Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.062051

ARTICLE

Joint Watermarking and Encryption for Social Image Sharing

Conghuan Ye[1,*], Shenglong Tan[1], Shi Li[1], Jun Wang[1], Qiankun Zuo[1] and Bing Xiong[2]

[1]School of Information Engineering, Hubei University of Economics, Wuhan, 430205, China
[2]School of Computer and Communication Engineering, Changsha University of Science & Technology, Changsha, 410114, China
*Corresponding Author: Conghuan Ye. Email: p2pgrid@hbue.edu.cn

Received: 09 December 2024; Accepted: 07 January 2025; Published: 16 April 2025

ABSTRACT: With the fast development of multimedia social platforms, content dissemination on social media platforms is becoming more popular. Social image sharing can also raise privacy concerns. Image encryption can protect social images. However, most existing image protection methods cannot be applied to multimedia social platforms because of encryption in the spatial domain. In this work, the authors propose a secure social image-sharing method with watermarking/fingerprinting and encryption. First, the fingerprint code with a hierarchical community structure is designed based on social network analysis. Then, discrete wavelet transform (DWT) from block discrete cosine transform (DCT) directly is employed. After that, all codeword segments are embedded into the LL, LH, and HL subbands, respectively. The selected subbands are confused based on Game of Life (GoL), and then all subbands are diffused with singular value decomposition (SVD). Experimental results and security analysis demonstrate the security, invisibility, and robustness of our method. Further, the superiority of the technique is elaborated through comparison with some related image security algorithms. The solution not only performs the fast transformation from block DCT to one-level DWT but also protects users' privacy in multimedia social platforms. With the proposed method, JPEG image secure sharing in multimedia social platforms can be ensured.

KEYWORDS: Multimedia security; digital watermarking; image encryption; image sharing; privacy protection

1 Introduction

The rapid development of mobile communication, cloud storage, and multimedia social networks makes content dissemination on social media platforms popular. Many users share social JPEG images with their smartphones on a social multimedia platform. Personal-generated social multimedia content is distributed on social media platforms [1]. Secure sharing depends on confidentiality and traceability. Thus, a double level of security techniques, such as joint encryption and watermarking/fingerprinting [2], should be applied. Content encryption can hide the original information of plaintext multimedia content to protect privacy. It is difficult to access plaintext without the correct key. With the sensitivity properties of initial values and control parameters, chaotic maps can generate the encryption keys for image encryption [3]. The noise-like signal makes non-authorized users ignore the method with which it is generated [4]. Those legal users with the correct keys can access the plaintext data successfully [5]. Due to the application value of chaotic systems in image encryption [6], various chaotic systems have been constructed recently. Wu et al. designed a circularly shifting chaotic map generation method [7]. A two-dimensional coupled complex chaotic map was designed in [8]. Multiscroll Hopfield neural network for video encryption was introduced in [9].

Image encryption schemes based on different chaotic systems have been researched in [10]. Most existing image encryption schemes were conducted in the spatial domain. For example, Kocak et al. proposed an encryption scheme based on a logistic exponential map [11] and a color image encryption algorithm using a 2D hyperchaotic map [12]. Feng et al. researched a pixel fusion strategy for image encryption [13], and a plane-level image encryption scheme [14]. Wang et al. proposed a color image encryption scheme [15]. Feng et al. [16] proposed a multi-channel image encryption scheme based on hyperchaotic maps. A color medical image encryption and compression scheme was proposed in [17]. The paper [18] presented an image encryption algorithm with a novel two-dimensional cross-hyperchaotic Sine-modulation-Logistic map (2D-CHSLM). A three-dimensional chaotic map for ship image encryption in [19]. A batch medical image encryption scheme was proposed in [20]. The research [21] encrypted face image based on DNA diffusion.

These proposed image encryption schemes can prevent sensitive content from being exposed by illegal users. The decrypted plaintext content could be illegal to use. Privacy may still be leaked. Security methods should be applied to the decrypted plaintext content to deter illegal redistribution [22]. Digital watermarking/fingerprinting can embed a specific mark into social multimedia content. Digital watermarking/fingerprinting is an effective technique to deter redistribution. Both encryption and watermarking can provide a way to protect multimedia content. They are applied to protect multimedia content separately [23,24]. Recently, the marriage of encryption and watermarking/fingerprinting for multimedia content protection has been rising. Image encryption schemes in the spatial domain are not desirable to social multimedia encryption. There are so many resource-constrained mobile devices in multimedia social networks. Apart from millions of professional cameras of media people, there are billions of personal smartphones used in the world, and most of them can take pictures/videos. If every single smartphone takes one picture every day, the number of generated images will be exceptionally large. It will be tough to imagine how much network bandwidth would be consumed within social media platforms [25]. In this case, image compression is a must for social media platforms [17].

The encryption technology in the spatial domain not only has high time complexity but also has no scalability. Image encryption in the spatial domain cannot meet the requests of various security levels, and it consumes more resources in cloud storage and secure communications. On the contrary, selective encryption, which is possible for the most important wavelet coefficients encryption in the transform domain, can improve the encryption efficiency. Selective encryption in the transform domain is scalable, and the encrypted content can be embedded into the watermark. On the other hand, once the encrypted image is decrypted, there is no way to protect it. Decrypted images can be used maliciously. Therefore, decrypted images need to be constantly monitored to prevent illegal misuse. As a copyright verification technology, digital watermarking can continuously monitor the use of images. Digital watermarking can prevent illegal misuse of plaintext images.

Joint watermarking and encryption would provide a higher level of security for social multimedia platforms. In [26], a digital watermarking method was proposed for the encrypted content. However, it did not cover social JPEG image protection. Because social photographs are becoming increasingly important on social media platforms as portable photography equipment becomes more common, they must be saved or sent economically.

In addition, digital watermarking [27] cannot trace who redistributes the watermarked copy on social multimedia platforms. With the help of digital watermarking, unique identification information can be embedded into the original content. Every copy will be different from each other. Although as an application of digital watermarking, digital fingerprinting can trace the source of the illegally redistributed copy, the existing fingerprinting schemes do not research the users' social relationships. They are not suitable for social multimedia tracking on social multimedia platforms. How to use social network analysis (SNA) to trace

social multimedia content is considered in [28]. The DWT can realize a hierarchical decomposition of a social image. It is possible to make a mapping relationship between the hierarchical community structure and the tree structure wavelet transform. The map relationship can be used for content tracing on social multimedia tracing.

If those existing joint watermarking and encryption methods are used in social multimedia platforms, they will face some challenges. First, most of them focus on the non-compressed content. It will transfer a huge volume of social images within social multimedia platforms. Second, most image encryption methods in the spatial domain do not have scalability for social multimedia distribution in social multimedia platforms. Third, resource-constrained mobile terminals and central servers will be a bottleneck for image security methods in the spatial domain. It will take a lot of computing and storage resources for those image security methods in the spatial domain. In this paper, to address privacy disclosure within multimedia social platforms to meet the double security level request, and implement scalable operations on encrypted images, a joint watermarking and encryption (JWE) scheme for social images is proposed.

As a nonsymmetrical decomposition, SVD can not only be used to embed watermarks but also to encrypt images. Although watermarking is often used for copyright protection, digital watermarking in the compressed-encrypted domain for social image security is novel. To save storage space and network bandwidth, social images are often compressed with JPEG standards. The rapid growth of JPEG image sharing within social multimedia platforms has magnified the requirement for multimedia content encryption and watermarking.

DWT from block DCTs can help to lower the time complexity of the JWE algorithm. In the meantime, scrambling along with SVD diffusion can increase the security level. The proposed scheme can provide a JWE scheme for balancing different security requirements and algorithm efficiency. The proposed scheme uses an 8D hyperchaotic map and GoL for permutation, SVD computing for diffusion and watermarking. The proposed scheme can overcome the shortcomings of existing image security schemes. First, a social fingerprint code is designed based on a hierarchical community structure. Then, the paper proposes a multimedia encryption scheme based on GoL confusion and SVD diffusion for wavelet coefficients, which are obtained from block DCTs.

There was no related research for privacy protection with GoL permutation and SVD diffusion for wavelet coefficients. Related techniques are introduced in Section 2. Section 3 details the privacy protection scheme. Then, the experimental results are demonstrated in Section 4. Section 5 concludes the paper.

