Joint Fingerprinting and Encryption for JPEG Images Sharing in Mobile Social Network

Conghuan Ye, Zenggang Xiong, Yaoming Ding, Guangwei Wang, Xuemin Zhang, Fang Xu
College of Computer and Information Science
Hubei Engineering University
Xiaogan, China
ychzzw@163.com

***Abstract*: The advent of mobile social network and smartphone has made social multimedia sharing in social network easier and more efficient. However, it can also cause serious security and privacy problems, secure social multimedia sharing and traitor tracing issues have become critical and urgent. In this paper, we propose a joint fingerprinting and encryption (JFE) scheme based on Game of Life (GL) and singular value decomposition (SVD) with the purpose of protecting JPEG images sharing in mobile social networks. Firstly, the fingerprint code is produced using social network analysis. After that, a fast inter-transformation from block DCTs to DWT is employed. Then, fingerprints are embedded into the LL, HL and LH subbands. At last, GL and SVD are used to for confusion and diffusion respectively. The proposed method, to the best of our knowledge, is the first JFE method using GL and SVD in the JPEG compressed domain for security and privacy in JPEG images sharing. The use of fingerprinting along with encryption can provide a double-layer of protection to JPEG images sharing in social network. Theory analysis and experimental results show the effectiveness of the proposed JFE scheme. Most importantly, the performance of inter-transformation between block DCT and one-level DWT has a profound effect on lowering computational cost in our proposed JFE scheme. In the end, our JFE method can secure JPEG images sharing in social networks and meet the real-time requirement.**

Keywords: security and privacy; joint fingerprinting and encryption; multimedia encryption; social multimedia sharing;

I. INTRODUCTION

The advent of mobile social network, cloud computing, and smartphone makes social multimedia sharing become pervasive in our daily lives. A group of users, geographically distributed, share the same social multimedia content-images, video, and audio with their mobile devices in a social networking community. The growth of social multimedia, user-generated, transmitted, consumed or shared in social network[1], underscores potential risks for the unethical use with the emergence of mobile devices such as smartphones. Social multimedia distribution within social network raises distinctive challenges such as privacy and security issues. Preserving privacy in publishing social multimedia becomes an important concern to prevent illegal use of social multimedia.

However, secure social multimedia sharing is still in its infancy and high dependent on both confidentiality and redistribution tracing, therefore, techniques, such as fingerprinting and encryption [2], need to be carried out. For the purpose of confidentiality of social multimedia sharing, cryptography techniques transform multimedia content into an enciphered, unintelligible form, that keep the encrypted content from illegal access difficult during the distribution processes without the decryption key. In order to achieve such type of security, employing chaotic systems with the properties of initial-value sensitivity and parameter sensitivity in generating the encryption keys has become one of the important topics in secure multimedia communication. Its main advantage lies in the observation that a chaotic signal looks like noise for non-authorized users ignoring the mechanism for generating it. Only the authorized customer who has the correct key can recover the data successfully [3].

A variety of chaos-based image encryption schemes have been proposed [4-6]. These proposed schemes reduce the risk of sensitive content being revealed by one other than the intended recipient. However, these schemes only focus on encrypting. Once users receive and decrypt the data, the content could be copied and delivered to an unauthorized user at their option. There are not ways to continue the work of protecting the multimedia content, therefore the privacy may still be leaked. In this case, extra protection schemes should be adopted to deter content redistribution. Digital fingerprinting, in which a user specific identification mark is embedded into a copy of original content, is a useful tool to trace redistributed content. Although encryption and fingerprinting are used to protect multimedia separately, there are some works[7, 8] used both techniques for the secure sharing of multimedia content. The need to apply both fingerprinting and encryption to digital images keeps rising in recent years [9-11].

However, these existing approaches seem not desirable to be applied to mobile multimedia content encryption because their encryption and decryption procedure in non-compressed domains makes the distribution of content will be very slow for large volume of multimedia data and do not meet the real-time constraint of social multimedia sharing in resources-constrained mobile social network environment. Apart from billions of camera exists, there are billions of smartphones which are being used in the world and majority of them are equipped with camera. If every smartphone clicks only one image per day then what is the volume of images and what amount of network bandwidth required to deliver these images within mobile social network environment is not tough to

DOI reference number: 10.18293/DMS2015-029

imagine. To save computation overhead and transmission bandwidth, compression is a must for image processing and distribution, especially in resource limited environments [12].

