháp để ước lượng các đại lượng này nhưng một phương pháp thông dụng và đơn giản nhất là phương pháp hợp lý cực đại. Bằng phương pháp này ta thay a bởi ước lượng $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$ và σ^2 bởi ước lượng $\hat{S}^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2$, ($\sigma = \hat{S}$). Ký hiệu: $x_{max} = \max\{x_1, x_2, \ldots, x_n\}$ và $x_{min} = \min\{x_1, x_2, \ldots, x_n\}$. Khi đó các đại lượng ngẫu nhiên: $V_1 = \frac{x_{max} - \bar{x}}{\hat{S}}$, $V_2 = \frac{\bar{x} - x_{min}}{\hat{S}}$, sẽ phân bố chuẩn $N_n(0,1)$ không phụ thuộc a và σ^2 mà chỉ phụ thuộc vào n.

Đặt $V=V_1+V_2$, do đại lượng ngẫu nhiên V_1, V_2 có phân bố chuẩn $N_n(0,1)$ nên V có phân bố chuẩn $N_n(0,2)$. Áp dụng định lý giới hạn trung tâm [108], ta có

$$T = \frac{V}{\sqrt{2}} \qquad (2.1)$$

sẽ có phân bố chuẩn $N_n(0,1)$ đã được lập thành bảng XII trong [108] với n=1,2,3,... và mức ý nghĩa α=0.1, 0.05,...

Đại lượng ngẫu nhiên T từ (2.1) có phân bố chuẩn $N_n(0,1)$ tức là ta có xác xuất $P\{T \geq x_0\} = \int_{x_0}^{\infty} p_n(t)dt$ trong đó $P_n(t)$ là hàm mật độ xác suất chuẩn $N_n(0,1)$ nếu cho trước n và giá trị xác suất sai số loại I với $\alpha = \alpha_0$, ta tìm được giá trị ngưỡng x_0 bởi phương trình sau đây:

$$\int_{x_0}^{\infty} P_n(t)dt = 1 - \int_{-\infty}^{x_0} p_n(t)dt = 1 - \alpha_0$$

Đó là những vấn đề cơ bản, làm cơ sở để xây dựng thuật toán phát hiện ảnh có giấu thông tin.

Do $T= \frac{V_1 + V_2}{\sqrt{2}}$ mà $(T \geq x_0) \Leftrightarrow (V_1+V_2 \geq \sqrt{2}\, x_0)$ nên sau khi xác định được x_0 ta có thể tìm được ngưỡng theo $t_0 = \sqrt{2}\, x_0$ (2.2)

Áp dụng giải quyết bài toán

Sau khi tìm được ngưỡng của bài toán ta áp dụng để phân loại ảnh như sau: kiểm tra V = $\frac{x_{max}-x_{min}}{\hat{S}}$

- Nếu V ≥ t_0 kết luận C ảnh không giấu thông tin

- Nếu V < t_0 kết luận C ảnh có giấu thông tin

Giá trị ngưỡng t_0 được tính toán theo (2.2) dựa trên x_0 tra cứu theo bảng phân bố chuẩn [108] với n=10 và độ tin cậy α=0.1, 0.05, 0.025, 0.01 được giá trị tương ứng t_0 =3.0349, 3.244, 3.414, 3.592.

2.1.2. Phát hiện bằng thống kê χ^2 một bậc tự do

2.1.2.1. Phân tích kỹ thuật "độ lệch chuẩn"

Hạn chế của kỹ thuật trình bày ở 2.1.1 là phụ thuộc vào dữ liệu ảnh và độ dài của thông tin đem giấu trong ảnh. Nếu dữ liệu của ảnh có độ nhiễu cao thì rất khó phát hiện vì dữ liệu của ảnh phân bố rất đều. Mặt khác, nếu lượng thông tin đem giấu thấp sẽ không làm thay đổi dữ liệu ban đầu của ảnh, điều này ảnh hưởng đến sự phân bố đều dữ liệu của ảnh trong công thức phát hiện.Vì vậy sau đây là một phương pháp khác phát hiện ảnh có giấu tin trên LSB.

2.1.2.2. Phương pháp phát hiện

Sử dụng định lý 2.3 trong [108] chúng ta xây dựng bổ đề 2.1.

Định lý 2.3 [108]: Gọi m là số lần xuất hiện một biến cố A trong dãy n phép thử Becnouli với xác suất xuất hiện biến cố A là P(A) = p > 0.

Khi đó, đại lượng ngẫu nhiên Y= $\frac{m-np}{\sqrt{npq}}$ *có xấp xỉ phân bố chuẩn N(0, 1), với q = 1 - p.*

Bổ đề 2.1: Giả sử cho trước một dãy nhị phân được lấy từ một nguồn ngẫu nhiên, độc lập s=s_o, s_1, ..., s_{n-1}. Ký hiệu n_0 và n_1 lần lượt là tần suất số "0" và "1" xuất hiện trong dãy (tức $n_0 + n_1 = n$)

$$Đặt \quad z = \frac{(n_0-n_1)^2}{n} \qquad (2.3)$$

Khi đó, nếu s là ngẫu nhiên, độc lập thì z có phân bố "χ – bình phương" (chi-square) 1 bậc tự do (với n >= 10)

Áp dụng bổ đề 2.1 vào việc phân loại ảnh có giấu thông tin trên LSB bằng cách tính tần suất các điểm ảnh của một ảnh cần kiểm tra được vector C^{26x10} (bỏ qua hàng cuối cùng của C vì hàng này có chứa các giá trị bằng 0) ta được C^{25x10}. Thực hiện tiếp một số bước:

1. Tìm giá trị lớn nhất của C^{25x10} ký hiệu là x_{max} = max{c_{ij}, i=$\overline{0,24}$, j=$\overline{0,9}$}. Giả sử giá trị max là $x_{max} = c_{i_0 j_0}$ ((i_0,j_0) có giá trị lớn nhất tại hàng i_0 của C^{25x10}).

2. Tính $n_{i_0}[0]= \sum_{j=0}^{4} X_{i_0,2j}$, $n_{i_0}[1]= \sum_{j=0}^{4} X_{i_0,2j+1}$, $n_{i_o}= n_{i_o}[0]+ n_{i_o}[1]$.

Áp dụng bổ đề 2.1 ta có $\frac{(n_{i_0}[0]-n_{i_0}[1])^2}{n_{i_0}}$ có phân bố χ^2 một bậc tự do.

3. Kết luận, nếu $\frac{(n_{i_0}[0]-n_{i_0}[1])^2}{n_{i_0}} \geq \chi_1^2(\alpha)$ thì ảnh kiểm tra là ảnh không chứa thông tin mật, ngược lại nếu $\frac{(n_{i_0}[0]-n_{i_0}[1])^2}{n_{i_0}} < \chi_1^2(\alpha)$ thì ảnh kiểm tra có chứa thông tin mật với xác suất sai số là α.

Thực hiện thử nghiệm trên cùng tập ảnh (gồm 500 ảnh) với các giá trị α = 0.1, 0.05, 0.025, 0.01, 0.005 tra bảng khi – bình phương [108] với n=1 được các giá trị tương ứng χ_1^2 =2.71, 3.84, 5.02, 6.63, 7.88. Thấy rằng kết quả phân loại hiệu quả khi χ_1^2 =2.71.

2.1.3. Phát hiện dựa trên phân tích tỉ lệ xám

2.1.3.1. Phát biểu bài toán

Để làm giảm thiểu sai số xảy ra khi phân loại ảnh có giấu tin trên miền LSB chúng ta áp dụng bổ đề Neyman – Pearson với xác suất α (sai số loại I) cho trước cực tiểu hóa xác suất β (sai số loại II).

2.1.3.2. Giải quyết bài toán

Trong phần này sử dụng một số bổ đề trong thống kê, từ đó có thể mở rộng các bổ đề này để có thể phân loại ảnh có giấu tin trên LSB.

Bổ đề 2.2 (Neyman – Pearson) [108]: Cho trước $f_0, f_1, f_2, \ldots$ là những hàm khả tích đối với độ đo ν (σ- hữu hạn) trên không gian S. Giả sử:

Cho tập con $w \subset S$ và các hằng số $c_1, c_2, c_3, \ldots$ thỏa mãn:

$$\int_w f_i(x)d\upsilon(x) = c_i$$

Tập con $w_0 \subset S$ và các hằng số $k_1, k_2, \ldots$ thoả mãn:

$$\begin{cases} f_0(x) \geq \sum_{i\geq 1} k_i f_i(x), x \in w_0 \\ f_0(x) < \sum_{i\geq 1} k_i f_i(x), x \notin w_0 \end{cases} \quad và \quad \int_{w_0} f_i(x)d\upsilon(x) = c_i$$

Khi đó:

$$\int_{w_0} f_0(x)d\upsilon(x) \geq \int_w f_0(x)d\upsilon(x)$$

Bổ đề 2.3 [109]: Nếu $P\{x|H_0\}$ có phân bố đa thức (phân bố mũ) và giả thuyết H_0 đúng thì đại lượng ngẫu nhiên:

$$-2\ ln\frac{P(x|H_1)}{P(x|H_0)} \text{ có phân bố } \chi^2. \qquad (2.5)$$

Bổ đề 2.4 [109, 110]: Giả sử $f_1, f_2, \ldots, f_k$ là k hàm khả tích đối với độ đo μ nào đó (σ- hữu hạn) trên không gian S, còn $A_1^*, A_2^*, \ldots, A_k^*$ là một phân hoạch của S thoả mãn điều kiện:

Nếu $x \in A_i^*$ *và* $f_i(x) \geq f_j(x)$ *với* $\forall j \neq i$, $i, j = 1,2,..., k$.