2 Basic Theory

2.1 SVD

For a matrix, SVD is an important matrix decomposition with nonnegative scalar entries. Usually, a social image is also a matrix. A given social image A with size M × N can be divided with SVD. As a useful tool in image processing, SVD is an approximation and factorization technique. A social image can be regarded as a matrix. SVD can be shown as follows:

$$A = USV^T \tag{1}$$

where A is a rectangular matrix. U is a unitary matrix, the same as V. Both U and V are orthogonal matrices. U is also called the left singular vectors of image A, whereas V is its right singular vectors. S is a singular value matrix. Then, U and V are always satisfied the following relationship:

$$I_N = U^T U = UU^T \tag{2}$$

$$I_M = V^T V = V V^T \tag{3}$$

Both I_N and I_M are identity matrices, their sizes are $N \times N$ and $M \times M$, respectively.

2.2 Chaotic Map

The 8D chaotic map can be described as follows:

$$\begin{cases} x^*_1 = \omega_1(x_2 - x_1) + x_4 \\ x^*_2 = \omega_2 x_1 - x_2 x_3 + x_4 \\ x^*_3 = x_1 x_2 - x_3 - x_4 + x_7 \\ x^*_4 = \omega_3(x_1 + x_2) + x_5 \\ x^*_5 = -x_2 - \omega_4 x_4 + x_6 \\ x^*_6 = -\omega_5(x_1 + x_5) + \omega_4 x_7 \\ x^*_7 = -\omega_6(x_1 + x_6 - x_8) \\ x^*_8 = -\omega_7 x_7 \end{cases} \tag{4}$$

$$X(0) = (x_1(0), x_2(0), \ldots, x_8(0)) \tag{5}$$

where (ω1, ω2, ω3, ω4, ω5, ω6, ω7) is control parameter. If the initial value $X(0)$ = (1, 1, 1, 1, 0, 0, 0, 0) and control parameter (ω1, ω2, ω3, ω4, ω5, ω6, ω7) = (10, 76, 3, 0.2, 0.1, 0.1, 0.2). The chaotic system evolves into a chaotic state. Both the control parameter and the initial value are secret keys. This 8D chaotic Map generates random values.

2.3 Secure Hash Algorithm (SHA)-3

SHA-3 can process messages of any size to a fixed length. At the same time, it can authenticate encryption and generate pseudo-random numbers. SHA-3 is a widely used hash function [29]. Through SHA-3 computing, the given type of message, a fixed length of 256/512-bit hash values can be generated. All hash values can ensure the consistency and integrity of the input message. In this work, the proposed encryption scheme will use a 256-bit hash value. For SHA-3, even if the original input information has changed a tiny bit, the new returned hash result will be different from the original hash result of the information. Furthermore, because computing is based on bit-level operations, its time performance is superior. Because SHA-3 is sensitive to the initial message, it often is used to generate keys.

2.4 CA (Cellular Automata)

Cellular automation [30] is a dynamic and complex system that is discrete in space and time. Cellular automation is a special form of finite-state machines. Cellular automation can generate chaotic behavior with simple operations, and its computational complexity is low, making it an effective way to encrypt multimedia content.

Two-dimensional cellular automation, also known as Game of Life, is composed of a cell matrix, in which each cell is a cell, and each cell has only two states, life and death (represented by 1 and 0, respectively). Every once in a while, all cells must use the rules of life and death to refresh their own state. In the two-dimensional matrix of the game of life, each cell has 8 neighbors, and the life and death of its surrounding neighbors determine whether the cell will live or die in the next period. In GoL, the Moore neighborhoods [31] can be represented by

$$NB(x_0, y_0, L) = \{(x, y) : |x - x_0| \le L, |y - y_0| \le L\} \tag{6}$$

where L is the neighborhood range. Then each cell transitions to the next state through the following life-and-death rules:

Rule 1: when the total number of neighbor cells surviving is less than 2, and the cell state is alive, the state changes from a living state to a dead state. When the cell state is dead, the state will not change.

Rule 2: when the total number of surviving cells in neighbors is greater than 3 and the cell state is survival, the state will change from survival state to death state. When the cell state is dead, the state will not change.

Rule 3: when the total number of surviving cells in the neighbor is 2, the state of the cell will not change.

Rule 4: when the total number of surviving cells of neighbors is 3 and the cell state is death, the state changes from death state to survival state. When the cell state is survival, the state will not change.

For binary cells $c_1, c_2, \ldots, c_9$, the transition rule [32] is of the form:

$$\phi\begin{pmatrix} c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 \\ c_7 & c_8 & c_9 \end{pmatrix} = \begin{cases} 1, & \text{if } \sum_{i=1}^{9} s\left(c_i,\ t\right) = 3 \\ 1, & \text{if } \sum_{i=1}^{9} s\left(c_i,\ t\right) = 3,\ i \neq 5 \\ 0, & otherwise \end{cases} \tag{7}$$

3 The Proposed JWE Algorithm

Important notations are listed below:

N_u the number of total users in a multimedia social platform

X^O the community code

X^I the user code

L^O the length of X^O

L^I the length of X^I

X_* half of the initial fingerprint codeword

Sum_* the sum of X_*

d_k fingerprint embedding strength control vector

Y_k multimedia content embedded with fingerprints

G^0 the cell grid of the initial state of CA

Pl_r original coefficient block

Cp_r scrambled coefficient block

A_i evolution matrix of GoL

I^{JWE} the watermarked and encrypted image

DWT discrete wavelet transform

DCT discrete cosine transform

GoL Game of Life

SVD singular value decomposition

DPCM joint encoding method of predictive coding

BS code A kind of fingerprint code

JPEG Joint Photographic Experts Group
QIM quantization index modulation
SNA social network analysis
JWE joint watermarking and encryption
CA Cellular Automata
NC Normalized correlation values
BER bit error ratio
SHA Secure Hash Algorithm
FRFT fractional Fourier transform

3.1 Fingerprint Code

The scheme in [33] is used to detect the hierarchical community structure of users within a multimedia social platform. A multilevel hierarchical fingerprint code is designed based on the community structure. According to Fig. 1, all users belong to different communities. They are encoded as community codes by [34]. Every user in a community is coded as a user code with Tardos scheme [35]. Then, every fingerprint codeword can be concatenated by a multilevel social codeword and a user codeword [36].

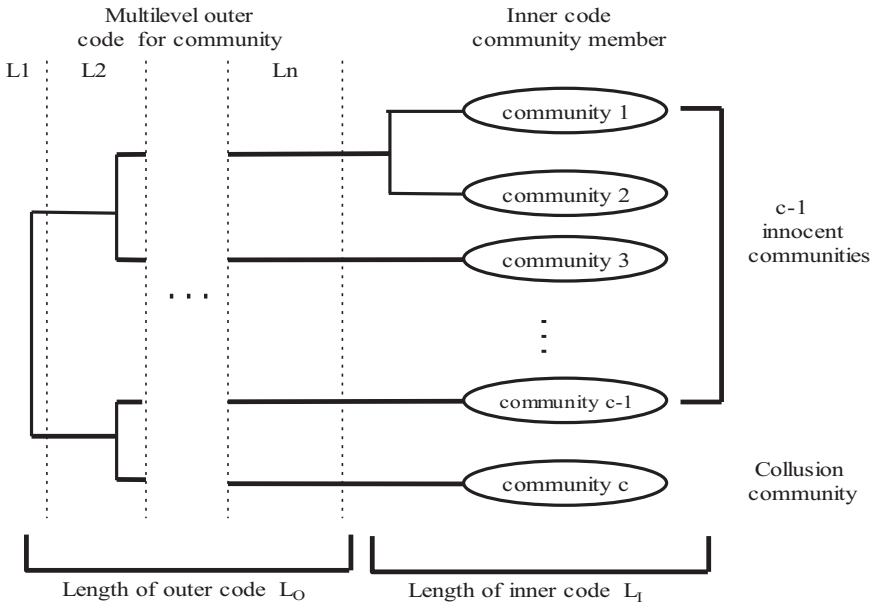


Figure 1: Encoding based on community structure

3.2 DWT from DCT Directly

The JPEG compression standard is based on the DCT transform [9]. Given an image, divide it into blocks of eight-by-eight size. Perform DCT on each image block. Every DCT block is quantized, then the quantized block is scanned by zigzag mode. JPEG adopts a joint encoding method of predictive coding (DPCM), discrete cosine transform (DCT), and entropy coding to remove redundant images and color data, belonging to the lossy compression format. JPEG can use lossy compression to remove redundant image data

and achieve better image quality with less disk space. Most images in multimedia social platforms are stored in JPEG format. Block coefficients in the DCT domain can be obtained from a JPEG image through partial decoding. These block coefficients are subsequently used to perform one-level DWT.

