Một thuật toán giấu tin trong ảnh có bảng màu

A New Data Hiding Algorithm in Palette Images

Đỗ Văn Tuấn và Phạm Văn Ất

Abstract: *This paper proposes a new algorithm to embed data in palette image. In each image block of original image, this algorithm can hide a bit by modifying at most one pixel of block. New color of modified pixel resembles the color of its some neighborhood pixels, so the image after hiding very close to the original image. The experimental results showed that the invisible of proposed algorithm is better than algorithms Fridrich and Ez Stego.*

Keywords: data hiding, steganography, security watermarking, Palette images

I. GIỚI THIỆU

Ngày nay, mạng Internet đóng vai trò quan trọng trong việc trao đổi dữ liệu giữa những người dùng. Bên cạnh những thuận lợi, vấn đề bảo mật thông tin trên Internet luôn là những thách thức đối với các cấp quản lý và các nhà nghiên cứu. Trước đây, các phương pháp mã hóa luôn là sự lựa chọn để bảo mật thông tin và đã mang lại những thành công nhất định. Tuy nhiên, việc truyền tải công khai các bản mã sẽ tạo ra sự chú ý, thách thức đối với các đối thủ, những người muốn khám phá nội dung của bản mã một cách trái phép. Gần đây, bên cạnh các phương pháp mật mã truyền thống, kỹ thuật giấu tin giữ vai trò quan trọng trong các bài toán bảo mật thông tin, bảo vệ bản quyền, xác thực dữ liệu.

Giấu tin là kỹ thuật nhúng thêm thông tin vào các dữ liệu đa phương tiện. Thông tin được nhúng có thể là các thông điệp bí mật cần trao đổi, hoặc là các thông tin về sản phẩm. Dữ liệu dùng để mang thông tin nhúng thường là những dạng dữ liệu phổ biến trên Internet như: ảnh, âm thanh, video. Theo [1], kỹ thuật giấu tin cần có một số tính chất cơ bản như: tính che giấu, tính khả nhúng và tính bảo mật. Theo định dạng ảnh, các kỹ thuật giấu được chia thành hai loại chính. Loại thứ nhất, gồm các kỹ thuật giấu tin trên ảnh không có bảng màu [2,9,10]. Ảnh không có bảng màu thường là những ảnh có số lượng màu lớn, dữ liệu ảnh chính là các giá trị màu của điểm ảnh. Lợi dụng sự hạn chế của hệ thống thị giác không phát hiện ra sự thay đổi nhỏ về màu sắc, các thuật toán giấu tin trên dạng ảnh này dễ dàng có được tính che giấu cao bằng cách thay đổi một lượng nhỏ giá trị màu trong vùng dữ liệu ảnh. Loại thứ 2, gồm các kỹ thuật giấu tin trên ảnh có bảng màu [3]-[8]. Đối với ảnh có bảng màu, dữ liệu ảnh là chỉ số màu của điểm ảnh. Hai chỉ số gần nhau có thể tham chiếu tới hai màu rất khác nhau. Do vậy, các thuật toán giấu tin trên dạng ảnh này gặp phải những khó khăn nhất định, bởi vì chỉ cần có thay đổi nhỏ về chỉ số màu có thể sẽ dẫn đến sự khác biệt lớn về màu sắc của điểm ảnh trước và sau khi thay đổi.

Với ảnh có bảng màu, để nâng cao tính che giấu, các kỹ thuật giấu tin thường tìm cách thay thế một màu có chỉ số chẵn bằng màu gần nhất có chỉ số lẻ hoặc ngược lại [3,4,7,8]. Dựa trên ý tưởng này, phương pháp Ez Stego [7] sắp xếp lại các màu trong bảng màu theo cường độ sáng. Cường độ sáng của màu c với các thành phần R_c, G_c, B_c được tính theo công thức:

$$l_c = 0.299R_c + 0.587G_c + 0.144B_c$$

Sau khi sắp xếp lại bảng màu, các màu giống nhau sẽ có chỉ số màu gần nhau. Tuy nhiên, theo Fridrich[3,4], hai màu khác nhau vẫn có thể có cường độ sáng bằng nhau, vì vậy tác giả đã sử dụng khoảng cách Euclid để đánh giá sự khác biệt về màu ứng với các chỉ số màu i và j theo công thức:

$$\boldsymbol{d} = \sqrt{(R_i - R_j)^2 + (B_i - B_j)^2 + (G_i - G_j)^2}$$

trong đó R_i, G_i, B_i và R_j, G_j, B_j là giá trị màu ứng với các chỉ số i và j trong bảng màu. Khi cần thay đổi một màu có chỉ số chẵn (hay lẻ), Fridrich sẽ duyệt các màu có chỉ số lẻ (hay chẵn) để tìm màu gần nhất (theo khoảng cách Euclid) với màu cần thay đổi. Tuy nhiên, chiến thuật thay thế màu gần nhất của các thuật toán vẫn có thể tạo ra các màu mới cô lập, vì vậy trong một số trường hợp, ảnh chứa tin giấu dễ bị phát hiện.

