

MỘT PHƯƠNG PHÁP THỦY VÂN THUẬN NGHỊCH MỚI DỰA TRÊN DỊCH CHUYỂN HISTOGRAM

Nguyễn Kim Sao¹, Lê Quang Hòa², Phạm Văn Ất¹

¹ Đại học Giao thông Vận tải Hà Nội

² Đại học Bách khoa Hà Nội

nksao@utc.edu.vn, hoa.lequang1@hust.edu.vn, phamvanat83@vnn.vn

TÓM TẮT - Bài báo đề xuất một phương pháp thủy vân thuận nghịch mới dựa trên dịch chuyển histogram (DCH). Trong khi hầu hết các phương pháp thủy vân dựa trên DCH không có khả năng đóng gói mọi thông tin cần thiết về ảnh gốc vào ảnh thủy vân, nên ở giai đoạn khôi phục chúng phải sử dụng một số thông tin phụ về ảnh gốc, thì phương pháp đề xuất đã khắc phục được nhược điểm trên và không cần sử dụng bất kỳ thông tin phụ nào về ảnh gốc để khôi phục dấu thủy vân cũng như ảnh gốc. Các phương pháp thủy vân như vậy gọi là có tính đóng gói hoặc độc lập thông tin phụ. Giải pháp đóng gói được sử dụng ở đây là kết hợp kỹ thuật chèn bit thấp và dịch chuyển histogram. Ảnh gốc được chia thành hai miền: miền đầu gồm một số ít điểm ảnh được sử dụng để nhúng thông tin phụ bằng kỹ thuật chèn bit thấp, miền thứ hai gồm phần còn lại của ảnh, dùng để nhúng dấu thủy vân theo phương pháp DCH. So sánh với các phương pháp độc lập thông tin phụ khác, phương pháp đề xuất có khả năng nhúng cao hơn và độ phức tạp tính toán thấp hơn. Ưu điểm của giải pháp đóng gói đề xuất là đơn giản, hiệu quả và có thể dễ dàng áp dụng đối với hầu hết các phương pháp thủy vân DCH khác.

Từ khóa - giấu tin, thủy vân thuận nghịch, dịch chuyển histogram, chèn bit thấp.

I. GIỚI THIỆU

Thủy vân (watermarking) là kỹ thuật nhúng một dãy bit (thường gọi là dấu thủy vân) vào ảnh số nhằm xác thực và bảo vệ bản quyền sản phẩm ảnh.

Thủy vân truyền thống chỉ có thể trích được dấu thủy vân mà không cho phép khôi phục ảnh gốc, tuy nhiên đối với nhiều trường hợp, việc sử dụng ảnh gốc là điều bắt buộc như các ứng dụng trong quân sự, giáo dục, y tế. Chính vì vậy, hướng nghiên cứu thủy vân thuận nghịch ngày càng được quan tâm. Thủy vân thuận nghịch là kỹ thuật thủy vân mà ngoài việc trích chọn dấu thủy vân còn khôi phục được ảnh gốc ban đầu.

Các hướng nghiên cứu chính của thủy vân thuận nghịch cho đến nay bao gồm: nén bảo toàn, mở rộng hiệu, dịch chuyển histogram (viết tắt là DCH), phép biến đổi nguyên, sử dụng đặc trưng JPEG, cộng modulo, dự báo.

Thủy vân thuận nghịch dựa trên nén bảo toàn [3], thực hiện nén dãy bit thấp của các điểm ảnh để tạo không gian dư thừa, sau đó dùng không gian này để lưu trữ dấu thủy vân.

Nhóm phương pháp sử dụng các phép biến đổi nguyên như tương phản [2], wavelet nguyên [13] ứng dụng các phép biến đổi nguyên khả nghịch để biến đổi không gian ảnh, dữ liệu được nhúng trên miền biến đổi, ảnh gốc được khôi phục bằng phép biến đổi ngược.

Phương pháp mở rộng hiệu [11] là phương pháp hiệu quả và được các nhà khoa học rất quan tâm. Hiệu hai điểm ảnh liên tiếp sẽ được mở rộng sang trái và thực hiện nhúng một bit thủy vân vào vị trí bên phải.

Trong phương pháp sử dụng các đặc trưng JPEG [1,6,12], các khối DCT lượng tử thường chứa những phần tử 0 và được sử dụng để nhúng các bit thủy vân.

Ở giải pháp cộng Modulo 256 [15], thủy vân được tạo ra bằng cách cộng modulo 256 giữa ảnh gốc và dấu thủy vân.

Gần đây, xuất hiện các phương pháp thủy vân dựa trên các ma trận sai số dự báo so với ảnh gốc ban đầu [10].

Theo [7], tiêu chí quan trọng để so sánh, đánh giá các phương pháp thủy vân thuận nghịch là khả năng nhúng, chất lượng ảnh và độ phức tạp tính toán. Nếu như phương pháp mở rộng hiệu [11] có khả năng nhúng tin cao thì trái lại thủy vân dựa trên DCH [4,5,8,9] có chất lượng ảnh tốt hơn.

Các phương pháp thủy vân thuận nghịch dựa trên DCH thường thực hiện như sau: Đầu tiên bằng cách DCH để tạo ra một cặp hai điểm ảnh liên tiếp a và b sao cho $h(a)$ lớn và $h(b)$ bằng 0 ($h(x)$ là histogram của ảnh tại điểm x). Sau đó nhúng một dãy bit thủy vân có độ dài $h(a)$ trên các điểm ảnh có giá trị bằng a .

