Equipment with new general education program, Volume 1, Issue 306 (February 2024)
ISSN 1859 - 0810

Xây dựng các lược đồ thủy vân bền vững bằng cách kết hợp phép biến đổi DWT và SVD

Nguyễn Nam Phương, Nguyễn Thùy Linh**
**ThS. Trường Cao Đẳng Yên Bái*
Received: 10/01/2024; Accepted: 18/01/2024; Published: 22/01/2024

Abstract: *This article presents some digital watermark schemes based on SVD and DWT transformations applied in copyright protection on digital image data. This is a new research direction in the world, with scientific significance and practical application.*
Keywords: *Digital watermark, SVD and DWT transformations*

1. Đặt vấn đề

Ngày nay, mạng Internet đã trở thành một trong các phương tiện truyền tải, chia sẻ thông tin, tài liệu một cách thuận tiện, hiệu quả. Tuy nhiên, vấn nạn sao chép và sử dụng không hợp pháp dữ liệu số ngày một tăng. Từ đó, cần thiết phải có các giải pháp chống sao chép để hạn chế việc vi phạm bản quyền các sản phẩm dữ liệu số. Một trong những giải pháp hữu hiệu để bảo vệ bản quyền là kỹ thuật thủy vân số. Bài báo trình bày một số lược đồ thủy vân bền vững dựa trên các phép biến đổi SVD, DWT ứng dụng trong việc bảo vệ bản quyền trên dữ liệu ảnh số. Đây là hướng nghiên cứu mới trên thế giới, có ý nghĩa khoa học và ứng dụng thực tiễn.

2. Nội dung nghiên cứu

2.1.Sơ lược về khái niệm kỹ thuật thủy vân số

Thủy vân số (tiếng Anh: digital watermark) là một loại "dấu ấn số" (thủy vân) được nhúng ngẫu nhiên vào một *tín hiệu* chống *nhiễu* như dữ liệu âm thanh, video hoặc hình ảnh. Nó thường được sử dụng để xác định quyền sở hữu bản quyền của tín hiệu đó.Thủy vân số dựa trên kết quả nghiên cứu của nhiều lĩnh vực khác nhau như: Mật mã học, kỹ thuật giấu tin, lý thuyết thống kê và xử lý tín hiệu số. Dựa trên mục đích sử dụng các lược đồ thủy vân được chia thành hai nhóm chính gồm *thủy vân bền vững* và *thủy vân dễ vỡ*. Thủy vân dễ vỡ là kỹ thuật nhúng thủy vân vào trong ảnh, khi có bất kì sự can thiệp hay thay đổi nào tới ảnh gốc thì dấu thủy vân sẽ không còn nguyên vẹn; kỹ thuật thủy vân này được ứng dụng trong bài toán xác thực tính toàn vẹn dữ liệu số. Trong khi đó thủy vân bền vững được ứng dụng trong bài toán bảo vệ bản quyền đối với các sản phẩm số.

2.2. Thủy vân bền vững dựa trên cac phép biến đổi SVD–DWT

2.2.1. Thủy vân trên miền SVD

Dựa trên khai triển, nhiều tác giả đề xuất các lược đồ thủy vân trên miền SVD. Theo các tài liệu nghiên cứu, dữ liệu ảnh được chia thành các khối F_i kích thước m×n, i = 1,…, n. Với mỗi khối F, các thuật toán áp dụng phép khai triển SVD để nhận được 3 ma trận U, D, V tương ứng.

Sau khai triển SVD, mỗi ma trận được nhúng một bit dấu thủy vân vào một hoặc hai phần tử của ma trận để nhận được ma trận U'. Từ U', bằng phép biến đổi SVD ngược sẽ nhận được khối ảnh thủy vân F'.

Thay việc sử dụng ma trận U để nhúng thủy vân, một số phương pháp nhúng dấu thủy vân trên các ma trận V, D. Theo kết quả thực nghiệm của các phương pháp thì nhúng thủy vân trên ma trận D có tính bền vững cao hơn so với nhúng thủy vân trên ma trận V và D. Tuy nhiên, chất lượng ảnh của các lược đồ thủy vân trên các ma trận U, V lại cao hơn các thuật toán trên ma trận D.