Để nâng cao chất lượng của ảnh sau khi giấu tin, trong [6] các tác giả G. Pan, Z. Wu, Y. Pan đã đề xuất thuật toán giấu tin cho ảnh ít màu bằng cách sử dụng một tập các khối mẫu có kích thước 3×3, các khối mẫu sẽ có sự ưu tiên khác nhau trong quá trình sử dụng để nhúng tin. Mỗi khối mẫu được xác định bởi 8 điểm xung quanh điểm tâm của khối, trong đó chia làm hai phần liên thông, một phần gồm các điểm có màu giống nhau được gọi là màu mẫu, phần còn lại gồm các điểu có màu khác màu mẫu được gọi là màu tham dự (nominated color). Thuật toán sẽ tìm các khối ảnh kích thước 3×3 trùng với một mẫu trong tập mẫu và nhúng một bít bằng cách biến đổi màu của điểm tâm khối thành màu mẫu hoặc màu tham dự. Với cách thay đổi như vậy, thuật toán có hai tính chất quan trọng: điểm ảnh được chọn để thay đổi luôn nằm trên biên của hai miền có màu khác nhau và không xuất hiện màu mới. Nhờ vậy, thuật toán có tính che giấu cao. Tuy nhiên, khối lượng tin có thể nhúng được còn chưa nhiều như chính nhận xét của các tác giả. Cũng cần nhận xét thêm, ý tưởng chọn điểm trên biên để thay đổi cũng đã được các tác giả M. Wu [11] và Y. C. Tseng[12] sử dụng để giấu tin trên ảnh nhị phân, nhưng mỗi phương pháp đều có cách chọn khác nhau.

Dựa trên phương pháp giấu tin theo khối bít và tính chẵn lẻ, bài báo này đề xuất một lược đồ giấu tin trên ảnh có bảng màu. Theo đó, vùng dữ liệu của ảnh gốc sẽ được chia thành các khối cùng kích thước. Với mỗi khối sẽ giấu được một bít và biến đổi nhiều nhất một phần tử. Khi cần biến đổi tính chẵn lẻ của khối, thuật toán sẽ thay thế giá trị của một phần tử bằng giá trị của phần tử liền kề nhưng khác tính chẵn lẻ. Với chiến thuật thay thế như vậy, thuật toán đề xuất cũng có hai tính chất giống như thuật toán [6], do đó nó cũng có tính che giấu khá cao.

Nội dung tiếp theo của bài báo được tổ chức như sau: Phần 2 giới thiệu một số ký hiệu và định nghĩa được sử dụng trong bài báo. Phần 3 trình bày nội dung thuật toán đề xuất. Tính đúng đắn của thuật toán được chứng minh trong Phần 4. Phần 5 trình bày kết quả thực nghiệm của thuật toán đề xuất và so sánh với hai thuật toán Fridrich, Ez Stego. Cuối cùng, Phần 6 là một số kết luận.

II. MỘT SỐ KÝ HIỆU VÀ ĐỊNH NGHĨA

Để tiện cho việc trình bày, trong bài báo sử dụng một số ký hiệu và định nghĩa như sau:

- Ký hiệu $I^{m\times n}$ là tập các ma trận nguyên không âm cấp m×n *(m hàng và n cột).*

- Với $F \in I^{m\times n}$, nói phần tử (i,j) có nghĩa là phần tử trên hàng i và cột j *(chỉ quan tâm đến vị trí)*, nói phần tử $F_{i,j}$ là phần tử trên hàng i, cột j và có giá trị bằng $F_{i,j}$ *(quan tâm đến cả vị trí và giá trị)*. Hai giá trị $F_{i,j}$, $F_{u,v}$ khác tính chẵn lẻ được ký hiệu là $F_{i,j}\# F_{u,v}$