Khi đó: $\sum_{i=1}^{k} \int_{A_i^*} f_i(x) d\mu(x) \geq \sum_{j=1}^{k} \int_{A_j} f_j(x) d\mu(x) d(x)$ (2.6)

Điều này suy ra phân hoạch A_1^*, A_2^*, ..., A_k^* là một phân hoạch tối ưu, theo nghĩa hàm lực lượng lớn nhất [108].

Đặt $f_0(x) = P(w \mid H_1)$, $f_1(x) = P(w \mid H_0)$, khi đó w_0 là miền tối ưu nếu:

$$w_0 = \{x \in S: \frac{f_0(x)}{f_1(x)} \geq t(\alpha)\} \quad (2.7)$$

Hay nói cách khác: $w_0 = \{x \in S: \frac{P(x \mid H_1)}{P(x \mid H_0)} \geq t(\alpha)\}$ (2.7')

Ở đây, theo bổ đề 2.2 nếu lấy $c_i = c = \alpha$, ta có $P\{w_0|H_0\} = \alpha$, thì w_0 được chọn như ở (2.7) hoặc (2.7') là miền làm cho xác suất β là bé nhất khi xác suất α cố định. Còn $t(\alpha)$ được xác định bằng bổ đề 2.3.

Để áp dụng cho việc tìm ảnh có chứa thông tin ẩn, trước hết ta giả sử $P\{x|H_0\}$ và $P\{x|H_1\}$ là mật độ xác suất đối với độ đo μ (σ - hữu hạn) nào đó khi lần lượt giả thuyết H_0, H_1 đúng. Theo bổ đề 2.2, chúng ta phải xác định miền w sao cho:

$$\int_w p(x \mid H_0) d\mu(x) = \alpha \quad (0 < \alpha < 1 \text{ cho trước})$$

và $\int_w p(x \mid H_1) d\mu(x) = 1 - \beta$ đạt giá trị lớn nhất (2.8)

Ứng dụng bổ đề 2.2, miền tối ưu: $w_0 = \{x: p(x \mid H_1) \geq t(\alpha).p(x \mid H_0)\}$ hay:

$$w_0 = \{x: \frac{p(x \mid H_1)}{p(x \mid H_0)} \geq t(\alpha)\} \quad (2.9)$$

$t(\alpha)$ được chọn sao cho $p(w \mid H_0) = \alpha$

Tiếp theo chúng ta sẽ giải bài toán trong thống kê toán học sau:

Mệnh đề 2.1: Giả sử cho trước một đại lượng ngẫu nhiên k chiều $X=(X_1, X_2, ..., X_k)$ có phân bố đa thức:

$$P(X_1=r_1, X_2=r_2, .., X_k=r_k) = \frac{n!}{r_1! r_2! .. r_k!} P_1^{r_1} P_2^{r_2} .. P_k^{r_k} \quad (r_i \geq 0),\ i = 1,..., k,$$

trong đó $n = \sum_{i=1}^{k} r_i$ cho trước.

Kiểm định giả thuyết H_0: $P_1 = P_1^0$, $P_2 = P_2^0$, ..., $P_k = P_k^0$, ($P_1^0, P_2^0, ..., P_k^0$ cho trước). Đối thuyết H_1: tồn tại i để $P_i \neq P_i^0$.

Khi đó đại lượng ngẫu nhiên:

$$-2\ln\lambda_{H_0} = -2n\sum_{i=1}^{k} \overline{P_i} \ln\frac{P_i^0}{\overline{P_i}} = -\sum_{i=1}^{k} 2n\frac{m_i}{n} \ln\frac{nP_i^0}{m_i} = \sum_{i=1}^{k} 2m_i \ln\frac{m_i}{nP_i^0} \quad (2.10)$$

có phân bố χ^2 với k-1 bậc tự do (giả thuyết H_0 đúng), với

$$\lambda_{H_0} = \left[\left(\frac{P_1^0}{\overline{P_1}} \right)^{\overline{P_1}} \left(\frac{P_2^0}{\overline{P_2}} \right)^{\overline{P_2}} ... \left(\frac{P_k^0}{\overline{P_k}} \right)^{\overline{P_k}} \right]^n$$ (theo bổ đề 2.2, 2.3 và ước lượng hợp lý nhất [108]) trong đó $\overline{P_i} = \frac{m_i}{n}$ (i =1,…, k) với m_i là tần suất xuất hiện biến cố i nào đó trong dãy n phép thử độc lập.

Chú ý: Trong thực nghiệm, t(α) trong (2.9) thường được chọn là 1, và P_i^0 nếu không cho trước thường được ước lượng bằng phương pháp hợp lý nhất, bằng cách thay P_i^0 bằng $\overline{P_i^0}$ với i =1,..., k. Do vậy công thức (2.10) có thể đơn giản thành:

$$-2\ln\lambda_{H_0} \approx \sum_{i=1}^{k} 2m_i \ln\frac{\overline{P_i}}{P_i^0} = \sum_{i=1}^{k} m_i 2\ln\frac{\overline{P_i}}{P_i^0} \quad (2.11)$$

Lúc đó đại lượng ngẫu nhiên $\sum_{i=1}^{k} m_i 2\ln\frac{\overline{P_i}}{P_i^0}$ có phân bố χ^2 với k-1 bậc tự do.

Nhưng nếu chọn k=1 thì đương nhiên $\sum m_i 2\ln\frac{\overline{P_i}}{P_i^0} > \ln k = \ln 1 = 0$ với H_0 đúng.

Hay:

$$\begin{cases} \sum_{i=1}^{k} m_i \ln\frac{\overline{P_i}}{P_i^0} > 0 & \text{nếu } H_0 \text{ đúng} \\ \sum_{i=1}^{k} m_i \ln\frac{\overline{P_i}}{P_i^0} < 0 & \text{nếu } H_1 \text{ đúng} \\ \sum_{i=1}^{k} m_i \ln\frac{\overline{P_i}}{P_i^0} = 0 & \text{thì chưa có kết luận} \end{cases} \quad (2.12)$$

Đây là bài toán tối ưu theo nghĩa xác suất α cho trước, cực tiểu hoá xác suất β.

Áp dụng vào bài toán phát hiện ảnh có giấu tin trên LSB ta được hai phương pháp phát hiện sau đây:

1/. Phương pháp 1

Áp dụng bổ đề 2.2 cho phân loại tập ảnh có giấu tin trên LSB, trong trường hợp không biết trước ảnh gốc của mỗi ảnh, chúng ta phải xây dựng một ảnh làm "mốc" bằng cách tìm một ảnh có kích thước xấp xỉ (độ rộng hàng và cột, nếu tương đồng biểu đồ tần suất càng tốt) ảnh cần phân loại.

Sử dụng hệ thức (2.12) làm cơ sở cho việc phát hiện ảnh có hay không chứa thông tin ẩn. Trong ứng dụng thực tế, nếu $\overline{P_i} \neq \overline{P_i^0}$ thì việc kiểm định giả thiết mới có ý nghĩa. Mặc dù vậy có thể $\overline{P_i} \neq \overline{P_i^0}$ với $\forall$i, (nếu $\exists$i:$\overline{P_i} = \overline{P_i^0}$ thì loại ra khỏi công thức), nhưng sự khác biệt không lớn lắm. Trường hợp như vậy, hệ thức (2.12) để

kiểm định giả thuyết H_0 cho độ chính xác không cao. Do đó, khi áp dụng vào việc phát hiện ảnh có hay không chứa thông tin ẩn, luận án đã cải tiến như sau:

Chúng ta biết rằng do tính chất của logarit với ∀t, ta đều có: $t\ln\frac{\overline{P_i}}{P_i^0} = \ln\left(\frac{\overline{P_i}}{P_i^0}\right)^t$. Do đó nếu chọn $t \geq 2$ thì $\left(\frac{\overline{P_i}}{P_i^0}\right)^t$ sẽ được tăng hoặc giảm lên t lần tùy theo $\frac{\overline{P_i}}{P_i^0} > 1$ hay $\frac{\overline{P_i}}{P_i^0} < 1$. Với t càng lớn thì sự khuyếch đại càng lớn nếu $\frac{\overline{P_i}}{P_i^0} > 1$ và ngược lại.

Thực tế giá trị của t phụ thuộc vào kích thước của ảnh, kích thước ảnh càng lớn, t càng lớn sao cho nó có khả năng phân loại tốt.

Cách phát hiện khi không có ảnh gốc

Giả sử có một ảnh bất kỳ Z, kiểm tra xem ảnh Z có giấu tin trên LSB hay không.

Khi không có ảnh gốc để kiểm tra chúng ta phải chọn một ảnh làm "mốc" như sau: chọn một ảnh gốc U có kích thước n = p * q xấp xỉ ảnh Z, tính tần suất các điểm ảnh được vector X={x_i, i = 0, ..., 255}. Đặt $P_i^0 = \frac{x_i}{n}$.

Nhúng thông tin vào LSB của ảnh U theo thuật toán giấu LSB ngẫu nhiên với giấu có tỷ lệ 100% trên LSB được ảnh stego S có chứa tin mật.