Trên miền SVD, lược đồ [7] được xem là một trong những lược đồ có tiềm năng ứng dụng cao. Theo [7], thuật toán sử dụng ảnh gốc I, dấu thủy vân $W=(w_1,...,w_t)$ có độ dài t bit 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:

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

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

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

Bước 3: Nhúng bit Wi 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. 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).

Bước 4: 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.

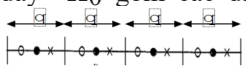
Nhận xét: Công thức tính $D_i^{'}(1,1)$ trong trường hợp $w_i = 1$ và $Z_i < q/4$ trình bày trong bước 2 chứa số hạng $-Z_i$, nhưng $+Z_i$ là: $D_i'(1,1) = D_i(1,1) - q/4 + Z_i$

Về mặt lý thuyết $D_i(1,1)$ 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 bit thủy vân wi = 0 hoặc wi = 1 . Nói cách khác nếu wi = 0 thì Di'(1,1) thuộc Ω0 và nếu wi = 1 thì Di'(1,1) thuộc Ω1. Trên hình dưới đây Ω0 gồm các điểm ○, Ω1 gồm các điểm ×:



Khi đó, trong quá trình trao đổi, ảnh thủy vân I' 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'.

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

Bước 2: Áp dụng phân tích SVD trên mỗi khối I_i^*: $I_i^* = U_i^* \times D_i^* \times V_i^{*T}$

Bước 3: Xác định bit 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 $Z_i^* \geq q/2$

Bước 4: So sánh dấu thủy vân $W^* = (w_1^*, ..., w_t^*)$ trích ra từ I* với dấu thủy vân gốc $W = (w_i, \ldots, w_i)$ bằng cách dùng hệ số Err: $\mathrm{Err} = \frac{1}{t}\sum_{i=1}^{1} w_i XOR w_i^*$

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 < τ (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'.

2.2.2. Phương pháp DMA: Thủy vân kết hợp SVD và DWT ba mức

Có nhiều nghiên cứu kết hợp phép SVD và DWT để xây dựng các lược đồ thủy vân nhằm làm tăng tính bền vững với các phép tấn công, tăng tính ổn định và tính ẩn của các lược đồ thủy vân. Kế thừa các nghiên cứu trước đây, H. Danyali và cộng sự [5] có đưa ra một lược đồ thủy vân. Chi tiết được trình bày dưới đây:

a) Thuật toán chuyển đổi sang dãy nhị phân

Thuật toán 1: Chuyển đổi từ số thực sang dãy nhị phân

```
Count = 1;
While(S~=0)
B(count)= mod(S, 2);
S= fix(S/2);
S = fix(S/2);
count = count + 1
end
```

Thuật toán 2: Chuyển đổi từ dãy nhị phân sang số thực

Algorithm 2

```
S= 0;
k =1
for i =2: size(B)
S = S+B(i) × k;
K= k×2;
end
```

b) Thuật toán nhúng thủy vân

Input: Ảnh $X_{M\times N}$, dấu thủy vân $W_{M_1\times N_1}$

Output: $X^*_{M\times N}$ chứa dấu thủy vân.

Bước 1: Áp dụng k mức phép biến đổi DWT cho ảnh X thu được các miền tần số kí hiệu là X_t^θ , trong đó $1 \leq l \leq K$ và $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$.

Bước 2: Áp dụng phép biến đổi SVD cho các vùng tần số, thu được:

$$X_K^\theta = U_X^\theta S_X^\theta (V_X^\theta)^T$$

Kí hiệu β_i^θ, i= 1,…,n là các (Singler Values) SV_S của S_x^θ, $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$ và r là hạng của ma trận S_x^θ.

Bước 3: Áp dụng SVD cho dấu thủy vân W và chuyển đổi các SV_s sang số nguyên ∈ [0…255].

