Một số lược đồ thủy vân mới dựa trên phân tích QR

Several New Watermarking Schemes Based on QR Decomposition

Trần Đăng Hiên, Đỗ Văn Tuấn, Nguyễn Ngọc Hưng, và Phạm Văn Ất

Abstract: *In this paper, we propose two watermarking schemes based on QR decomposition, called QR-1 and QR-N. In comparision with watermarking schemes based on SVD decomposition of R. Sun et.al and P. Bao et.al, the proposed schemes have lower computational complexity, higher security, better quality of watermarked image and more robustness against some image processing attacks. Moreover, scheme QR-1 is also more robustness than the scheme based on QR decomposition of Song Wei et.al.*

Keywords*: Robust watermarking, SVD decomposition, QR decomposition.*

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 lược đồ thủy vân có thể được chia thành hai nhóm chính: **thủy vân dễ vỡ** và **thủy vân bền vững**. 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 lược đồ thủy vân bền vững thường được ứng dụng trong bài toán bảo vệ quyền chủ sở hữu.

Các phép biến đổi SVD (Singular Value Decomposition: $A = U \times D \times V^T$) và QR (QR Decomposition: $A=Q\times R$) cũng giống như DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) đều là các phép biến đổi ma trận trực giao và có cùng một tính chất quan trọng là tập trung năng lượng ảnh vào một số phần tử cố định của miền biến đổi. Năng lượng ảnh tập trung vào phần tử *D(1,1)* trong phép biến đổi SVD và hàng đầu của ma trận *R* trong phép biến đổi QR. Các phần tử này có tính ổn định cao, vì vậy có thể sử dụng chúng để xây dựng các lược đồ thủy vân bền vững trước các phép tấn công. Một nhận xét tương tự cũng được nêu ra trong [5].

Phép biến đổi SVD được dùng khá nhiều để xây dựng các lược đồ thủy vân. Có hai hướng nghiên cứu xây dựng các lược đồ thủy vân dựa trên cách tiếp cận này. *Hướng thứ nhất*: Nhúng dấu thủy vân vào ma trận

D bằng cách nhúng vào phần tử *D(1,1)* [16], nhúng vào một số phần tử đầu trên đường chéo [17,18], nhúng vào tất cả các phần tử trên đường chéo [1], hoặc nhúng vào toàn bộ *D* [11]. *Hướng thứ hai*: Nhúng dấu thủy vân vào các phần tử trên cột thứ nhất của ma trận *U* và/hoặc *V* [3,6]. Ngoài ra, có nhiều nghiên cứu sử dụng đồng thời phân tích SVD với các phép biến đổi ma trận khác như DCT, DWT,… để xây dựng các lược đồ thủy vân kết hợp như trong [2,7,9,10,15].

Phân tích QR có một số ưu điểm so với phân tích SVD nhưng chưa được quan tâm nhiều trong việc xây dựng các lược đồ thủy vân. Gần đây Song Wei [14] đã sử dụng phân tích QR xây dựng lược đồ thủy vân (ký hiệu là SW) bằng cách nhúng dấu thủy vân trên phần tử *Q(2,1), Q(3,1)* của ma trận Q. Ngoài ra, có một số nghiên cứu khác sử dụng phân tích QR kết hợp với các phép biến đổi ma trận khác để xây dựng lược đồ thủy vân như trong [5,12].

Trong bài báo này chúng tôi đề xuất hai lược đồ thủy vân dựa trên phân tích QR đối với miền không gian ảnh. Khác với lược đồ SW, các lược đồ đề xuất sử dụng hàng đầu của ma trận *R* để nhúng thủy vân. Lược đồ thứ nhất nhúng thủy vân vào một phần tử trên hàng đầu của *R*, lược đồ thứ hai nhúng thủy vân trên cả hàng đầu của *R*. Ngoài ra cách nhúng bít thủy vân của lược đồ đề xuất cũng khác so với lược đồ SW. Trong lược đồ SW (Song Wei), một bít thủy vân được nhúng bằng cách thay đổi giá trị hai phần tử *Q(2,1), Q(3,1)* để *Q(2,1)* lớn hơn hoặc nhỏ hơn *Q(3,1)* tùy thuộc vào bít cần nhúng bằng *0* hoặc *1*. Trong khi, lược đồ đề xuất sử dụng ý tưởng của phương pháp QIM (Quantization index modulation) [4] để nhúng bít thủy vân vào một phần tử trên hàng đầu của *R*.

So với các lược đồ thủy vân dựa trên phân tích SVD trong [1,16] và QR trong [14] thì lược đồ đề xuất bền vững hơn trước một số phép biến đổi ảnh, đặc biệt là phép nén JPEG. Ngoài ra, so với các lược đồ [1,16], lược đồ đề xuất còn có thêm một số ưu điểm là: Số lượng phép tính ít hơn, tính bảo mật cao hơn, chất lượng ảnh thủy vân tốt hơn.

Các phần còn lại của bài báo được tổ chức như sau: Phần 2 trình bày một số khái niệm cơ sở được sử dụng trong bài báo. Phần 3 trình bày hai lược đồ thủy vân dựa trên phân tích SVD. Phần 4 đề xuất hai lược đồ thủy vân dựa trên phân tích QR. Phần 5 phân tích một số ưu điểm của các lược đồ thủy vân đề xuất. Phần 6 trình bày kết quả thử nghiệm và Phần 7 là kết luận.

II. MỘT SỐ KHÁI NIỆM CƠ SỞ

II.1. Phân tích SVD

Mọi ma trận thực *Y* cấp $m\times n$ cho trước luôn luôn có thể phân tích thành tích của 3 ma trận thực như sau [8, trang 448]:

$$Y = U \times D \times V^T$$

Trong đó :

U là ma trận trực chuẩn cấp $m\times m$.

V là ma trận trực chuẩn cấp $n\times n$.

D là ma trận đường chéo cấp $m\times n$ có tính chất:

$D(1,1)\geq D(2,2)\geq ..\geq D(s,s)\geq 0$, với $s=min(m,n)$.

II.2. Phân tích QR

Mọi ma trận thực *Y* cấp $m\times n$ cho trước luôn luôn có thể phân tích thành tích của 2 ma trận thực như sau [8, trang 223]:

$$Y = Q\times R$$

Trong đó:

Q là ma trận trực chuẩn cấp $m\times m$.

R là ma trận tam giác trên cấp $m\times n$.