A fast one-level DWT can be gotten from block DCTs directly. The computational complexity is lowered. Compared with DCT, the tree structure haar wavelet transform is hierarchical because it decomposes an input image into several multiresolution subbands which can be processed independently. Because the DWT does not partition an image block, it causes fewer visual artifacts than the DCT. An image is decomposed into LL, LH, HL, and HH subbands through fast one-level DWT. The LL subband is called as approximation subband, LH is the horizontal detail component, HL is the vertical detail component, and HH is the diagonal detail component. The LL subband can be decomposed into four components through DWT.

The JPEG compressed image is firstly decompressed block DCTs of the JPEG image into many single pixels. In the end, it is possible to perform DWT on these pixels. DWT is an invertible transform, and so does DCT. Given an image, there is a one-to-one map relationship between DWT and block DCTs [37]. The one-level DWT of a JPEG image can be obtained from block DCTs directly. Thus, without involving inverse DCT, we can perform the watermarking and encryption scheme in the DWT domain to avoid full decoding of JPEG images. Because the computational time of inverse DCT can be avoided [38], the DWT from block DCTs can lower the computational cost of the proposed watermarking and encryption operation. The DWT from block DCTs is efficient because it will not take a large amount of time to inter-converse between the spatial pixel data and the DCT coefficients. Hence, the direct conversion between one-level DWT coefficients and the block DCTs can prevent full decoding.

Given an image I_0 with size $(L \times S) \times (K \times S)$. It can be divided into $L \times K$ blocks. An image block is denoted as BL_{ij} with size $S \times S$. $C_{ij}(u, v)$ is the DCT coefficient block. It can be represented as

$$C_{ij}(u,\ v) = \sqrt{\frac{2}{S}}\alpha(v) \sum_{q=0}^{S-1} \sqrt{\frac{2}{S}}\alpha(u) \sum_{q=0}^{S-1} I(p,\ q) \cos\left(\frac{(2p+1)\,u\pi}{2S}\right) \cos\left(\frac{(2p+1)\,v\pi}{2S}\right) \tag{8}$$

where $u,\ v = 1,\ 2, \ldots.,\ S$, $\alpha(v)$, $\alpha(u) = \begin{cases} 1/\sqrt{2}, & if\ (v = 0\ or\ u = 0) \\ 1, & else \end{cases}$.

Perform DCT on Sb_{ij}, then $C_{ij}(u,\ v) = B_1 \times BL_{ij} \times B_1^T$. $BL_{ij} = {B_1}^{-1} \times C_{ij} \times \left(B_1^T\right)^{-1}$ is the inverse transform, where B_1 and B_1^T are block DCTs, both of them are orthogonal matrices. Therefore I_0 is as follows:

$$I = \begin{bmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_1 \end{bmatrix}^{-1}_{LS \times LS} \times \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1K} \\ C_{21} & C_{22} & \cdots & C_{2K} \\ \vdots & \vdots & \ddots & \vdots \\ C_{L1} & C_{L2} & \cdots & C_{LK} \end{bmatrix} \times \begin{bmatrix} B_1^T & 0 & \cdots & 0 \\ 0 & B_1^T & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_1^T \end{bmatrix}^{-1}_{KS \times KS} \tag{9}$$

B_4, C_{part}, and B_5 are used to denote the right three matrices of the above equation. DWT uses the simplest haar wavelet. It can be expressed as the following equation:

$$KR = H \times I_0 \times Q^T \tag{10}$$

The haar wavelet is both symmetric and separable. For the DWT, H contains $h_z(k)$, $h_z(k)$ is a haar basis function. Then $h_0(z) = h_{00}(z) = \frac{1}{\sqrt{LS}}$, $z \in [0, 1]$.

$$h_k(z) = h_{pq}(z) = \frac{1}{\sqrt{LS}} \begin{cases} 2^{p/2}, & (q-1)/2^p \le z < (q-0.5)/2^p \\ -2^{p/2}, & (q-0.5)/2^p \le z < q/2^p \\ 0, & \text{otherwize}, z \in [0, 1] \end{cases} \tag{11}$$

The image I_0 can be recovered according to the inverse transform $I_0 = H^T \times KR \times Q$. KR can be represented by

$$KR = A_1 \times C_{part} \times A_2 \tag{12}$$

where $A_1 = H \times B_4$, $A_2 = B_5 \times Q^T$, KR is the wavelet coefficient matrix. Through the inverse transformation from DWT to block DCTs, block DCT coefficients can be obtained from the wavelet coefficient matrix KR directly as follows:

$$C_{part} = A_1^T \times KR \times A_2^T \tag{13}$$

Given a JPEG image, perform DWT from block DCTs directly, the JPEG image is decomposed LL approximation component, and LH, HL, and HH detail components. We can transform LL subband repeatedly. For a given community structure, the DWT splitting scheme is determined using social network analysis (SNA). According to Fig. 1, the number of communities is c. The number of total community layers of a multimedia social network is $n + 1$.

3.3 The Privacy Protection Scheme

The proposed scheme is shown in Fig. 2. The whole JWE processes include fingerprinting embedding and encryption.

1) Fingerprint embedding

Suppose there are N_u users in a multimedia social platform. The fingerprint embedding is based on quantization index modulation (QIM). The user fingerprint codeword is embedded with an improved QIM scheme. Coefficients in the LL subband are chosen to compose the host vector $X^I = (x_1, x_2, \ldots, x_{L^I})$ to embed personal user code, and the authors choose another robust coefficient sequence in the horizontal and vertical components to compose another coefficient vector $X^O = (x_1, x_2, \ldots, x_{L^O})$ for multilevel community codeword embedding. The user codeword embedding scheme is based on Eq. (14). The multilevel community fingerprint codeword embedding scheme is as follows:

$$y_j^{(i)} = q_{x_j} = round\left(\frac{x_j + d_i^{(j)}}{\Delta_Z}\right) \times \Delta_Z \tag{14}$$

where Δ_Z is a constant, x_j is a wavelet coefficient set with length L^O, it is used to embed multilevel community fingerprint codeword, $i, j = 1, \ldots, L^O$. *Round* is a *Floor* and *Ceiling* operation.

To detect fingerprint information for content redistribution tracing, the fingerprinted coefficients are gained to compose a vector z. By deducting, user k related to the least T_k is determined as the illegal distributor.