Các phương pháp này cho chất lượng ảnh tốt, vì các điểm ảnh chỉ thay đổi tối đa một đơn vị. Tuy nhiên để khôi phục thủy vân và ảnh gốc cần biết a , mà giá trị này rất khó tích hợp (đóng gói) trong ảnh thủy vân. Giữa người gửi và người nhận ảnh thủy vân phải trao đổi một thông tin phụ (giá trị a). Ngoài ra, việc không đóng gói được mọi thông tin cần thiết vào ảnh thủy vân còn dẫn đến các hạn chế khác như không cho phép áp dụng thủy vân nhiều mức cũng như không thể sử dụng lược đồ khóa công khai.

Gần đây đã có một số phương pháp nhằm khắc phục nhược điểm nêu trên: Hwang và các cộng sự [5] (sau đây gọi là phương pháp Hwang) đã xây dựng các cặp a, b đặc biệt để sau khi nhúng thủy vân, giá trị của chúng vẫn không

thay đổi. Do đó a có thể được xác định từ ảnh thủy vân. Masaaki Fujiyoshi [4] (sau đây gọi là phương pháp MF) sử dụng phương pháp DHC như của Ni và cộng sự [9] để xác định a, b và đưa ra một quan hệ giữa histogram của ảnh gốc và ảnh thủy vân tại các điểm a, b . Giá trị a được xác định bằng cách dò tìm các điểm ảnh thỏa mãn quan hệ trên.

Cả hai phương pháp này đều có nhược điểm là tốn nhiều thời gian cho việc tìm a và khả năng nhúng không cao.

Trong bài báo này, chúng tôi đưa ra một phương pháp tích hợp a vào ảnh bằng cách chia ảnh thành miền 8 điểm ảnh (miền nhỏ) và miền còn lại (miền lớn). Các giá trị a, b được xác định bằng kỹ thuật DCH trên miền lớn (chứ không phải trên toàn ảnh). Giá trị a (gồm 8 bit) được nhúng vào miền nhỏ theo kỹ thuật chèn bit thấp. Bằng cách này, việc xác định a từ ảnh thủy vân rất đơn giản và nhanh chóng. Giải pháp này có thể dễ dàng ứng dụng để cải tiến hầu hết các phương pháp thủy vân DCH đã biết với mục đích đóng gói sản phẩm.

Các phương pháp mà việc khôi phục dấu thủy vân và ảnh gốc không cần sử dụng thông tin phụ đi kèm, trong [4] gọi là độc lập thông tin phụ (free from side information), ở đây chúng tôi gọi là tích hợp hay đóng gói.

Bằng cả phân tích lý thuyết và thực nghiệm đã chứng tỏ phương pháp đề xuất có tốc độ thực hiện nhanh hơn (khối lượng tính toán ít hơn), khả năng nhúng cao hơn so với các phương pháp Hwang và MF.

Cũng cần nhận xét rằng, các phương pháp thủy vân thuận nghịch nói chung và các phương pháp thủy vân thuận nghịch dựa trên dịch chuyển histogram nói riêng thuộc loại dễ vỡ nên các bài báo liên quan đều không xét tính bền vững của các phương pháp này.

Nội dung tiếp theo của bài báo được tổ chức như sau: mục II trình bày những kiến thức cơ sở về phương pháp thủy vân thuận nghịch dựa trên DCH. Mục III giới thiệu các công trình liên quan gồm hai phương pháp Hwang và MF. Mục IV trình bày phương pháp đề xuất. Mục V đánh giá so sánh phương pháp đề xuất với các phương pháp liên quan bằng phân tích lý thuyết và thử nghiệm trên máy tính, cuối cùng là kết luận ở mục VI.

II. NHỮNG KIẾN THỨC CƠ SỞ

Bài báo này chỉ xét các ảnh đa cấp xám có giá trị điểm ảnh trong miền \mathcal{D} :

$$\mathcal{D} = \{x \text{ nguyên} \mid 0 \leq x \leq 255\}$$

Một ảnh đa cấp xám I kích cỡ $M \times N$ có thể xem như một ma trận cấp $M \times N$ (M hàng, N cột) gồm các phần tử $I(i, j)$ thuộc \mathcal{D} . Nhiều khi chỉ cần xét một miền con J nào đó của I , và ký hiệu $P(J)$ là tập cặp chỉ số (i, j) thuộc J . Khi đó:

$$P(I) = \{(i, j) \mid 1 \leq i \leq M, 1 \leq j \leq N\}, P(J) \subseteq P(I)$$

Dưới đây sẽ trình bày khái niệm histogram, cặp histogram và phương pháp thủy vân dựa trên DCH đối với ảnh I .

A. Histogram và cặp histogram

Histogram của ảnh I (hoặc của miền con J) tại điểm $x \in \mathcal{D}$, ký hiệu $h(x)$, là số điểm ảnh của I (hoặc của J) có giá trị bằng x .

Theo [14] hai giá trị a, b liên tiếp ($b = a + 1$ hoặc $a - 1$) trên miền \mathcal{D} được gọi là một cặp histogram nếu:

$$h(a) > 0, h(b) = 0$$

Dưới đây a và $h(a)$ được gọi là đỉnh và chiều cao của cặp (a, b) .