Digital watermarking is not new for the multimedia protection but fingerprinting for the compressed encrypted images is relatively new and appealing. To save space, a large volume of data is being kept in the compressed format. For the various reasons, there is a great issue of security protection for these compressed images. Growth of compressed image has magnified the need for more advanced encryption and fingerprinting techniques. [13].

In fact, there are some problems about the existing joint fingerprinting and encryption schemes. First, most existing schemes are not focus on the compressed content. As a result, there are huge volume of multimedia content has to be distributed. Second, there is no scalability in some existing schemes when they are used in secure content sharing in mobile social network environment. Then, the processing speed about encryption and fingerprinting may be a bottleneck when dealing with social multimedia data in social network for both central servers and resources-constrained devices, such as smartphone. At last, the distribution method will cost a lot of resources, especially network bandwidth.

In this article, we mainly focuses on the problem of privacy leakage, the illegal duplication and redistribution of social multimedia content in resources-constrained mobile social network environment. We are trying to deal with the issues of security and privacy in JPEG images sharing in mobile social network environment. We also are trying to address new future challenges of JFE (joint fingerprinting and encryption) in the area of JPEG images sharing. we present a novel JFE method using SNA (social network analysis) to deal with the issues of JPEG images sharing. Firstly, we describe a method for fingerprint code produced by dendrogram of hierarchical and overlapping structure of social network. Then, we propose a JFE method based on GL (Game of Life) and SVD in the DWT domain directly from the JPEG content. By using our technique, one is well able to design a privacy-preserving and secure social multimedia sharing in resources-constrained mobile social network environment.

According to our best knowledge, there has been no report yet on the implantation of JFE scheme based on GL and SVD using social network analysis for secure social multimedia sharing in resources-constrained mobile social network environment. The remainder of this paper is organized as follows. Related works are introduced in Section 2. In Section 3, techniques used in this paper will be introduced. Section 4 details the proposed JFE scheme based on GL and SVD. Then, the experimental results will be given in Section 5. Finally, conclusions are drawn in Section 6.

II. Related works

There have been some related works on access control to content security [14-16]. Commutative encryption and watermarking (CEW) could be used for providing more comprehensive security protection for multimedia content. D. Bouslimi et al. proposed a joint encryption and watermarking algorithm in [17]. The convergence of the two technologies is now facilitating privacy and security studies [18]. Two robust watermarking algorithms were proposed to watermark compressed JPEG images in encrypted domain [19] and JPEG2000 compressed and encrypted images [20] respectively. Kundur and Karthik [21] proposed a novel architecture for joint fingerprinting and decryption (JFD) that holds promise for a better compromise between practicality and security. Another joint fingerprinting and decryption (JFD) scheme based on vector quantization is proposed with the purpose of protecting media distribution [22].

However, all the above schemes did not be applied to JPEG images sharing in resources-constrained mobile social network environment. In view of the increasingly important role played by digital imaging in mobile multimedia social network with the emergence of smartphone, it is necessary for large amount of image data to be economically stored and/or transmitted. In these cases, the fingerprinting and encryption should be implemented in the compressed content to avoid the process of fully decoding and encoding. In social networks, practical multimedia contents are stored and transmitted in compressed JPEG format. Understanding the inherent characteristics of JPEG may play a useful role in digital image forensics[23]. As the perceptual information concentrates at low-frequency DCT coefficients, this leads to the research on selective encryption for JPEG images[24]. Lian proposed to encrypt the DC coefficient and the sign bit of all AC coefficients using a spatiotemporal chaotic system [25]. However, Wu and Kuo [26] stated that selective encryption is not suitable for DCT-based compression algorithms because some perceptual attacks were able to restore a perceptual image. The encrypted data is not secure in visual perception since the encryption of signs of DCT coefficients cannot fully scramble the original data.

