Một thuật toán thủy vân bền vững khóa công khai cho ảnh màu dựa trên sự hoán vị ngẫu nhiên trong các tập con

A New Public Key Robust Watermarking Algorithm for Color Images Based on Random Permutation in Subsets

Đỗ Văn Tuấn, Trần Đăng Hiên, Cao Thị Luyên và Phạm Văn Ất

Abstract*: This paper proposes a new watermarking algorithm that is an improvement of the public key robust watermarking algorithm for color images of R.Munir. In this new algorithm, the public key is a real sequence chosen according to a normal distribution with mean = 0 and variance = 1, and the secret key is a random permutation in subsets of the public key. The theoretical analysis and experimental results show that the proposed algorithm is more robust than R.Munir algorithm while quality of watermarked images is the same.*

Keywords*: Robust watermarking, public key watermarking, correlation*

I. GIỚI THIỆU

Hiện nay, các thông tin quan trọng thường được lưu trữ và truyền tải dưới dạng các tệp dữ liệu số như: ảnh, âm thanh và video. Với sự trợ giúp của phần mềm, người dùng có thể dễ dàng tạo ra các bản sao có chất lượng ngang bằng so với dữ liệu gốc. Bên cạnh đó, vấn nạn sao chép, tái phân phối bất hợp pháp, làm giả dữ liệu số ngày một gia tăng. Do vậy, bài toán bảo vệ dữ liệu số nói chung và ảnh số nói riêng đang nhận được nhiều sự quan tâm của các nhà nghiên cứu trong và ngoài nước.

Thủy vân ảnh là kỹ thuật nhúng thông tin vào dữ liệu ảnh trước khi ảnh được phân phối trên môi trường trao đổi không an toàn, việc nhúng thông tin vào ảnh sẽ làm giảm chất lượng ảnh. Tuy nhiên, thông tin đã nhúng sẽ là dấu vết để nhận biết sự tấn công trái phép, hoặc để xác định thông tin về chủ sở hữu.

Dựa vào mục đích sử dụng, các thuật toán thủy vân có thể được chia thành hai nhóm chính: thủy vân dễ vỡ [4,7,8,13,16,17] và thủy vân bền vững [5,6,10, 15]. Thủy vân dễ vỡ, gồm những thuật toán nhúng tin nhằm phát hiện ra sự biến đổi dù chỉ vài bít trên dữ liệu số. Do vậy, thủy vân dễ vỡ thường được ứng dụng trong bài toán xác thực tính toàn vẹn của dữ liệu trên môi trường trao đổi công khai.

Trái với thủy vân dễ vỡ, thủy vân bền vững yêu cầu dấu thủy vân phải tồn tại *(bền vững)* trước những phép tấn công nhằm loại bỏ dấu thủy vân, hoặc trong trường hợp loại bỏ được dấu thủy vân thì ảnh sau khi bị tấn công cũng không còn giá trị sử dụng. Do vậy, những thuật toán thủy vân bền vững thường được ứng dụng trong bài toán bảo vệ quyền chủ sở hữu. Theo kết quả khảo sát trong [5], các phép tấn công phổ biến nhằm loại bỏ dấu thủy vân thường được sử dụng là: nén JPEG, thêm nhiễu, lọc, xoay, cắt xén, làm mờ, thay đổi kích thước, thay đổi sáng tối, thay đổi tương phản. Hầu hết các thuật toán thủy vân bền vững thường nhúng dấu thủy vân trên miền biến đổi của ảnh [5,6,10,15] thông qua các phép biến đổi như DFT, DCT, DWT, SVD và NMF.

Mặt khác, dựa vào việc sử dụng khóa người ta chia các thuật toán thủy vân thành hai nhóm: thủy vân khóa bí mật [1,3-7,11-14] và thủy vân khóa công khai [9,10,15-17]. Thuật toán thủy vân khóa bí mật sử dụng chung một khóa cho cả hai quá trình nhúng và kiểm tra dấu thủy vân. Trong khi thủy vân khóa công khai sử dụng khóa bí mật để nhúng dấu thủy vân và khóa công khai để kiểm tra dấu thủy vân. Đối với thuật toán thủy vân bí mật, do sử dụng chung khóa cho cả hai

quá trình nên cần phải có công đoạn trao đổi khóa giữa người nhúng và người kiểm tra dấu thủy vân, điều này dẫn đến việc bảo mật khóa gặp phải những khó khăn. Tuy nhiên, hạn chế này không xuất hiện trong thuật toán thủy vân khóa công khai.

Dựa trên ý tưởng của ba thuật toán thủy vân I.J.Cox[5], M.Barni[6] và R.Munir[10], bài báo này đề xuất một thuật toán mới tương tự như thuật toán R.Munir nhưng có một số cải tiến trong việc xây dựng khóa bí mật, nhờ đó tính bền vững của thuật được cải thiện rõ rệt. Nội dung tiếp theo của bài báo được tổ chức như sau: Mục 2 trình bày tóm tắt các thuật toán thủy vân I.J.Cox[5], M.Barni[6] và R.Munir[10]. Mục 3 trình bày thuật toán đề xuất. Việc so sánh tính bền vững của thuật toán đề xuất với thuật toán R.Munir bằng cả phân tích lý thuyết và kết quả thực nghiệm được trình bày trong Mục 4. Cuối cùng là một số kết luận được trình bày trong mục 5.

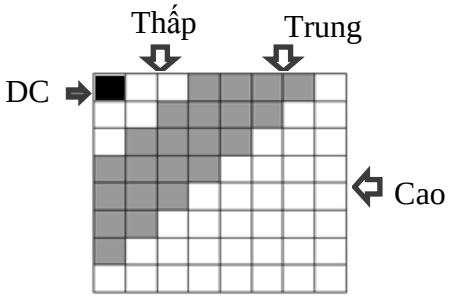
II. MỘT SỐ THUẬT TOÁN THỦY VÂN BỀN VỮNG TRÊN MIỀN DCT

Như đã nói ở trên, thuật toán đề xuất là sự phát triển tiếp theo của ba thuật toán thủy vân bền vững trên miền DCT là I.J.Cox [5], M.Barni [6] và R.Munir [10], trong đó hai thuật toán I.J.Cox [5] và M.Barni [6] sử dụng khóa bí mật còn thuật toán R.Munir [10] sử dụng khóa công khai. Để tiện theo dõi, phần này sẽ trình bày tóm tắt miền DCT và nội dung ba thuật toán trên.