II.3. Chuẩn véc tơ và ma trận

Để tiện lợi cho việc tính toán, dưới đây sẽ sử dụng chuẩn 1 (1-norm) [8, trang 52-54] được định nghĩa là tổng giá trị tuyệt đối các phần tử của véc tơ hoặc ma trận:

$$\|Y\| = \sum_{i=1}^{m}\sum_{j=1}^{n}|Y(i,j)|$$

II.4. Ảnh gốc và ảnh thuỷ vân

Trong các lược đồ thủy vân dưới đây chỉ xét ảnh đa cấp xám *I* có kích thước $M\times N$ (nếu *I* là ảnh màu thì sử dụng công thức $I=0.299R+0.587G+0.114B$ để chuyển sang đa cấp xám). Như vậy ảnh thực chất là một ma trận nguyên không âm. Giả sử *I* là ảnh gốc và *I'* là ảnh sau khi nhúng dấu thuỷ vân (ảnh thuỷ vân). Để đánh

giá chất lượng của ảnh thuỷ vân I' có thể sử dụng chuẩn của ma trận hiệu $I' - I$:

$$\left\| I' - I \right\| = \sum_{i=1}^{M} \sum_{j=1}^{N} \left| I'(i,j) - I(i,j) \right|$$

Nếu giá trị này càng nhỏ thì I' càng giống I và chất lượng ảnh thuỷ vân càng tốt. Rõ ràng $\|I' - I\|$ phụ thuộc vào kích thước của ảnh. Để có một đánh giá độc lập với kích thước ảnh, có thể dùng đại lượng sau:

$$Diff = \frac{\left\| I' - I \right\|}{M \times N} \quad (1)$$

nó chính là độ sai khác trung bình giữa ảnh gốc và ảnh thuỷ vân.

Dưới đây sẽ dùng *Diff* để đánh giá chất lượng ảnh của các lược đồ thuỷ vân. Lược đồ nào có *Diff* nhỏ hơn thì có chất lượng ảnh thuỷ vân tốt hơn.

III. LƯỢC ĐỒ THỦY VÂN DỰA TRÊN PHÂN TÍCH SVD

Để tiện theo dõi và so sánh, trong phần này chúng tôi trình bày hai lược đồ thủy vân, lược đồ thứ nhất nhúng một bít thủy vân vào phần tử đầu trên đường chéo ma trận D (của mỗi khối ảnh), gọi là lược đồ SVD-1 [16] và lược đồ thứ hai nhúng một bít vào tất cả các phần tử trên đường chéo ma trận D (của mỗi khối ảnh), gọi là lược đồ SVD-N [1]. Đây là hai lược đồ phổ biến được sử dụng trong khá nhiều nghiên cứu sau này. Ngoài ra, chúng còn được dùng để kết hợp với các phép biến đổi ma trận khác (DCT, DWT,…) tạo ra các lược đồ mới.

III.1. Lược đồ SVD-1

III.1.1. Thuật toán nhúng thủy vân

Trong thuật toán này, đầu vào là ảnh I, dấu thủy vân $W=(w_1,...,w_t)$ có độ dài t bít và một số nguyên dương q dùng làm hệ số lượng tử. Đầu ra là ảnh I' chứa dấu thủy vân W. Các bước của thuật toán như sau:

<u>Bước 1:</u> Chia ảnh I thành t khối không giao nhau từng đôi một và có cùng kích thước $m \times n$, ký hiệu là $I_i, i=1,2,...,t$.

<u>Bước 2:</u> Áp dụng phân tích SVD trên mỗi khối I_i:

$$I_i = U_i \times D_i \times V_i^T$$

<u>Bước 3:</u> Nhúng bít w_i vào phần tử $D_i(1,1)$ của ma trận đường chéo D_i:

Bước 3.1: Tính:

$$Z_i = D_i(1,1) \bmod q$$

q là hệ số lượng tử cho trước, nó thể hiện tính bền vững của lược đồ thủy vân. Nếu hệ số q càng nhỏ thì tính bền vững của lược đồ càng thấp, nhưng chất lượng ảnh thủy vân càng cao. Ngược lại hệ số q càng lớn thì tính bền vững của lược đồ càng cao, nhưng chất lượng ảnh thủy vân càng thấp (xem mục III.1.3). Vì vậy hệ số q nên được chọn sao cho cân bằng giữa tính bền vững và chất lượng ảnh theo yêu cầu thực tế sử dụng.

Bước 3.2: Điều chỉnh $D_i(1,1)$ thành $D_i'(1,1)$:

Trường hợp $w_i = 0$:

Nếu $Z_i < 3q/4$, $D_i'(1,1) = D_i(1,1) + q/4 - Z_i$.

Ngược lại, $D_i'(1,1) = D_i(1,1) + 5q/4 - Z_i$.

Trường hợp $w_i = 1$:

Nếu $Z_i < q/4$, $D_i'(1,1) = D_i(1,1) - q/4 - Z_i$.

Ngược lại, $D_i'(1,1) = D_i(1,1) + 3q/4 - Z_i$.

Sau khi thực hiện nhúng w_i vào D_i ta nhận được D_i' chỉ khác D_i tại vị trí $(1,1)$.

<u>Bước 4:</u> Tính $I_i' = U_i \times D_i' \times V_i^T$, ảnh I' tạo từ các khối I_i' là ảnh chứa dấu thủy vân W.

<u>Nhận xét:</u> Công thức tính $D_i'(1,1)$ trong trường hợp $w_i=1$ và $Z_i < q/4$ trình bày trong bước 3 chứa số hạng $-Z_i$, nhưng trong [16] là $+ Z_i$, nghĩa là:

$$D_i'(1,1) = D_i(1,1) - q/4 + Z_i \quad (2)$$

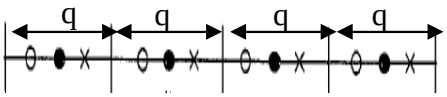
Theo chúng tôi tài liệu [16] có sự nhầm lẫn giữa dấu cộng và dấu trừ. Điều này có thể lý giải như sau. Trong [16] các tác giả nói rõ đã dùng phương pháp QIM để nhúng bít thủy vân w_i vào $D_i(1,1)$. Về mặt lý thuyết theo phương pháp QIM [4] và [12], $D_i(1,1)$ cần được biến đổi một cách ít nhất để rơi vào tập:

$$\Omega_0 = \left\{ x \in \Re \mid x = \frac{q}{4} (\bmod q) \right\}$$

hoặc

$$\Omega_1 = \left\{ x \in \Re \mid x = \frac{3q}{4} (\bmod q) \right\}$$

tùy thuộc bít thủy vân $w_i=0$ hoặc $w_i=1$. Nói cách khác nếu $w_i=0$ thì $D_i'(1,1)$ thuộc Ω_0 và nếu $w_i=1$ thì $D_i'(1,1)$ thuộc Ω_1. Trên hình dưới đây Ω_0 gồm các điểm ○, Ω_1 gồm các điểm ×:



Trong khi đó, $D_i'(1,1)$ tính theo (2) rõ ràng không luôn luôn thuộc Ω_1. Như vậy, có thể thấy công thức (2) là sai. Cũng có thể chỉ ra sự nhầm lẫn của công thức (2) qua một ví dụ đơn giản sau đây.