$$T_k = \|z - y_k\|^2, \; k = 1, \ldots, L \tag{15}$$

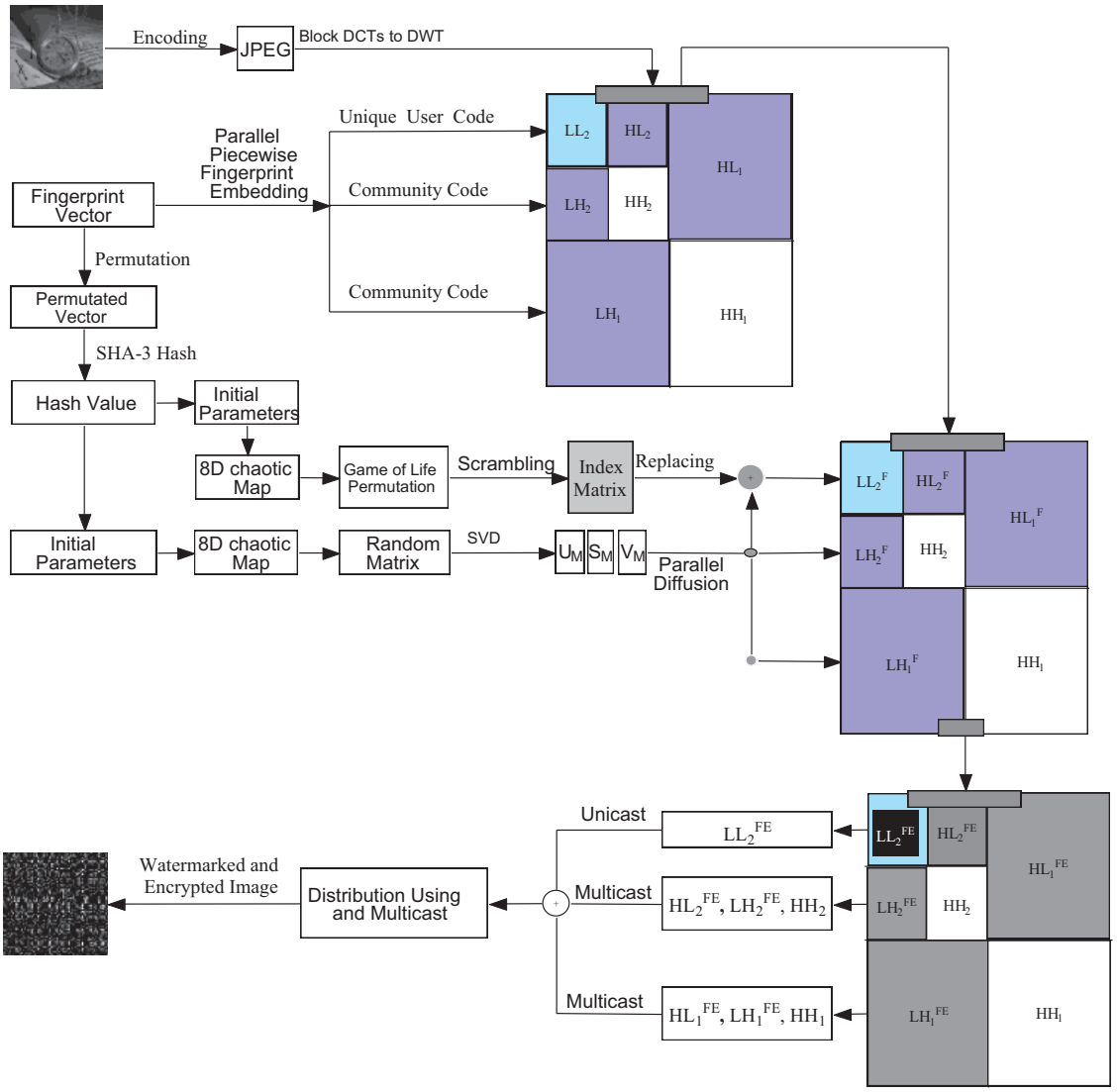


Figure 2: Architecture of proposed JWE

2) Encryption algorithm

Visual quality is essential to digital multimedia content such as images. Image encryption which hides the original information should resist algorithm attacks. If the encrypted content is unintelligent, the encryption algorithm is secure. We focus on JPEG image security on multimedia social platforms. With the proposed encryption algorithm, the encrypted image must appear as noise. It is difficult to obtain original plaintext information from encrypted content without a decryption key. Because it is necessary to massively disseminate encrypted content in parallel [39] for near real-time requests of resource-constrained devices in multimedia social platforms. Existing image encryption in the spatial domain is not feasible because of the high volumes of uncompressed content. Resource-constrained devices in multimedia social platforms cannot decrypt the encrypted content.

If the existing encryption and fingerprinting algorithms are applied to the compressed JPEG image, the total encrypted and fingerprinting time will be longer. Big data problems will be produced when the JPEG image is embedded into the fingerprint codeword repeatedly and distributed to users. To solve these

issues, partial encryption is proposed. Selected important content is encrypted to lower computation time for the JWE. CA can show dynamical chaotic behavior with several quite simple rules, which can offer the benefit of lowering computation complexity. The chaotic behavior makes CA an interesting system for image encryption [40]. Conversation of DWT from block DCTs helps in achieving this fast computation capability. Chaotic CA is used to encrypt fast too. SVD is performed for the confused matrices in the real number domain.

The lowest computational complexity can be obtained by selective encryption, which is efficient without compromising encryption security. In this paper, we propose a joint watermarking and encryption method for JPEG image security to overcome the drawbacks of conventional permutation-only type image cipher. The novel JWE scheme is based on CA and SVD in Fig. 2. Coefficients in the DWT domain are watermarked and encrypted. Image encryption includes permutation with CA and diffusion with SVD operation. The random matrix for SVD is produced with a chaotic map. The proposed coefficient encryption algorithm has the following steps:

Step 1: Permute codeword of user. The confused codeword vector is divided into two different parts: $X = X_1 + X_2$. The sum of both parts is calculated. Sum_{X_1} is the sum of the first part, and Sum_{X_2} is the second part. Get Th through subtracting two sums Sum_{X_1} and Sum_{X_2}. The initial value is generated from Th using SHA-3 to get V^{Th}. V^{Th} is divided into 16 equal parts ${V^{Th}}_1$, ${V^{Th}}_2$,..., ${V^{Th}}_{16}$. Each part is a 16-bit binary number. We can compute initial values $x_1, x_2, \ldots, x_8$, and control parameters $(\omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6, \omega_7)$ with ${V^{Th}}_1$, ${V^{Th}}_2$,..., ${V^{Th}}_{16}$, respectively, the initial values and control parameters are secret keys in the proposed encryption algorithm.

Fig. 3 shows the state change of GoL with a 6 × 6 matrix, Fig. 3 (left) demonstrates the first state of the GoL; state 1 is regarded as a living cell. Fig. 3 (middle) displays a 6 × 6 matrix to permute. The encrypted matrix corresponding to Fig. 3 (middle) is shown in Fig. 3 (right). Through inverse GoL, the original matrix can be obtained from the encrypted matrix. Where the matrix A_0 and k can be regarded as keys.

0	1	0	0	1	0
0	0	0	1	0	1
1	0	0	0	0	0
0	0	1	0	0	0
0	0	0	0	1	0
1	0	0	0	0	1

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

	1				5	
				9		4
6						
		5				
					6	
5						0

Figure 3: Matrix element mixing based on GoL (left, original GoL, middle, original image, right, encrypted image)

Step 2: There exists a strong correlation between adjacent coefficients in an image. For image encryption, the correlation between adjacent coefficients should be broken. The wavelet coefficients are scrambled based on GoL. The evolution of GoL is based on an orthogonal grid composed of square cells. They only have two states, alive or dead. For image encryption in the wavelet domain, the GoL can achieve both scrambling and diffusion effects simultaneously. The state change method of the evolution matrix of GoL is as follows:

(1) A chaotic sequence $(x_1 x_2 \cdots x_{M\times N})$ is generated based on the 8D chaotic map, then a two-dimensional grid of cells G^0 can be created from the generated chaotic sequence. G^0 is the seed of GoL. The main rule is that whether the corresponding cell is alive or not depend on the value of x_i. A cell is dead if and only if its corresponding x_i is less than the average value of $x_1 x_2 \cdots x_{M\times N}$, else it is alive. G^0 is used to encrypt the coefficient matrixes of the original image. Run the $M \times N$ GoL automaton for k generations to obtain $\{A_1, A_2, \ldots, A_k\}$ matrices from the initial random configuration A_0.

(2) Given I_G is the coefficient matrix in the DWT domain, then a set of $\{Pl_1, Pl_2, \ldots, Pl_k\}$ can be gotten for the original matrix.

(3) For Pl_r $(r = 1, \ldots, m)$, assume matrix Pl_r is the input block; while matrix Cp_r is the scrambled block. A_1 is the first encrypted matrix scrambled with GoL. Set row = 1, col = 1.

(4) If $A_1(i, j) = 1$, put the value of P_e (row, col), in $Cp_r(i, j)$. Increment (row, col) to point to the neighbor in matrix Pl_r from row to col.

(5) Use the life and death rules of GoL to generate the k-th generation matrix $A_k(i, j)$, replace the corresponding plaintext coefficients in Pl_r one by one into the encryption matrix $Cp_r(i, j)$.

(6) Put the remaining value in Pl_r into the corresponding $Cp_r(i, j)$, where $A_p(i, j) = 0$ and $p = 1, 2, \ldots, k$.

(7) Steps 3, 4, and 5 are used to confuse every independent Cp_r with the original GoL grid.

Step 3: Perform the one-level DWT transform from the block DCTs for a given JPEG image. The LL subband is scrambled based on GoL in Step 2.

Step 4: Scrambled content is diffused with the 8D chaotic map and SVD computing to enhance image security. With the 8D chaotic map, a chaotic sequences $RP^J_{M\times N} = \{rp^J_1, rp^J_2, \ldots, rp^J_{M\times N}\}$ is generated, and then we can get the sequences $CP^J_{M\times N} = \{cp^J_1, cp^J_2, \ldots, cp^J_{M\times N}\}$, where $cp_i = \text{ceiling}(fp_i)$. Arrange $CP^J_{M\times N} = \{cp^J_1, cp^J_2, \ldots, cp^J_{M\times N}\}$ into an $M \times N$ matrix CP^J. Perform SVD on CP^J, then, $CP^J = U_{CP} V_{CP} V^T_{CP}$.