Mỗi điểm ảnh $(i, j) \in P(I)$ có giá trị $I(i, j) = a$ có thể nhúng được một bit w theo công thức:

$$I'(i, j) = \begin{cases} a & \text{nếu } w = 0 \\ b & \text{nếu } w = 1 \end{cases}$$

Khi đó, thuật toán khôi phục w và $I(i, j)$ từ $I'(i, j)$ đơn giản như sau:

$$I(i, j) = a,$$

$$\text{if } I'(i, j) = a \text{ thì } w = 0 \text{ else } w = 1.$$

Nhận xét 2.1: Bằng việc sử dụng cặp histogram (a, b) có thể nhúng thuận nghịch một dãy $h(a)$ bit trên các điểm ảnh (i, j) có giá trị $I(i, j) = a$. Đôi khi để cho gọn ta nói nhúng $h(a)$ bit trên cặp histogram (a, b) .

Nhận xét 2.2: Sau khi nhúng, số điểm ảnh có giá trị bằng a giảm khoảng một nửa (giả định số bit 0 và 1 trong dãy thủy vân xấp xỉ bằng nhau), nên $h(a)$ giảm một nửa. Hay nói cách khác:

$$h'(a) \approx \frac{1}{2} h(a)$$

trong đó h' là histogram của ảnh thủy vân I'

B. Dịch chuyển histogram

Giả sử điểm ảnh a có $h(a) > 0$. Để tạo cặp histogram $(a, a - 1)$ có thể sử dụng kỹ thuật DCH như sau: Đầu tiên tìm điểm $z < a$ có $h(z) = 0$, sau đó DCH trên đoạn $[z + 1, a - 1]$ sang trái theo thuật toán

```
for  $(i, j) \in P(I)$  and  $I(i, j) \in [z + 1, a - 1]$ 
     $I'(i, j) = I(i, j) - 1$ 
End
```

Tương tự để tạo cặp histogram $(a, a + 1)$ có thể làm như sau: Đầu tiên tìm điểm $z > a$ có $h(z) = 0$, sau đó DCH trên đoạn $[a + 1, z - 1]$ sang phải theo thuật toán:

```
for  $(i, j) \in P(I)$  and  $I(i, j) \in [a + 1, z - 1]$ 
     $I'(i, j) = I(i, j) + 1$ 
End
```

Nhận xét 2.3: Ảnh sau khi DCH sang trái có thể dễ dàng khôi phục bằng phép dịch chuyển sang phải và ngược lại.

C. Các phương pháp thủy văn thuận nghịch dựa trên dịch chuyển histogram

Các phương pháp này dựa trên kỹ thuật DCH để tạo ra các cặp histogram, sau đó nhúng thủy văn trên các cặp histogram nhận được.

Để tạo ra một cặp histogram, theo như mục II.B, cần có một điểm z với $h(z) = 0$. Nếu không tồn tại điểm z như vậy, có thể chọn $z < a$ (hoặc $z > a$) có $h(z)$ nhỏ nhất, thường ký hiệu là $minL$ (hoặc $minR$). Khi đó, muốn khôi phục ảnh, cần bổ sung giá trị $minL$ (hoặc $minR$) và vị trí các điểm ảnh $I(i, j)$ có giá trị bằng $minL$ (hoặc $minR$) vào trước dấu thủy văn để tạo thành một dãy bit cần nhúng. Dãy bit thực nhúng, ký hiệu B , sẽ gồm tập thông tin hỗ trợ H và dấu thủy văn W :

$$B = H \oplus W$$

Các phương pháp dựa trên DCH khác nhau chủ yếu ở cách tạo ra các cặp histogram có chiều cao lớn để tăng khả năng nhúng tin. Nhóm các phương pháp này có ưu điểm là chất lượng ảnh thủy văn tốt vì giá trị các điểm ảnh chỉ phải thay đổi tối đa một đơn vị. Để khôi phục dãy bit đã nhúng B và ảnh gốc cần phải biết định của các cặp histogram. Thông tin này khó có thể đưa vào H để tích hợp trong ảnh thủy văn nên thường phải trao đổi bên ngoài. Như vậy, nếu chỉ biết ảnh thủy văn thì vẫn chưa thể thực hiện được việc khôi phục cần thiết. Hầu hết các phương pháp thủy văn đều mắc phải nhược điểm này.

Gần đây, có một số công trình nghiên cứu khắc phục được nhược điểm nêu trên như các phương pháp Hwang và MF. Tuy nhiên các phương pháp này vẫn còn tồn tại một số hạn chế về khả năng nhúng tin và độ phức tạp tính toán như sẽ trình bày dưới đây.

III. NHỮNG CÔNG TRÌNH LIÊN QUAN

A. Phương pháp Hwang

Hwang và các cộng sự, trước tiên tìm điểm *peak* đạt cực đại histogram:

$$h(peak) = \max\{h(x) | x \in \mathcal{D}\}$$

(nếu tồn tại nhiều điểm cực đại thì chọn điểm đầu tiên). Sau đó DCH sang trái và sang phải để tạo thành các cặp histogram $(peak - 1, peak - 2)$ và $(peak + 1, peak + 2)$, cuối cùng sử dụng các cặp trên để nhúng dãy bit thủy văn. Bằng cách tạo ra hai cặp histogram đặc biệt như trên, giá trị *peak* không thay đổi sau khi thủy văn. Do đó, có thể tính được *peak* từ ảnh thủy văn I' theo công thức:

$$h'(peak) = \max\{h'(x) | x \in \mathcal{D}\} \tag{3.1}$$

Từ đó xác định các đỉnh $peak - 1, peak + 1$ của các cặp histogram và khôi phục được dấu thủy văn cũng như ảnh gốc ban đầu.