Ký hiệu $\overline{P_i} = \frac{y_i}{n}$ (y_i là tần suất xuất hiện điểm ảnh i trong ảnh stego S).

Tiếp theo lập vector C={c_i, $c_i = \left[t\ln\frac{\overline{P_i}}{P_i^0}\right]$, i = 0, ..., 255} (2.13)

([x] là phép toán lấy giá trị nguyên của x).

Giá trị t được chọn sao cho: max{c_i} – min{c_i} ≥ 400, i = 0, …, 255. Việc lựa chọn này dựa trên đánh giá trên cùng một tập ảnh (gồm 500 ảnh) với các giá trị t khác nhau, để có được giá trị t phù hợp việc lựa chọn như $\chi_i^2(\alpha)$ (tương tự trong 2.1.2.2).

Tính tần suất điểm ảnh của ảnh Z (ảnh cần kiểm tra) được vector F={f_1, f_2, ..., f_{255}}. Lập tích vô hướng: $c_f = \sum_{i=0}^{255} c_i f_i$, (với c_i tính theo (2.13))

Nếu c_f > 0, kết luận Z là ảnh có giấu tin trên LSB.

Nếu c_f < 0, kết luận Z là ảnh không giấu tin trên LSB.

Nếu c_f = 0, thì chưa có kết luận.

2. Phương pháp 2

Phương pháp thứ 2 phân loại ảnh theo công thức (2.11) như sau:

$$-2\ln\lambda_{H_0} = -2n\sum_{i=1}^{k}\overline{P_i}\ln\frac{P_i^0}{\overline{P_i}} = -\sum_{i=1}^{k}2n\frac{m_i}{n}\ln\frac{nP_i^0}{m_i} = \sum_{i=1}^{k}2m_i\ln\frac{m_i}{nP_i^0}$$

Đặt T= $\sum_{i=1}^{k} 2m_i \ln \frac{m_i}{nP_i^0}$ có phân bố χ^2 k-1 bậc tự do khi giả thuyết H_0 đúng, tức là có xác xuất: P ($T \geq t_0$) = $\int_{t_0}^{\infty} p_n(t)dt$

Trong đó $p_n(t)$ là hàm mật độ xác suất. Ta có thể xác định được t_0 qua phương trình sau:

$$\int_{t_0}^{\infty} p_n(t)dt = 1 - \int_{-\infty}^{t_0} p_n(t)dt = 1 - \alpha_0$$

Nếu biết được n và $\alpha = \alpha_0$, ta có thể xác định được t_0 bằng cách tra bảng χ^2 với k - 1 bậc tự do trong với k =256, độ tin cậy α = 0.1, ta được t_0 = 284.33.

Chọn một ảnh gốc C bất kỳ có kích thước n = p * q, thống kê tần số của các điểm ảnh lưu vào vector một chiều X = {x_i | i= 0,..., 255}. Đặt $\overline{P_i^0} = \frac{x_i}{n}$.

Sử dụng thuật toán giấu tin LSB bằng phương pháp giấu ngẫu nhiên để tạo ra 11 ảnh có giấu tin (ký hiệu S_0, .., S_10) có tỉ lệ tin giấu trên miền LSB từ 0 % đến 100 % (mỗi lần tăng lên 10%). Sau đó mỗi ảnh ta thống kê tần suất điểm ảnh được véc tơ Y = {y_i | i = 0,..., 255}.

Ký hiệu $\overline{P_i} = \frac{x_i}{n}$ với i = 0,..., 255. Áp dụng công thức (2.11) được: $T=\sum_{i=0}^{255} 2x_i \ln \frac{\overline{P_i}}{\overline{P_i^0}}$ cho mỗi cặp ảnh (C, S_i) i = 0,...,10 ta được kết quả trong bảng 2.1.

Bảng 2.1: Kết quả thử nghiệm đánh giá T

Lượng tin giấu (%)	0	10	20	30	40	50	60	70	80	90	100
(C, S_i)	0	159.4	454.30	807	924.6	1064.8	1020.20	1167.40	1279	1352.20	1660.80

Vấn đề ở chỗ chúng ta không biết trước ảnh gốc, làm thế nào để phát hiện một ảnh bất kỳ có giấu thông tin hay không. Nghiên cứu thực nghiệm trên các ảnh giấu tin thấy rằng các cặp giá trị (x_{2i}, x_{2i+1}) càng gần nhau khi lượng thông tin giấu tăng lên, điều đó làm cho S cũng tăng lên. Khi không có ảnh gốc để so sánh, chúng ta có thể coi "mốc" so sánh là ảnh được giấu 100% trên miền LSB, khi đó các cặp POV có giá trị rất gần nhau, tức là $x_{2i} \approx x_{2i+1} = \frac{x_{2i}+x_{2i+1}}{2}$. Khi đó giá trị S sẽ thay đổi như bảng 2.2. Dựa vào bảng này chúng ta có thể chọn t=500 làm ngưỡng để phân loại một cách tin cậy với tỉ lệ giấu xấp xỉ từ 30% trở lên.

Bảng 2.2: Kết quả thử nghiệm đánh giá T

Lượng tin giấu (%)	0	10	20	30	40	50	60	70	80	90	100
(C, S_i)	1477.20	1537.9	749.9	587.7	496.8	485	427.90	357.10	228.80	172.4	133.80

2.1.4. Phát hiện bằng phương pháp ước lượng thông tin giấu trên miền LSB

2.1.4.1. Phương pháp ước lượng khi có ảnh gốc

Để ước lượng thông tin giấu trên LSB dựa trên lý thuyết trùng khớp sau:

Định lý 2.4: Cho X_0, X_1 là hai đại lượng ngẫu nhiên độc lập nhau, có phân bố lần lượt là p0(t), p1(t) khi đó

$$P\{X_{0,i}=X_{1,i}\} = \sum_{0\le t\le m-1} p_0(t).p_1(t)$$

Sau đây là nội dung cụ thể của phương pháp.

Để ứng dụng định lý 2.4 vào bài toán ước lượng thông tin nhúng trong ảnh số. Ta cần xác định được $P_0(t)$, $P_1(t)$. Trong trường hợp m=2, tức là t chỉ nhận một trong hai giá trị 0 hoặc 1. Để đơn giản ở đây ta xét ngôn ngữ của thông tin được nhúng là tiếng Anh. Từ [37] thống kê trên 10000 ký tự các văn bản tiếng Anh chính thống, tần số đơn các ký tự trong văn bản tiếng Anh tự nhiên xuất hiện không đều. Trong đó ký tự e xuất hiện nhiều nhất (chiếm 12.9%) so với tổng số các ký tự xuất hiện trong văn bản. Còn chữ z xuất hiện rất ít (chiếm 0.05%). Chuyển các ký tự trong một bản rõ bất kỳ sang chuỗi nhị phân với mỗi ký tự thành chuỗi 8 bit, ta thấy giá trị trung bình chữ số 0 xuất hiện trong văn bản xấp xỉ bằng E[X=0]=2.4912, đem chia cho 8 (độ dài bit của một ký tự chữ cái) ta có 1/8*E[X=0]=0.3114, đây chính là xác suất để chữ số 0 xuất hiện trong văn bản tiếng anh dưới dạng nhị phân tức là $P_0(t=0)=0.3114$ và do đó $P_0(t=1)=1-0.3114=0.6886$. Còn $P_1(t=0)$ và $P_1(t=1)$ trên LSB của ảnh gốc được ước lượng bằng phương pháp hợp lý cực đại cho ta kết quả như sau: $P_1(t=0)\approx 0.505$, $P_1(t=1)\approx 0.495$.

Vậy xác suất xuất hiện trùng khớp với bit thông tin và bit LSB của gốc là: $P_0(t=0) \cdot P_1(t=0) + P_0(t=1) \cdot P_1(t=1) = 0.3114 * 0.505 + 0.6886 * 0.495 = 0.498114 \approx 0.5$.

Giả sử ta có $X = x_1x_2x_3.....x_n$ là một chuỗi thông tin bất kỳ với $x_i \in \{0,1\}$ i=1,2,...,n và $Y = y_1y_2y_3...y_m$ là dãy các bit LSB của các điểm ảnh của một ảnh gốc nào đó (ảnh 24 bit màu hoặc ảnh cấp xám 8-bit) tức $y_i \in \{0,1\}$. Theo ước lượng trên ta có $P\{x_i=y_i\} \approx 0.5$, vì độ dài bản thông tin tính ra bit là n, nên số các điểm ảnh không bị đảo bit (bitwise) ở LSB sẽ xấp xỉ là $\frac{n}{2}$. Như vậy nếu ta ước lượng được số điểm ảnh bị đảo bit là bao nhiêu thì ta có thể ước lượng xấp xỉ được độ dài bản thông tin được giấu trong ảnh.