Step 5: Diffuse each subband with orthonormal matrices U_{CPK} and V^T_{CPK}, as

$$I^{\mathrm{JWE}} = \begin{cases} U_{CP} I V^T_{CP}, & M \le N \\ V_{CP} I U^T_{CP}, & M > N \end{cases}$$

I^{JWE} is the encrypted and watermarked image I^{JWE}.

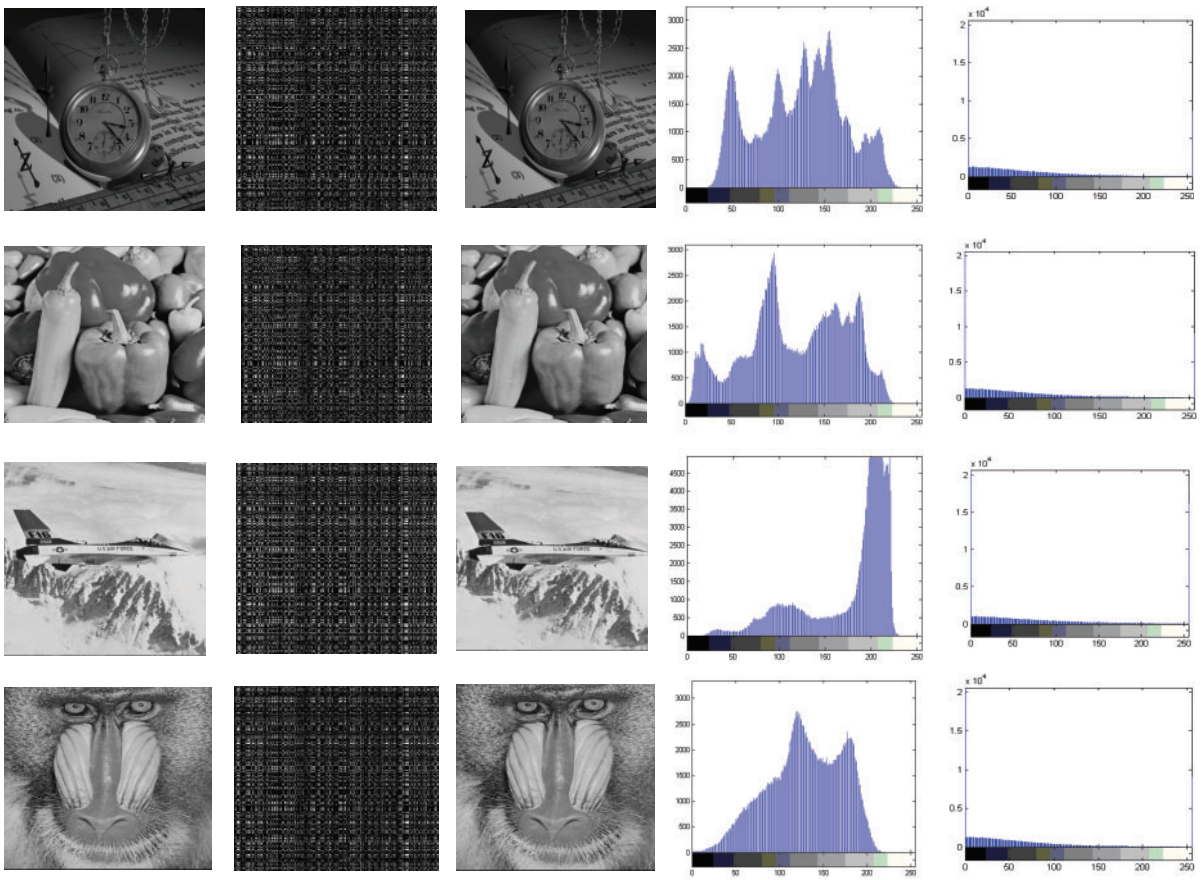
4 Experiment Results and Security Analysis

The experimental results and security analysis are demonstrated in this section. The proposed scheme runs with a MATLAB platform on an Intel(R) Core (TM) i5-10500 CPU and 16-GB RAM computer. To show the effectiveness of the proposed scheme, we used the very popular standard benchmarking gray images of size 512 × 512, "Peppers, Airplane, Fishing boat, Baboon, and Watch" to carry out the cryptanalyses. The encrypted images are exhibited in Fig. 4b. Fig. 4c shows the decrypted image with fingerprints. From the experimental results, according to those encrypted images in Fig. 4b, it is very difficult to get the original information.

4.1 Perceptual Effect

Generally, to get confidentiality for secure sharing, it should not perceive the original content from the encrypted object. The watermark information hidden in the images should not be perceived. The watermark embedding should not impact the visual quality. In the proposed encryption algorithm, the LL subband

is scrambled with Game of Life. After that, SVD is used to diffuse the permuted image. Fig. 4b shows the encrypted images. All encrypted images are unintelligible because of noise-like signals. Therefore, the proposed privacy protection method shows high perceptual security. Fig. 4b,c shows the encrypted and decrypted results, respectively. All encrypted images are not perceived. Their visual quality is extremely poor. According to Fig. 4b, the original information cannot be perceptible. Thus, the JWE method can ensure privacy protection.



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

Figure 4: Experimental results: (a) the original images; (b) the encrypted images; (c) decrypted and fingerprinted images; (d) the grey histogram of the original images; (e) the grey histogram of the encrypted images

4.2 Imperceptibility of Marks

To protect the multimedia content further after the encrypted content is decrypted. The fingerprint information is embedded when the image is decrypted. To preserve the visual quality of the original content, the fingerprint information hidden in the image should be imperceptible and perceptually undetectable. Related experimental results of decrypted fingerprinted images are shown in Fig. 4c. The visual quality of the watermarked images has not changed apparently. To have verification capability later, it should not perceive any watermark information from decrypted images. From Fig. 4c, it is apparent that the watermark cannot be perceived from the decrypted and watermarked images.

4.3 Resisting Exhaustive Attack

The keys used in the encryption process include: initial values x_1, x_2,..., x_8, and control parameters (ω_1, ω_2, ω_3, ω_4, ω_5, ω_6, ω_7). The total key space is about $10^{16\times15} = 10^{240}$. Therefore, with a large key space, the proposed encryption algorithm can resist the brute-force attack.

4.4 Statistical Attack Discussion

1) Histogram attack analysis

To evaluate the encryption effect, histogram attacks should be analyzed. A key part in the DWT domain is selected to encrypt a JPEG image. The histograms of the encrypted content should be different from their corresponding original content. Therefore, if all encrypted images have similar histograms, and all of them are significantly different from their corresponding original histograms, the algorithm is regarded as a good encryption method. Fig. 4d,e shows the original histograms and their corresponding encrypted histograms, respectively. Comparing Fig. 4d,e, it can be found that the encrypted histograms are remarkably similar, the original histograms are different from each other. On the other hand, those similar encrypted histograms are different from the original ones from Fig. 4d. Therefore, similar encrypted histograms make statistical attacks difficult. Histogram analysis shows the scheme can resist statistical attacks.

2) Correlation coefficient analysis

Image encryption algorithms should effectively resist statistical attacks based on correlation coefficient analysis. 3000 pairs (horizontal, vertical, and diagonal) of adjacent pixels were randomly selected from the image to analyze the correlation between these pixels before and after encryption. From Fig. 5 (left), the correlation coefficient of the Lena image is high before encryption, the adjacent correlation of the encrypted Lena image is decreased in Fig. 5 (right), which effectively destroys all the correlations of the original image.