Nhận xét 3.1: Khả năng nhúng (số bit) của phương pháp Hwang trên ảnh I , ký hiệu C_h , theo nhận xét 2.1 bằng:

$$C_h = h(peak - 1) + h(peak + 1)$$

Nhận xét 3.2: Theo nhận xét 2.2, nếu tiếp tục nhúng trên I' (nhúng mức 2) thì khả năng nhúng C'_h chỉ bằng khoảng một nửa C_h :

$$C'_h \approx \frac{1}{2} C_h$$

B. Phương pháp MF

Phương pháp MF tìm điểm cực đại histogram *peak* như bước đầu của phương pháp Hwang. Sau đó DCH trái để được cặp histogram (*peak*, *peak* - 1) và thực hiện nhúng tin trên cặp histogram tìm được. Để tìm giá trị *peak* từ ảnh thủy vân, M. Fujiyoshi dựa trên tính chất sau của *peak*:

$$h'(peak - 1) + h'(peak) = h(peak) \quad (3.2)$$

Giá trị $h(peak)$ được đưa vào 16 bit đầu của tập H . Nói cách khác, $h(peak)$ được biến đổi thành một dãy 16 bit nhị phân và được nhúng vào 16 điểm ảnh đầu của I có giá trị bằng *peak* theo thuật toán trong mục II.A.

Việc xác định *peak* được thực hiện bằng cách duyệt từng giá trị x trên miền \mathcal{D} , ứng với mỗi x , trích 16 bit đầu tiên từ các điểm ảnh $I'(i, j)$ có giá trị bằng x hoặc $x - 1$ theo thuật toán trong mục II.A. Gọi $g(x)$ là giá trị trích được, nếu $h'(x - 1) + h'(x) = g(x)$ thì x thỏa mãn điều kiện (3.2), nên có thể xem đó là *peak*. Từ đỉnh *peak* tìm được, dễ dàng khôi phục được dấu thủy vân và ảnh gốc.

Phương pháp MF có khả năng nhúng không cao do chỉ sử dụng một cặp histogram, việc xác định *peak* bằng cách dò từng bước như trên tốn khá nhiều thời gian. Ngoài ra, do có thể còn có các giá trị khác *peak* cũng thỏa mãn điều kiện (3.2), nên không thể khẳng định chắc chắn giá trị nhận được theo cách trên đúng là *peak* cần tìm.

Nhận xét 3.3: Khả năng nhúng của MF trên I , ký hiệu C_{mf} và khả năng nhúng trên I' , ký hiệu C'_{mf} được tính theo các công thức

$$C_{mf} = \max\{h(x)|x \in \mathcal{D}\}$$

$$C'_{mf} = \max\{h'(x)|x \in \mathcal{D}\}$$

Vì chiều cao cực đại của h' xấp xỉ bằng h , nên C'_{mf} gần bằng C_{mf} .

IV. PHƯƠNG PHÁP ĐỀ XUẤT

Ý tưởng phương pháp đề xuất là chia ảnh I thành 2 miền: I_1 gồm 8 điểm ảnh và I_2 là phần còn lại. Sau đó xây dựng histogram $h(x)$ trên I_2 . Việc nhúng tin được thực hiện bằng phương pháp DCH trên I_2 (chứ không phải trên I), còn giá trị *peak* được lưu trữ trên các bit thấp của I_1 . Chi tiết thuật toán như sau:

A. Thuật toán nhúng thủy vân

Bước 1: Chia ảnh thành 2 miền I_1 và I_2 . Ở đây I_1 gồm 8 điểm ảnh đầu của I , I_2 là phần còn lại. Tuy nhiên, về nguyên tắc, I_1 gồm 8 điểm ảnh bất kỳ. Cũng có thể dùng một khóa ngẫu nhiên để chọn các điểm ảnh cho I_1 .

Bước 2: Xây dựng histogram $h(x)$ trên I_2 và xác định các giá trị *peak*, *minL* và *minR* theo các công thức:

$$h(peak) + h(peak + 1) = \max\{h(x) + h(x + 1)|x \in \mathcal{D}/\{255\}\}$$

$$h(minL) = \min\{h(x)|x \in [0, peak], x \in \mathcal{D}\}$$

$$h(minR) = \min\{h(x)|x \in [peak, 255], x \in \mathcal{D}\}$$

Bước 3: Xác định tập thông tin hỗ trợ H :

Tham số	Ý nghĩa	Độ dài bit lưu trữ
V	8 bit thấp của miền I_1	8
$minL$	Điểm cực tiểu bên trái	8
C_L	Số điểm cực tiểu bên trái	8
M_L	Vị trí các điểm ảnh có giá trị bằng <i>minL</i>	$9 \times 2 \times C_L$
$minR$	Điểm cực tiểu bên phải	8
C_R	Số điểm cực tiểu bên phải	8
M_R	Vị trí các điểm ảnh có giá trị bằng <i>minR</i>	$9 \times 2 \times C_R$