II.1. Miền DCT

Ảnh gốc I được chia thành các khối ảnh có kích thước 8×8 điểm. Áp dụng phép biến đổi DCT cho mỗi khối ảnh sẽ nhận được các khối DCT tương ứng có kích thước 8×8. Các hệ số trên khối DCT được chia thành ba vùng: tần số thấp, tần số trung và tần số cao (Hình 1).

Theo tính chất của phép biến đổi Cosine rời rạc [2], năng lượng của ảnh thường tập trung vào các hệ số góc trên bên trái của khối, đặc biệt là phần tử DC. Do vậy, nếu nhúng dấu thủy vân vào các hệ số tần số thấp thì sẽ tăng tính bền vững nhưng lại giảm chất lượng của ảnh *(tính che giấu thấp).* Trái lại, nếu sử dụng các hệ số vùng tần số cao để nhúng dấu thủy vân thì tính che giấu cao nhưng tính bền vững lại thấp. Để cân bằng giữa tính bền vững và tính che giấu của ảnh thủy vân, các thuật toán thủy vân thường nhúng dấu thủy vân trên các hệ số DCT thuộc vùng tần số trung.



Hình 1. Khối DCT kích thước 8×8

II.2. Thuật toán của I.J.Cox

Thuật toán thủy vân I.J.Cox[5] sử dụng các hệ số DCT thuộc vùng tần số thấp *(trừ phần tử DC)* và tần số trung của ảnh I để nhúng dấu thủy vân, ký hiệu các hệ số này là $D = (d_1, d_2, \dots, d_n)$. Độ dài của dãy D thường được chọn bằng 25% kích thước ảnh. Dấu thủy vân là một dãy số thực được tạo ngẫu nhiên theo phân bố chuẩn $N(0,1)$, ký hiệu dãy này là $W = (w_1, w_2, \dots, w_n)$. W được dùng như là một khóa bí mật trong thuật toán thủy vân và thuật toán kiểm tra dấu thủy vân. Dấu thủy vân W được nhúng vào dãy D theo công thức:

$$d_i' = d_i + \omega d_i w_i, \qquad i = 1, .., n \qquad (2.1)$$

(trong thử nghiệm các tác giả chọn $\omega = 0.1$*).* Áp dụng phép biến đổi Cosine rời rạc ngược (IDCT) cho các khối DCT sau khi đã nhúng dấu thủy vân ta sẽ nhận được ảnh I'.

Trong quá trình truyền tải, ảnh I' có thể bị tấn công trở thành ảnh I^*. Để kiểm tra dấu thủy vân của ảnh I^* *(xác định quyền tác giả đối với ảnh* I^**)*, trong [5] làm như sau:

- Xác định dấu thủy vân $W^* = (w_1^*, w_2^*, \dots, w_n^*)$ tương ứng với ảnh I^* theo công thức:

$$w_i^* = \frac{d_i^* - d_i}{\omega d_i}$$

Trong đó, d_i^* và d_i lần lượt là các hệ số DCT của ảnh I^* và ảnh gốc I.

- Tính hệ số tương quan giữa W và W^* theo công thức:

$$Sim(W, W^*) = \frac{\sum_{i=1}^{n} w_i w_i^*}{\sqrt{\sum_{i=1}^{n} (w_i^*)^2}} \qquad (2.2)$$

Hệ số tương quan $Sim(W, W^*)$ được so sánh với ngưỡng T: nếu $Sim(W, W^*) > T$ thì kết luận ảnh I^* có nhúng thủy vân. Điều đó cũng có nghĩa là I^* vẫn thuộc quyền của tác giả có ảnh gốc I.

Kết quả thực nghiệm trong [5] khẳng định thuật toán này bền vững đối với các phép xử lý ảnh thông dụng như: cắt xén, co giãn, lọc, thêm nhiễu, nén JPEG, làm mờ... Tuy nhiên, chất lượng ảnh thủy vân chưa cao do tác giả sử dụng các hệ số DCT trong vùng tần số thấp để nhúng dấu thủy vân. Ngoài ra, thuật toán này còn có nhược điểm là cần sử dụng ảnh gốc trong thuật toán kiểm tra dấu thủy vân.

II.3. Thuật toán M.Barni

Dựa vào thuật toán [5], M.Barni[6] đề xuất thuật toán mới không sử dụng ảnh gốc trong quá trình kiểm tra dấu thủy vân. Thuật toán [6] chỉ khác [5] ở hai chỗ. Thứ nhất, để nhúng dấu thủy vân thay cho (2.1) trong [6] sử dụng công thức:

$$d_i' = d_i + \omega |d_i| w_i$$

Thứ hai, để kiểm tra dấu thủy vân trên ảnh I^* thay cho (2.2) trong [6] tính giá trị trung bình của tích vô hướng *(để thống nhất với các tài liệu, trong bài báo gọi là hệ số tương quan)* giữa khóa bí mật W và dãy D^**(dãy hệ số DCT của ảnh* I^**)* theo công thức:

$$Corr(D^*, W) = \frac{1}{n} \sum_{i=1}^{n} d_i^* w_i \qquad (2.3)$$

Hệ số tương quan $Corr(D^*, W)$ được so sánh với ngưỡng T: nếu $Corr(D^*, W) > T$ thì kết luận ảnh I^* có nhúng thủy vân. Trong thử nghiệm các tác giả chọn $T = 0.7$.

Các kết quả phân tích và thực nghiệm cho thấy: so với thuật toán [5] thì thuật toán [6] có tính bền vững cao hơn và chất lượng ảnh tốt hơn. Tuy nhiên, cả hai thuật toán này đều sử dụng khóa bí mật nên việc triển khai ứng dụng còn gặp nhiều khó khăn do phải trao đổi khóa.