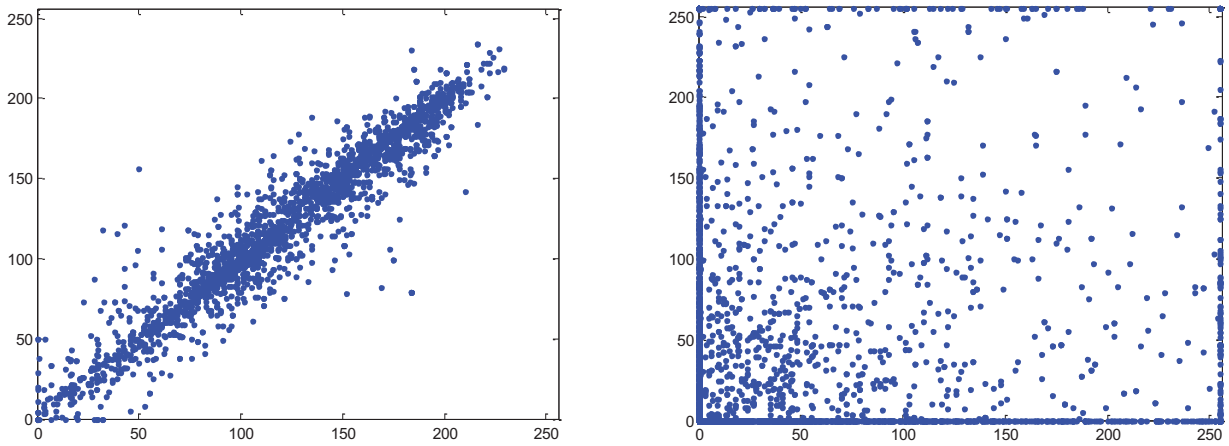


Figure 5: Correlation analysis: (left) original image; (right) encrypted image

4.5 The Encryption Process Analysis

The unintelligibility of images can be enhanced by the GoL scrambling operation. GoL permutation based on a single coefficient in the LL subband can achieve the effect of scrambling and diffusion. GoL permutation of a single coefficient will take 16 times as much as the running time of that GoL permutation of a 4×4 coefficient block. However, both GoL permutations can get similar unintelligibility of encrypted images in the DWT domain. Because the SVD diffusion matrices still protect the image, even if the permutation

operation based on GoL is cracked, the original image information will still not be leaked. The image encryption comparison is shown in Fig. 6. The SVD diffusion can enhance unintelligibility from Fig. 6e. Therefore, the proposed encrypted scheme with SVD computing can be applied in areas where confidentiality is in high demand; otherwise, only the GoL permutation method can meet the unintelligibility request. In the higher security level, both GoL permutation and SVD diffusion are applied. Even if the GoL permutation is cracked, a rough sketch of the original image will be revealed; the rough sketch makes the perceptual quality unacceptable at the higher security level.

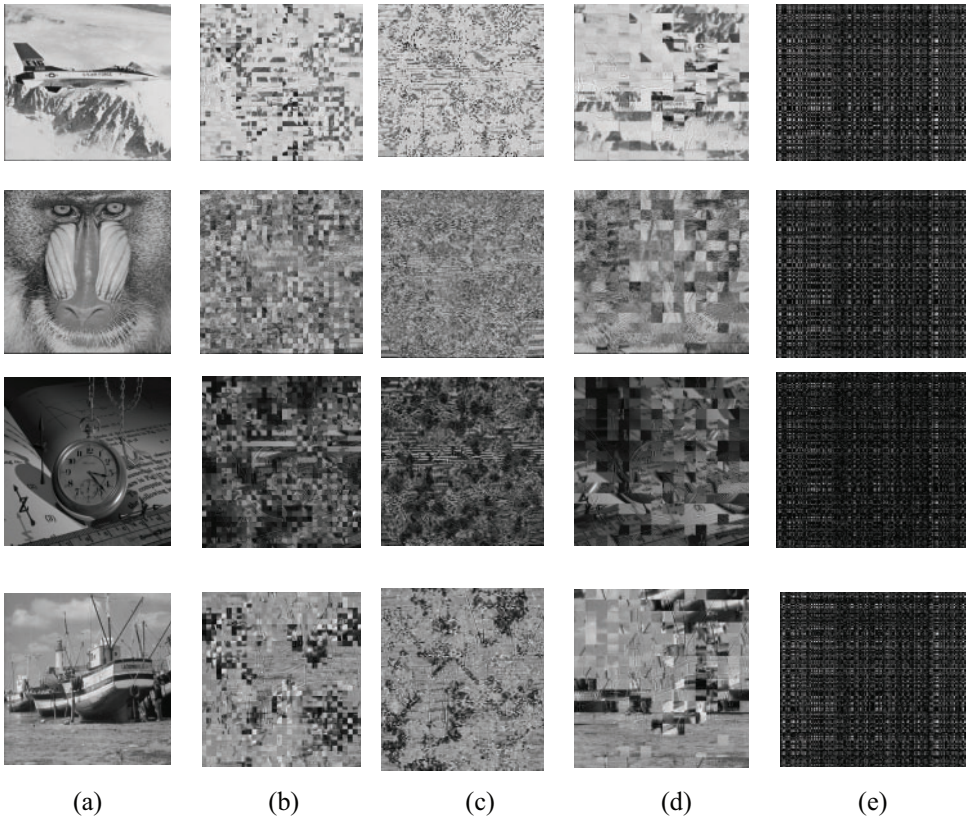


Figure 6: Comparison of encrypted images: (a) plaintext images; (b) images with 4 × 4 block permutation based on GoL for the LL2 subband; (c) images which are permuted based on GoL by single coefficient permutation in the LL subband; (d) images which are permuted by 4 × 4 block permutation based on GoL for LL subband; (e) 4 × 4 block permutation based on GoL in the LL2 subband and SVD diffusion

4.6 Analysis of Gaussian Noise Attack

Normalized correlation (NC) values and bit error ratio (BER) for extracting image watermarks are tested. Table 1 shows watermark extraction with different intensities of Gaussian noise added to the host image. Table 1 shows the host image with different intensities of Gaussian noise added, and how it affects the extracted image watermark. The image watermark is still clear after adding Gaussian noise with a mean of 0.01. Its normalized correlation coefficients are all above 0.78.

Table 1: Features of extracted watermarks under gaussian noise attack

Gaussian noise	Host image	Watermark	BER	NC
0.001	Airplane	Fishing boat	0.2324	0.7846
	Baboon		0.0648	0.8506
	Watch		0.2236	0.9312
0.005	Airplane	Fishing boat	0.2298	0.7849
	Baboon		0.0467	0.8591
	Watch		0.2634	0.8905
0.01	Airplane	Fishing boat	0.2137	0.7837
	Baboon		0.1267	0.8581
	Watch		0.2529	0.8978

4.7 Comparative Analysis of Encryption Efficiency

With the proposed joint watermarking and encryption scheme, important coefficients are chosen to encrypt. The proposed selective scheme encryption process is shown in Fig. 2. First, the LL subband is chosen to confuse. The encrypted results are shown in Fig. 6. The LL subband is chosen to encrypt. Here, the single coefficient is permutated in the LL subband. Only permutation in the LL subband can get unintelligible visual results. From Fig. 6, all permuted images are not perceptual.

The proposed JWE method is compared with some related research. The considered techniques include two encryption algorithms [41,42]. Their encryption algorithms have a high time complexity because of the full encryption. In addition, all security operations are performed in the spatial domain. It is inefficient to encrypt all pixels for image sharing in social multimedia platforms. Rostami et al.'s image encryption [41] consists of three steps. Firstly, a one-dimensional chaotic mapping is used to generate a chaotic matrix, and the image is divided into many blocks. Then, the values of the chaotic matrix are XORed with the values in each block. Secondly, use one-dimensional logical mapping to generate a pixel matrix that is equal in size to the length and width of the image, and shuffle the positions of the image pixels. Finally, generate a new chaotic matrix using the new initial values and perform an XOR operation with the blocks divided by the image.

Diaconu proposed a cyclic displacement and chaos encryption technique [42], which mainly consists of two steps. The first step is to convert the pixel values of the original image into an 8-bit binary array, count the number of 1s, and divide the count by 2 to find the remainder. If the remainder is 0, the binary array is cyclically shifted to the right by counting bits in the form of a linked list. If the remainder is 1, the binary array is cyclically shifted to the left by counting bits in the form of a linked list; The second step is to use logical mapping to generate two encryption matrices equal in size to the length and width of the image, and then perform two XOR operations with the pixel values of the three color components of the image to obtain the encrypted image.

The proposed JWE scheme can improve the performance problem through selective important content permutation and SVD diffusion. Wavelet decomposition makes all security operations perform in parallel. The permutation and diffusion process in parallel will be faster than the joint encryption/watermarking algorithm. In the proposed technique, SVD diffusion operation can meet higher security requests. SVD operation is also revertible, then the decryption will be fast.

In this subsection, the time efficiency is evaluated. For social image sharing, if a privacy protection algorithm has a higher time complexity, then the algorithm will not be considered a feasible scheme. The

encryption time is below 0.7 s. Therefore, the JWE scheme has a low time complexity, and it can provide privacy protection services to social platform users within strict time deadlines.

Encrypt 4 images of the same size using both the above methods and the method described in this article, and the resulting data is shown in Table 2. From the table, it can be seen that the entropy values of the proposed algorithm are lower than algorithms in [41] and [42]. From the perspective of time complexity analysis, the algorithm proposed in this article only takes 0.7 s to encrypt an image, while Rostami's algorithm requires 56 s for computation, and Diaconu's algorithm has a computation time of up to 192 s. By comparing and analyzing the above two parameters, the algorithm proposed in this paper is significantly superior to the other two encryption algorithms in run time.