Để ước lượng độ dài thông tin giấu trong LSB ảnh ta thực hiện các khảo sát sau:

Có 2 ảnh C_1, C_2, hai ảnh này sau đó được giấu tin với tỉ lệ thông tin lần lượt bằng 12% và 9 % kích thước hai ảnh S_1 và S_2. Thống kê tần số các điểm ảnh của từng cặp ảnh (C_i,S_i) lưu vào các cặp vector (C_i^{256}, S_i^{256}) và tính hiệu $|C_i^{256} - S_i^{256}|$ ta thấy rằng nếu $S_i^j=C_i^j$ tức là không nhúng thông tin, nghĩa là $|S_i^j - C_i^j| =0$. Ngược lại, $|S_i^j-C_i^j| >0$ là do lượng tin được nhúng vào trong C_i đã làm cho các điểm ảnh có sự thay đổi. Mỗi điểm ảnh cùng lắm chỉ nhúng được 1 bit thông tin do đó tổng các

hiệu $\sum_{j=0}^{255}|C_i^j - S_i^j|$ chính là số các bit thông tin đã được nhúng. Nếu gọi n_i là độ dài số bit của thông tin đã được nhúng trong ảnh gốc C_i thì theo định lý 2.4, ta có ước lượng:

$$n_i - \frac{n_i}{2} \approx \sum_{j=0}^{255}|C_i^j - S_i^j| \quad \Leftrightarrow \quad n_i \approx 2\sum_{j=0}^{255}|C_i^j - S_i^j| = N_i \tag{2.14}$$

Nếu cho trước một cặp ảnh gốc và ảnh có giấu thông tin tương ứng, chúng ta có thể ước lượng được độ dài (tính theo bit) của bản thông tin đã được nhúng trong ảnh đó.

Xét lại ví dụ, áp dụng (2.14) với cặp ảnh (C_1, S_1) ở trên ta có $2\sum_{j=0}^{255}|C_1^j - S_1^j| =$ 30440. Vậy độ dài thông tin nhúng trong S_1 là $n_1 \approx 30440$ chiếm tỉ lệ (so với kích thước của ảnh) là $\frac{30440}{393216} \approx 7.74\%$. Xét cặp ảnh ($C_2$, S_2) ta có $2\sum_{j=0}^{255}|C_2^j - S_2^j|$ =22348, chiếm tỉ lệ nhúng là $\frac{22348}{393216} \approx 5.68\%$.

Vấn đề đặt ra ở đây là một số trường hợp trong thực tế chúng ta không biết trước ảnh gốc mà chỉ biết ảnh quan sát nào đó, chúng ta phải tìm cách xây dựng một ảnh làm "mốc" từ ảnh quan sát.

2.1.4.2. Phương pháp ước lượng khi không có ảnh gốc

Khi không có ảnh gốc chúng ta cần phải xây dựng một ảnh làm "mốc" từ một ảnh được xét. Theo [95] sau khi giấu chuỗi bit thông tin với tỉ lệ 100% trên miền LSB của ảnh C (xấp xỉ 12.5% kích cỡ của ảnh), thì giá trị tần suất của các cặp PoV (x_{2i}, x_{2i+1}) xấp xỉ bằng nhau. Từ đó đưa ra ý tưởng một ảnh bất kỳ với vector tần số điểm ảnh $X=\{x_0, x_2, x_3, \ldots, x_{255}\}$, ta có thể ước lượng vector tần số điểm ảnh $Y=\{y_0, y_1, \ldots, y_{255}\}$ với:

$$y_{2i} = y_{2i+1} = \frac{x_{2i} + x_{2i+1}}{2}, \; i=0,\ldots 127 \tag{2.15}$$

Sau đó ta có thể ước lượng xấp xỉ tỉ lệ thông tin giấu trong ảnh theo công thức sau: $L=\frac{pq}{8pq}100 - [\frac{1}{pq}\sum_{i=0}^{255}abs(x_i - y_i)] .100$ (2.16)

Nếu ảnh có giấu tin thì giá trị của $|x_i-y_i|$ tiến tới 0 và L tiến tới 12.5. Trường hợp ảnh là ảnh gốc thì $[\frac{1}{pxq}\sum_{i=0}^{255}abs(x_i - y_i)] *100$ tiến tới 12.5 và L tiến tới 0.

Thực tế, ảnh khi giấu thông tin với tỉ lệ giấu trên 100% LSB của ảnh (ứng với 12.5% kích cỡ ảnh) không hoàn toàn làm cho $y_{2i}=y_{2i+1}=(x_{2i}+x_{2i+1})/2$ theo (2.15), vì vậy công thức (2.16) được thay đổi với sai số Δx như sau:

$$L=\frac{pq}{8pq}100 - [\frac{1}{pq}\sum_{i=0}^{255}abs(x_i - y_i)] .100-\Delta x \tag{2.17}$$

Dựa vào thực nghiệm trên một tập ảnh lớn tác giả thấy Δx=3.5 cho kết quả tin cậy.

Để đưa ra ước lượng xấp xỉ với tỉ lệ giấu trên miền LSB ứng với tỉ lệ 0%, 10%, 20%, …, 100%. Chúng tôi thực hiện khảo sát trên một tập 10 ảnh chuẩn cùng kích cỡ 512×512 tải về từ [107]. Sau đó chúng ta thực hiện giấu tin bằng kỹ thuật giấu LSB phương pháp ngẫu nhiên trên tập ảnh này với tỉ lệ giấu 0%, 10%, ... 100%. Thực hiện ước lượng cho từng tập ảnh ta được giá trị ước lượng cho trong bảng 2.4.

Bảng 2.4. Ước lượng xấp xỉ thông tin giấu trên LSB với tập 10 ảnh chuẩn

Lượng tin giấu (%)	0	10	20	30	40	50	60	70	80	90	100
Tỉ lệ ước lượng xấp xỉ	0	0.07	0.23	0.47	0.8	1.49	1.9	2.69	4.03	5.73	6.68

Từ đó chúng tôi xây dựng được phương trình bậc hai ước lượng xấp xỉ từ bảng dữ liệu trên như sau: $-3.54x^2 + 38.64x=y$ (2.18)

Do đó, ứng với mỗi giá trị L tìm được từ (2.17) của ảnh ta thay x=L vào phương trình (2.18) ta sẽ nhận được y tương ứng chính là lượng thông tin xấp xỉ đã giấu vào ảnh.

Vậy áp dụng (2.18) cho bảng 2.4 ta được giá trị xấp xỉ mới theo bảng 2.5. Để đánh giá giá trị ước lượng xấp xỉ đối với mỗi ảnh ứng với tỉ lệ nhúng p chúng ta tính trị trung bình $\bar{x}(p)$ và độ lệch chuẩn s(p) cho mỗi p trên 10 ảnh

Bảng 2.5. Kết quả ước lượng xấp xỉ theo (2.18) trên tập 10 ảnh chuẩn

Lượng tin giấu (%)		0	10	20	30	40	50	60	70	80	90	100
Tỉ lệ ước lượng xấp xỉ	$\bar{x}(p)$	0	2.68	8.94	17.59	28.84	49.93	60.64	78.33	98.26	100.02	100.07
	s(p)	0	0.07	0.24	0.48	0.81	1.49	1.90	2.69	4.03	5.73	6.68

2.2. KỸ THUẬT PHÁT HIỆN MÙ TRÊN LSB CỦA MIỀN TẦN SỐ

2.2.1. Phân tích kỹ thuật giấu LSB trên miền tần số

Giấu tin trên miền tần số cosine hay wavelet là hình thức giấu tin trên LSB của các hệ số cosine trên miền tần số giữa như các kỹ thuật [23, 69, 70, 94, 104] hay trên các băng tần cao LH, HL, HH như các kỹ thuật [42, 73, 91]. Theo nhận định của các nhà giấu tin phương pháp giấu trên các hệ số này không làm ảnh hưởng đến chất lượng ảnh.

Theo Provos và các cộng sự, kỹ thuật giấu thông tin trên LSB của các hệ số cosine cũng gây ra cân bằng các cặp PoV của hệ số cosine [71]. Do đó nhóm tác giả áp dụng phương pháp thống kê χ^2 với n bậc tự do cho các cặp PoV của hệ số cosine …, (-8, -7), (-6,-5), (-4, -3), (-2, -1), (2, 3), (4, 5), (6, 7)… không kiểm tra trên cặp (0, 1) vì cặp này ít sử dụng trong giấu tin [104].

Luận án thấy rằng phương pháp thống kê này cũng có thể áp dụng tương tự cho phát hiện ảnh có giấu tin trên miền tần số wavelet, vì nó cũng làm cân bằng các cặp PoV trên các hệ số wavelet.

Ngoài ra luận án đưa ra một phương pháp khác phát hiện mù cho ảnh có giấu tin trên LSB của các hệ số cosine cho kết quả tốt hơn trình bày trong mục sau.

2.2.2. Phương pháp phát hiện

Áp dụng biểu thức (2.11) được xây dựng từ mở rộng bổ đề Neyman – Pearson trong 2.1.3 cho miền tần số cosine ta có thuật toán dưới đây. Trong trường hợp không có ảnh gốc để so sánh chúng ta phải xây dựng một ảnh làm "mốc" bằng cách coi như ảnh được giấu tin với tỉ lệ giấu 100% tổng số các hệ số cosine có thể giấu của ảnh.

Thuật toán áp dụng cho ảnh giấu tin trên LSB của miền tần số DCT

Đầu vào: Cho một tập ảnh JPEG bất kỳ (gồm có giấu tin trên hệ số cosine và ảnh gốc)

Đầu ra: Phân loại tập đó thành hai tập: ảnh có giấu trên tin và ảnh không giấu tin trên LSB của hệ số cosine.