II.4. Thuật toán R.Munir

Dựa trên thuật toán M.Barni, R.Munir[10] đề xuất thuật toán thủy vân khóa công khai. Trong đó, khóa công khai $P = (p_1, p_2, \dots, p_n)$ là dãy số thực được tạo ngẫu nhiên theo phân bố chuẩn $N(0,1)$, khóa bí mật $S = (s_1, s_2, \dots, s_n)$ là một hoán vị ngẫu nhiên của P, còn dấu thủy vân $W = (w_1, w_2, \dots, w_n)$ là tổ hợp tuyến tính của P và S:

$$w_i = \lambda p_i + (1 - \lambda) s_i, \qquad với\ 0 < \lambda < 1 \qquad (2.4)$$

(*trong thực nghiệm các tác giả chọn* $\lambda = 0.4$). Dấu thủy vân W được nhúng vào ảnh I theo công thức:

$$d_i' = d_i + \omega |d_i| w_i\ ,\ \ với\ 0 < \omega < 1 \qquad (2.5)$$

Để kiểm tra dấu thủy vân trên ảnh I^*, trong [10] sử dụng hệ số tương quan giữa khóa công khai P và dãy D^* *(dãy hệ số DCT của ảnh* I^* *)* được tính như sau:

$$Corr(D^*, P) = \frac{1}{n} \sum_{i=1}^{n} d_i^* p_i \qquad (2.6)$$

Hệ số tương quan $Corr(D^*, P)$ được so sánh với ngưỡng T: nếu $Corr(D^*, P) > T$ thì kết luận ảnh I^* có được nhúng thủy vân và I^* vẫn thuộc về tác giả có ảnh I'. Trong thực nghiệm các tác giả chọn $T = 0.5$.

III. THUẬT TOÁN ĐỀ XUẤT

III.1. Phân tích tính bền vững của thuật toán R.Munir

Từ các công thức (2.4), (2.5) và (2.6) dễ dàng suy ra:

$$Corr(D', P) = \frac{1}{n} \sum_{i=1}^{n} d_i p_i + \frac{\lambda \omega}{n} \sum_{i=1}^{n} |d_i| (p_i)^2 + \frac{\omega(1 - \lambda)}{n} \sum_{i=1}^{n} |d_i| p_i s_i \qquad (3.1)$$

Chúng ta nhận thấy rằng, mục đích của việc tấn công nhằm tạo ra ảnh mới I^* gần giống với ảnh I' đã được khẳng định quyền tác giả. Trong trường hợp ảnh I^* sai khác ít so với I' thì hệ số tương quan $Corr(D^*, P)$ xấp xỉ bằng $Corr(D', P)$. Như vậy tính bền vững của thuật toán phụ thuộc vào $Corr(D', P)$. Nói cụ thể, hệ số này càng lớn thì tính bền vững của thuật toán càng cao, hệ số này càng nhỏ thì tính bền vững càng thấp. Để tăng tính bền vững cần xây dựng khóa bí mật S sao cho hệ số nói trên lớn. Trong công thức (3.1), do D và P là hai dãy cho trước, nên hệ số tương quan $Corr(D', P)$ chỉ phụ thuộc vào số hạng thứ 3 của vế trái. Tức là phụ thuộc vào:

$$C(s) = \sum_{i=1}^{n} |d_i| p_i s_i \qquad (3.2)$$

Do P là dãy số thực ngẫu nhiên theo phân bố chuẩn với kỳ vọng toán học bằng 0, nên số phần tử dương và số phần tử âm của P xấp xỉ bằng nhau. Ngoài ra độ chênh lệch giữa các phần tử p_i của dãy cũng khá lớn, vì vậy nếu xây dựng dãy S bằng cách hoán vị ngẫu nhiên dãy P như trong thuật toán R.Munir, có thể nhận được hệ số $C(s)$ nhỏ, thậm chí có giá trị âm. Điều này làm giảm tính bền vững của thuật toán.

Để làm tăng giá trị hệ số $C(s)$, có thể phân hoạch tập $N = \{1,2,..,n\}$ thành các tập con sao cho trên mỗi tập con các giá trị p_i cùng dấu và có độ chênh lệch nhỏ, sau đó tiến hành hoán vị ngẫu nhiên các phần tử p_i trên mỗi tập con để nhận được khóa bí mật $S = (s_1, s_2, \dots, s_n)$. Với cách làm này đảm bảo hệ số $C(s)$ luôn có giá trị dương đủ lớn, do vậy tính bền vững của thuật toán được cải thiện. Thuật toán đề xuất được thực hiện dựa trên ý tưởng này.

III.2. Phương pháp xây dựng khóa bí mật

Khóa bí mật $S = (s_1, s_2, \dots, s_n)$ được tạo từ khóa công khai $P = (p_1, p_2, \dots, p_n)$ theo các bước:

Bước 1: Phân hoạch tập N thành các tập con $N^k = \{\alpha(k,1), \alpha(k,2), .., \alpha(k,\beta_k)\}$, k = 1..m, sao cho hai tính chất sau đây thỏa mãn với mỗi k:

1) $\max\{p_j \mid j \in N^k\} \le \min\{p_j \mid j \in N^{k+1}\}$
2) Các phần tử p_i với $i \in N^k$ có cùng dấu

(Hai tính chất này đảm bảo giá trị các phần tử p_i trên mỗi tập con N^k cùng dấu và độ chênh lệch nhỏ)

Bước 2: Hoán vị ngẫu nhiên tập N^k để nhận được dãy

$$R^k = (\partial(k,1), .., \partial(k,\beta_k))$$

Bước 3: Xác định khóa bí mật $S = (s_1, .., s_n)$ theo công thức:

$$s_{\partial(k,i)} = p_{\alpha(k,i)}, với\ i = 1, .., \beta_k\ và\ k = 1, .., m$$