Table 2: Comparison of the encryption algorithms

Image	Proposed		[41]		[42]	
	Entropy	Time (s)	Entropy	Time (s)	Entropy	Time (s)
Plane	6.85686331	0.5961	7.99972415	43.0971	7.99971570	158.6377
Baboon	6.72414890	0.6587	7.99972561	42.4773	7.99971582	158.9323
Watch	5.98332156	0.6432	7.99976891	42.1421	7.99978153	159.2884
Peppers	6.25747512	0.6928	7.99972315	47.3456	7.99976258	158.6079

4.8 Algorithms Comparison

The algorithm proposed by Anand et al. is to perform DWT transform on the host image, select its horizontal and vertical components for singular value decomposition, and then divide the image watermark into two equal parts multiplied by an incremental factor K and added to two singular value matrices. Then, the inverse transform is used to obtain the embedded watermark image [43].

The algorithm was used to embed and extract image watermarks for Plane, Baboon, and Watch. The data obtained is shown in Table 3. The algorithm exhibits good robustness in dealing with some attacks, which is better than the algorithm proposed in this paper. However, the algorithm's robustness in handling cropping attacks and noise attacks is not as good as the algorithm proposed in this paper. Both algorithms have their advantages, so different watermarking algorithms can be selected for embedding watermarks and fingerprints in different application fields.

Table 3: Comparison watermark NC value with Anand algorithm

Attack type	Proposed	[43]	Proposed	[43]	Proposed	[43]
	Plane		Baboon		Watch	
No attack	0.9995	0.9989	0.9978	0.9908	0.9969	0.9993
Upper left corner cropping (1/16)	0.9536	0.5523	0.8561	0.2912	0.9826	0.8965
Center cropping (1/16)	0.9851	0.3158	0.9128	0.1891	0.9759	−0.0217
Around cropping (1/8)	0.6752	−0.1561	0.9230	0.1726	0.9745	−0.3612
Salt & pepper (0.005)	0.8636	0.8028	0.8751	0.8327	0.9253	0.8938
Salt & pepper (0.01)	0.8123	0.7102	0.8631	0.6958	0.9189	0.7821
Salt & pepper (0.02)	0.7712	0.5123	0.8230	0.6128	0.9279	0.5587
Gaussian noise (0.001)	0.7905	0.6127	0.8504	0.5736	0.8398	0.4367

(Continued)

Table 3 (continued)

Attack type	Proposed	[43]	Proposed	[43]	Proposed	[43]
	Plane		Baboon		Watch	
Gaussian noise (0.005)	0.7821	0.6539	0.8602	0.6312	0.8968	0.5129
Gaussian noise (0.01)	0.7735	0.6678	0.8728	0.6218	0.8874	0.5357

Table 4 summarizes the roles of the proposed security method and some image security schemes such as hybrid watermarking and encryption technique in the fractional Fourier transform (FRFT) domain [44], image encryption scheme in [18], watermarking scheme in [45], and multi-layer security method in [43]. In Table 4, selective encryption means that only the important part, rather than the whole content, is encrypted.

Table 4: Comparisons of the related schemes

	Proposed	[18]	[44]	[45]	[43]
Watermarking	Yes	No	Yes	Yes	Yes
Selective encryption	Yes	No	No	No	No
Tracing	Yes	No	Yes	Yes	Yes
Scalability	Yes	No	No	No	No
Communication security	Yes	Yes	No	No	Yes
Watermark domain	DWT	No	FRFT	DWT&DCT	DWT
Compressed domain	Yes	No	No	No	No
Block DCTs to DWT	Yes	No	No	No	No
Encryption domain	DWT	Spatial	No	No	Spatial
Encryption scheme	GoL&SVD	Chaos	No	No	Chaos

As the existing image security schemes only provide part security protection, a highly comprehensive security measure is not guaranteed. These schemes are not scalable, and their encryption is performed in the spatial domain to protect uncompressed spatial domain images. As we all know, compressed multimedia such as JPEG images is the main medium on social multimedia platforms. Uncompressed multimedia content sharing on social multimedia platforms will bring about multimedia big data issues. Social multimedia platforms will suffer heavy computational and communication burdens in the case of numerous uncompressed images. For a secure social image-sharing method, the scheme should be sensitive to scalability so that the fingerprinted content can be protected according to the security requirements. This can be achieved by introducing scalable joint encryption and fingerprinting for social JPEG images. Most importantly, the proposed fast transformation from block DCTs to DWT can not only protect JPEG images in the compressed domain but also improve the performance of the proposed security algorithm.

5 Conclusion

The JWE algorithm is proposed for JPEG image sharing in multimedia social platforms to focus on the privacy problem. With the JWE method, full decoding of JPEG images can be avoided through DWT from block DCTs. This fast transformation can save running time for some secure operations. The encryption includes selective GoL permutation and further diffusion with SVD computing. Selective permutation,

which can meet fast requests in multimedia social platforms, encrypts important parts. The research will help the development of related areas such as secure multimedia storage systems and multimedia communication. Related analysis shows that the proposed scheme can not only resist brute-force attacks and histogram attacks but also owns visual security. Furthermore, because only the important parts are chosen to encrypt, it has a lower time complexity than those encryption schemes in the spatial domain. Finally, the time efficiency of the JWE scheme is desirable, so it is a suitable candidate technology for privacy protection in multimedia social platforms.

In the future, the authors will research new challenges of social JPEG image distribution. The main research direction will be secure content sharing to avoid the effects of multimedia big data.

Acknowledgement: The editors and anonymous referees whose comments and recommendations have helped to improve this work are appreciated by the authors. The authors would like to express their gratitude for the guidance and support provided by the research group.

Funding Statement: This related work is funded by NSFC Grants 61502154, 61972136, the NSF of Hubei Province (2023AFB004, 2024AFB544), Hubei Provincial Department of Education Project (No. Q20232206), and Project of Hubei University of Economics (No. T201410).

Author Contributions: The following contributions to the work are confirmed by the authors: study conception and design: Conghuan Ye, Bing Xiong; gathering of data: Shenglong Tan, Qiankun Zuo; analysis and interpretation of results: Shi Li, Jun Wang; draft manuscript preparation: Conghuan Ye, Shenglong Tan, Shi Li, Jun Wang, Qiankun Zuo, Bing Xiong. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data is included in the paper.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Liz-López H, Keita M, Taleb-Ahmed A, Hadid A, Huertas-Tato J, Camacho D. Generation and detection of manipulated multimodal audiovisual content: advances, trends and open challenges. Inf Fusion. 2024;103:102103. doi:10.1016/j.inffus.2023.102103.
2. Meng B, Yuan X, Zhang Q, Lam C-T, Huang G. Encryption-then-embedding-based hybrid data hiding scheme for medical images. J King Saud Univ-Comput Inf Sci. 2024;36(1):101932. doi:10.1016/j.jksuci.2024.101932.
3. Lai Q, Hua HQ. Secure medical image encryption scheme for Healthcare IoT using novel hyperchaotic map and DNA cubes. Expert Syst Appl. 2025;264:125854. doi:10.1016/j.eswa.2024.125854.
4. Yao M, Chen Z, Deng HW, Wu XM, Liu TZ, Cao C. A color image compression and encryption algorithm combining compressed sensing, Sudoku matrix, and hyperchaotic map. Nonlinear Dyn. 2025;113(3):2831–65. doi:10.1007/s11071-024-10334-2.
5. Chen J, Xue J, Wang Y, Huang L, Baker T, Zhou Z. Privacy-preserving and traceable federated learning for data sharing in industrial IoT applications. Expert Syst Appl. 2023;213:119036. doi:10.1016/j.eswa.2022.119036.
6. Wang MJ, Zou Y, Li ZJ. A memristive Ikeda map and its application in image encryption. Chaos Soliton Fract. 2025;190:115740. doi:10.1016/j.chaos.2024.115740.
7. Wu ZH, Zhang YX, Bao H, Lan RS. Hua ZY: ND-CS: a circularly shifting chaotic map generation method. Chaos Soliton Fract. 2024;181:114650. doi:10.1016/j.chaos.2024.114650.
8. Hua ZY, Yao JH, Zhang YX, Bao H, Yi S. Two-dimensional coupled complex chaotic map. IEEE Trans Ind Inform. 2024; 1–11. doi:10.1109/TII.2024.3431085.
9. Yu F, Lin Y, Yao W, Cai S, Lin H, Li Y. Multiscroll hopfield neural network with extreme multistability and its application in video encryption for IIoT. Neural Netw. 2025;182:106904. doi:10.1016/j.neunet.2024.106904.