Bước 4: Xác định dãy bit thực nhúng:

$$B = H \oplus W$$

Ở đây, W là dãy bit thủy vân có độ dài: $size(W) = h(peak) + h(peak + 1) - size(H)$

Bước 5: Nhúng giá trị *peak* bằng cách chèn vào các bit thấp của miền I_1 . Kết quả được miền I'_1

Bước 6: Tạo các cặp histogram (*peak*, *peak* - 1) và (*peak* + 1, *peak* + 2) bằng cách dịch chuyển histogram như sau:

```

for  $(i, j) \in P(I_2)$  and  $I(i, j) \in [\min L + 1, \text{peak} - 1]$ 
     $I'(i, j) = I(i, j) - 1$ 
End
    
```

và

```

for  $(i, j) \in P(I_2)$  and  $I(i, j) \in [\text{peak} + 2, \min R - 1]$ 
     $I'(i, j) = I(i, j) + 1$ 
End
    
```

Bước 7: Nhúng dãy bit $B = b_1 b_2 \dots b_L$ ($L = \text{size}(B)$) trên các điểm ảnh có giá trị bằng peak hoặc $\text{peak} + 1$ như sau:

```

k = 0,
for  $(i, j) \in P(I_2)$  and  $I(i, j) \in [\text{peak}, \text{peak} + 1]$ 
    k = k + 1
    if  $b_k = 0$  then
         $I'(i, j) = I(i, j)$ 
    Else if  $I(i, j) = \text{peak}$  then
         $I'(i, j) = I(i, j) - 1$ 
    Else
         $I'(i, j) = I(i, j) + 1$ 
    End
End
End
    
```

Sau khi thực hiện bước 7 được I'_2 . Ảnh thủy vân I' gồm 2 miền I'_1 và I'_2 .

Nhận xét 4.1: Sau khi nhúng thủy vân, các điểm ảnh bị biến đổi gồm: Các điểm trong I_1 và các điểm trong I_2 có giá trị thuộc khoảng $[\min L, \min R]$.

B. Thuật toán khôi phục thủy vân và ảnh gốc

Dấu thủy vân W và ảnh gốc I được khôi phục từ ảnh thủy vân I' theo các bước:

Bước 1: Chia ảnh I' thành hai miền I'_1 và I'_2 như trong thuật toán nhúng.

Bước 2: Trích 8 bit thấp của miền I'_1 để được peak

Bước 3: Dựa vào peak để trích dãy bit B được nhúng trong miền I'_2 như sau:

```

k = 0,
for  $(i, j) \in P(I_2)$  and  $I(i, j) \in [\text{peak} - 1, \text{peak} + 2]$ 
    k = k + 1
    if  $I'(i, j) \in [\text{peak}, \text{peak} + 1]$  then
         $b_k = 0$ 
    Else
         $b_k = 1$ 
    End
End
End
    
```

Bước 4: Tách B để nhận được tập thông tin hỗ trợ H và dấu thủy vân W

Bước 5: Sử dụng H để khôi phục ảnh gốc

5.1: Khôi phục I_1 : Chèn giá trị V vào các bit thấp của miền I'_1

5.2: Khôi phục các điểm trong I_2 có giá trị thuộc khoảng $[minL, minR]$.

```

for (i, j) ∈ P(I2) and I'(i, j) ∈ [minL + 1, minR - 1]
    if I'(i, j) < peak
        I(i, j) = I'(i, j) + 1
    else if I'(i, j) > peak + 1 then I(i, j) = I'(i, j) - 1
end
end
    
```

5.3: Khôi phục các điểm trong I_2 có giá trị bằng $minL, minR$

```

for (i, j) ∈ P(I2) and I'(i, j) ∈ {minL, minR}
    if (i, j) ∈ ML ∪ MR then
        I(i, j) = I'(i, j)
    else if I'(i, j) = minL then
        I(i, j) = I'(i, j) + 1
    else I(i, j) = I'(i, j) - 1
end
end
    
```

C. Ví dụ

Để hiểu rõ hơn về phương pháp đề xuất, chúng tôi trình bày một ví dụ trong đó I cho trong hình 1 và W là một dãy 8 bit: 00001111

6	5	5	8	7	5	5	5	1	6
5	6	5	5	5	6	5	6	5	7
5	6	6	7	4	5	5	5	2	4
6	5	9	5	6	6	9	6	5	5
6	5	6	5	3	6	8	2	6	7
5	5	5	5	5	6	11	6	6	6
5	6	6	6	6	5	6	6	6	8
6	5	5	5	6	5	5	6	5	6
6	6	0	5	6	3	5	6	6	5

Hình 1. Ảnh gốc

6	4	4	8	6	5	4	5	1	6
5	6	5	5	5	6	5	6	5	8
5	6	6	8	3	5	5	5	1	3
6	5	10	5	6	6	10	6	5	5
6	5	6	5	2	6	9	1	6	8
5	5	5	5	5	6	11	6	6	6
5	6	6	6	6	5	6	6	6	9
6	5	5	5	6	5	5	6	5	6
6	6	0	5	6	2	5	6	6	5

Hình 2. Ảnh sau khi chèn peak vào I1 và dịch chuyển histogram trên I2 (các số nghiêng là số bị biến đổi)

6	4	4	8	6	5	4	5	1	7
4	7	4	5	4	6	5	6	5	8
5	6	6	8	3	5	5	4	1	3
6	5	10	5	6	6	10	6	5	4
6	5	6	5	2	6	9	1	6	8
5	5	4	5	5	6	11	6	6	7
5	6	7	6	6	5	6	7	6	9
7	5	5	5	6	5	5	6	5	6
6	6	0	5	6	2	4	7	7	4

Hình 3. Ảnh thủy vân (các số đậm là các số có biến đổi)

Bước 1: I_1 gồm 8 điểm ảnh đầu của I (8 ô màu xám), I_2 là phần còn lại.