$W = U_W S_W (V_W)^T$; $\alpha = 255 / \beta_1^W$;

$\beta_i^W = \beta_i^W \times \alpha; i = 1, ..., r.$

Bước 4: Chuyển đổi sang dãy nhị phân

$\beta_i^W \xrightarrow{Thuat\ toan\ 1} \beta_i^{W^{ar}}$ $\quad$ $\beta_i^\theta \xrightarrow{Thuat\ toan\ 1} \beta_i^{W^{ar}}$

Bước 5: Chèn $\beta_i^{W^{ar}}$ vào $\beta_i^{\theta^{ar}}$ như sau:

$\beta_i^{LL^{ar}}(1) = \beta_i^{W^{ar}}(1)$ $\quad \beta_i^{HL^{ar}}(2) = \beta_i^{W^{ar}}(5)$

$\beta_i^{LL^{ar}}(2) = \beta_i^{W^{ar}}(2)$ $\quad \beta_i^{HL^{ar}}(4) = \beta_i^{W^{ar}}(6)$

$\beta_i^{LH^{ar}}(3) = \beta_i^{W^{ar}}(3)$ $\quad \beta_i^{HH^{ar}}(5) = \beta_i^{W^{ar}}(7)$

$\beta_i^{LH^{ar}}(4) = \beta_i^{W^{ar}}(4)$ $\quad \beta_i^{HH^{ar}}(4) = \beta_i^{W^{ar}}(8)$

Bước 6: Khôi phục các giá trị SV_s từ các chuỗi nhị phân theo thuật toán 2 được $S_X^{*\theta}$

Bước 7: Áp dụng phép biến đổi SVD ngược được $X_K^{*\theta}$: $X_K^{*\theta} = U_X^{\theta}.S_X^{*\theta}(V_X^{\theta})^T$

Bước 8: Áp dụng phép biến đổi IDWT ngược được ảnh chứa dấu thủy vân với $(X_{M\times N}^*)$.

Các bước này có thể mô tả qua sơ đồ sau:

c) Thuật toán trích thủy vân

Input: Ảnh chứa dấu thủy vân $X_{M\times N}^*$.

Output: Dấu thủy vân W.

Bước 1: Áp dụng K mức phép biến đổi DWT cho ảnh $X_{M\times N}^*$ thu được các miền tần số $X_L^{*\theta}$, $1 \le l \le K$, $\theta \in \{LL_K, LH_K, HL_K, HH_K\}$.

Bước 2: Áp dụng SVD cho các mức tần số

$X_K^{*\theta} = U_X^{*\theta} S_X^{*\theta}(V_X^{*\theta})^T$

Bước 3: Chuyển đổi các Singular Values (SV_s) $\beta_i^{*\theta}$ sang chuỗi nhị phân $\beta_i^{*\theta ar}$

$\beta_i^{w^{*\theta}} \xrightarrow{Thuat\ toan\ 1} \beta_i^{*\theta^{ar}}$

Bước 4: Trích các bit nhị phân của dấu thủy vân từ $\beta_i^{*\theta ar}$ như sau:

$\beta_i^{ext^{ar}}(1) = \beta_i^{*LL^{ar}}(1)$ $\quad \beta_i^{ext^{ar}}(5) = \beta_i^{*HL^{ar}}(2)$ $\quad \beta_i^{ext^{ar}}(2) = \beta_i^{*LL^{ar}}(2)$

$\beta_i^{ext^{ar}}(6) = \beta_i^{*HL^{ar}}(4)$ $\quad \beta_i^{ext^{ar}}(3) = \beta_i^{*LL^{ar}}(2)$ $\quad \beta_i^{ext^{ar}}(7) = \beta_i^{*HL^{ar}}(2)$

$\beta_i^{ext^{ar}}(4) = \beta_i^{*LL^{ar}}(4)$ $\quad \beta_i^{ext^{ar}}(8) = \beta_i^{*HL^{ar}}(4)$

Bước 5: Chuyển đổi các giá trị sang số thực: $\beta_i^{ext} = \beta_i^{ext} / \alpha$

Bước 6: Áp dụng phép biến đổi SVD ngược thu được dấu thủy vân

$W^{ext} = V_w S_w^{ext}(V_w)^T$

2.3. Thực nghiệm, phân tích và so sánh các lược đồ thủy vân

2.3.1. Ảnh thử nghiệm và các độ đo

Để thử nghiệm, nghiên cứu sử dụng các ảnh đa cấp xám, kích thước 512×512 và thủy vân là các hình logo ảnh có kích thước 64×64. Các chương trình được viết trên môi trường Matlab.