Với $w_i=1$ thì $D_i(1,1)= 20q +q/6$, khi đó theo công thức (2) thì $D_i'(1,1)=20q+q/12$. Theo thuật toán trích bít, do $D_i'(1,1) \bmod q = q/12<q/2$ suy ra $w'_i=0$. Như vậy bít trích ra khác với bít đã nhúng. Từ đó thấy (2) bị sai.

III.1.2. Thuật toán kiểm tra dấu thủy vân (để xác định bản quyền)

Ảnh *I'* đã nhúng thủy vân có thể bị tấn công bởi các phép biến đổi ảnh như thêm nhiễu, lọc, làm mờ, nén JPEG ..., khi đó ảnh *I'* bị biến đổi thành ảnh *I** (gọi *I** là phiên bản tấn công của *I'*). Thuật toán dưới đây sẽ kiểm tra sự tồn tại của dấu thủy vân trong ảnh *I** để kết luận về bản quyền đối với *I** của tác giả có ảnh *I'*.

<u>Bước 1:</u> Chia ảnh *I** thành *t* khối như trong thuật toán nhúng thủy vân, ký hiệu là I_i^*, $i=1,...,t$.

<u>Bước 2:</u> Áp dụng phân tích SVD trên mỗi khối I_i^*:

$$I_i^* = U_i^* \times D_i^* \times V_i^{*T}$$

<u>Bước 3:</u> Xác định bít w_i^* từ $D_i^*(1,1)$ như sau:

$Z_i^* = D_i^*(1,1) \bmod q$

$w_i^* = 0$ nếu $Z_i^* < q/2$

$w_i^* = 1$ nếu $Z_i^* \geq q/2$

<u>Bước 4:</u> So sánh dấu thủy vân $W^* = (w_1^*,...,w_t^*)$ trích ra từ *I** với dấu thủy vân gốc $W = (w_1,...,w_t)$ bằng cách dùng hệ số *Err*:

$$Err = \frac{1}{t}\sum_{i=1}^{t} w_i \; XOR \; w_i^* \qquad (3)$$

Ta nhận thấy *Err* là độ sai khác trung bình giữa *W* và *W**, nó có giá trị trong đoạn [0, 1] và *Err* = 0 nếu $w_i = w_i^*$ (với $\forall i$), *Err* = 1 nếu $w_i \neq w_i^*$ (với $\forall i$).

Hệ số *Err* được so sánh với ngưỡng $\tau \in [0,1]$, nếu $Err < \tau$ (tức là *W** khá gần với *W*) thì kết luận ảnh *I** có nhúng dấu thủy vân *W* và ảnh *I** vẫn thuộc về tác giả có ảnh *I'*.

<u>Ghi chú:</u> Dưới đây sẽ dùng *Err* để đánh giá độ bền vững của các lược đồ thuỷ vân. Lược đồ nào có *Err* nhỏ hơn thì bền vững hơn trước các phép biến đổi ảnh.

III.1.3. Nhận xét về lược đồ SVD-1

Trong lược đồ này sử dụng một thuật toán nhúng một bít thủy vân vào phần tử thực *x* (bước 3, mục III.1.1). Sau khi nhúng thì *x* bị thay đổi thành *x'* có độ sai khác không quá *q/2*:

$$|x-x'| \leq q/2$$

Gọi *x** là một phiên bản tấn công của *x'* và ta cần trích một bít từ *x**. Cũng có thể thấy rằng nếu mức độ biến đổi giữa *x** và *x'* không quá *q/4* :

$$|x^*-x'| < q/4$$

thì bít trích rút từ *x** sẽ trùng với bít thủy vân ban đầu. Như vậy ta có thể nói thuật toán này có mức sai số *q/2* và độ bền vững *q/4*.

III.2. Lược đồ SVD-N

III.2.1. Thuật toán nhúng thủy vân của lược đồ này cũng gồm 4 bước như thuật toán nhúng thuỷ vân của lược đồ SVD-1, chỉ khác ở bước 3 như sau.

<u>Bước 3:</u> Nhúng bít w_i vào D_i để nhận D_i':

Bước 3.1: Tính :

$$x_i = \|X_i\| + 1$$

$$k_i = \left\lfloor \frac{x_i}{q} \right\rfloor$$

Trong đó véc tơ X_i gồm các phần tử trên đường chéo của ma trận D_i :

$X_i=(D_i(1,1), D_i(2,2),\ldots,D_i(s,s))$, với $s=min(m,n)$.

Bước 3.2: Điều chỉnh k_i:

Trường hợp $w_i=1$:

Nếu k_i lẻ thì $k_i = k_i+1$.

Ngược lại k_i không thay đổi.

Trường hợp $w_i = 0$:

Nếu k_i chẵn thì $k_i = k_i +1$.

Ngược lại k_i không thay đổi.

Bước 3.3: Điều chỉnh D_i thành D_i':

$$x_i^{'} = q \times k_i + \frac{q}{2}$$

$$X_i^{'} = X_i \times \frac{x_i^{'}}{x_i}$$

thu được ma trận D_i' với đường chéo là véc tơ $X_i^{'}$.

Ghi chú: Trong lược đồ [1], hệ số lượng tử q được tính theo I_i. Ở đây để đơn giản và tiện so sánh với các lược đồ trong mục IV, q được xem là cố định.

III.2.2. Thuật toán kiểm tra dấu thủy vân của lược đồ này cũng gồm 4 bước như thuật toán kiểm tra dấu thuỷ vân của lược đồ SVD-1, chỉ khác ở bước 3 như sau.