In addition, the traditional fingerprinting methods do not consider the relationship between users in social network; then they cannot be applied to secure sharing in social network. How to use SNA to embed fingerprint information in encrypted contents and how to make the content sharing system robust against attacks is not deeply considered. In order to address social multimedia sharing, the authors proposed a secure content sharing method in the TSH transform domain in [27] through mapping the community structure of social network into the tree structure wavelet transform. With the different wavelet bases and decomposition levels, the DWT can extract different kinds of information from the media, and is therefore very likely to map community structure of social network into the tree structure of DWT, which can be used to joint fingerprinting and encryption. To encrypt the important content only, DWT domain algorithm can improve the encryption speed.

III. Basic theory

A. SVD

SVD is a very useful tool in linear algebra, which is a factorization and approximation technique. From the perspective of image processing, an image can be viewed as a matrix with non negative scalar entries. Mathematically, SVD of a rectangular matrix A is expressed as

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

where S is also known as singular value matrix in SVD domain, U and V are the unitary matrices. Both of U and V components are composed of eigenvectors of matrix A , and T represents the conjugate transpose operation. U and V are also orthogonal matrices. Therefore, the following conditions are always satisfied

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

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

where I_N and I_M are identity matrices with size $N \times N$ and $M \times M$, respectively.

B. Chaotic maps

The Logistic Map is a well-known continuous dynamical system. A 1D Logistic map is described as follows:

$$x_{n+1} = ux_n(1 - x_n) \tag{4}$$

where u ∈ [0,4], x_n ∈ (0,1), n=0,1,2,…. The research result shows that the system is in a chaotic state under the condition that 3.56994<u≤4. This Logistic Map generates continuous values between [0, 1], which are discretized (binaries) in order to fulfill the initial CA to later encryption. The piecewise linear chaotic map (PWLCM) can be described in Eq. (5):

$$y_{n+1} = F(y_n, \eta) = \begin{cases} y_n / \eta, & 0 \le y_n < \eta \\ (y_n - \eta)/(0.5 - \eta), & \eta \le y_n < 0.5 \\ 0, & y_n = 0.5 \\ F(1 - y_n, \eta), & 0.5 \le y_n < 1 \end{cases} \tag{5}$$

where y_n ∈ (0, 1), n=0, 1, 2, …. When control parameter η ∈ (0, 0.5), Eq. (2) evolves into a chaotic state, and η can serve as a secret key.

C. MD5

A cryptographic hash function is designed to ensure message integrity. MD5 takes a sequence of data as input and output a 128-bit "fingerprint" or "message digest" of the input. A MD5 hash is typically expressed as a 32 digit hexadecimal number. The MD5 hash function is one way, even if there is only a tiny bit change between two input sequences, the returned MD5 hash value will be totally different. It takes a message with a variable-length and returns a fixed-length output of 128 bits. As MD5 is fast and sensitive to the input message, it is employed in our JFE scheme to partially determine the control parameter and the initial condition of a chaotic tent map. A small change in the given fingerprints affects the control parameter and the initial condition of the chaotic map. As a result, the change will effectively spread to the whole cipher-image.

D. CA (Cellular Automata)

CA [28] is a dynamical complex space and time discrete system. GL (Game of Life) is governed by its local rules and by its immediate neighbors, which specifies how CA evolves in time. In general, the state of a cell at the next generation depends on its own state and the sum of the neighbor cells. In (2-D) CA, Moore neighborhoods method is used [29]. The Moore neighborhood of range L is defined by

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

At every time step, all the cells update their states synchronously by applying rules (transition function). Each cell computes its new state by applying the following transition rules.

(1) Any live cell with fewer than two live neighbors dies.
(2) Any live cell with two or three live neighbors lives on to the next generation.
(3) Any live cell with more than three live neighbors dies, as if by overcrowding.
(4) Any dead cell with exactly three live neighbors becomes a live cell, as if by reproduction.