Định nghĩa 2.1 Phép nhân đồng vị ⊗ hai ma trận $A \in I^{m\times n}, B \in I^{m\times n}$ ký hiệu là C = A ⊗ B và được xác định theo công thức: $C_{i,j} = A_{i,j} \times B_{i,j}$ với i=1,2,…,m và j = 1,2,…,n

Định nghĩa 2.2 Phép toán SUM trên ma trận $A \in I^{m\times n}$ là một số nguyên, ký hiệu SUM(A) và tính theo công thức:

$$SUM(A) = \sum_{i=1}^{m}\sum_{j=1}^{n} A_{i,j}$$

Định nghĩa 2.3 Phép toán MOD trên ma trận nguyên $F \in I^{m\times n}$ là ma trận nhị phân cấp m×n ký hiệu là:

C = MOD(F) và được tính theo công thức: $C_{i,j} = F_{i,j}$ mod 2 với i =1,2,...,m và j = 1,2,…,n

Định nghĩa 2.4 Trên ma trận $F \in I^{m\times n}$, phần tử (u,v) được gọi là liền kề với phần tử (i,j) ký hiệu là:

(i,j)⇔(u,v) nếu Max{|u-i|, |v-j|}= 1

Định nghĩa 2.5 Ma trận nhị phân $K \in I^{m\times n}$ được gọi là ma trận liên thông nếu với mỗi cặp hai phần tử bất

kỳ không kề nhau (i,j) và (u,v) có giá trị $K_{i,j}=K_{u,v}=1$ luôn tồn tại dãy các phần tử (p_t,q_t), t=1,…,k sao cho: $K_{p_t,q_t}=1$, t= 1,..k và

$$(i,j)\Leftrightarrow(p_1,q_1)\Leftrightarrow(p_2,q_2)\Leftrightarrow....\Leftrightarrow(p_k,q_k)\Leftrightarrow(u,v)$$

III. THUẬT TOÁN ĐỀ XUẤT

Với ảnh có bảng màu, dữ liệu ảnh là một ma trận gồm các chỉ số màu có giá trị nguyên từ 0 đến 255. Ma trận dữ liệu ảnh được chia thành các ma trận con cùng cấp và thuật toán sẽ giấu một bít dữ liệu trên mỗi ma trận con. Để tiện cho việc theo dõi, dưới đây sẽ trình bày thuật toán giấu một bít vào một ma trận con.

III.1. Ý tưởng của thuật toán đề xuất

Giả sử cần nhúng một bít tin mật b vào ma trận con $F \in I^{m\times n}$. Thuật toán đề xuất dựa trên ý tưởng giấu tin của Wu-Lee[11], sử dụng ma trân nhị phân $K \in I^{m\times n}$ làm khóa bí mật và biến đổi nhiều nhất một phần tử trên F để $SUM(F\otimes K)$ cùng tính chẵn lẻ với b.

Trong thuật toán Wu-Lee, $F_{i,j}$ là các giá trị 0 hoặc 1, nên việc biến đổi một phần tử trên F chỉ đơn giản là chuyển từ 0 sang 1 hoặc từ 1 sang 0. Ở đây, $F_{i,j}$ có giá trị từ 0 đến 255. Vấn đề chọn phần tử nào để biến đổi và chọn giá mới cho phần tử cần biến đổi để nâng cao chất lượng của ảnh sau khi giấu tin là các nội dung chính của thuật toán đề xuất.

Trong thuật toán đề xuất sử dụng ma trận khóa nhị phân liên thông K với điều kiên SUM(K) $\geq$ 3. Khi thực hiện thành công *(có giấu tin)*, thuật toán sẽ cho ma trận G thỏa mãn các điều kiện:

- $1\leq$ SUM(MOD(G)$\otimes$K) $\leq$ SUM(K) – 1 (3.1)
- SUM(G$\otimes$K) mod 2 = b (3.2)
- F và G khác nhau tối đa một phần tử

Các điều kiện (3.1) và (3.2) được sử dụng để khôi phục tin giấu.