Bước 3: Xác định bít w_i* từ đường chéo của D_i*:

Bước 3.1: Tính:

$$x_i^* = \left\| X_i^* \right\| + 1$$

$$k_i^* = \left\lfloor \frac{x_i^*}{q} \right\rfloor$$

Trong đó véc tơ X_i^* gồm các phần tử trên đường chéo của ma trận D_i^*:

$$X_i^* = \left(D_i^*(1,1), D_i^*(2,2),\ldots, D_i^*(s,s)\right)$$

Bước 3.2: Xác định w_i*:

$w_i^* = 0$ nếu k_i^* *MOD 2 =1*

$w_i^* = 1$ nếu k_i^* *MOD 2 =0*

III.2.3. Nhận xét về lược đồ SVD-N

Trong lược đồ này sử dụng một thuật toán nhúng một bít thủy vân vào véc tơ thực X (bước 3, mục III.2.1). Sau khi nhúng X bị thay đổi thành X'. Có thể chứng minh độ sai khác giữa X và X' không quá $3q/2$:

$$||X-X'|| \le 3q/2$$

Gọi X^* là một phiên bản tấn công của X' và ta cần trích một bít từ X^*. Sử dụng giả thiết $||X|| > 3$ (thực tế $||X||$ có giá trị vào khoảng *1000*), có thể chứng minh rằng tồn tại một giá trị $0 < p < q/2$ sao cho khi :

$$|\, ||X^*||-||X'||\, | < p$$

thì bít trích rút từ X^* sẽ trùng với bít thủy vân ban đầu. Như vậy ta có thể nói thuật toán này có mức sai số $3q/2$ và độ bền vững p (với $p < q/2$).

IV. CÁC LƯỢC ĐỒ THỦY VÂN MỚI DỰA TRÊN PHÂN TÍCH QR

Trong phần này chúng tôi đề xuất hai lược đồ thủy vân, lược đồ thứ nhất nhúng một bít thủy vân vào một phần tử tùy ý trên hàng đầu ma trận R (của mỗi khối ảnh), gọi là lược đồ QR-1 và lược đồ thứ hai nhúng một bít trên cả hàng đầu ma trận R (của mỗi khối ảnh), gọi là lược đồ QR-N.

IV.1. Lược đồ QR-1

IV.1.1. Thuật toán nhúng thủy vân

Để tiện trình bầy thuật toán, chọn phần tử $R(1,1)$ để nhúng một bít của dấu thủy vân. Đầu vào của thuật toán là ảnh I, dấu thủy vân $W = \left(w_1,\ldots,w_t\right)$ và hệ số lượng tử q. Đầu ra của thuật toán là ảnh I' chứa dấu thủy vân W. Các bước của thuật toán như sau:

Bước 1: Chia ảnh I thành t khối không giao nhau từng đôi một và có cùng kích thước $m \times n$, ký hiệu là $I_i, i=1,2,\ldots,t$.

Bước 2: Áp dụng phân tích QR trên mỗi khối I_i:

$$I_i=Q_i \times R_i$$

Bước 3: Nhúng bít w_i vào phần tử $R_i(1,1)$ của ma trận tam giác trên R_i.

Bước 3.1: Tính:

$$k_i = \left\lfloor \frac{R_i(1,1)}{q} \right\rfloor$$

Bước 3.2: Điều chỉnh $R_i(1,1)$ thành $R_i'(1,1)$:

$$R_i^{'}(1,1) = k_i \times q + \left(\left(k_i \bmod 2\right) XOR\, w_i\right) \times q$$

Sau khi thực hiện nhúng w_i vào $R_i(1,1)$ ta nhận được R_i' chỉ khác R_i tại vị trí (1,1). Nếu chọn phần tử khác để nhúng, ví dụ $R_i(1,k)$, thì R_i' khác R_i tại vị trí $(1,k)$.

<u>Bước 4:</u> Tính $I_i^{'} = Q_i \times R_i^{'}$, ảnh I' tạo từ các khối $I_i^{'}$ là ảnh chứa dấu thủy vân W.

IV.1.2. Thuật toán kiểm tra dấu thủy vân

Cho I^* là một phiên bản tấn công của I' và hệ số lượng tử q, thuật toán dưới đây sẽ kiểm tra sự tồn tại của dấu thủy vân trong ảnh I^* để kết luận về bản quyền đối với I^* của tác giả có ảnh I'.

<u>Bước 1:</u> Chia ảnh I^* thành t khối như trong thuật toán nhúng thủy vân, ký hiệu là I_i^*, $i=1,...,t$.

<u>Bước 2:</u> Áp dụng phân tích QR cho từng khối I_i^* :

$$I_i^* = Q_i^* \times R_i^*$$

<u>Bước 3:</u> Xác định bít w_i^* từ $R_i^*(1,1)$ như sau :

$$k_i^* = \left\lfloor \frac{R^*{}_i(1,1) + \frac{q}{2}}{q} \right\rfloor$$

$$w_i^* = k_i^* \, MOD\, 2$$

<u>Bước 4:</u> So sánh dấu thủy vân $W^* = \left(w_1^*,...,w_t^*\right)$ trích ra từ I^* với dấu thủy vân gốc $W = \left(w_1,...,w_t\right)$ tương tự bước 4 trong mục III.1.2.

IV.1.3. Nhận xét về lược đồ QR-1

Trong lược đồ này sử dụng một thuật toán khác để nhúng một bít thủy vân vào phần tử thực x (bước 3, mục IV.1.1). Sau khi nhúng x bị thay đổi thành x' có độ sai khác không quá q:

$$|x-x'| \le q$$

Gọi x^* là một phiên bản tấn công của x' và ta cần trích một bít từ x^*. Cũng có thể thấy rằng nếu mức độ biến đổi giữa x^* và x' không quá $q/2$:

$$|x^*-x'| < q/2$$

thì bít trích rút từ x^* sẽ trùng với bít thủy vân ban đầu. Như vậy, thuật toán này có mức sai số q và độ bền vững $q/2$.

Nếu trong thuật toán III.1.1 chọn $q=2\partial$ và trong thuật toán IV.1.1 chọn $q=\partial$, thì sẽ thấy hai thuật toán này hoàn toàn tương đương về mức độ sai số và độ bền vững. Tuy nhiên thuật toán IV.1.1 tỏ ra đơn giản hơn về lập trình.

IV.2. Lược đồ QR-N

IV.2.1. Thuật toán nhúng thủy vân của lược đồ này cũng gồm 4 bước như thuật toán nhúng thuỷ vân của lược đồ QR-1, chỉ khác ở bước 3 như sau.

<u>Bước 3:</u> Nhúng bít w_i của dấu thủy vân vào hàng đầu của ma trận R_i.

Bước 3.1: Tính:

$$x_i = X_i(1) + X_i(2) + \ldots + X_i(n)$$

$$k_i = \left\lfloor \frac{x_i}{q} \right\rfloor$$

$$x_i^{'} = k_i \times q + \left(\left(k_i \, MOD\, 2\right) \oplus w_i\right) \times q$$

trong đó véc tơ X_i gồm các phần tử trên hàng đầu của ma trận R_i:

$$X_i = (R_i(1,1), R_i(1,2),\ldots,R_i(1,n)).$$

<u>Nhận xét:</u> X_i là véc tơ dương (xem nhận xét 1, mục V).