For binary cells $c_1, c_2, \ldots, c_9$, we say that the transition function, at any time t, for GL rule [30] is of the form:

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

IV. THE PROPOSED JFE ALGORITHM

Notations

For ease of reference, important notations used throughout the paper are listed below.

N_u	the number of users
X^O	the robust coefficients vector for the outer code
X^I	the robust coefficients vector for the inner code
L^O	the length of the outer code
L^I	the length of the inner code
X_*	the half of original fingerprint vector

Sum_*	the sum of half fingerprint vector
d_k	the dither sequence
Y_k	the fingerprinted coefficients vector
G^0	the initial two-dimensional grids of cells
Pl_r	the input image patch;
Cp_r	the output scrambled matrix patches
A_i	the GL matrix
I^{JFE}	the encrypted and fingerprinted image

A. Fingerprint Encoding Using Social network analysis

We try to use method in [31] to get the overlapping and hierarchical structure of social network for fingerprint encoding. As shown in Fig.1, users are placed into c communities. These communities are encoded by outer code that is constructed by BS code [32], and the users in each community are encoded by the inner code produced with Tardos scheme [33]. Therefore, Fingerprint code for N_u users can be concatenated by a multilevel outer code for communities and an inner Tardo code for users in the communities, which is detailed in our previous work [34].

B. DWT from DCT directley

DCT is adopted in the JPEG compression standard [9]. The image is first divided in 8x8 blocks and each of these is transformed with the DCT. DCTs convert data from the spatial domain into the frequency domain. The transformed blocks are quantized with a uniform scalar quantizer, zig-zag scanned and entropy coded with variable length coding (VLC)，this mode is simply regarded as Joint Photographic Experts Group (JPEG). The block-based segmentation of the source image is fundamental limitation of the DCT-based compression system. The JPEG compression methods actually gained widespread acceptance as image compression methods. Most compressed multimedia contents in social network are stored as block DCT coefficients and motion vectors. The compressed JPEG images are partially decoded to obtain block DCT coefficients which are subsequently used to construct one-level DWT.

To lower the computational complexity, we use a fast inter transformation between one-level DWT and block DCTs. Compared with DCT, the wavelet transform is closer to the human visual system (HVS) because it splits the input image into several statistically frequency bands that can be processed independently. DWT also causes fewer visual artifacts than DCT because the wavelet transform does not decompose the image into blocks for processing. In the DWT transform, an image is split into one approximation (also called LL subband) and three details in horizontal, vertical, and diagonal directions which are named (or coefficients in LH subband), (coefficients in HL subband), and (coefficients in HH subband). The LL subband is then itself split into a second-level approximation and details, and the process is repeated.

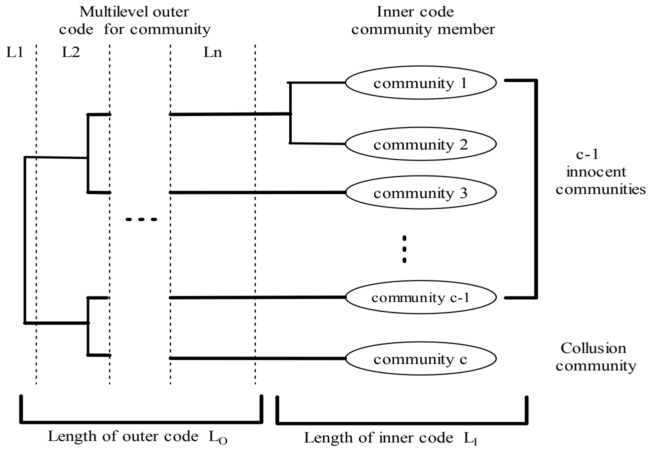

Multilevel outer code for community
Inner code community member
L1
L2
Ln
community 1
community 2
community 3
community c-1
community c
c-1 innocent communities
Collusion community
Length of outer code L_O
Length of inner code L_I