Bước 2: Histogram $h(x)$ trên I_2 và các đại lượng liên quan:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	...	255
$h(x)$	1	1	2	2	2	32	34	3	2	2	0	1	0	...	0

$peak = 5$ (biểu diễn nhị phân là 00000101); $minL = 1$; $minR = 10$.

Bước 3: Tập thông tin hỗ trợ H :

Tham số	V	$minL=1$	$C_L=1$	$M_L=\{(1,9)\}$	$minR=10$	$C_R=0$	M_R rỗng
Nhị phân	11110100	00000001	00000001	000000001000001001	00001010	00000000	

Bước 4: Dãy bit thực nhúng (có độ dài bằng $h(5) + h(6) = 66$):

$$B = H \oplus W = 111101000000000100000001000000001000001001000010100000000000001111$$

Bước 5: Những giá trị *peak* (00000101) bằng cách chèn vào các bit thấp của miền I_1 . Kết quả được miền I_1'

6	4	4	8	6	5	4	5
---	---	---	---	---	---	---	---

Bước 6: Tạo các cặp histogram (5, 4) và (6,7) bằng cách DCH, kết quả được ma trận ở hình 2.

Bước 7: Những dãy bit B trên các điểm ảnh có giá trị bằng 5 hoặc 6 được ảnh thủy vân như hình 3.

V. SO SÁNH PHƯƠNG PHÁP ĐỀ XUẤT VỚI CÁC PHƯƠNG PHÁP HWANG VÀ MF

Mục này sẽ so sánh các phương pháp bằng cả phân tích lý thuyết và thực nghiệm trên máy tính.

A. Phân tích lý thuyết

1. Khả năng nhúng

Đối với phương pháp đề xuất, khả năng nhúng C_{dx} trên I và C'_{dx} trên I' được tính theo các công thức:

$$C_{dx} = \max\{h(x) + h(x + 1) | x \in \mathcal{D}\}$$

$$C'_{dx} = \max\{h'(x) + h'(x + 1) | x \in \mathcal{D}\}$$

Từ đó và các nhận xét 3.1, 3.2, 3.3 có thể rút ra các kết luận sau:

a. Khả năng nhúng của phương pháp đề xuất trên ảnh gốc I (nhúng mức 1) lớn hơn phương pháp Hwang không nhiều và xấp xỉ hai lần phương pháp MF

b. Khả năng nhúng của phương pháp đề xuất trên ảnh thủy vân I' (nhúng mức 2) lớn hơn khoảng hai lần cả hai phương pháp Hwang và MF

Kết luận này phù hợp với kết quả thực nghiệm trong mục V.B.

2. Độ phức tạp tính toán

Ba phương pháp chỉ khác nhau ở việc xác định giá trị *peak* từ ảnh thủy vân, vì vậy chỉ cần tập trung đánh giá khối lượng tính toán của công đoạn tìm *peak* trong các phương pháp.

- **Phương pháp Hwang:** Để xác định *peak* theo công thức (3.1), trước tiên cần sử dụng $M \times N$ phép cộng để xây dựng histogram h' của ảnh I' (cỡ $M \times N$). Sau đó, thực hiện 256 phép so sánh để xác định cực đại của $h'(x)$. Như vậy, khối lượng tính toán để xác định *peak* của Hwang gồm: $(M \times N)$ phép cộng và 256 phép so sánh.

- **Phương pháp MF:** Trong phương pháp này, cũng cần sử dụng $M \times N$ phép cộng để xây dựng histogram $h'(x)$. Sau đó, với mỗi x thuộc \mathcal{D} , cần kiểm tra điều kiện:

$$h'(x - 1) + h'(x) = g(x) \tag{4.1}$$

Để xác định 16 bit của $g(x)$ cần duyệt trên ảnh I' (kích thước $M \times N$) để tìm ra 16 phần tử có giá trị bằng x hoặc $x - 1$ (gấp x lấy bit 0, gấp $x - 1$ lấy bit 1). Việc này cần trung bình $(16 + M \times N)/2$ phép so sánh. Sau đó cần 15 phép dịch chuyển và 15 phép cộng để chuyển 16 bit ra dạng thập phân. Vậy để xác định $g(x)$ cần thực hiện: $(16 + M \times N)/2$ phép so sánh, 15 phép dịch chuyển và 15 phép cộng. Sau khi có $g(x)$, cần thêm một phép cộng và một phép so sánh để kiểm tra điều kiện (4.1). Trung bình cần duyệt khoảng $256/2$ giá trị x (một nửa số phần tử của \mathcal{D}). Từ đó suy ra khối lượng tính toán để xác định *peak* của MF khoảng: $(M \times N + 128 \times 16)$ phép cộng, 128×15 phép dịch chuyển và $64 \times (18 + M \times N)$ phép so sánh.