III.2. Nội dung thuật toán giấu tin

Bước 1: Đặt s = SUM(MOD(F)$\otimes$K)

Bước 2: Kiểm tra điều kiện giấu tin, xét hai trường hợp:

1) Nếu s = 0 hoặc s = SUM(K), không giấu tin và kết thúc thuật toán.
2) Nếu 1$\leq$ s $\leq$SUM(K)-1, chuyển sang Bước 3

Bước 3: Xét hai khả năng:

1) Nếu s mod 2 = b, đặt G = F và kết thúc thuật toán
2) Nếu s mod 2 $\neq$ b, chuyển sang Bước 4

Bước 4: Xây dựng tập $\prod$ theo công thức

$$\prod=\begin{cases}\{(i,j)|\ K_{i,j}=1, F_{i,j}\ chẵn, \exists(u,v): (u,v)\Leftrightarrow(i,j) và\ F_{u,v}\#F_{i,j}\}, nếu\ s=1\\ \{(i,j)|K_{i,j}=1, F_{i,j}\ lẻ, \exists(u,v): (u,v)\Leftrightarrow(i,j) và\ F_{u,v}\#F_{i,j}\}, nếu\ s=SUM(K)-1\\ \{(i,j)|K_{i,j}=1, \exists(u,v): (u,v)\Leftrightarrow(i,j) và\ F_{u,v}\#F_{i,j}\}, nếu\ 2\leq s\leq SUM(K)-2\end{cases}$$

Bước 5: Biến đổi F để nhận được G, thực hiện tuần tự như sau:

1) Chọn một phần tử (i,j) $\in \prod$

2) Chọn một phần tử (u,v) sao cho: (u,v) $\Leftrightarrow$ (i,j) và $F_{u,v}$ # $F_{i,j}$ (*Theo định nghĩa của* $\prod$, *luôn tồn tại (u,v) như vậy)*

3) Thay $F_{i,j}$ bằng $F_{u,v}$. Đặt G = F, kết thúc thuật toán.

Nhận xét 1: Dễ dàng thấy rằng, khi thuật toán thực hiện thành công *(kết thúc tại Bước 3 hoặc Bước 5)*, G luôn thỏa mãn các điều kiện (3.1) và (3.2). Như vậy, để chứng minh tính đúng đắn của thuật toán chỉ cần chỉ ra $\prod \neq \emptyset$. Điều này sẽ được chứng minh trong mục 4.

Nhận xét 2: Trong Bước 5 có thể có nhiều cách chọn (i,j) và (u,v). Dưới đây sẽ trình bày phương pháp xác định (i,j) và (u,v) để thuật toán giấu tin có thể đạt được tính che giấu cao.

Đầu tiên chọn (i,j) sao cho:

(i,j) $\in \prod$ và g(i,j) = max {g(p,q)| (p,q) $\in \prod$}

Ở đây g(p,q) là số phần tử trên ma trận F liền kề với (p,q) và có giá trị bằng $F_{p,q}$.

Sau khi đã có (i,j), (u,v) được chọn trong tập $\Omega_{i,j}$ gồm các phần tử liền kề với (i,j) và khác tính chẵn lẻ với $F_{i,j}$:

$$\Omega_{i,j}=\{(p,q)\,|\,(p,q)<=>(i,j)\ va`\ F_{p,q}\#F_{i,j}\}$$

Với mỗi (p,q) $\in \Omega_{i,j}$, gọi f(p,q) là số phần tử trong $\Omega_{i,j}$ có giá trị bằng $F_{p,q}$.

Chọn (u,v) sao cho:

$$(u,v) \Leftrightarrow (i,j) \text{ và } f(u,v) = \max\{f(p,q) | (p,q) \in \Omega_{i,j}\}$$

Cách chọn này đảm bảo hai yêu cầu:

- Phần tử được chọn để biến đổi nằm trên khóa K và xung quanh nó có nhiều phần tử cùng giá trị với nó nhất.
- Giá trị thay thế khác tính chẵn lẻ với phần tử được chọn và xung quanh phần tử được chọn có nhiều phần tử cùng giá trị với giá trị thay thế.

Do phần tử được chọn (i,j) nằm trên khóa K *($K_{i,j}=1$)*, nên sau khi thay đổi giá trị $F_{i,j}$ từ chẵn sang lẻ hoặc ngược lại thì SUM(F⊗K) sẽ thay đổi tính chẵn lẻ, do đó ma trận G luôn thỏa mãn điều kiện (3.2). Mặt khác cách thay đổi màu tại điểm (i,j) như vậy, sẽ rất khó phát hiện vì xung quanh nó luôn có các điểm cùng màu với màu mới và nhiều khả năng tồn tại các điểm cùng màu mới màu cũ của điểm (i,j). Điều này làm tăng tính che giấu của thuật toán.