Figure 1. Fingerprint coding using social network analysis

Obtaining one-level DWT of JPEG compressed images is time consuming using existing methods, which first decompress the block DCTs of images into pixel data and then perform DWT on the data. In fact, both DCT and DWT are linear and invertible transforms, and a linear relationship exists between block DCT coefficients and its DWT coefficients [35]. Our JFE method can directly obtain the JPEG image's one-level DWT coefficients for fingerprinting and encryption in the DWT domain from the block DCT coefficients without involving inverse DCT (IDCT) to maintain low computational cost. Because the consumed time of IDCT and that of DCT occupy prodigious proportions of that of full decoding and encoding, respectively [36]. These approaches are inefficient because a large amount of time is spent on the inter-conversion between the DCT coefficients and spatial pixel data. Hence, the fast direct conversion between the block DCTs and one-level DWT coefficients, which will prevent full decoding and encoding, is indispensable for resource-constrained mobile social network environment.

Let's consider an image (or a frame) I with a size of $(L\times S)\times(K\times S)$. We can divided this image into $L\times K$ blocks, which are denoted as BL_{ij} with a size of $S\times S$. $C_{ij}(u,v)$ representing the DCT coefficients of blocks can be expressed 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 $u,v=1,2,...,S,\ \alpha(u),\alpha(v)=\begin{cases}1/\sqrt{2}, u=0\ or\ \ v=0\\ 1, \qquad else\end{cases}$.

According to Eq.(8), the 2D DCT transform of Sb_{ij} can be rewritten and represented in matrix formats $C_{ij}(u,v)=B_1\times BL_{ij}\times B_1^T$ The inverse transform of it can be expressed as $BL_{ij}=B_1^{-1}\times C_{ij}\times(B_1^T)^{-1}$,where B_1 and B_1^T are orthogonal matrix of the block DCT. So the whole image can be expressed as

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

The three matrices on the right of Eq.(9) are denoted as B_4, C_{part} and B_5, respectively. We can also compute the one-level DWT coefficients of image I. Here, the DWT will be taken using the haar wavelet, which is the simplest possible wavelet. It is both separable and symmetric and can be expressed in matrix form

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

For the Haar wavelet transform, H contains the Haar basis functions, $h_z(k)$. They are defined over the continuous, closed interval $z \in [0,1]$. Then the Haar basis functions are $h_0(z) = h_{00}(z) = \frac{1}{\sqrt{LS}}, z \in [0,1]$.

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

The inverse Haar wavelet transform can be expressed as $I = H^T \times KR \times Q$. Then, we obtain coefficient matrix KR in DWT domain using this expression:

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

where $A_1 = H \times B_4$, $A_2 = B_5 \times Q^T$. This may contributes to reduce computational cost. Through the inverse transformation in Eq.(13), we can directly obtain the set of block DCT coefficients from the DWT coefficient matrix using:

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

In the DWT transform [37], an image is split into *LL*, *LH*, *HL*, and *HH* subband. In this paper, we transform middle-frequency subbands repeatedly. For a given code scheme, we define the splitting scheme for multi-level DWT through social network analysis. For example, in Fig.1, the number of the layers of community structure is $n+1$, then the number of the layers of outer code is n, and the LH and HL subbands for community code embedding will be split into n levels according to Fig.1.

C. The JFE process

The architecture of JFE scheme based on DWT and chaotic CA is designed and shown in Fig.2. The JFE process is composed of two processes: fingerprinting and encryption.

1) Fingerprint embedding

To simplify the description of embedding method, we only discuss embedding of a unique fingerprint using an improved QIM scheme. Suppose N_u is a set of users. We choose coefficients in all LH-level and HL-level subbands to create a vector, $X^O = (x_1, x_2, ..., x_{L^O})$ of host signals to embed outer code, and choose another robust coefficients sequence in LL subband to create a vector, $X^I = (x_1, x_2, ..., x_{L^I})$. The outer code hiding scheme is described in Eq. (14), to hide fingerprint codeword. The hiding scheme is as follow:

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

Where x_j is a vector which represents the host signal with length L^O, i, j = *1*, … , L^O, round is an operation of *Floor and Ceiling*, and Δ is a constant.

In this case, to identify the embedded fingerprint, the multimedia producer needs to obtain the fingerprinted coefficients, which compose a vector *z*. By deducting, the difference is as follow:

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

Here, the least T_k, which is related to user k, determines who the traitor is.