Bước 3.2: Điều chỉnh R_i thành R_i':

$$X_i^{'} = \frac{x_i^{'}}{x_i} X_i$$

thu được ma trận R_i' với hàng đầu là véc tơ $X_i^{'}$

IV.2.2. Thuật toán kiểm tra dấu thủy vân của lược đồ này cũng gồm 4 bước như thuật toán kiểm tra dấu thuỷ vân của lược đồ QR-1, chỉ khác ở bước 3 như sau.

<u>Bước 3:</u> Xác định bít w_i^* từ hàng đầu của R_i^*:

Bước 3.1: Tính:

$$x_i^* = X_i^*(1) + X_i^*(2) + \ldots + X_i^*(n)$$

$$k_i^* = \left\lfloor \frac{x_i^* + \frac{q}{2}}{q} \right\rfloor$$

trong đó véc tơ X_i^* gồm các phần từ trên hàng đầu của ma trận R_i^*:

$$X_i^* = \left(R_i^*(1,1), R_i^*(1,2), ..., R_i^*(1,n)\right).$$

Bước 3.2: Xác định w_i*:

$$w_i^* = k_i^* \, MOD \, 2$$

IV.2.3. Nhận xét về lược đồ QR-N

Trong lược đồ này sử dụng một thuật toán nhúng một bít thủy vân vào véc tơ thực dương *X* (bước 3, mục IV.2.1). Sau khi nhúng *X* bị thay đổi thành *X'* có độ sai khác không quá *q*:

$$\|X\text{-}X'\| \le q$$

Gọi *X** là một phiên bản tấn công của *X'* và ta cần trích một bít từ *X**. Cũng có thể thấy rằng nếu mức độ biến đổi giữa *X** và *X'* không quá *q/2*:

$$|\,\|X^*\|\text{-}\|X'\|\,| < q/2$$

thì bít trích rút từ *X** sẽ trùng với bít thủy vân ban đầu. Như vậy thuật toán có mức sai số *q* và độ bền vững *q/2*. Từ đó suy ra thuật toán này có mức sai số ít hơn và độ bền vững cao hơn so với thuật toán nhúng một bít dùng trong lược đồ SVD-N.

V. MỘT SỐ ƯU ĐIỂM CỦA CÁC LƯỢC ĐỒ ĐỀ XUẤT

Mục này sẽ chỉ ra một số ưu điểm của các lược đồ thủy vân dựa trên phân tích QR so với các lược đồ thủy vân tương tự dựa trên phân tích SVD.

Để tiện trình bày ta giả sử ảnh *I* được chia thành các khối vuông có kích thước *n×n* và ký hiệu *A* là khối đại diện. Khi đó có thể xem *A* là ma trận nguyên không âm cấp *n×n*. Các lược đồ thủy vân dựa trên phân tích QR sử dụng công thức:

$$A = Q \times R \qquad (4)$$

Trong khi các lược đồ thủy vân dựa trên phân tích SVD sử dụng công thức:

$$A = U \times D \times V^T \qquad (5)$$

<u>Nhận xét 1:</u> Do *A* là ma trận của một khối ảnh nên *A* dương hoặc có rất ít phần tử bằng *0*. Từ đó có thể chứng minh: Các phần tử trên cột *1* của *Q*, hàng *1* của *R* trong (4), cột *1* của *U* và cột *1* của *V* trong (5) đều cùng dương hoặc cùng âm. Để đơn giản, dưới đây giả thiết các phần tử nói trên đều dương.

V.1. Tốc độ thực hiện

Do công thức (4) có độ phức tạp tính toán thấp hơn so với công thức (5), nên các lược đồ thủy vân dựa trên phân tích QR sẽ có tốc độ thực hiện nhanh hơn so với các lược đồ thủy vân dựa trên phân tích SVD.

V.2. Khả năng lựa chọn phần tử nhúng thủy vân

Do *Q* là ma trận trực chuẩn, nên từ (4) suy ra hệ số tương quan giữa các cột của *A* bằng hệ số tương quan giữa các cột tương ứng của *R*:

$$\rho(A_i, A_j) \equiv \frac{(A_i, A_j)}{\sqrt{(A_i, A_i) * (A_j, A_j)}}$$

$$= \frac{(R_i, R_j)}{\sqrt{(R_i, R_i) * (R_j, R_j)}} \equiv \rho(R_i, R_j)$$

Để ý rằng đối với cột R_1 thì phần tử đầu tiên dương, các phần tử còn lại bằng *0*, nên với *i=1* ta có:

$$\rho(A_1, A_j) = \frac{R(1, j)}{\sqrt{\sum_{i=1}^{n} R(i, j)^2}} \qquad (6)$$

Do *A* là một khối ảnh nên các cột của *A* thường có độ tương quan cao, nghĩa là:

$$\rho(A_1, A_j) \approx 1$$

Nên từ (6) suy ra các phần tử trên hàng đầu của *R* đều lớn và có giá trị tương đương nhau trong khi các phần tử còn lại đều nhỏ về giá trị tuyệt đối. Như vậy ta có thể chọn bất kỳ phần tử nào trên hàng đầu của *R* để nhúng bít thủy vân. Trong khi đó ma trận *D* trong phân tích SVD chỉ có phần tử *D(1,1)* lớn, các phần tử còn lại đều nhỏ nên chỉ có thể chọn *D(1,1)* để nhúng thủy vân. Như vậy trong lược đồ QR-1 ta có nhiều lựa chọn phần tử để nhúng thủy vân hơn so với lược đồ SVD-1. Điều này cho phép chọn ngẫu nhiên phần tử dùng để nhúng theo một khóa nhị phân (hoặc nguyên) và bằng cách đó sẽ làm tăng độ bảo mật của lược đồ QR-1.

V.3. Chất lượng ảnh sau khi nhúng thủy vân

Dưới đây sẽ chứng minh lược đồ dựa trên phân tích QR có chất lượng ảnh thuỷ vân tốt hơn (giá trị *Diff* nhỏ hơn) so với lược đồ dựa trên phân tích SVD.