III.3. Minh họa thuật toán

Giả sử K bằng :

0	1	0
1	0	1
0	1	1

Hình 3.1 Khóa K

Dãy bít cần giấu: $b_1b_2b_3b_4$ = 1100, ảnh được chia thành 4 khối:

F^1			F^2		
145	46	253	139	179	200
120	34	46	47	78	78
105	230	139	16	39	39
245	76	34	195	246	195
78	53	57	57	249	230
53	78	64	231	23	199
F^3			F^4		

Hình 3.2 Ảnh trước khi giấu tin

Trong ví dụ này: SUM(K) = **5**, dưới đây sẽ minh họa thuật toán giấu bít b_i vào khối F^i (i = 1,2,3,4).

Giấu b_1 =1 vào F^1:

s = SUM(MOD(F^1)⊗K)= 1, do 0<s<SUM(K) sang Bước 3: s mod 2 = b_1, $G^1 = F^1$

Giấu b_2=1 vào F^2:

s = SUM(MOD(F^2)⊗K)= 4, do 0<s<SUM(K) sang Bước 3: s mod 2 ≠ b_2, sang bước 4:

$$\prod = \{(1,2), (2,1), (3,2), (3,3)\}$$

Theo nhận xét 2: g(1,2)=0, g(2,1)=0, g(3,2)=1, g(3,3)=1, nên chọn (i,j)=(3,2);

Khi đó: $\Omega_{3,2}$={(2,2),(2,3),(3,1)} và f(2,2)=1, f(2,3)=1, f(3,1)=0.

Chọn (u,v) = (2,2) và thay $F^2_{3,2}$ bằng $F^2_{2,2}$, đặt $G^2=F^2$.

Giấu b_3= 0 vào F^3:

s = SUM(MOD(F^3)⊗K) = 1, do 0<s<SUM(K) sang Bước 3: s mod 2 ≠ b_3, sang bước 4:

$$\prod = \{(1,2), (2,1), (3,2), (3,3)\}$$

Theo nhận xét 2: g(1,2)=0, g(2,1)=1, g(3,2)=1, g(3,3)=0, nên chọn (i,j)=(2,1)

Khi đó $\Omega_{2,1}$={(1,1), (2,2), (3,1)} và f(1,1)=0, f(2,2)=1, f(3,1)=1

Chọn (u,v)=(3,1), thay $F^3_{2,1}$ bằng $F^3_{3,}1$ và đặt $G^3 = F^3$.

Giấu b_4=0 vào F^4:

s = SUM(MOD(F^4)⊗K) = 3, do 0<s<SUM(K) sang Bước 3: s mod 2 ≠ b_4, sang bước 4:

$$\prod = \{(1,2), (2,1), (2,3), (3,2), (3,3)\}$$

Theo nhận xét 2, chọn (i,j) = (1,2) và (u,v) = (1,1). Thay $F^4_{1,2}$ bằng $F^4_{1,1}$ và đặt $G^4 = F^4$.

Như vậy, các G^i nhận được sau khi kết thúc thuật toán giấu tin như hình sau:

G^1			**G^2**		
145	46	253	139	179	200
120	34	46	47	78	78
105	230	139	16	78	39
245	76	34	195	195	195
53	53	57	57	249	230
53	78	64	231	23	199
G^3			**G^4**		

Hình 3.3 Ảnh sau khi giấu tin

III.4. Thuật toán khôi phục thông tin

Giả sử G là ma trận giấu một bít tin mật và K là ma trận khóa được sử dụng trong thuật toán giấu tin. Dựa trên các điều kiện (3.1) và (3.2), có thể xây dựng thuật toán khôi phục bít tin mật như sau:

Bước 1: Tính s'= SUM(MOD(G)⊗K)

Bước 2: Kiểm tra G có giấu tin hay không

Nếu s'= 0 hoặc s'= SUM(K), kết luận G không chứa tin giấu

Trái lại, tính b = s' mod 2, b là bít tin mật cần khôi phục.

III.5. Tính bảo mật của sơ đồ

Mục đích của giấu tin là để bảo vệ dữ liệu được nhúng trên các môi trường trao đổi thông tin. Vì vậy, mỗi một sơ đồ giấu tin đều phải có tính an toàn bảo mật bằng cách đưa vào các khóa bí mật. Khóa bí mật được sử dụng trong cả thuật toán giấu tin và khôi phục thông tin.

Trong lược đồ đề xuất, sử dụng một ma trận nhị phân liên thông K cấp m×n làm khóa bí mật. Do đó số phương án khóa xấp xỉ bằng 2^{mxn}. Đây là một số khá lớn, vì vậy, việc dò tìm khóa K để trích rút thông tin mật đã nhúng trong ảnh là một việc làm tương đối khó khăn. Như vậy, vai trò của khóa K là để ngăn ngừa việc sử dụng trái phép thông tin mật đã nhúng trong ảnh, làm cho quá trình trao đổi thông tin trở lên an toàn hơn.