- **Phương pháp đề xuất:** Giá trị *peak* được trích ra từ 8 điểm ảnh của I' , vì vậy chỉ cần sử dụng: 8 phép trích bit thấp, 7 phép dịch chuyển và 7 phép cộng.

Từ các phân tích trên, có thể kết luận: khối lượng tính toán của phương pháp đề xuất ít hơn nhiều so với cả hai phương pháp Hwang và MF. Điều này hoàn toàn phù hợp với kết quả thử nghiệm trong phần V.B.

3. Chất lượng ảnh

Do khả năng nhúng của các phương pháp khác nhau, nên không thể dùng tiêu chuẩn PSNR để so sánh chất lượng ảnh của chúng. Để khách quan, ở đây sử dụng hệ số biến đổi ảnh (số điểm ảnh cần thay đổi để nhúng 1 bit) là tiêu chí so sánh chất lượng ảnh. Chúng ta nhận thấy, ảnh bị thay đổi là do dịch chuyển histogram. Ngoài ra, số điểm ảnh cần dịch chuyển tỷ lệ thuận với số bit nhúng được. Từ đó suy ra hệ số biến đổi ảnh của cả ba phương pháp trên là tương đương.

B. Thử nghiệm

Để minh họa các kết quả phân tích lý thuyết, chúng tôi tiến hành thử nghiệm trên bộ ảnh mẫu trong [16]. Các ảnh từ hình 4 đến hình 8 có kích thước 512×512 , hình 9 có kích thước 256×256 và hình 10 có kích thước 1024×1024 .

Dấu thủy vân W lấy từ ảnh nhị phân hình 11. Chương trình viết bằng ngôn ngữ MatLab R2012a và chạy trên máy tính Lenovo Ideapad S410p.



Hình 4. Lena



Hình 5. Peppers



Hình 6. Sailboat



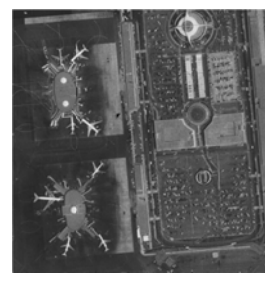
Hình 7. Boat



Hình 8. Tiffany



Hình 9. Sight



Hình 10. Airport



Hình 11. Water mark

1. So sánh khả năng nhúng tin

Khả năng nhúng tin của mỗi phương pháp trên từng ảnh ở mức 1 và mức 2 được trình bày trong hai bảng dưới đây.

Bảng 1. Khả năng nhúng tin trên ảnh gốc I (mức 1)

STT	Ảnh thử nghiệm	Số bit nhúng tối đa của các lược đồ		
		Hwang	MF	Đề xuất
1	Lena	5535	2919	5696
2	Pepper	5263	2712	5854
3	Tiffany	5788	2956	5854
4	Boat	7592	3906	7738
5	Sailboat	7109	3707	7364
6	Sight	2232	1200	2331
7	Airport	44894	22723	45395
	<i>Tổng</i>	<i>78413</i>	<i>40123</i>	<i>80232</i>

Bảng 2. Khả năng nhúng tin trên ảnh thủy vân I' (mức 2)

STT	Ảnh thử nghiệm	Số bit nhúng tối đa của các lược đồ		
		Hwang	MF	Đề xuất
1	Lena	2737	2803	5421
2	Pepper	2628	2662	5243
3	Tiffany	2902	2934	5785
4	Boat	3847	3836	7556
5	Sailboat	3543	3657	6739
6	Sight	1096	1165	2298
7	Airport	22639	22673	44385
	<i>Tổng</i>	<i>39392</i>	<i>39730</i>	<i>77427</i>

Nhận xét 5.1: Từ các bảng trên có thể kết luận: khả năng nhúng của phương pháp đề xuất

Ở mức 1, gấp 1.02 lần so với Hwang và gấp 2 so với MF.

Ở mức 2, gấp 1.97 lần so với Hwang và gấp 1.95 so với MF.

Ở cả hai mức, gấp 1.34 lần so với Hwang và gấp 1.97 so với MF.

2. So sánh thời gian xác định *peak* từ ảnh thủy vân

Bảng dưới đây thống kê thời gian xác định *peak* từ ảnh thủy vân của mỗi phương pháp trên các ảnh gốc khác nhau.

Bảng 3. Thời gian xác định *peak*

STT	Ảnh thử nghiệm	Thời gian trích giá trị <i>peak</i> (tính bằng micro giây)		
		Hwang	MF	Đề xuất
1	Lena	6700	949500	7.5
2	Pepper	6600	491200	7.4
3	Tiffany	6600	1891400	7.5
4	Boat	6600	579900	7.5
5	Sailboat	6700	635700	7.5
6	Sight	1600	186100	7.5
7	Airport	29100	89700	7.5
	<i>Tổng</i>	<i>63900</i>	<i>4823500</i>	<i>52.4</i>

Nhận xét 5.2: Bảng 3 cho thấy, thời gian dò tìm *peak* của phương pháp Hwang và MF phụ thuộc vào kích thước ảnh, của phương pháp đề xuất độc lập với kích thước ảnh.

Nhận xét 5.3: Thời gian dò tìm giá trị *peak* của phương pháp Hwang gấp khoảng 1219 lần và của phương pháp MF gấp 92051 lần so với phương pháp đề xuất.