10. SaberiKamarposhti M, Ghorbani A, Yadollahi M. A comprehensive survey on image encryption: taxonomy, challenges, and future directions. Chao Soliton Fract. 2024;178:114361. doi:10.1016/j.chaos.2023.114361.
11. Kocak O, Erkan U, Toktas A, Gao S. PSO-based image encryption scheme using modular integrated logistic exponential map. Expert Syst Appl. 2024;237:121452. doi:10.1016/j.eswa.2023.121452.
12. Toktas F, Erkan U, Yetgin Z. Cross-channel color image encryption through 2D hyperchaotic hybrid map of optimization test functions. Expert Syst Appl. 2024;249:123583. doi:10.1016/j.eswa.2024.123583.
13. Feng W, Zhang J, Chen Y, Qin ZT, Zhang YS, Ahmad M, et al. Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. Expert Syst Appl. 2024;246:123190. doi:10.1016/j.eswa.2024.123190.
14. Huang YH, Zhang QL, Zhao YB. Color image encryption algorithm based on hybrid chaos and layered strategies. J Inf Secur Appl. 2025;89:103921. doi:10.1016/j.jisa.2024.103921.
15. Wang SF, Pan JG, Cui YR, Chen ZJ, Zhan W. Fast color image encryption algorithm based on DNA coding and multi-chaotic systems. Mathematics. 2024;12(20):3297. doi:10.3390/math12203297.
16. Feng W, Yang J, Zhao X, Qin Z, Zhang J, Zhu Z, et al. A novel multi-channel image encryption algorithm leveraging pixel reorganization and hyperchaotic maps. Mathematics. 2024;12(24):3917. doi:10.3390/math12243917.
17. Bencherqui A, Tahiri MA, Karmouni H, Alfidi M, Motahhir S, Abouhawwash M, et al. Optimal algorithm for color medical encryption and compression images based on DNA coding and a hyperchaotic system in the moments. Eng Sci Technol, Int J. 2024;50:101612. doi:10.1016/j.jestch.2023.101612.
18. Wang MX, Teng L, Zhou WJ, Yan XP, Xia ZQ, Zhou S. A new 2D cross hyperchaotic Sine-modulation-Logistic map and its application in bit-level image encryption. Expert Syst Appl. 2025;261:125328. doi:10.1016/j.eswa.2024.125328.
19. Yan XP, Hu Q, Teng L, Su YN. Unmanned ship image encryption method based on a new four-wing three-dimensional chaotic system and compressed sensing. Chao Soliton Fract. 2024;185:115146. doi:10.1016/j.chaos.2024.115146.
20. Zhang ZY, Cao YH, Zhou NR, Xu XY, Mou J. Novel discrete initial-boosted Tabu learning neuron: dynamical analysis, DSP implementation, and batch medical image encryption. Appl Intell. 2025;55(1):61. doi:10.1007/s10489-024-05918-9.
21. Teng L, Du LB, Leng ZY, Wang XL. Chaotic image encryption based on partial face recognition and DNA diffusion. Appl Intell. 2024;54(21):10360–73. doi:10.1007/s10489-024-05613-9.
22. Adesina AO, Ayobioloja PS, Obagbuwa IC, Odule TJ, Afolorunso AA, Ajagbe SA. An improved text-based and image-based CAPTCHA based on solving and response time. Comput Mater Contin. 2023;74(2):2661–75. doi:10.32604/cmc.2023.031245.
23. Tan T, Zhang L, Zhang M, Wang S, Wang L, Zhang Z, et al. Commutative encryption and watermarking algorithm based on compound chaotic systems and zero-watermarking for vector map. Comput Geosci. 2024;184:105530. doi:10.1016/j.cageo.2024.105530.
24. Guan Q, Deng H, Liang W, Zhong X, Ma M. Multi-images encryption and watermarking with small number of keys via computational ghost imaging. Optics Laser Technol. 2024;168:109957. doi:10.1016/j.optlastec.2023.109957.
25. Wang LN, Zhou NR, Sun B, Cao YH, Mou J. Novel self-embedding holographic watermarking image encryption protection scheme. Chin Phys B. 2024;33(5):050501. doi:10.1088/1674-1056/ad1c5b.
26. Singh HK, Baranwal N, Singh KN, Singh AK, Zhou H. GAN-based watermarking for encrypted images in healthcare scenarios. Neurocomputing. 2023;560:126853. doi:10.1016/j.neucom.2023.126853.
27. Emmanuel Oluwatobi Asani MG-D, Ajagbe SA, Falola PB, Adeniyi EA, Adigun MO. Triple watermarking scheme for digital images. J Hunan Univ Nat Sci. 2023;50(10):10.
28. He X, Li L, Tong F, Peng H. Multi-level privacy protection for social media based on 2D compressive sensing. IEEE Internet Things J. 2023;11(4):6878–92. doi:10.1109/JIOT.2023.3313812.
29. Bayat-Sarmadi S, Mozaffari-Kermani M, Reyhani-Masoleh A. Efficient and concurrent reliable realization of the secure cryptographic SHA-3 algorithm. IEEE Trans Comput Aided Des Integr Circuits Syst. 2014;33(7):1105–9. doi:10.1109/TCAD.2014.2307002.
30. Wolfram S. A new kind of science. USA: Wolfram Media; 2002.

31. Wolfram S. Theory and applications of cellular automata. 1986 [cited 2024 Dec 20]. https://www.amazon.com/Applications-Cellular-Automata-INCLUDING-1983-1986/dp/9971501236.
32. Adamatzky A. Game of life cellular automata. London: Springer; 2010.
33. Shen H, Cheng X, Cai K, Hu MB. Detect overlapping and hierarchical community structure in networks. Physica A. 2009;388(8):1706–12. doi:10.1016/j.physa.2008.12.021.
34. Boneh D, Shaw J. Collusion-secure fingerprinting for digital data. IEEE Trans Inf Theory. 1998;44(5):1897–905. doi:10.1109/18.705568.
35. Tardos G. Optimal probabilistic fingerprint codes. J ACM. 2008;55(2):1–24. doi:10.1145/1346330.1346335.
36. Ye C, Ling H, Zou F, Lu Z. A new fingerprinting scheme using social network analysis for majority attack. Telecommun Syst. 2013;54(3):315–31. doi:10.1007/s11235-013-9736-8.
37. Davis BJ, Nawab SH. The relationship of transform coefficients for differing transforms and/or differing subblock sizes. IEEE Trans Signal Process. 2004;52(5):1458–61. doi:10.1109/TSP.2004.826165.
38. Wang L, Ling H, Zou F, Lu Z. Real-time compressed-domain video watermarking resistance to geometric distortions. IEEE Multimed. 2012;19(1):70–9. doi:10.1109/MMUL.2011.76.
39. Kundur D, Karthik K. Video fingerprinting and encryption principles for digital rights management. Proc IEEE. 2004;92(6):918–32. doi:10.1109/jproc.2004.827356.
40. Wolfram S. Gad-el-Hak M: a new kind of science. Appl Mech Rev. 2003;56:B18. doi:10.1115/1.1553433.
41. Rostami MJ, Shahba A, Saryazdi S, Nezamabadi-pour H. A novel parallel image encryption with chaotic windows based on logistic map. Comput Electr Eng. 2017;62:384–400. doi:10.1016/j.compeleceng.2017.04.004.
42. Diaconu AV. Circular inter-intra pixels bit-level permutation and chaos-based image encryption. Inf Sci. 2016;355:314–27. doi:10.1016/j.ins.2015.10.027.
43. Anand A, Singh AK. An improved DWT-SVD domain watermarking for medical information security. Comput Commun. 2020;152:72–80. doi:10.1016/j.comcom.2020.01.038.
44. Liu SX, Yu NN, Xi SX, Ji XX, Yuan H, Wang XL, et al. Hybrid watermarking and encryption techniques for securing three-dimensional information. Phys Scr. 2024;99(5):055543. doi:10.1088/1402-4896/ad3bef.
45. Nawaz SA, Li JB, Bhatti UA, Shoukat MU, Li DK, Raza MA. Hybrid watermarking algorithm for medical images based on digital transformation and MobileNetV2. Inf Sci. 2024;653:11981. doi:10.1016/j.ins.2023.119810.