IV. TÍNH ĐÚNG ĐẮN CỦA THUẬT TOÁN

Trước hết ta xét một số khái niệm và bổ đề sau:

Đặt:

$Q_1 = \{(i,j) | K_{i,j} = 1$ và $F_{i,j}$ lẻ$\}$ (4.1)

$Q_2 = \{(u,v) | K_{u,v} = 1$ và $F_{u,v}$ chẵn$\}$ (4.2)

Từ (4.1) và (4.2) dễ dàng suy ra:

$Q_1 \cap Q_2 = \Phi$ và $|Q_1| + |Q_2| = SUM(K)$ (4.3)

Bổ đề: Nếu $Q_1 \neq \Phi$, $Q_2 \neq \Phi$ và K là ma trận nhị phân liên thông thì luôn tồn tại hai phần tử (i,j) và (u,v) sao cho:

$(i,j) \Leftrightarrow (u,v)$, $(i,j) \in Q_1$ và $(u,v) \in Q_2$

Chứng minh bổ đề

Do $Q_1 \neq \Phi$ và $Q_2 \neq \Phi$ nên có thể chọn một phần tử $(i_0,j_0) \in Q_1$ và $(u_0,v_0) \in Q_2$. Nếu hai phần tử $(i_0,j_0) \Leftrightarrow (u_0,v_0)$ thì đương nhiên bổ đề đúng với (i,j)= (i_0,j_0) và (u,v) = (u_0,v_0). Trong trường hợp hai phần tử (i_0,j_0) và (u_0,v_0) không kề nhau, thì do K liên thông nên phải tồn tại dãy các phần tử (p_t,q_t), t = 1,…,k sao cho:

$K_{p_t,q_t} = 1$, t= 1,..k

$(i_0,j_0) \Leftrightarrow (p_1,q_1) \Leftrightarrow (p_2,q_2) \Leftrightarrow .... \Leftrightarrow (p_k,q_k) \Leftrightarrow (u_0,v_0)$

Nếu cả k phần tử của dãy thuộc Q_2, thì bổ đề đúng với (i,j) = (i_0,j_0) và (u,v) = (p_1,q_1). Trong trường hợp trái lại *(dãy có ít nhất một phần tử* $\in Q_1$*)*, gọi (p_h,q_h) là phần tử cuối cùng của dãy thuộc Q_1. Nếu h= k thì bổ đề đúng với (i,j) = (p_k,q_k) và (u,v) = (u_0,v_0). Nếu h<k thì do (p_h,q_h) là phần tử cuối cùng thuộc Q_1 nên (p_{h+1},q_{h+1}) phải thuộc Q_2, do đó bổ đề đúng với (i,j)=(p_h,q_h) và (u,v) = (p_{h+1},q_{h+1}).

Vậy bổ đề được chứng minh.

Chứng minh tính đúng đắn của thuật toán:

Trước hết từ (4.1) dễ dàng suy ra:

$$s = SUM(MOD(F)\otimes K) = |Q_1| \qquad (4.4)$$

Theo nhận xét 1 trong mục 3, để chứng minh tính đúng đắn của thuật toán chỉ cần chỉ ra $\prod \neq \emptyset$. Ta xét lần lượt xét ba trường hợp: s =1, s = SUM(K)-1 và 1<s<SUM(K)-1.

1) *Nếu s =1 thì theo Bước 4 (mục 3):*

$\prod = \{(i,j) | K_{i,j} = 1, F_{i,j}$ chẵn, $\exists (u,v): (u,v) \Leftrightarrow (i,j)$ và $F_{u,v} \# F_{i,j}\}$

Ngoài ra từ (4.3) và (4.4) ta có:

$|Q_1| = s = 1$

$|Q_2| = SUM(K) - |Q_1| = SUM(K) - 1$

Vậy $Q_1 \neq \Phi$ và $Q_2 \neq \Phi$ nên theo bổ đề suy ra tồn tại $(u,v) \in Q_1$, $(i,j) \in Q_2$ và $(u,v) \Leftrightarrow (i,j)$. Theo định nghĩa Q_1, Q_2 thì: $F_{u,v}$ lẻ, $K_{i,j}$= 1 và $F_{i,j}$ chẵn. Từ đó suy ra $(i,j) \in \prod$, vậy $\prod \neq \Phi$.