Để dễ hình dung cách xây dựng khóa bí mật S ta xét ví dụ minh họa với khóa công khai $P = (0.5, -0.3, 0.1, -0.5, 0.4, 0.3, 0.4, -0.7, 0.1, -0.3)$ và tập $N = \{1,2,3,4,5,6,7,8,9,10\}$. Giả sử N được phân hoạch thành 3 tập con: $N^1 = \{2,4,8,10\}$, $N^2 = \{3,6,9\}$ và $N^3 = \{1,5,7\}$. Gọi ba hoán vị ngẫu nhiên tương ứng của $N^1, N^2\ và\ N^3$ là $R^1 = \{4,2,10,8\}, R^2 = \{9,3,6\}\ và\ R^3 = \{5,7,1\}$. Khi đó, khóa bí mật S sẽ là:

$$S = (0.4, -0.5, 0.3, -0.3, 0.5, 0.1, 0.4, -0.3, 0.1, -0.7)$$

Nhận xét: Việc phân hoạch tập N thành các tập con cũng có thể được thực hiện theo 1 trong 3 phương án sau:

1) Phân hoạch tập N theo dãy $DP = (|d_1|p_1, .., |d_n|p_n)$
2) Phân hoạch tập N theo dãy P sau đó mỗi tập con nhận được lại phân hoạch theo dãy DP
3) Thực hiện như phương án 2 nhưng theo thứ tự ngược lại. Tức là, trước tiên phân hoạch N theo dãy DP sau đó mỗi tập con nhận được lại phân hoạch theo dãy P.

III.3. Nội dung thuật toán đề xuất

Thuật toán đề xuất được thực hiện theo các bước giống như thuật toán R.Munir và chỉ khác ở cách xây dựng khóa bí mật S, cụ thể như sau:

III.3.1. Thuật toán thủy vân

Thuật toán sẽ xây dựng khóa công khai P, khóa bí mật S, dấu thủy vân W và nhúng W vào ảnh gốc I để nhận được ảnh thủy vân I'. Nội dung thuật toán gồm các bước:

Bước 1: Xác định vị trí nhúng dấu thủy vân

Chia ảnh gốc I thành các khối điểm ảnh 8×8. Áp dụng phép biến đổi DCT trên các khối điểm ảnh để

nhận được các khối DCT tương ứng. Ký hiệu $D = (d_1, d_2, \dots, d_n)$ là dãy các hệ số DCT được chọn (*trong miền tần số trung bình trên các khối DCT của ảnh I)* dùng để nhúng dấu thủy vân.

Bước 2: Tạo khóa công khai $P = (p_1, p_2, \dots, p_n)$ là một dãy số thực giả ngẫu nhiên theo phân bố chuẩn $N(0,1)$

Bước 3: Xây dựng khóa bí mật S theo mục 3.2

Bước 4: Xây dựng dấu thủy vân $W = (w_1, , \dots, w_n)$ theo công thức:

$$w_i = \lambda p_i + (1-\lambda)s_i \text{ , với } 0 < \lambda < 1$$

Bước 5: Nhúng W vào D theo công thức:

$$d_i' = d_i + \omega |d_i| w_i \text{ , với } 0 < \omega < 1$$

Bước 6: Áp dụng phép biến đổi IDCT cho các khối DCT sau khi đã nhúng dấu thủy vân để nhận được ảnh I'.

III.3.2. Thuật toán kiểm tra dấu thủy vân

Trước các phép tấn công như nén JPEG, thay đổi kích thước, lọc, nhiễu, cắt .., ảnh I' có thể bị biến đổi thành ảnh I^*. Khi đó, thuật toán xác định quyền tác giả đối với ảnh I^* được thực hiện theo các bước:

Bước 1: Thực hiện các thao tác biến đổi như Bước 1 trong thuật toán thủy vân để nhận được dãy hệ số DCT của ảnh I^*, ký hiệu $D^* = (d_1^*, d_2^*, .., d_n^*)$

Bước 2: Tính hệ số tương quan $Corr(D^*, P)$ theo công thức:

$$Corr(D^*, P) = \frac{1}{n}\sum_{i=1}^{n} d_i^* p_i$$

Bước 3: So sánh $Corr(D^*, P)$ với ngưỡng T *(trong thực nghiệm chọn* $T = 0.5$*)*

Nếu $Corr(D^*, P) > T$, kết luận ảnh I^* có chứa dấu thủy vân W và thuộc về tác giả có ảnh I'. Trái lại, ảnh I^* không thuộc về tác giả có ảnh I'.

IV. ĐÁNH GIÁ TÍNH BỀN VỮNG CỦA CÁC THUẬT TOÁN THỦY VÂN

IV.1. Một số khái niệm cần dùng

Để tiện cho việc trình bày ta ký hiệu $\Omega(N)$ là tập các hoán vị của dãy $N = (1,2,..,n)$. Khi đó, nếu viết $\alpha \in \Omega(N)$ thì có nghĩa $\alpha = (\alpha(1), \alpha(2), .., \alpha(n))$ là một hoán vị của N.

Trước khi phân tích tính bền vững của thuật toán R.Munir và thuật toán đề xuất ta xét bổ đề sau:

Bổ đề 1: Cho hai dãy số thực $X = (x_1, x_2, \dots, x_n)$ và $Y = (y_1, y_2, \dots, y_n)$, trong đó X là dãy đơn điệu tăng. Giả sử $Z = (z_1, z_2, .., z_n)$ và $Q = (q_1, q_2, .., q_n)$ là các hoán vị của Y, trong đó Z đơn điệu giảm và Q đơn điệu tăng. Khi đó:

$$\min\left\{\sum_{i=1}^{n} x_i y_{\alpha(i)} \ | \alpha \in \Omega(N)\right\} = \sum_{i=1}^{n} x_i z_i \qquad (4.1)$$

$$\max\left\{\sum_{i=1}^{n} x_i y_{\alpha(i)} \ | \alpha \in \Omega(N)\right\} = \sum_{i=1}^{n} x_i q_i \qquad (4.2)$$

Chứng minh:

Xét α bất kỳ, $\alpha \in \Omega(N)$. Do Z là một hoán vị của Y và Z đơn điệu giảm nên nếu đặt:

$a_i = (z_1 + .. + z_i) - \left(y_{\alpha(1)} + .. + y_{\alpha(i)}\right), i = 1 \dots n-1$ thì $a_i \geq 0, \forall i$. Ngoài ra bằng một số phép biến đổi đơn giản có thể nhận được:

$$\sum_{i=1}^{n} x_i z_i - \sum_{i=1}^{n} x_i y_{\alpha(i)} = \sum_{i=1}^{n-1} (x_i - x_{i+1}) a_i$$

Vì $a_i \geq 0$ và $(x_i - x_{i+1}) \leq 0$ *(do X đơn điệu tăng)* nên từ đẳng thức trên suy ra:

$$\sum_{i=1}^{n} x_i z_i \leq \sum_{i=1}^{n} x_i y_{\alpha(i)}$$

Do bất đẳng thức này đúng với $\forall \alpha \in \Omega(N)$, nên:

$$\sum_{i=1}^{n} x_i z_i = \min\left\{\sum_{i=1}^{n} x_i y_{\alpha(i)} \ | \alpha \in \Omega(N)\right\}$$

Vậy (4.1) được chứng minh. Bằng cách lập luận tương tự ta sẽ nhận được (4.2). Bổ đề được chứng minh.

IV.2. Độ đo tính bền vững

Như phân tích trong mục 3.1, tính bền vững của thuật toán R.Munir và thuật toán đề xuất có thể được đánh giá thông qua hệ số:

$$C(s) = \sum_{i=1}^{n} u_i s_i \qquad (4.3)$$

Trong đó, $u_i = |d_i|p_i$ và $S = (s_1,\dots,s_n)$ là một hoán vị của $P = (p_1,..,p_n)$. Rõ ràng giá trị $C(s)$ trong công thức (4.3) không thay đổi nếu hoán vị đồng thời giữa U và S, nên không giảm tính tổng quát có thể giả thiết U là một dãy đơn điệu tăng.

Giả sử $\alpha = \big(\alpha(1),\dots,\alpha(n)\big) \in \Omega(N)$, khi đó mỗi S có thể được biểu diễn qua một α như sau:

$$S = \big(p_{\alpha(1)},..,p_{\alpha(n)}\big)$$

nên $C(s)$ trong (4.3) có thể xem như một hàm của α:

$$C(\alpha) = \sum_{i=1}^{n} u_i p_{\alpha(i)}$$

Như vậy, tính bền vững của thuật toán được đánh giá thông qua giá trị $C(\alpha)$. Vì α không xác định duy nhất *(α được chọn một cách ngẫu nhiên)* nên ta sử dụng các đại lượng C_{min} và C_{max} như sau:

$$C_{min} = \min\{C(\alpha)\}$$
$$C_{max} = \max\{C(\alpha)\}$$

Khi đó, giá trị trung bình:

$$C_{TB} = \frac{1}{2}(C_{min} + C_{max}) \quad (4.4)$$

có thể xem như một độ đo của tính bền vững. Thuật toán nào có hệ số C_{TB} lớn hơn được xem là bền vững hơn.

Trong mục IV.3 sẽ so sánh tính bền vững của thuật toán R.Munir và thuật toán đề xuất với m = 2 *(phân hoạch tập N thành 2 tập con)*, gọi là thuật toán New2. Trong mục IV.4 sẽ đánh giá tính bền vững của thuật toán đề xuất theo tham số m. Trong mục IV.5 sẽ đối sánh tính bền vững của các thuật toán thông qua các kết quả thực nghiệm.

IV.3. So sánh tính bền vững của thuật toán R.Munir và New2

Với m = 2, theo Bước 1 mục 3.2 tập N được phân hoạch thành hai tập con N^1 và N^2 sao cho:

$$p_i \le 0, \forall i \in N^1 \text{ và } p_i > 0, \forall i \in N^2$$

Gọi n_1, n_2 là số phần tử của các tập N^1 và N^2. Do P là dãy ngẫu nhiên theo phân bố chuẩn $N(0,1)$ nên n_1 xấp xỉ n_2. Mặt khác, với giả thiết U đơn điệu tăng và do u_i cùng dấu với p_i ($vì\ u_i = |d_i|p_i$) nên ta có:

$$N^1 = \{1,..,n_1\} \text{ và } N^2 = \{n_1+1,..,n_1+n_2\}$$

Gọi $C_{\min\_New2}$, $C_{\min\_Munir}$, $C_{\max\_New2}$ và $C_{\max\_Munir}$ là C_{min} và C_{max} của các thuật toán New2, R.Munir, khi đó:

$$C_{\min\_New2} = \min \sum_{\alpha\in\Omega(N^1)} u_i p_{\alpha(i)} + \min \sum_{\beta\in\Omega(N^2)} u_i p_{\beta(i)} \quad (4.5)$$

$$C_{\min\_Munir} = \min \sum_{\alpha\in\Omega(N)} u_i p_{\alpha(i)} \quad (4.6)$$

$$C_{\max\_New2} = \max \sum_{\alpha\in\Omega(N^1)} u_i p_{\alpha(i)} + \max \sum_{\beta\in\Omega(N^2)} u_i p_{\beta(i)} \quad (4.7)$$

$$C_{\max\_Munir} = \max \sum_{\alpha\in\Omega(N)} u_i p_{\alpha(i)} \quad (4.8)$$

Giả sử $X = (x_1,..,x_n)$ là một hoán vị của P thỏa mãn hai điều kiện:

$X^1 = (x_1,..,x_{n_1})$ là một hoán vị của $(p_1,..,p_{n_1})$ và X^1 đơn điệu giảm

$X^2 = (x_{n_1+1},..,x_n)$ là một hoán vị của $(p_{n_1+1},..,p_n)$ và X^2 đơn điệu giảm