Các bước thực hiện

Bước 1: Chọn ảnh I trong tập ảnh đầu vào, thực hiện các bước 2 và 3 cho đến khi xét hết các ảnh đầu vào.

Bước 2: Thống kê tần số các hệ số DCT của ảnh I (bỏ qua các hệ số 0 và 1) vào ma trận $X^n = \{x_i, i=1, 2, ..., n\}$ (giá trị n được xác định từ số các hệ số (trừ hệ số "0" và "1") có tần số lớn hơn 0) với x^i là tần số của hệ số cosine có giá trị i. Thực hiện tính P_j^0 với $P_{2j}^0 = P_{2j+1}^0 = \frac{x_{2j}+x_{2j+1}}{2}$ $(0<j<\frac{n}{2})$.

Áp dụng công thức (2.11) ta có: $T = \sum_{i=0}^{n} 2x_i \ln \frac{x_i}{(pq)P_i^0}$.

Bước 3: Chọn $t_0 = 500$ (theo tập mẫu thử nghiệm trên 1200 ảnh). Nếu $T > t_0$ thì I lưu vào tập ảnh gốc, ngược lại I lưu vào tập ảnh có giấu tin trên LSB của hệ số cosine.

2.3. KẾT QUẢ THỬ NGHIỆM

2.3.1. Các kết quả thử nghiệm trên miền không gian

Thử nghiệm trên tập 2088 ảnh để so sánh đánh giá các kỹ thuật đề xuất của luận án với kỹ thuật phát hiện khác: χ_n^2 [95], LLRT [80], RS [31], DI[102].

2.3.2. Các kết quả thử nghiệm trên miền tần số

KẾT LUẬN CHƯƠNG 2

Chương này đưa ra bốn phương pháp cải tiến phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian và một phương pháp phát hiện mù trên LSB của miền tần số. Dựa trên tập thử nghiệm gồm 2088 ảnh để so sánh kỹ thuật cải tiến của luận án với một số kỹ thuật phát hiện mù khác.

Các kết quả thử nghiệm cho thấy các kỹ thuật phát hiện do luận án đưa ra trong chương này là tương đương hoặc tốt hơn kỹ thuật phát hiện khác trong một số trường hợp.

Chương 3. MỘT SỐ KỸ THUẬT PHÁT HIỆN CÓ RÀNG BUỘC

Chương này đưa ra bốn kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng kỹ thuật giấu tin DIH, IWH, HKC, RVH. Chúng đều là trường hợp riêng của kỹ thuật giấu LSB, tuy nhiên tỉ lệ thay đổi trên LSB của ảnh thường thấp so với lượng thông tin đem giấu (hoặc kích cỡ ảnh), vì vậy phát hiện bằng các kỹ thuật phát hiện mù trên LSB của ảnh thường cho kết quả không cao. Trong phần này luận án đưa ra các phương pháp phát hiện tối ưu hơn so với phát hiện mù trên LSB cho các kỹ thuật giấu DIH, IWH, HKC, RVH và phương pháp ước lượng xấp xỉ lượng bit thông tin giấu trong ảnh sử dụng các kỹ thuật này.

3.1. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU HKC

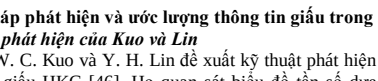
3.1.1. Tóm lược kỹ thuật giấu HKC

Kỹ thuật HKC do J. H. Hwang và các cộng sự đề xuất năm 2006 [41], dựa trên phương pháp dịch chuyển biểu đồ tần suất như sau: chọn điểm Peak là điểm có cột tần suất lớn nhất trong biểu đồ tần suất, sau đó chọn hai điểm Zero1 và Zero2 (các điểm có cột tần suất có giá trị bằng 0) ở bên trái và bên phải điểm Peak. Sau đó thực hiện làm rỗng hai cột tần suất tại vị trí Peak+1 và Peak -1. Thực hiện giấu thông tin vào ảnh theo nguyên tắc: giả sử cần giấu bit b, quét ảnh theo thứ tự raster nếu điểm ảnh có giá trị bằng Peak - 2 hoặc Peak + 2, thì kiểm tra bit b cần nhúng: nếu bit thông tin là "1" thì điểm ảnh có giá trị là Peak - 2 sẽ tăng lên 1, hoặc điểm ảnh có giá trị là Peak + 2 sẽ giảm đi "1", còn nếu bit thông tin là "0" thì vẫn duy trì như cũ (ngầm hiểu đã giấu vào Peak -2 hoặc Peak +2). Quá trình giấu kết thúc khi giấu hết các bit thông tin.

3.1.2. Phương pháp phát hiện và ước lượng thông tin giấu trong ảnh

3.1.2.1. Kỹ thuật phát hiện của Kuo và Lin

Năm 2008, W. C. Kuo và Y. H. Lin đề xuất kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu HKC [46]. Họ quan sát biểu đồ tần số dựa vào đỉnh Peak trước và sau khi giấu thấy hai giá trị lân cận hai bên của đỉnh peak bị tụt xuống do giấu tin như mô tả trong hình 3.1 (a) và (b), vì vậy họ đưa ra định lý 3.1 để xây dựng kỹ thuật phát hiện dưới đây.



Hình 3.1. Điểm Peak: (a) chưa giấu tin, (b) giấu đầy đủ, (c) giấu không đầy đủ

Định lý 3.1: Có năm cặp giá trị liên tiếp (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5) *với* (x_3, y_3) *là cặp giá trị điểm Peak. Tỉ lệ thay đổi của 5 điểm liên tục và mối quan hệ láng giềng được định nghĩa lần lượt như biểu thức (3.1) và (3.2):*

$$\frac{y_3-y_2}{y_3} \approx \frac{y_3-y_4}{y_3} \approx \tau_1, 0.4 \le \tau_1 \le 0.6 \quad (3.1)$$

$$\left|\frac{y_1-y_2}{y_2}\right| \approx \left|\frac{y_4-y_5}{y_4}\right| \le \tau_2 \quad (3.2)$$

τ_2 là giá trị ngưỡng.

Áp dụng định lý này, Kuo và Lin đưa ra thuật toán phát hiện ảnh có giấu tin sử dụng kỹ thuật HKC theo các bước sau:

1. Tìm cặp giá trị điểm peak (x_{max}, y_{max})
2. Tính tỉ lệ thay đổi và mối quan hệ láng giềng sử dụng định lý 3.1.
3. Nếu năm cặp giá trị liên tiếp lân cận (x_{max}, y_{max}) thoả mãn (3.1) và (3.2), thì kết luận ảnh có giấu tin trong vùng này, ngược lại ảnh không giấu tin.

3.1.2.2. Phương pháp phát hiện cải tiến từ phương pháp của Kuo và Lin

Với kỹ thuật phát hiện của Kuo (dựa trên định lý 3.1) trong một số trường hợp giấu tin của HKC nghiên cứu sinh thấy không phù hợp khi thông tin không được giấu hết vào vị trí cột tần số lân cận Peak. Ví dụ như hình 3.1 (a) điểm peak là 146, sau khi giấu tin hai cột giá trị lân cận peak là 145 và 147 bị tụt xuống, nhưng lượng bit giấu ít hơn độ lớn của 2 cột này cho lên giá trị của 144 không bằng 145 và giá trị 147 không bằng 148 (xem hình 3.1 (c)), theo ví dụ ta có y_1=1520, y_2=600, y_3=3300, y_4=580, y_5=1600, kiểm tra lại biểu thức (3.1) và (3.2) ta thấy $(y_3-y_2)/y_3$=0.8182 và $(y_3-y_4)/y_3$ =0.8242 và $\left|\frac{y_1-y_2}{y_2}\right|$ =1.5333 và $\left|\frac{y_4-y_5}{4}\right| = 1.7586$ không thỏa mãn (3.1) và (3.2)

Để có thể phát hiện một cách tổng quát hơn với kỹ thuật của Kuo và Lin chúng tôi đưa ra định lý 3.2 chỉnh sửa của Kuo và Lin như sau:

Định lý 3.2: Có năm cặp giá trị liên tiếp (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5) trong đó (x_3, y_3) là cặp giá trị điểm Peak. Khi đó ảnh có giấu tin sử dụng kỹ thuật giấu HKC nếu mối quan hệ của năm cặp giá trị này thỏa mãn biểu thức (3.1') và (3.2'):

$$\frac{y_3-y_2}{y_3} \approx \frac{y_3-y_4}{y_3} \approx \tau_1, 0.4 \le \tau_1 < 1 \qquad (3.1')$$

$$\frac{y_2}{y_1} \approx \frac{y_4}{y_5} <= 1 \qquad (3.2')$$

Áp dụng định lý này vào bài toán phát hiện ảnh giấu sử dụng HKC.

3.1.2.3. Phương pháp phát hiện HKC khác và ước lượng thông tin

Mặt khác chúng ta thấy có thể đưa ra biểu thức đơn giản hơn phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu HKC. Dựa vào phân tích ví dụ: ảnh gốc ban đầu có biểu đồ tần số như hình 3.1 (a) tổng hai cột giá trị lân cận (h_{144}, h_{145}) bên trái và hai cột giá trị lân cận bên phải (h_{147}, h_{148}) của điểm Peak (h_{146}) luôn lớn hơn Peak (tức $h_{144}+h_{145} > h_{146}$, $h_{147}+h_{148} > h_{146}$), trong khi với biểu đồ tần số của ảnh có giấu tin hình 3.1 (c) thì $h_{144}+h_{145} < h_{146}$, $h_{147}+h_{148} < h_{146}$.