Một số độ đo để đánh giá chất lượng ảnh, tính ẩn, bền vững của lược đồ thủy vân:

Độ đo PSNR: $PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)(db)$

trong đó: $MSE = \frac{\sum M,N[X(m,n) - Y(m-n)]^2}{M*N}$

- Độ đo MSSIM: $MSSIM(X,Y) = \frac{1}{M}\sum_{j=1}^{M} SSIM(X_j, Y_j)$

trong đó: $SSIM(X,Y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2}$

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} X_i, \mu_y = \frac{1}{N}\sum_{i=1}^{N} Y_i$$

$$\sigma_x = \left(\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_i)^2\right)^{\frac{1}{2}}, \sigma_y = \left(\frac{1}{N-1}\sum_{i=1}^{N}(y_i - \mu_i)^2\right)^{\frac{1}{2}}$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y)$$

Độ đo tính bền vững: $\rho = \frac{\sum_{i,j=1}^{M_{L,N_L}}(w(i,j) - \bar{W})(W^*(i,j) - \bar{W}^*)}{\sqrt{(\sum_{i,j}^{M_{L,N_L}}(W(i,j) - \bar{W})^2)(\sum_{i,j=1}^{M_{L,N_L}}(W^*(i,j) - \bar{W}^*)^2)}}$

$$NC = \frac{\sum_{i=1,j=1}^{M,N}[W(i,j)W'(i,j)]}{\sum_{i=1,j=1}^{M,N}[W(i,j)]^2}$$

$$r = \frac{\sum_{i=1,j=1}^{M,N}[W(i,j) - \widehat{W}][W'(i,j) - \widehat{W'}]}{\sqrt{[\sum_{i=1,j=1}^{M,N}(W(i,j) - \widehat{W})^2][\sum_{i=1,j=1}^{M,N}(W'(i,j) - \widehat{W'})^2]}}$$

2.3.2. Kết quả thử nghiệm: Kết quả lược đồ DMA

Bảng 2.1: Kết quả thử nghiệm về chất lượng ảnh sau khi nhúng thủy vân:

	House	Pirate	Tree	Lena	Pepper	Plane
PSNR(dB)	63.78	63.41	63.11	63.44	63.32	63.83
MSSIM	0.9999	0.9999	0.9999	0.9999	0.9999	0.9999

Bảng 2.2: Kết quả thử nghiệm tính bền vững của lược đồ thủy vân:

	House	Pirate	Tree	Lena	Pepper	Plane
ρ	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

3. Kết luận

Bài báo tập trung xây dựng các lược đồ thủy vân bền vững dựa vào sự kết hợp của phép biến đổi DWT và SVD. Những đóng góp chính của bài báo bao gồm:1) Trình bày chi tiết về phép biến đổi DWT và SVD; 2) Cải tiến, phát triển lược đồ thủy vân bền vững trên miền DWT – SVD; 3) Xây dựng phần mềm thực hiện nhúng và trích dấu thủy vân nhằm khảo sát tính bền vững của lược đồ thủy vân DWT – SVD.

Tài liệu tham khảo

1. G. Bhatnagar, B Raman, *"A new robust reference watermarking scheme based on DWT-SVD"*, journal Computer Standards & Interfaces, Elsevier, 2009.

2. Tri H. Nguyen, Duc M. Duong, Duc A. Duong, "Robuts and high capacity watermarking for image based on DWT-SVD", IEEE RIVF, 2015.

3. 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