V.3.1. So sánh các lược đồ SVD-1 và QR-1

Gọi *A* là khối ảnh gốc có kích thước $n \times n$, *B* là khối sau khi nhúng một bít vào *D(1,1)* để được *D'(1,1)=D(1,1)+d* theo lược đồ SVD-1 và *C* là khối sau khi nhúng một bít vào *R(1,k)* để được *R'(1,k)=R(1,k)+ r (với* $1 \le k \le n$*)* theo lược đồ QR-1. Nếu cả hai lược đồ dùng chung một thuật toán nhúng bít trên một phần tử, ví dụ thuật toán mô tả tại bước 3 mục IV.1.1, thì theo nhận xét IV.1.3 suy ra: $|d| \le q$, $|r| \le q$. Khi đó từ (5) ta có :

$$A = U \times D \times V^T = \sum_{i=1}^{n} D(i,i) \times U_i \times V_i^T$$

$$B = \left(D(1,1) + d\right) \times U_1 \times V_1^T + \sum_{i=2}^{n} D(i,i) \times U_i \times V_i^T$$

Từ đó suy ra :

$$B - A = d \times U_1 \times V_1^T$$

và:

$$\|B - A\| = |d| (\sum_{i=1}^{n} U(i,1))(\sum_{i=1}^{n} V(i,1))$$

$$\le |d| \sqrt{n \sum_{i=1}^{n} U^2(i,1)} \sqrt{n \sum_{i=1}^{n} V^2(i,1)}$$

Do *U* và *V* là các ma trận trực chuẩn và do $|d| \le q$ nên :

$$\|B - A\| \le q \times n \qquad (7)$$

dấu đẳng thức xảy ra khi các phần tử *U(i,1)* bằng nhau, các phần tử *V(i,1)* bằng nhau và $|d| = q$.

Mặt khác từ (4) suy ra :

$$\|C - A\| = |r| \sum_{i=1}^{n} |Q(i,k)| \le |r| \sqrt{n \sum_{i=1}^{n} Q^2(i,k)}$$

Vì Q trực chuẩn nên và $|r| \le q$ nên:

$$\|C - A\| \le q \times \sqrt{n} \qquad (8)$$

dấu đẳng thức xảy ra khi các giá trị *|Q(i,k)|* bằng nhau và $|r|=q$.

Gọi Ω_n là tập tất cả các khối ảnh kích thước $n \times n$, từ (7) và (8) suy ra:

$$\max\{\|B - A\| \mid A \in \Omega_n\} = q \times n$$

$$\max\{\|C - A\| \mid A \in \Omega_n\} = q \times \sqrt{n}$$

Vậy :

$$\max\{\|B - A\| \mid A \in \Omega_n\} = \sqrt{n} \times \max\{\|C - A\| \mid A \in \Omega_n\} \qquad (9)$$

Từ (1) và (9) có thể kết luận: Giá trị *Diff* của lược đồ SVD-1 lớn hơn giá trị *Diff* của lược đồ QR-1 khoảng $\sqrt{n}$ lần. Đánh giá này hoàn toàn phù hợp với kết quả thực nghiệm trong mục 6 dưới đây.

V.3.2. So sánh các lược đồ SVD-N và QR-N

Bằng cách lập luận tương tự cũng có thể thấy rằng kết luận trong V.3.1 đối với các lược đồ SVD-1 và QR-1 vẫn đúng đối với các lược đồ SVD-N và QR-N. Điều này cũng được kiểm chứng bằng kết quả thực nghiệm.

VI. KẾT QUẢ THỬ NGHIỆM

VI.1. Bộ ảnh thử nghiệm

Để thử nghiệm tính hiệu quả của lược đồ thủy vân, các tác giả thường sử dụng bộ ảnh chuẩn nêu trong [13, trang 326] gồm: *Baboon, Lena, Pepper, Airplane* (Hình 1). Dưới đây chúng tôi cũng sử dụng bộ ảnh này làm ảnh gốc (đều là ảnh *24* bít màu có kích thước *256×256*) và chọn logo Trường Đại học Công nghệ (ảnh nhị phân kích thước *32×32*) làm dấu thủy vân (Hình 1.e).

VI.2. So sánh tính bền vững của các lược đồ thủy vân

Mục đích thử nghiệm là so sánh tính bền vững của 5 lược đồ: SVD-1, SVD-N, SW và hai lược đồ đề xuất QR-1, QR-N trước bốn phép tấn công (biến đổi ảnh): thêm nhiễu, làm mờ, nén JPEG, lọc trung vị. Đối với một lược đồ thủy vân thì hai đặc trưng chất lượng ảnh và tính bền vững có tính chất đối nghịch. Nói cách khác, nếu chất lượng ảnh cao thì tính bền vững giảm và ngược lại. Vì vậy để việc so sánh được chính xác, trong thử nghiệm đã chọn các tham số sao cho chất lượng ảnh thủy vân (*giá trị Diff*) của các lược đồ tương đương nhau như chỉ ra trong Bảng 1. Các tham

số được chọn cụ thể như sau:với SVD-1, SVD-N hệ số lượng tử *q=16*, với SW ngưỡng *T=0.005*, với QR-1, QR-N hệ số lượng tử *q=40*.

(a) (b) (c) (d) (e)

Hình 1. a)Ảnh Baboon, b)Lena, c)Pepper, d)Airplane và e)Ảnh logo Trường ĐHCN

Bảng 1. Chất lượng ảnh của các lược đồ thuỷ vân (Diff càng nhỏ thì chất lượng càng cao)

Ảnh	**Giá trị của Diff**				
	SVD-1	**SVD-N**	**SW**	**QR-N**	**QR-1**
Lena	0.4429	0.4406	0.3478	0.4032	0.4259
Baboon	0.4790	0.4283	0.8604	0.4083	0.4252
Pepper	0.4899	0.4317	0.3691	0.3992	0.3742
Airplane	0.4740	0.4384	0.4720	0.4360	0.5655

Bảng 2. Giá trị Err của các lược đồ thủy vân (Err càng nhỏ thì càng bền vững).

Ảnh	**Biến đổi**	**Hệ số**	**SVD-1**	**SVD-N**	**SW**	**QR-N**	**QR-1**
Baboon	Thêm nhiễu	1%	0	0.0088	0.0303	0.0039	0
		3%	0.0368	0.4658	0.1328	0.1660	0
		5%	0.3046	0.5205	0.1953	0.3857	0.0068
	Làm mờ	r =1 px	0.4638	0.5146	0.2402	0.3867	0.3057
		r =3 px	0.5655	0.5791	0.3682	0.4990	0.4521
	Nén JPEG	10	0.1822	0.6729	0.2686	0.2871	0.0176
		30	0.0931	0.5400	0.1670	0.1582	0
		60	0	0.2764	0.1006	0.0039	0
	Lọc trung vị	r =1 px	0.1613	0.5117	0.4453	0.3730	0.2881
		r =2 px	0.3116	0.5400	0.4072	0.3858	0.3653
Lena	Nhiễu	1%	0	0.0273	0.0986	0.0020	0
		3%	0.0986	0.4385	0.2354	0.1563	0
		5%	0.3330	0.5656	0.3301	0.3750	0.0059
	Làm mờ	r =1 px	0.3154	0.3994	0.2686	0.2900	0.2802
		r =3 px	0.5170	0.4619	0.3330	0.4766	0.4336
	Nén JPEG	10	0.1463	0.4512	0.3193	0.2412	0.0117
		30	0.0645	0.3516	0.2432	0.0997	0
		60	0	0.0840	0.1182	0	0