Cũng dựa vào mối quan hệ bị thay đổi này giữa các vùng lân cận h_{Peak} chúng ta có thể ước lượng được số bit thông tin giấu trong ảnh dựa vào h_{Peak-1} và h_{Peak+1}. Ban đầu để giấu tin chúng ta phải dịch chuyển h_{Peak-1} sang h_{Peak-2}, h_{Peak+1} sang h_{Peak+2}, nghĩa là làm cho h_{Peak-1}= 0, h_{Peak+1} = 0. Sau khi giấu tin các bit "1" của chuỗi thông tin làm dịch chuyển một phần h_{Peak-2}, h_{Peak+2} sang h_{Peak-1}, h_{Peak+1} (theo thuật toán giấu HKC) còn các bit "0" ngầm định được giấu vào các điểm ảnh Peak-2 và Peak+2.

Gọi L_0, L_1 là số bit "0" và bit "1" của chuỗi thông tin M cần giấu khi đó: $L_1 = h_{Peak-1} + h_{Peak+1}$, còn $L_0 \approx L_1$ vì chuỗi thông tin M là đại lượng ngẫu nhiên có phân bố i.i.d [61] nên xác suất bit "0" và xác suất bit "1" xấp xỉ bằng nhau và bằng 0.5 (P(0)≈ P(1) =0.5). Vậy độ dài bit thông tin M được giấu trong ảnh sử dụng HKC được tính theo biểu thức sau: $L = 2L_1 = 2(h_{Peak-1} + h_{Peak+1})$.

Từ các vấn đề phân tích ở trên chúng ta có được định lý 3.3 cho phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu HKC.

Định lý 3.3 - Có năm cặp giá trị liên tiếp (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5) *với điểm Peak (điểm max) là* x_3 *và* $y_3 = h_{Peak}$. *Khi đó ảnh có giấu tin bằng HKC nếu thỏa mãn mối quan hệ sau:*

$$y_1 + y_2 < y_3 \quad (3.3)$$

$$y_4 + y_5 < y_3 \quad (3.4)$$

và lượng bit thông tin đã giấu được tính bằng biểu thức:

$$L = 2(y_2 + y_4) \quad (3.5)$$

Áp dụng định lý 3.3 chúng ta có thể phát hiện và ước lượng số bit thông tin cho ảnh có giấu tin bằng kỹ thuật HKC.

3.1.3. Các kết quả thử nghiệm

3.1.3.1. Thử nghiệm: thử nghiệm và đánh giá trên tập 2088 ảnh, so sánh phát hiện giữa các kỹ thuật của Kuo và Lin, của Kuo và Lin được cải tiến, kỹ thuật đề xuất.

3.1.3.2. Nhận xét

3.2. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU DIH

3.2.1. Tóm lược kỹ thuật giấu tin DIH

Kỹ thuật giấu thuận nghịch dựa trên biểu đồ giá trị sai phân DIH (Difference Image Histogram) do nhóm tác giả Lee và các cộng sự đề xuất năm 2004 [82]. Ban đầu nhóm tác giả tính các giá trị sai phân của các điểm ảnh theo công thức d(i,j)=I(i+1,j)-I(i,j) và tính biểu đồ tần số cho các giá trị sai phân này. Họ thấy rằng các giá trị tần số tập trung phần lớn vào các hệ số sai phân có giá trị -2, -1, 0, 1, 2 do đó có thể giấu thông tin dựa vào các giá trị này. Để giấu có thể khôi phục ảnh gốc, họ sẽ phải dịch chuyển các cột tần số có giá trị sai phân lớn hơn 1 và nhỏ hơn -1 để làm rỗng các cột tần số có giá trị bằng 2 và -2. Sau đó chuỗi bit thông tin sẽ được giấu vào các điểm ảnh mà giá trị sai phân của nó có giá trị là 1 hoặc -1, nếu bit thông tin giấu là 1 thì hệ số sai phân nếu là 1 chuyển thành 2, nếu là -1 chuyển thành -2, ngược lại giữ nguyên.

3.2.2. Phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu DIH

3.2.2.1. Phân tích kỹ thuật giấu DIH

Theo quá trình giấu tin trong phần 3.2.1 chúng ta thấy rằng kỹ thuật giấu DIH chỉ giấu được một lượng tin rất thấp, khả năng giấu phụ thuộc vào tần suất của hệ số sai phân bằng 1 và -1. Ví dụ ta có Lena.bmp kích cỡ 512×512 điểm ảnh thì khả năng giấu số bit lớn nhất của ảnh là $L = h_{-1} + h_1 = 19877$ (tương đương với tỉ lệ giấu lớn nhất R_{max}=7.58). Tỉ lệ giấu này chỉ làm thay đổi rất nhỏ nội dung ảnh gốc.

Chúng ta sử dụng một số phương pháp phát hiện mù trên LSB trong chương 2 để phát hiện ảnh có giấu tin bằng kỹ thuật giấu DIH như sau: sử dụng tập ảnh $\boldsymbol{C}_{0_1}$ gồm 600 ảnh (lấy ra từ tập ảnh gốc $\boldsymbol{C}_0$) cùng giấu thông tin là dữ liệu ảnh nhị phân kích cỡ 128×56 điểm ảnh (tương ứng với chuỗi 7168 bit) được tập ảnh $\boldsymbol{S}_{\text{DIH_7168}}$. Sau đó sử dụng một số kỹ thuật phát hiện mù trên LSB cho tập ảnh $\boldsymbol{S}_{\text{DIH_7168}}$ được kết quả phát hiện trong bảng 3.1.

Bảng 3.1. Phân loại ảnh trên tập $\boldsymbol{S}_{\text{DIH_7168}}$ sử dụng kỹ thuật phát hiện mù trên LSB

	"Độ lệch chuẩn"	χ^2	*"Tỉ lệ xám"*	χ_o^2 *[95]*	*LLRT [80]*
Ảnh gốc	462	582	406	595	297
Ảnh có giấu tin	138	18	194	5	303

Để kiểm tra bằng phương pháp ước lượng thông tin giấu trên LSB của ảnh, luận án sử dụng ảnh Lena.bmp giấu một lượng thông tin là dữ liệu ảnh nhị phân kích cỡ 128×56 pixel (tương ứng với chuỗi 7168 bit) được tỉ lệ 2.73 % miền LSB của ảnh được ảnh đã giấu tin Lena_stego.bmp. Sử dụng kỹ thuật ước lượng RS, DI, "Trùng khớp" ta được kết quả ước lượng trong bảng 3.2.

Bảng 3.2. Ước lượng thông tin giấu cho ảnh Lena.bmp và ảnh Lena_stego.bmp

	RS [31]	***DI [102]***	***"trùng khớp"***
Lena.bmp	R = 0.15137 %	R = 12 %	R = 0.037 %
Lena_Stego.bmp	R = 6.359 %	R = 9 %	R = 3 %

Từ hai bảng kiểm tra 3.1 và 3.2 có thể thấy rằng đa số kỹ thuật phát hiện mù trên LSB chỉ phát hiện tốt với tỉ lệ giấu cao còn trong trường hợp này tỉ lệ giấu so với kích cỡ của ảnh là quá nhỏ (7168 bit chỉ bằng từ 2 đến 3% miền LSB của ảnh). Vì vậy dựa vào phân tích đặc trưng của tập ảnh gốc và ảnh sau khi giấu tin sử dụng kỹ thuật giấu DIH luận án này đưa ra phương pháp phát hiện tối ưu hơn và có thể ước lượng thông tin đã giấu trong ảnh trong mục tiếp theo.

3.2.2.2. Phương pháp phát hiện và ước lượng thông tin

Bằng phương pháp phân tích biểu đồ tần số sai phân của ảnh trước và sau khi giấu tin chúng ta có thể phát hiện và ước lượng được xấp xỉ ảnh có giấu tin sử dụng DIH như sau: khi nhúng một thông tin giống nhau vào một tập ảnh gốc sử dụng kỹ thuật DIH nhận được một tập ảnh stego có giấu tin. Thực hiện tính toán lại biểu đồ tần số sai phân trên từng cặp ảnh (gốc, có giấu tin) chúng ta dễ dàng nhận thấy DIH đã thay đổi tính chất tự nhiên của các giá trị sai phân.

Hay mối quan hệ của các h_i như sau trong ảnh gốc: $h_1 + h_{-1} > h_2 + h_{-2} > h_3 + h_{-3} > \ldots > h_{10} + h_{-10} > \ldots$

Còn đối với ảnh có giấu tin, thì: $h_1 + h_{-1} > h_2 + h_{-2}$, $h_2 + h_{-2} \le h_3 + h_{-3}$.

Sự thay đổi này là do DIH tạo ra, nó thay đổi tần số $h_{\pm 2}$ của ảnh để giấu thông tin. Đây chính là vấn đề mấu chốt để phát hiện ảnh stego, chúng ta đưa ra biểu thức phát hiện sau:

$$S(O) = \begin{cases} \text{ảnh O có giấu tin} & \text{nếu } (h_2 + h_{-2})/(h_3 + h_{-3}) \\ \text{ảnh O không giấu tin} & \text{nếu ngược lại} \end{cases}$$

Với T là ngưỡng để phân loại.