3. So sánh hệ số biến đổi ảnh

Bảng dưới đây thống kê số phần tử cần biến đổi để nhúng một bit của mỗi phương pháp trên các ảnh thử nghiệm.

Bảng 4. Hệ số biến đổi ảnh

STT	Ảnh thử nghiệm	Hệ số biến đổi ảnh		
		Hwang	MF	Đề xuất
1	Lena	46.73	65.68	45.91
2	Pepper	49.23	34.88	44.69
3	Tiffany	43.10	53.22	44.01
4	Boat	33.71	54.92	33.58
5	Sailboat	36.10	51.61	35.33
6	Sight	28.84	6.93	28.06
7	Airport	44.67	10.05	22.62
	<i>Trung bình</i>	<i>40.34</i>	<i>39.61</i>	<i>36.31</i>

Bảng 4 cho thấy, hệ số biến đổi ảnh giữa các phương pháp có sự chênh lệch không nhiều, song ở mức trung bình, phương pháp đề xuất có sự biến đổi ảnh thấp hơn.

VI. KẾT LUẬN

Bài báo đề xuất một phương pháp thủy vân thuận nghịch có tính chất độc lập thông tin phụ (đóng gói ảnh thủy vân) bằng giải pháp kết hợp nhúng bit thấp và dịch chuyên histogram. Từ ảnh thủy vân có thể trích dấu thủy vân và khôi phục ảnh gốc mà không cần thông tin phụ kèm theo. Giải pháp đề xuất có thể dễ dàng sử dụng cho hầu hết các phương pháp thủy vân thuận nghịch DCH đã biết nhằm đóng gói ảnh thủy vân.

So với các phương pháp cùng có tính chất đóng gói hiện có, phương pháp đề xuất có khả năng nhúng tin cao hơn và thời gian thực hiện nhanh hơn.

VII. TÀI LIỆU THAM KHẢO

[1] Almohammad, Adel, Gheorghita Ghinea, and Robert M. Hierons. "JPEG steganography: a performance evaluation of quantization tables." Advanced Information Networking and Applications, 2009. AINA'09. International Conference on. IEEE, 2009.

[2] Coltuc, Dinu, and J-M. Chassery. "Very fast watermarking by reversible contrast mapping." Signal Processing Letters, IEEE 14.4 pp.255-258, 2007

- [3] Fridrich, Jessica, Miroslav Goljan, and Rui Du. "Invertible authentication." *Photonics West 2001-Electronic Imaging*. International Society for Optics and Photonics, 2001.
- [4] Fujiiyoshi, Masaaki. "A Histogram shifting-based blind reversible data hiding method with a histogram peak estimator." *Communications and Information Technologies (ISCIT), 2012 International Symposium on*. IEEE, 2012.
- [5] Hwang, JinHa, JongWeon Kim, and JongUk Choi. "A reversible watermarking based on histogram shifting." *Digital Watermarking*. Springer Berlin Heidelberg, pp. 348-361, 2006.
- [6] Iwata, Motoi, Kyosuke Miyake, and Akira Shiozaki. "Digital steganography utilizing features of JPEG images." *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 87.4, pp.929-936, 2004.
- [7] Khan, Asifullah, et al. "A recent survey of reversible watermarking techniques." *Information Sciences* 279 pp.251-272, 2014.
- [8] Kuo, Wen-Chung, Dong-Jin Jiang, and Yu-Chih Huang. "Reversible data hiding based on histogram." *Advanced Intelligent Computing Theories and Applications. With Aspects of Artificial Intelligence*. Springer Berlin Heidelberg, pp.1152-1161, 2007.
- [9] Ni, Zhicheng, et al. "Reversible data hiding." *Circuits and Systems for Video Technology, IEEE Transactions on* 16.3: pp.354-362, 2006.
- [10] Ou, Bo, Yao Zhao, and Rongrong Ni. "Reversible watermarking using prediction error histogram and blocking." *Digital Watermarking*. Springer Berlin Heidelberg, pp.170-180, 2011.
- [11] Tian, Jun. "Reversible data embedding using a difference expansion." *IEEE Trans. Circuits Syst. Video Techn.* 13.8, pp. 890-896, 2003.
- [12] Đỗ Văn Tuấn, Nguyễn Kim Sao, Nguyễn Thanh Toàn, Phạm Văn Át, "Một sơ đồ nhúng tin thuận nghịch mới trên ảnh JPEG", *Tạp chí Công nghệ thông tin và truyền thông*, pp.41-52, 2014
- [13] Xuan, Guorong, et al. "Reversible data hiding using integer wavelet transform and companding technique." *Digital Watermarking*. Springer Berlin Heidelberg, pp.115-124, 2005.
- [14] Xuan, Guorong, et al. "Optimum histogram pair based image lossless data embedding." *Transactions on Data Hiding and Multimedia Security IV*. Springer Berlin Heidelberg, pp. 84-102, , 2009
- [15] Zhang, Weiming, Biao Chen, and Nenghai Yu. "Improving various reversible data hiding schemes via optimal codes for binary covers." *Image Processing, IEEE Transactions on* 21.6, pp.2991-3003, 2012
- [16] Signal & Image Processing Institute, University of Southern California, "The USC-SIPI Image Database", <http://sipi.usc.edu/database>.