Khi đó dãy Y:

$$Y = (y_1,y_2,..,y_n) = (x_{n_1+1},..,x_n,x_1,..,x_{n_1})$$

là một hoán vị của P và Y đơn điệu giảm. Theo kết luận (4.1) của Bổ đề 1, các giá trị $C_{\min\_New2}$, $C_{\min\_Munir}$ *(trong các công thức (4.5) và (4.6))* có thể xác định thông qua X^1, X^2 và Y như sau:

$$C_{\min\_New2} = \sum_{i\in N^1} u_i x_i + \sum_{i\in N^2} u_i x_i \quad (4.9)$$

$$C_{\min\_Munir} = \sum_{i\in N^1} u_i y_i + \sum_{i\in N^2} u_i y_i \quad (4.10)$$

Do u_i và x_i cùng dấu, còn u_i và y_i nói chung là khác dấu, nên từ (4.9) và (4.10) suy ra $C_{\min\_New2} > 0$ và $C_{\min\_Munir} < 0$, có nghĩa là:

$$C_{\min\_New2} > C_{\min\_Munir} \quad (4.11)$$

Để dễ hình dung cách đánh giá $C_{\min\_New2}$ và $C_{\min\_Munir}$, ta xét ví dụ minh họa với các dãy U và P như sau:

$$U = (-60,-28,-10,5,15,28,35)$$

$$P = (-1.8, -2.5, -2, 1, 1.5, 1.8, 2)$$

Với m = 2, ta phân hoạch tập $N = \{1,2,3,4,5,6,7\}$ thành hai tập con $N^1 = \{1,2,3\}$ và $N^2 = \{4,5,6,7\}$. Do đó, $X = (-1.8, -2, -2.5,\ 2, 1.8,\ 1.5, 1)$ và $Y = (2, 1.8, 1.5, 1, -1.8, -2, -2.5)$. Theo hai công thức (4.9), (4.10), các giá trị $C_{\min\ \_New2}$ và $C_{\min\ \_Munir}$ tương ứng là:

$$C_{\min\ \_New2} = \sum_{i=1}^{7} u_i x_i = 108 + 56 + 25 + 10 + 27 + 42 + 35 = 303$$

$$C_{\min\ \_Munir} = \sum_{i=1}^{7} u_i y_i = -120 - 50.4 - 15 + 5 - 27 - 56 - 87.5 = -350.9$$

Để xác định $C_{\max\ \_New2}$ và $C_{\max\ \_Munir}$, ta xây dựng dãy $Z = (z_1, .., z_n)$ là một hoán vị của P thỏa mãn hai điều kiện :

- $Z^1 = (z_1, .., z_{n_1})$ là một hoán vị của $(p_1, .., p_{n_1})$ và Z^1 đơn điệu tăng
- $Z^2 = (z_{n_1+1}, .., z_n)$ là một hoán vị của $(p_{n_1+1}, .., p_n)$ và Z^2 đơn điệu tăng

Khi đó đương nhiên Z đơn điệu tăng. Theo kết luận (4.2) của Bổ đề 1, các giá trị $C_{\max\ \_New2}$ trong (4.7) và $C_{\max\ \_Munir}$ trong (4.8) có thể xác định qua Z như sau:

$$C_{\max\ \_New2} = \sum_{i \in N^1} u_i z_i + \sum_{i \in N^2} u_i z_i$$

$$C_{\max\ \_Munir} = \sum_{i=1}^{n} u_i z_i$$

Do đó:

$$C_{\max\ \_New2} = C_{\max\ \_Munir}$$

Kết hợp đẳng thức này với (4.4) và (4.11) suy ra:

$$C_{\mathrm{TB}\ \_New2} > C_{\mathrm{TB}\ \_Munir}$$

Như vậy có thể kết luận thuật toán New2 bền vững hơn thuật toán R.Munir. Điều này hoàn toàn phù hợp với các kết quả thực nghiệm trong mục IV.5.

IV.4. Đánh giá tính bền vững của thuật toán đề xuất theo tham số m

Nếu mỗi tập N^1, N^2 tiếp tục được phân hoạch thành hai tập con, thì N được phân hoạch thành 4 tập con (m = 4) và ta có thuật toán New4. Bằng cách lập luận tương tự như trong mục 4.3, có thể chỉ ra rằng: so với thuật toán New2 thì thuật toán New4 có hệ số C_{min} tăng, tuy nhiên C_{max} lại có thể giảm. Như vậy, về lý thuyết chưa khẳng định được khi tăng giá trị tham số m thì tính bền vững của thuật toán sẽ tăng. Tuy nhiên, kết quả thực nghiệm cho thấy, hệ số C_{TB} tăng theo giá trị tham số m. Điều này có nghĩa, tính bền vững của thuật toán đề xuất cũng có xu hướng tăng theo m.

Mặt khác, khi tham số m càng tăng thì tính bảo mật của thuật toán càng giảm *(vì số phương án xác định khóa bí mật S sẽ giảm)*. Tuy nhiên, trong thực tế, dãy DCT thường có độ dài $n \approx 25\%$ kích thước ảnh, với ảnh kích thước 200×200 thì $n \approx 10000$ và nếu ta chọn m =10 thì số phương án tìm *S* khi biết khóa công khai *P* sẽ là $(1000!)^{10}$, đây là số đủ lớn để đảm bao sự an toàn cho thuật toán đề xuất.

IV.5. Kết quả thực nghiệm

Đối với các thuật toán thủy vân bền vững, chất lượng ảnh thủy vân và mức độ bền vững của dấu thủy vân là hai tính chất quan trọng. Theo [6], chất lượng ảnh thủy vân được đánh giá bằng hệ số PSNR. Thuật toán có hệ số PSNR càng lớn thì chất lượng ảnh thủy vân càng cao. Hệ số PSNR của ảnh thủy vân I' so với ảnh gốc *I* kích thước m×n được tính theo công thức:

$$PSNR = 20.log_{10}\left(\frac{\mathrm{MAX}}{\sqrt{MSE}}\right)$$

Trong đó, MAX là giá trị cực đại của điểm ảnh và MSE được xác định theo công thức:

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - I'(i,j)]^2$$

Dưới đây trình bày hai kết quả thực nghiệm: Bảng 1 so sánh chất lượng ảnh thủy vân và hệ số tương quan khi ảnh chưa bị tấn công, hệ số tương quan của các thuật toán được tính theo công thức (2.3) và (2.6). Bảng 2 so sánh tính bền vững khi ảnh bị tấn công giữa thuật toán R.Munir và thuật toán đề xuất với tham số m = 10 *(New10)*.

a) So sánh chất lượng ảnh thủy vân và hệ số tương quan khi ảnh chưa bị tấn công

Để so sánh chất lượng ảnh thủy vân, hệ số tương quan khi ảnh chưa bị tấn công của thuật toán đề xuất với hai thuật toán R.Munir[10] và M.Barni[6], chúng tôi sử dụng chung tập khóa công khai *P (P được sinh bởi hàm normrnd trong matlab)* và các tham số $\omega = 0.4,\ \lambda = 0.6$. Dấu thủy vân được nhúng cố định trên 7840 hệ số DCT *(n=7840)* của ảnh gốc "Baboon" có kích thước 226×226. Kết quả trong Bảng 1 là giá trị trung bình của 20 lần thực hiện với các hoán vị ngẫu nhiên theo từng thuật toán *(sử dụng hàm randperm trong matlab).*

Các số liệu trong Bảng 1 cho thấy, chất lượng ảnh thủy vân của các thuật toán xấp xỉ bằng nhau. Tuy nhiên, hệ số tương quan của thuật toán đề xuất luôn cao hơn thuật toán R.Munir và xấp xỉ bằng thuật toán khóa bí mật M.Barni với tham số m = 10.

Bảng 1. Hệ số tương quan của ảnh thủy vân và PSNR

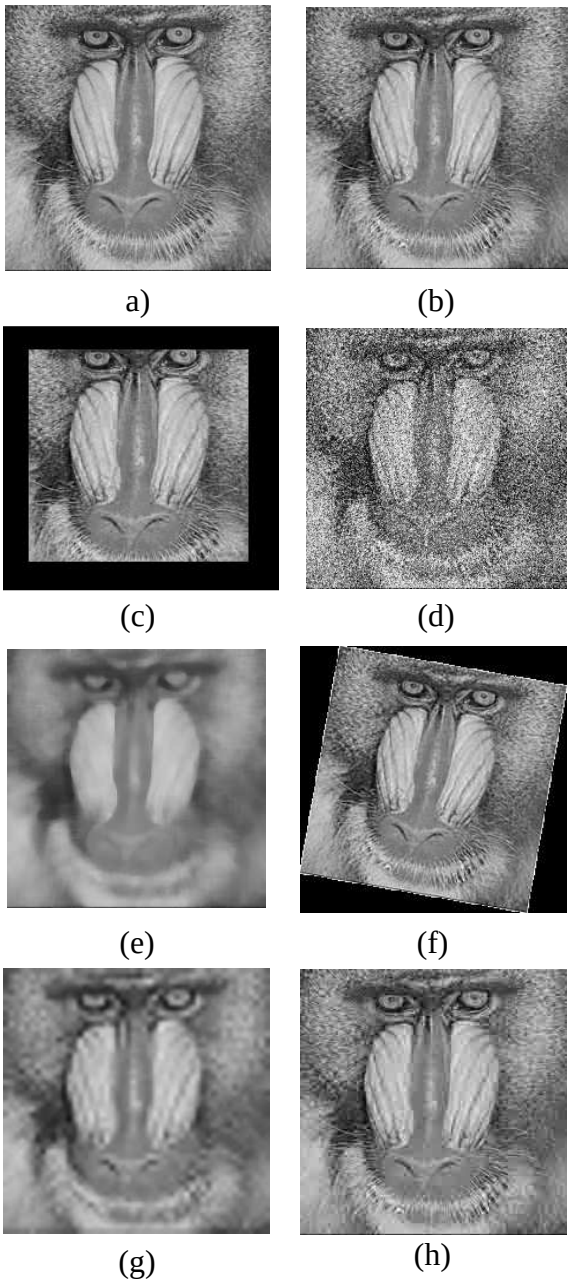
STT	Thuộc tính	New2	New4	New10	R.Munir	M.Barni
1	Hệ số tương quan	10.57	11.69	13.68	5.47	13.99
2	PSNR (dB)	41.54	41.79	41.76	41.78	41.75

Bảng 2. Hệ số tương quan của ảnh đã bị tấn công

STT	Phép tấn công	Hệ số tương quan	
		New10	R.Munir
1	Không tấn công	13.28	5.51
2	Phép cắt 20%	8.839	0.24
3	Thêm nhiễu Gause 30%	6.35	2.614
4	Lọc nhiễu trung bình (2×2)	0.783	0.02
5	Nén JPEG (low)	7.366	2.989
6	Thay đổi kích thước 226→50→226	1.366	0.3
7	Phép xoay 10^0	0.634	0.087

b) So sánh tính bền vững khi ảnh bị tấn công

Để so sánh tính bền vững giữa thuật toán đề xuất với thuật toán R.Munir, chúng tôi chọn một số phép tấn công điển hình (Bảng 2), sử dụng phần mềm Photoshop để thực hiện các thao tác tấn công trên ảnh thủy vân (Hình 2).



Hình 2. Ảnh thực nghiệm của thuật toán đề xuất**:** *(a) Ảnh gốc Baboon, (b) Ảnh thủy vân, (c) Ảnh thủy vân đã cắt 20%, (d) Ảnh thủy vân thêm nhiễu với cường độ 30%, (e) Ảnh thủy vân được lọc trung vị với kích thước mặt nạ 2×2, (f) Ảnh thủy vân xoay 10^0, (g) Ảnh thủy vân sau khi thay đổi kích thước 226→50→226, (h) Ảnh nén JPEG với chất lượng thấp.*

Các số liệu trong Bảng 2 cho thấy, trước các phép tấn công, thuật toán đề xuất bền vững hơn thuật toán R.Munir. Nếu ta chon ngưỡng $T = 0.5$, thuật toán đề xuất chống được tất cả các phép tấn công trong Bảng 2, trong khi thuật toán R.Munir chỉ chống được hai phép tấn công nén JPEG và thêm nhiễu Gause.