2) *Nếu s = SUM(K) - 1 thì theo Bước 4:*

$\prod = \{(i,j) | K_{i,j} = 1, F_{i,j}$ lẻ, $\exists (u,v): (u,v) \Leftrightarrow (i,j)$ và $F_{u,v} \# F_{i,j}\}$

Ngoài ra từ (4.3) và (4.4) ta có:

$|Q_1| = s = SUM(K) - 1$

$|Q_2| = SUM(K) - |Q_1| = 1$

Vậy $Q_1 \neq \Phi$ và $Q_2 \neq \Phi$ nên theo bổ đề suy ra tồn tại $(i,j) \in Q_1$, $(u,v) \in Q_2$ và $(i,j) \Leftrightarrow (u,v)$. Theo định nghĩa Q_1, Q_2 thì: $K_{i,j} = 1$, $F_{i,j}$ lẻ, $F_{u,v}$ chẵn. Từ đó suy ra $(i,j) \in \prod$, vậy $\prod \neq \Phi$.

3) Nếu 1< s < SUM(K) -1 thì theo Bước 4:

$\prod = \{(i,j) \mid K_{i,j} = 1, \exists (u,v): (u,v) \Leftrightarrow (i,j)$ và $F_{u,v} \# F_{i,j}\}$

Ngoài ra từ (4.3) và (4.4) ta có:

$1 < |Q_1| < SUM(K) - 1$

$|Q_2| = SUM(K) - |Q_1| > 1$

Vậy $Q_1 \neq \Phi$ và $Q_2 \neq \Phi$ nên theo bổ đề suy ra tồn tại $(i,j) \in Q_1$, $(u,v) \in Q_2$ và $(i,j) \Leftrightarrow (u,v)$. Theo định nghĩa Q_1, Q_2 thì: $K_{i,j} = K_{u,v} = 1$, $F_{i,j}$ lẻ, $F_{u,v}$ chẵn. Từ đó suy ra cả (i,j) và (u,v) đều thuộc $\prod$, vậy $\prod \neq \Phi$.

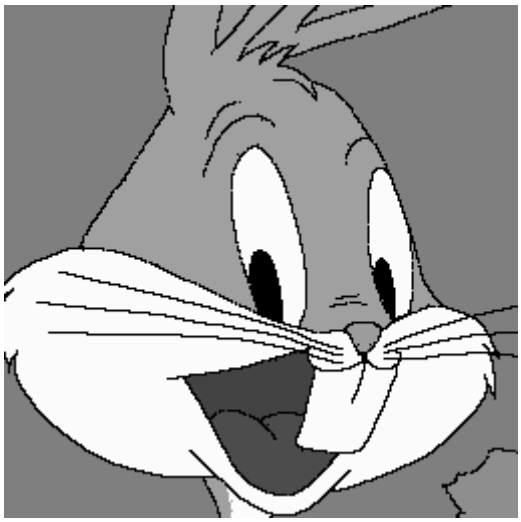
V. THỰC NGHIỆM

Để so sánh tính che giấu của thuật toán đề xuất với hai thuật toán Ez Stego và Fridrich, chúng tôi đã cài đặt và thực hiện giấu tin theo cả ba thuật toán trên cùng các tham số đầu vào được cho như sau:

- Dữ liệu nhúng là 461 bít được tạo ngẫu nhiên
- Ảnh gốc có 8 màu và kích thước 256× 256

a) Ảnh gốc

Ảnh sau khi nhúng 461 bít của các thuật toán:



b) Ảnh của lược đồ đề xuất

c) Ảnh của thuật toán Fridrich

d) Ảnh của thuật toán Ez Stego

Kết quả thực nghiệm cho thấy rằng, trên các ảnh của hai thuật toán Fridrich, Ez Stego có xuất hiện màu cô lập, nhưng màu cô lập không xuất hiện trên ảnh của thuật toán đề xuất. Thay vào đó, các màu bị biến đổi của ảnh trong thuật toán đề xuất chỉ xuất hiện ở những vị trí giáp ranh và luôn tồn tại các điểm ảnh lân cận có màu giống với màu bị biến đổi.

6. KẾT LUẬN

Bài báo đề xuất một thuật toán giấu tin mới áp dụng cho ảnh có bảng màu. Theo đó, dữ liệu ảnh được chia thành các khối cùng cấp m×n, mỗi khối có thể giấu được một bít và biến đổi nhiều nhất một phần tử của khối. Khi cần biến đổi một phần tử, thuật toán sẽ lựa chọn vị trí thay đổi và giá trị thay thế hợp lý để không làm xuất hiện màu cô lập, do đó nâng cao chất lượng của ảnh sau khi giấu tin. Kết quả thực nghiệm chỉ ra rằng, tính che giấu của thuật toán đề xuất tốt hơn so với hai thuật toán Ez Stego và Fridrich.