Ngoài ra chúng ta có thể ước lượng xấp xỉ thông tin đã giấu dựa vào $h_{\pm 2}$. Vì thông tin đem giấu là một chuỗi bit có phân bố độc lập nên xác suất số bit 0 xuất hiện trong chuỗi thông tin xấp xỉ bằng xác xuất số bit 1 trong chuỗi và bằng 0.5 (p(0) = p(1) = 0.5). Vì vậy ½ chuỗi thông tin sẽ được giấu trong $h_{\pm 1}$ và phần còn lại được giấu trong $h_{\pm 2}$, do đó độ dài xấp xỉ của thông tin được tính như sau:

$$L = 2*(h_{-2} + h_2)$$

3.2.3. Các kết quả thử nghiệm

3.2.3.1. Thử nghiệm: thử nghiệm và đánh giá trên tập 2088 ảnh

3.2.3.2. Nhận xét

3.3. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU IWH

3.3.1. Tóm lược kỹ thuật giấu tin IWH

Cũng xuất phát từ yêu cầu khôi phục xấp xỉ ảnh gốc sau khi tách thông tin, vào năm 2006 Xuan và các cộng sự đề xuất kỹ thuật giấu IWH (Integer Wavelet Histogram) [99]. Kỹ thuật này có ý tưởng gần giống kỹ thuật giấu tin DIH, tuy nhiên khác ở chỗ thay vì dịch chuyển các cột tần số giá trị sai phân thì họ sử dụng phương pháp dịch chuyển tần số của các hệ số biến đổi wavelet nguyên. Ban đầu họ thực hiện phép biến đổi Wavelet cho miền dữ liệu ảnh theo chuẩn biến đổi trong kỹ thuật nén JPEG2000 để được bốn băng tần (LL, LH, HL, HH). Họ thực hiện nhúng thông tin vào ba băng tần cao LH, HL, HH nơi được cho là ít ảnh hưởng đến ảnh gốc. Tính tần số của các hệ số IWT, các cột tần số có giá trị lớn hơn Z (Z là một số nguyên chọn tùy ý) sẽ bị dịch chuyển sang phải, mục đích làm rỗng cột tần số có giá trị Z, thông tin được giấu vào hệ số có giá trị Z-1 và Z. Nếu trong trường hợp số bit cần giấu lớn hơn số hệ số wavelet có giá trị Z-1, thì thực hiện tiếp giấu thông tin sang hệ số có giá trị -(Z+1) giá trị đối xứng qua hệ số 0, việc thực hiện giấu tương tự, ban đầu chúng ta phải làm rỗng cột tần số -Z, sau đó giấu thông tin vào các hệ số có giá trị là -(Z-1) và –Z. Nếu vẫn còn bit thông tin tiếp tục giấu vào hệ số Z-2, cho đến khi giấu xong thông tin. Giả sử việc giấu dừng lại ở hệ số có giá trị bằng S và hệ số bắt đầu giấu tin là T.

3.3.2. Phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu IWH

3.3.2.1. Phân tích kỹ thuật giấu IWH

Với kỹ thuật giấu IWH chúng ta thấy khó phát hiện tin cậy bằng các phương pháp phát hiện hay ước lượng bằng kỹ thuật trùng khớp như đã nêu trong 3.2. Vì vậy chúng ta phải dựa vào phân tích biểu đồ tần số các hệ số wavelet của ảnh trước và sau khi giấu tin.

3.3.2.2. Phương pháp phát hiện và ước lượng thông tin

Để tấn công và ước lượng thông tin giấu sử dụng kỹ thuật IWH, đầu tiên tác giả đưa ra một số phân tích trong quá trình giấu tin dựa trên 3 thử nghiệm:

Trong thử nghiệm thứ nhất, chúng tôi sử dụng ảnh Lena (kích thước 512 x 512 điểm ảnh) và thông tin giấu là một ảnh Logo nhị phân (128x56 pixel) (ứng với 7168 bit). Tính tần số của các giá trị wavelet trong 3 miền băng tần cao (LH, HL,HH). Nhúng thông tin bằng phương pháp IWH với Peak chọn khởi điểm là T=2, nhận được điểm dừng S=-2.

Thử nghiệm thứ hai, cũng chọn ảnh Lena và thông tin ảnh Logo như thí nghiệm thứ nhất, nhưng nhúng thông tin chọn T=4, nhận được điểm dừng S=3.

Thử nghiệm thứ ba, sử dụng đầu vào tương tự như thử nghiệm thứ nhất nhưng chọn T=6 và nhận được S=-5.

So sánh sự khác biệt giữa biểu đồ tần số các hệ số wavelet của ảnh gốc và ảnh có giấu tin, thấy rằng trong một ảnh điển hình thì $h_0 > h_1 > h_2 > h_3 > \ldots$ và $h_0 > h_{-1} > h_{-2} > h_{-3} > \ldots$ với h_i là số hệ số IW có giá trị bằng i. Trong khi đó với ảnh stego trong thí nghiệm 1 ta thấy $h_4 > h_3$, $h_3 \approx h_2$, $h_{-4} > h_{-3}$, $h_{-3} < h_{-2}$., trong thí nghiệm thứ hai có $h_5 \approx h_6$, $h_{-5} \approx h_{-4}$, $h_4 < h_3$, $h_4 < h_5$, trong thí nghiệm thứ ba $h_7 \approx h_8$, $h_5 \approx h_6$, $h_{-7} \approx h_{-8}$, $h_{-5} \approx h_{-6}$.

Phân tích chi tiết các vấn đề trên trình bày trong toàn văn.

Từ các vấn đề phân tích ở trên, luận án đưa ra thuật toán tổng quát ước lượng độ dài thông tin như sau:

1. Khởi tạo độ dài thông tin L=0, quét toàn bộ tần số với từng giá trị i (i≥0, i≤ max (các hệ số wavelet nguyên của các băng tần cao)), nếu gặp giá trị đầu tiên $(h_i+h_{i+1})/2 < h_{i+2}$, dừng quét, đặt Peak =i là vị trí đầu tiên để ước lượng.
2. Nếu $h_{Peak} \approx h_{Peak+1}$, $L=L+h_{Peak}+h_{peak+1}$; đặt Peak =-Peak và thực hiện tiếp bước 3. Ngược lại thực hiện bước 4.
3. Nếu $h_{Peak} \approx h_{Peak+1}$, $L=L+h_{Peak}+h_{peak+1}$; đặt Peak = -Peak – 1 và quay lại bước 2. Ngược lại quay lại bước 4.
4. Nếu $h_{Peak+1} < h_{Peak+2}$ và $h_{Peak+1} < h_{Peak}$ thì $L= L + 2 * h_{Peak+1}$. Quá trình giấu kết thúc ở đây.

3.3.3. Các kết quả thử nghiệm

3.3.3.1. Thử nghiệm: *thử nghiệm và đánh giá trên tập 2088 ảnh*

3.3.3.2. Nhận xét

3.4. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU RVH

3.4.1. Tóm lược kỹ thuật giấu tin RVH

Giấu tin ngang dọc hay còn gọi là kỹ thuật RVH (Reversible Vertical Horizontal Technique) do P.Mohan Kumar và K.L.Shunmuganathan đề xuất vào tháng 3 năm 2010 [45]. Kỹ thuật giấu này sử dụng chiến lược giấu nhiều lần nhằm nâng cao chất lượng ảnh và dung lượng giấu.

Quá trình giấu tin sẽ chia ra làm 2 giai đoạn: Giai đoạn một gọi là giấu theo chiều ngang HEm (horizontal embedding proceduce) và giai đoạn hai gọi là giấu theo chiều dọc VEm (Vertical embedding procedure). Chuỗi bit thông tin M với độ dài là L_M được chia làm 2 chuỗi con M_1 và M_2 độ dài lần lượt là L_{M1} và L_{M2}. Tạo ra chuỗi thông tin B_1 bằng cách ghép hai chuỗi là chuỗi bit S_1 và chuỗi bit phụ A_1, nghĩa là là $B_1=S_1||A_1$. Tương tự, $B_2=S_2||A_2$. Chuỗi A_1 và A_2 sẽ được giới thiệu ở phía sau. Đầu tiên, các bit thông tin B_1 sẽ nhúng theo chiều ngang vào O bằng thủ tục HEm, cho ảnh ra T. Tiếp theo bản đồ định vị các cặp điểm ảnh được sử dụng để giấu tin được nén nhị phân thành CM_1 có chiều dài là LC_1, CM_1 được nhúng bằng kỹ thuật thay thế LSB tuần tự vào LC_1 bit LSB đầu tiên của ảnh T tạo ra ảnh U, LC_1 bit LSB của ảnh T trước khi nhúng CM_1 được lưu vào A_1 để khôi phục sau này. Tiếp theo chuỗi bit thông tin B_2 được nhúng theo chiều dọc vào U bằng cách sử dụng thủ tục VEm để cho ra ảnh kết quả V. Bản đồ định vị vị trí các cặp điểm ảnh có thể sử dụng giấu tin được nén lại thành CM_2 có chiều dài LC_2, CM_2 được nhúng bằng kỹ thuật thay thế LSB tuần tự vào LC_2 bit LSB đầu tiên của V tạo ra ảnh stego X. LC_1 bit LSB của ảnh V trước khi nhúng CM_2 sẽ được lưu vào A_2.