V. KẾT LUẬN

Bài báo đề xuất một thuật toán thủy vân khóa công khai mới trên miền DCT. Khóa công khai là một dãy số thực giả ngẫu nhiên theo phân bố chuẩn N(0,1), khóa bí mật là một hoán vị ngẫu nhiên trên từng tập con của khóa công khai. Các phân tích lý thuyết và kết quả thực nghiệm cho thấy, thuật toán đề xuất bền vững hơn thuật toán R.Munir và chống được một số phép tấn công điển hình như: thêm nhiễu, cắt, lọc, nén JPEG, thay đổi kích thước, xoay.

TÀI LIỆU THAM KHẢO

[1] B.C.MOHAN and S.KUMAR, *"A Robust Digital Image Watermarking Scheme Using Singular Value Decomposition"*, Journal of Multimedia 3(1), p.7-15, 2008.

[2] G.K.WALLACE, *"The JPEG Still Picture Compressing Standard"*, IEEE Transaction on Consumer Electonics, 1991.

[3] H.YANG, H.UNIV, CHANGSHA *"Semi-Fragile Watermarking for Image Authentication and Tamper Detection Using HSV Model"*, Multimedia and Ubiquitous Engineering, 2007.

[4] H. Y.KIM, RICARDO L. DE QUEIROZ, *"Alteration – Locating Authentication Watermarking for Binary and Halftone Images"*, IEEE Transactions on Signal Processing, 2004.

[5] I. J. COX, J. KILIAN, T. LEIGHTON, T. SHAMOON, *"Secure spread spectrum watermarking for images, audio and video"*, Proc IEEE Internat. Conf. on Image Processing (ICIP'96) Vol. III, Lausanne, Swizerland, 16-19 September 1996, pp. 243-246

[6] M. BARNI, F. BARTOLINI, V. CAPPELLINI, A.Piva, *"A DCT-Domain System for Robust Image Watermarking"*, Signal Processing 66 (1998), pp 357-372

[7] M. WU, B. LIU, *"Data Hiding in Binary Image for Authentication and Annotation"*, IEEE Transactions on Multimedia, Vol. 6, No. 4, August 2004.

[8] M. WU, E. TANG AND B. LIU, *"Data Hiding in Digital Binary Image,"* IEEE Int. Conf. Multimedia and Expo, ICME'00, New York, USA, 2000.

[9] P.W.WONG, *"A Public Key Watermarking for Image Verification and Authentication"*, 08186-8821, IEEE, 1998.

[10] R. MUNIR, B. RIYANTO, S. SUTIKNO, W.P. AGUNG, *"Derivation of Barni Algorithm into Its Asymmetric Watermarking Technique Using Statistical Approach"*, International Journal on Electrical Engineering and Informatics - Volume 1, Number 2, 2009

[11] S.RAWAT, B.RAMAN, *"A Chaos-Based Rubust Watermarking Algorithm for Rightful Ownership Protection"*, International Journal of Image and Graphics, Vol.11, No.4, p.471-493, 2011.

[12] S.SAHA, D.BHATTACHARYYA, S.K. BANDYOPADHAYAY, *"Security on Fragile and Semi-Fragile Watermarking Authentication"*, International Journal of Computer Applications, Vol.3-No.4, June 2010.

[13] S.S. BEDI, S.VERMA, G.TOMAR, *"An Adaptive Data Hiding Technique for Digital Image Authentication"*, International Journal of Computer Threory and Engineering, Vol. 2, No. 3, June 2010.

[14] X. WU, J. HU, Z. GU, J. HUANG, *"A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters"* Conferences in Research and Practice in Information Technology, Vol. 44, Australian Computer Society, 2005.

[15] Y. FU, *"A Novel Public Key Watermarking Scheme based on Shuffling"*, 2007 International Conference on Convergence Information Technology, IEEE Computer Society

[16] Y. Y. KIM, *Ricardo L. de Queiroz "A Public-Key Authentication Watermarking for Binary Images"*, 0-7803-8554-3/04 ©2004 IEEE.

[17] Y. Y. KIM, *"A New Public-Key Authentication Watermarking for Binary Document Images Resistant to Parity Attacks"*, 0-7803-9134, 2005 IEEE.

Nhận bài ngày: 18/04/2013

SƠ LƯỢC VỀ CÁC TÁC GIẢ

ĐỖ VĂN TUẤN

Sinh ngày 9/6/1975 tại Hải Dương.

Tốt nghiệp đại học tại Học viện Kỹ thuật Quân sự năm 2002. Tốt nghiệp Thạc sĩ 2007 tại Trường Đại học Công nghệ – Đại học Quốc gia Hà Nội.

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

Lĩnh vực quan tâm: Giấu tin, mật mã, thủy vân số

Email: dvtuanest@gmail.com

TRẦN ĐĂNG HIÊN

Sinh ngày 06/08/1983 tại Hà Nội.

Tốt nghiệp đại học tại Trường Đại học Giao thông Vận tải năm 2005. Tốt nghiệp Thạc sĩ năm 2010 tại Trường Đại học Công nghệ – Đại học Quốc gia Hà Nội.

Hiện giảng dạy tại Khoa CNTT, Đại học Công nghệ - Đại học Quốc gia Hà Nội.

Lĩnh vực quan tâm: Giấu tin, thủy vân số, phát hiện ảnh giả mạo.

Email: hientd_68@yahoo.com

CAO THỊ LUYÊN

Ngày sinh 28/4/1979 tại Hưng Yên.

Tốt nghiệp Đại học năm 2001 và Thạc sĩ năm 2005 tại Trường Đại học Khoa học Tự nhiên.

Hiện giảng dạy tại Khoa CNTT, Trường Đại học Giao thông Vận tải.

Lĩnh vực quan tâm: Giấu tin, thủy vân số, xử lý ảnh

Email: luyenct28042000@yahoo.com

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. Nhận chức danh PGS năm 1984

Hiện giảng dạy tại Khoa CNTT, Trường Đại học Giao thông Vận tải.

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

Email: phamvanat83@vnn.vn