	Lọc trung vị	r =1 px	0.1309	0.2559	0.4023	0.2998	0.1465
		r =2 px	0.2266	0.4199	0.3916	0.4258	0.3594
Pepper	Nhiễu	1%	0	0.0186	0.0918	0.0088	0.0049
		3%	0.0368	0.3254	0.2412	0.2012	0.0088
		5%	0.3438	0.3672	0.3418	0.3896	0.0137
	Làm mờ	r =1 px	0.4203	0.4727	0.2617	0.3486	0.2773
		r =3 px	0.5362	0.4854	0.4395	0.5049	0.4883
	Nén JPEG	10	0.1885	0.5205	0.3643	0.2861	0.0225
		30	0.0425	0.3193	0.2686	0.1631	0.0078
		60	0	0.0449	0.1260	0.01270	0
	Lọc trung vị	r =1 px	0.1019	0.2588	0.4189	0.2939	0.1211
		r =2 px	0.2365	0.4473	0.4326	0.3994	0.2705
Airplane	Nhiễu	1%	0	0.0576	0.0537	0.0068	0
		3%	0.0155	0.3090	0.2158	0.1807	0
		5%	0.3008	0.4707	0.2773	0.3691	0.0059
	Làm mờ	r =1 px	0.4002	0.3682	0.2588	0.2910	0.3418
		r =3 px	0.4932	0.4766	0.4033	0.4268	0.4668
	Nén JPEG	10	0.1645	0.4502	0.3271	0.2539	0.0127
		30	0.0320	0.3086	0.2451	0.0879	0
		60	0	0.0459	0.0791	0.0059	0
	Lọc trung vị	r =1 px	0.1365	0.2588	0.4297	0.2139	0.4023
		r =2 px	0.2402	0.3428	0.4287	0.2939	0.4844

Bảng 3. Giá trị Err theo lược đồ SVD-1 và QR-1 tại các vị trí nhúng khác nhau.

Ảnh	**Biến đổi**	**Hệ số**	**SVD-1 (1,1)**	**SVD-1 (2,2)**	**QR-1 (1,1)**	**QR-1 (1,8)**
Baboon	Nhiễu	1%	0	0.0105	0	0
		3%	0.0368	0.1622	0	0
		5%	0.3046	0.4389	0.0068	0.0098
	Làm mờ	r =1 px	0.4638	0.4776	0.3057	0.3281
		r =3 px	0.5655	0.5956	0.4521	0.4609
	Nén JPEG	10	0.1822	0.2335	0.0176	0.0127
		30	0.0931	0.1237	0	0
		60	0	0.0301	0	0
	Lọc trung vị	r =1 px	0.1613	0.3416	0.2881	0.3164
		r =2 px	0.3116	0.5489	0.4072	0.4189
Lena	Nhiễu	1%	0	0.0415	0	0
		3%	0.0986	0.1563	0	0
		5%	0.3330	0.4961	0.0059	0.0078
	Làm mờ	r =1 px	0.3154	0.4545	0.2802	0.2773
		r =3 px	0.5170	0.6032	0.4336	0.4150
	Nén JPEG	10	0.1463	0.1866	0.0117	0.0215
		30	0.0645	0.0693	0	0
		60	0	0.0146	0	0
	Lọc trung vị	r =1 px	0.1309	0.3672	0.2998	0.2842
		r =2 px	0.2266	0.5264	0.3594	0.3750
Pepper	Nhiễu	1%	0	0.0539	0.0049	0.0098
		3%	0.0368	0.1279	0.0088	0.0117
		5%	0.3438	0.4824	0.0137	0.0166
	Làm mờ	r =1 px	0.4203	0.5036	0.2773	0.2715
		r =3 px	0.5362	0.5826	0.4883	0.4795

	Nén JPEG	10	0.1885	0.2163	0.2861	0.0313
		30	0.0425	0.0993	0.1631	0.0127
		60	0	0.0246	0.01270	0
	Lọc trung vị	r =1 px	0.1019	0.3089	0.1211	0.3223
		r =2 px	0.2365	0.4993	0.2705	0.4043
Airplane	Nhiễu	1%	0	0.0020	0.0068	0
		3%	0.0155	0.1057	0.1807	0
		5%	0.3008	0.4915	0.3691	0.0137
	Làm mờ	r =1 px	0.4002	0.5169	0.2588	0.3125
		r =3 px	0.4932	0.5910	0.4268	0.4609
	Nén JPEG	10	0.1645	0.2015	0.2539	0.0098
		30	0.0320	0.0907	0.0879	0
		60	0	0.0106	0.0059	0
	Lọc trung vị	r =1 px	0.1365	0.3114	0.2139	0.3975
		r =2 px	0.2402	0.4802	0.2939	0.4688

Tính bền vững của các lược đồ thủy vân trước các phép tấn công được đo bằng giá trị *Err* trong công thức (3) và các giá trị này được thống kê trong Bảng 2.

Từ Bảng 2 có thể rút ra các kết luận sau:

- *Lược đồ QR-1 và SVD-1*: Trước phép tấn công lọc trung vị thì SVD-1 bền vững hơn QR-1. Tuy nhiên, đối với ba phép tấn công còn lại thì QR-1 bền vững hơn SVD-1.

- *Lược đồ QR-1 và SW:* Trước phép tấn công làm mờ thì SW bền vững hơn QR-1. Tuy nhiên, đối với ba phép tấn công còn lại thì QR-1 bền vững hơn SW.

- *Lược đồ QR-N và SVD-N:* Tính bền vững của hai lược đồ này thấp hơn so với ba lược đồ SVD-1, SW và QR-1.

VI.3. So sánh SVD-1 và QR-1 tại các vị trí nhúng thủy vân khác nhau

Bảng 3 thống kê giá trị *Err* của 2 phương án đối với SVD-1 (nhúng trên *D(1,1)* và *D(2,2)*) và 2 phương án đối với QR-1 (nhúng trên *R(1,1)* và *R(1,8)*).