3.4.2. Phương pháp phát hiện và ước lượng thông tin

3.4.2.1. Phân tích vấn đề giấu tin RVH

Sau khi nhúng một chuỗi thông tin M với dung lượng lớn (tỉ lệ khoảng 90% khả năng nhúng lớn nhất của ảnh) vào ảnh cấp xám cover_Baboon.bmp kích cỡ 512x512 sử dụng kỹ thuật giấu RVH ta được ảnh stego_Baboon.bmp. Tính tần số điểm ảnh của hai ảnh (cover_Baboon.bmp và stego_Baboon.bmp) chúng ta không nhận thấy dấu hiệu khác biệt gì, tuy nhiên khi tính tần số riêng biệt trên các cột

chẵn, các cột lẻ sẽ thấy sự khác biệt rõ rệt trên biểu đồ tần số của chúng, giá trị của cột tần số chẵn sẽ chênh lệch rất lớn so với cột tần số lẻ.

3.4.2.2. Phương pháp phát hiện và ước lượng thông tin

Theo thủ tục nhúng ngang HEm, từ ảnh gốc O, các pixel của ảnh O được nhóm theo hướng ngang thành các cặp (x, y), các cặp này được phân hoạch vào hai tập E_1 và $\overline{E_1}$, tập E_1 bao gồm các cặp pixel (x,y) có thể nhúng ngang, nghĩa là y có giá trị lẻ, trong khi $\overline{E_1}$ là tập chứa các cặp (x,y) không thể nhúng ngang, y có giá trị chẵn. Sau khi giấu B_1 thì ta thấy tần số của số bit 0 và bit 1 của các LSB trên các cột pixel y có sự chênh lệch khá rõ, trong khi với ảnh chưa giấu tin thì tần số của hai bit này xấp xỉ nhau.

Đối với thủ tục nhúng dọc VEm, quét ảnh U theo chiều dọc với thứ tự quét từ trên xuống dưới, từ trái sang phải để nhóm các cặp điểm ảnh (u,v), chúng ta phân loại ảnh vào hai tập E_2 và $\overline{E_2}$, tập E_2 gồm các cặp điểm ảnh có thể sử dụng để nhúng dọc, nghĩa là v có giá trị chẵn, tập $\overline{E_2}$ gồm các cặp điểm ảnh không thể sử dụng nhúng dọc. Sau khi giấu B_2 thì tần số của số bit 0 và bit 1 của các LSB trên các hàng v khác nhau rất rõ khi lượng thông tin giấu lớn.

Từ vấn đề đó chúng ta xây dựng được biểu thức tính xác suất của bit 0 và bit 1 trên các cột (3.6) hoặc trên các hàng (3.7) của ma trận điểm ảnh được xét:

$$P_{LSB_H}(b) = \begin{cases} P_{R-H} \times (0.5 \times P'_{E1} + P'_{\overline{E1}}) + P_{\overline{R-H}} \times 0.5 & \text{nếu } b = 0 \\ P_{R-H} \times (0.5 \times P'_{E1}) + P_{\overline{R-H}} \times 0.5 & \text{nếu } b = 1 \end{cases} \quad (3.6)$$

$$P_{LSB_V}(b) = \begin{cases} P_{R-V} \times (0.5 \times P'_{E2}) + P_{\overline{R-V}} \times 0.5 & \text{nếu } b = 0 \\ P_{R-V} \times (0.5 \times P'_{E2} + P'_{\overline{E2}}) + P_{\overline{R-V}} \times 0.5 & \text{nếu } b = 1 \end{cases} \quad (3.7)$$

Với ảnh gốc thì $P_{LSB_even_H}(0)$ và $P_{LSB_even_H}(1)$ trên các cột chẵn là xấp xỉ nhau, nhưng với ảnh có giấu tin bằng RVH thì chúng chênh lệch nhau.

Dựa vào vấn đề khác biệt tìm ra ở trên, luận án đưa ra biểu thức (3.8) có thể sử dụng để phân biệt ảnh có giấu tin sử dụng kỹ thuật giấu RVH với một ảnh tự nhiên.

$$W(X) = \begin{cases} \text{Đúng} & \text{nếu } |P_{LSB}(0) - P_{LSB}(1)| > T \\ \text{Sai} & \text{nếu ngược lại} \end{cases} \quad (3.8)$$

Từ biểu thức (3.8), một ảnh bất kỳ bị nghi ngờ là ảnh có giấu tin sử dụng kỹ thuật giấu sử dụng kỹ thuật giấu RVH nếu giá trị của $|P_{LSB}(0) - P_{LSB}(1)| > T$, ($0 \leq T \leq 1$) trên các cột lẻ (hoặc cột chẵn) hoặc các hàng chẵn (hoặc hàng lẻ). Ngưỡng T được sử dụng để điều khiển ngưỡng quyết định ảnh đang xét là ảnh có giấu tin sử dụng kỹ thuật RVH hay không. Giá trị của T tùy thuộc vào từng ứng dụng cụ thể. Trong phần thực nghiệm cho thấy với T=0.035 cho kết quả phân loại rất tốt.

Dựa vào sự thay đổi chênh lệch giữa xác xuất của bit "0" và bit "1" theo các hàng chẵn trong ma trận dữ liệu ảnh ta có thể ước lượng sấp xỉ thông tin giấu trong ảnh: $L=2*L_H = 4* |P_{LSB_H}(0) – P_{LSB_H}(1)| * m/2 *n$

3.4.3. Các kết quả thử nghiệm

3.4.3.1. Thử nghiệm: *thử nghiệm và đánh giá trên tập 2088 ảnh*

3.4.3.2. Nhận xét

KẾT LUẬN CHƯƠNG 3

Các phương pháp giấu tin HKC, DIH, IWH, RVH là các trường hợp riêng của kỹ thuật giấu LSB, nó làm thay đổi rất ít trên LSB của miền không gian hay miền

biến đổi. Do vậy nếu sử dụng một số phương pháp phát hiện mù trong chương 2 cho kết quả phân loại không cao, còn nếu dùng kỹ thuật phát hiện mù bằng phương pháp ước lượng có thể phát hiện ra ảnh nhưng không thể ước lượng chính xác bit thông tin đã giấu mà nó chỉ ước lượng được số bit tương ứng đã thay đổi trên LSB của ảnh.

Chương này đã đưa ra phương pháp phát hiện tối ưu cho từng kỹ thuật giấu đã biết (HKC, DIH, IWH, RVH) và có thể ước lượng xấp xỉ thông tin giấu trong ảnh sử dụng các kỹ thuật giấu này.

KẾT LUẬN CHUNG

Phát hiện ảnh có giấu tin đang là bài toán cấp thiết hiện nay trong lĩnh vực an toàn bảo mật thông tin nói chung, lĩnh vực an ninh, chính trị và quốc phòng nói riêng. Phát hiện ảnh có giấu tin đòi hỏi phải được nghiên cứu một cách toàn diện từ các vấn đề của bài toán giấu tin trong ảnh.

Các phương pháp tiến hành nghiên cứu, lý thuyết và các kết quả thực nghiệm được trình bày trong hai chương chính là chương 2 và 3. Các kết quả chính của luận án đã bám sát vào mục tiêu đề ra bao gồm:

1/. Đề xuất bốn kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian bằng: phương pháp phân tích độ lệch chuẩn (công bố trên công trình số 1), thống kê χ^2 một bậc tự do (công bố trên công trình số 3), phân tích "tỉ lệ xám" (công bố trên công trình số 2), phương pháp ước lượng thông tin giấu trên LSB của miền không gian ảnh sử dụng lý thuyết trùng khớp (công bố trên công trình số 4).

2/. Đề xuất một kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền tần số wavelet hoặc cosine bằng phân tích tỉ lệ xám giữa ảnh bất kỳ và ảnh được dựng lên làm "mốc" (công bố trên công trình số 2).

3/. Đề xuất bốn kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng kỹ thuật giấu biết trước như:

- Kỹ thuật giấu HKC, trong đó cải tiến kỹ thuật phát hiện HKC của Wen – Chung Kuo (giấu dựa trên dịch chuyển biểu đồ tần suất). Đồng thời đề xuất một phương pháp hiện khác và có thể ước lượng thông tin đã giấu, kỹ thuật này đơn giản và hiệu quả hơn kỹ thuật phát hiện của Wen – Chung Kuo (công bố trên công trình số 7).
- Kỹ thuật giấu DIH (kỹ thuật giấu thông tin dựa trên dịch chuyển biểu đồ tần suất các hệ số sai phân của các điểm ảnh) (công bố trên công trình số 5)
- Kỹ thuật giấu IWH (kỹ thuật giấu thông tin dựa trên các hệ số wavelet nguyên) (công bố trên công trình số 5)
- Kỹ thuật giấu RVH (giấu hai pha ngang dọc) (công bố trên công trình số 6).

Với một số phương pháp phát hiện mù trên LSB của miền không gian ảnh, chúng ta không cần biết rõ phương pháp giấu là phương pháp nào, mà chỉ biết nó đã làm thay đổi tính tự nhiên trên LSB của miền không gian (hoặc miền tần số) khi chưa giấu tin. Còn với các kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng kỹ thuật giấu biết trước, luận án đã đưa phương pháp phát hiện tối ưu hơn (so với phát hiện mù) và có thể ước lượng xấp xỉ thông tin đã giấu trong ảnh.