Trong [6], các tác giả G. Pan, Z. Wu, Y. Pan đã thực nghiệm giấu tin trên cùng ảnh được sử dụng trong bài báo này. Qua quan sát cho thấy, tính che giấu của thuật toán [6] có phần cao hơn so với thuật toán đề xuất, nhưng lượng thông tin giấu ít hơn. Thử nghiệm trong [6] nhúng 289 bít, còn thực nghiệm trong bài báo này nhúng 461 bít.

TÀI LIỆU THAM KHẢO

[1] PHẠM VĂN ẤT, NGUYỄN HIẾU CƯỜNG, ĐỖ VĂN TUẤN, BÙI HỒNG QUẾ, TRẦN ĐĂNG HIÊN, *Một số nhận xét về phương pháp giấu tin của Chen – Pan – Tseng*, Kỷ yếu Hội thảo: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông, 2007

[2] PHẠM VĂN ẤT, ĐỖ VĂN TUẤN, NGUYỄN HIẾU CƯỜNG, *Thuật toán giấu tin dung lượng cao*, Tạp chí Khoa học Giao thông vận tải, số 19 năm 2007

[3] J. FRIDRICH, *Secure steganographic methods for palette images*, Proceedings of 3rd Int. Workshop on Information Hiding,1999.

[4] J. FRIDRICH, J.DU, *Secure Steganographic Methods for Pallete Image.* The 3rd Information Hiding Workshop, Lecture Notes in Computer Science. 1768, 47-60 (2000)

[5] M.Y. WU, Y. H. HO, JIA-HONG LEE, *An iterative method of palette-based image steganography*, Pattern Recognition Letters 25, 301–309, (2004)

[6] GANG PAN, ZHAOHUI WU, YUNHE PAN, *A Data Hiding Method for Few – Color Images.* IEEE Proceedings of the 2002 International Conference on Acoustic, Speech, and Signal Processing, ICASSP 02, Vol. 4, 13-17 May 2002

[7] R. MACHADO. EZ STEGO, http://www.scribd.com/doc/62118082/105/EZ-Stego

[8] S.M. KIM, ZIQIANG CHENG, KEE YOUNG YOO, *A New Steganography Scheme based on an Index-color Image*, Sixth International Conference on Information Technology, (2009)

[9] S. KR GHOSAL, *A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique*. IEM, (2011)

[10] V. K. SHARMA, V. SHRIVASTAVA, *A Steganography Algorithm For Hiding Image In Image By Improved Lsb Substitution By Minimizedetection*, Journal of Theoretical and Applied Information Technology (2012)

[11] M. WU, J. LEE. *A novel data embedding method for two-color fascimile images.* In Proceedings of international symposium on multimedia information processing. Chung-Li, Taiwan, R.O.C, 1998

[12] YU-CHEE TSENG, HSIANG-KUANG PAN. *Secure and Invisible Data Hiding in 2-Color Images.* INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, 887 - 896 vol.2

Nhận bài ngày: 02/02/2012

SƠ LƯỢC VỀ TÁC GIẢ

PHẠM VĂN ẤT

Sinh ngày 12/6/1945 tại Hà Nội.

Tốt nghiệp Đại học năm 1967 và tiến sĩ năm 1980 tại Trường Đại học Tổng hợp Hà Nội. Năm 1984 nhận học hàm PGS.

Hiện giảng dạy tại Khoa CNTT – Trường Đại học Giao thông Vận tải Hà Nội.

Lĩnh vực quan tâm: Lý thuyết ma trận, xử lý ảnh, an toàn thông tin, phân tích dữ liệu.

Email: phamvanat83@vnn.vn

ĐỖ VĂN TUẤN

Sinh ngày 9/6/1975 tại Hải Dương.

Tốt nghiệp Đại học HVKTQS năm 2002, Thạc sĩ năm 2007 tại Trường Đại học Công nghệ – ĐHQGHN.

Hiện giảng dạy tại Khoa CNTT – Trường Cao đẳng Thương mại và Du lịch Hà Nội.

Lĩnh vực quan tâm: Giấu tin, mật mã, phát hiện ảnh giả mạo

Email: dvtuanest@gmail.com