Kết quả trong Bảng 3 cho thấy: Với lược đồ SVD-1 thì nhúng trên *D(2,2)* có tính bền vững thấp hơn hẳn khi nhúng trên *D(1,1)*, còn với lược đồ QR-1 thì nhúng trên *R(1,8)* vẫn có tính bền vững như khi nhúng trên *R(1,1)*. Điều này phù hợp với phân tích trong mục V.2.

VII. KẾT LUẬN

Bài báo đề xuất hai lược đồ thủy vân QR-1 và QR-N trên miền không gian ảnh. Các lược đồ thuỷ vân này có độ phức tạp tính toán thấp hơn so với các lược đồ thuỷ vân dựa trên phân tích SVD. Kết quả thực nghiệm trên bộ ảnh chuẩn và bốn phép tấn công cho thấy: Với các tham số được chọn để chất lượng ảnh thủy vân của các lược đồ tương đương thì tính bền vững của QR-1 tốt hơn SVD-1 và SW trước một số phép tấn công. Ngoài ra, lược đồ đề xuất có thể chọn một phần tử bất kỳ trên hàng đầu của *R* để nhúng thuỷ vân mà không thay đổi tính bền vững, trong khi lược đồ SVD-1 chỉ bền vững khi chọn phần tử đầu tiên trên đường chéo của ma trận D. Nên trong lược đồ QR-1 có thể thiết kế việc chọn phần tử để nhúng thuỷ vân một cách ngẫu nhiên theo một khoá nguyên hoặc nhị phân để nâng cao tính bảo mật. Việc kết hợp các phép biến đổi ma trận khác như DCT, DWT, SVD với QR để xây dựng các lược đồ thủy vân kết hợp có độ bền vững cao hơn sẽ là hướng nghiên cứu tiếp theo của các tác giả bài báo.

TÀI LIỆU THAM KHẢO

[1] P. BAO, X. MA, *"Image adaptive watermarking using wavelet domain singular value decomposition"*, IEEE Transactions on Circuits and Systems for Video Technology, pp. 96-102, 2005.

[2] BHATNAGAR, GAURAV, AND BALASUBRAMANIAN RAMAN, *"A new robust reference watermarking scheme based on DWT-SVD"*, Computer Standards & Interfaces, pp. 1002-1013, 2009.

[3] C. C. CHANG, P. TSAI, C. C. LIN, *"SVD-based digital image watermarking scheme"*, Pattern Recognition Letters, Volume 26, Issue 10, pp. 1577-1586, July 2005.

[4] B. CHEN AND G. W. WORNELL, *"Quantization index modulation: a class of provably good methods for digital watermarking and information embedding", IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

[5] H. CHEN, AND Y. ZHU, *"A robust watermarking algorithm based on QR factorization and DCT using quantization index modulation technique"*, Journal of Zhejiang University SCIENCE C, pp. 573-584, 2012.

[6] K. L. CHUNG, W. N. YANG, Y. H. HUANG, S. T. WU, & Y. C. Hsu, *"SVD-based watermarking algorithm"*, Applied Mathematics and Computation, 188(1), 54-57, 2007.

[7] U. M. GOKHALE, AND Y. V. JOSHI, *"A Semi Fragile Watermarking Algorithm Based on SVD-IWT for Image Authentication"*, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2012.

[8] G.H. GOLUB, C.F.V. LOAN, *Matrix Computations*, third ed., Johns Hopkins University Press, Baltimore MD, 1996.

[9] C. C. LAI,*"An improved SVD-based watermarking scheme using human visual characteristics"*, Optics Communications, pp. 938-944, 2011.

[10] F. LIU, Y. LIU, *"A watermarking algorithm for digital image based on DCT and SVD"*, in Proc. Congr. image and signal processing (CISP '08), vol. 1, Sanya, Hainan, pp. 380-383, May 2008.

[11] R. LIU AND T. TAN, *"An SVD-based watermarking scheme for protecting rightful ownership"*, IEEE Trans. Multimedia., vol. 4, no. 1, pp. 121–128, Mar. 2002.

[12] NADERAHMADIAN YASHAR AND SAIED HOSSEINI-KHAYAT, *"Fast watermarking based on QR decomposition in wavelet domain"*, Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. IEEE, 2010.

[13] D. SALOMON, *Data Compression: The Complete Reference*, 3rd ed., Springer, 2004.

[14] W. SONG, J. HOU, Z. LI, L. HUANG, *"Chaotic system and QR factorization based robust digital image watermarking algorithm"*, *J. Cent. South Univ. Technol.*, 18(1):116-124, 2011.

[15] D. STANESCU, D. BORCA, V. GROZA, M. STRATULAT, *"A hybrid watermarking technique using singular value decomposition"*, in Proc. IEEE Int. Workshop Haptic Audio visual Environments and Games (HAVE '08), Ottawa, Ont., pp. 166-170, October 2008.

[16] R. SUN, H. SUN, T. YAO, *"A SVD and quantization based semi-fragile watermarking technique for image authentication"*, Proc. Internat. Conf. Signal Process. 2, pp. 1952–1955, 2002

[17] X. SUN, J. LIU, J. SUN, Q. ZHANG, W. JI, *"A robust image watermarking scheme based on the relationship of SVD"*, in Proc. Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP '08), Harbin, pp. 731-734, August 2008.

[18] X. ZHU, J. ZHAO, H. XU, *"A digital watermarking algorithm and implementation based on improved SVD"*, in Proc. 18th Int. Conf. Pattern Recognition (ICPR '06), vol. 3, Hong Kong, pp. 651-656, 2006.

Nhận bài ngày: 16/08/2013

SƠ LƯỢC VỀ TÁC GIẢ

TRẦN ĐĂNG HIÊN

Sinh ngày 06/08/1983 tại Hà Nội.

Tốt nghiệp Đại học năm 2005. Tốt nghiệp Thạc sỹ năm 2010 tại Trường Đại học Công nghệ – Đại học Quốc gia Hà Nội.

Hiện giảng dạy tại Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội.

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

Email:hientd_68@yahoo.com

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 sỹ 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

NGUYỄN NGỌC HƯNG

Sinh ngày 9/12/1987 tại Hưng Yên.

Tốt nghiệp Đại học năm 2009. Hiện là nghiên cứu viên tại Phòng Tin học Viễn thông, Viện CNTT, Viện Hàn lâm Khoa học Công nghệ Việt Nam.

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

Email: nnhung@ioit.ac.vn

PHẠM VĂN ẤT

Sinh ngày 12/6/1945 tại Hà Nội.

Tốt nghiệp Đại học năm 1967 và Tiến sỹ năm 1980 tại Trường Đại học Tổng hợp Hà Nội.

Năm 1984 nhận học hàm Phó Giáo sư.

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