2) Encryption algorithm

Digital media contents like image and video are tightly related to visual quality. Generally, social multimedia encryption algorithms should be not only secure against cryptographic attacks but also secure in human perception. The more degraded their visual quality is, the higher the security is.

In this paper, we focus on JPEG images in mobile social network, so the encrypted output must ideally "appear" random to make estimation of the original image from the encrypted one computationally difficult without access to the decryption key ; traditional multimedia content encryption algorithms are considered computationally infeasible for high volumes of multimedia content in resources-constrained devices or for near real-time or massively parallel distribution of multimedia content flows [38].

The traditional solution applies a encryption algorithm on the compressed image in JPEG format, with which the total processing time will be longer. In order to overcome some limitations, we propose the notion of partial encryption, in which a smaller subset of the important content in the DWT domain is encrypted to lower computation and delay while integrating the fingerprinting with encryption. CA (Cellular automata) is capable of developing chaotic behavior using simple operations or rules offering the benefit of high speed computation, which makes CA an interesting platform for digital image scrambling [39]. CA capable of exhibiting chaos is attractive in cryptography because it is possible to have a great number of possible keys in the keyspace. Fast computation helps in achieving this capability. We are interested to use chaotic CAs in order to take advantage for fast cryptography. SVD performs an optimal matrix decomposition in a least-square domain for matrices in real number domain.

Permutation-only type image cipher is superior in the aspect of efficiency due to its lowest computational complexity. To overcome the drawbacks of conventional permutation-only type image cipher, a novel JPEG image fingerprinting and encryption method based on CA and SVD in the DWT domain is proposed in Fig.2. The encryption process is composed of substitution with GL and diffusion based on SVD of random matrix in the DWT domain. The proposed encryption algorithm can be divided into the following steps:

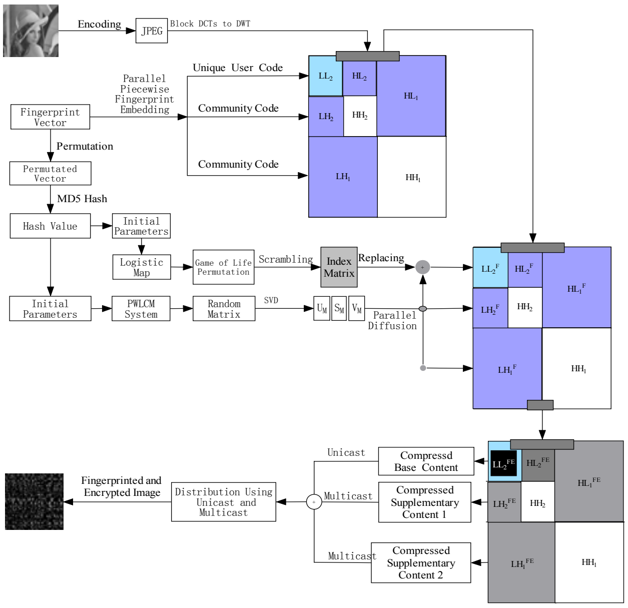

Encoding
JPEG
Block DCTs to DWT
Unique User Code
Parallel Piecewise Fingerprint Embedding
Fingerprint Vector
Community Code
Community Code
Permutation
Permutated Vector
MD5 Hash
Hash Value
Initial Parameters
Logistic Map
Game of Life Permutation
Scrambling
Index Matrix
Replacing
Initial Parameters
PWLCM System
Random Matrix
SVD
U_M S_M V_M
Parallel Diffusion
LL_2 HL_2 HL_1 LH_2 HH_2 LH_1 HH_1
LL_2^F HL_2^F HL_1^F LH_2^F HH_2 LH_1^F HH_1
LL_2^{FE} HL_2^{FE} HL_1^{FE} LH_2^{FE} HH_2 LH_1^{FE} HH_1
Unicast
Compressd Base Content
Multicast
Compressed Supplementary Content 1
Multicast
Compressed Supplementary Content 2
Distribution Using Unicast and Multicast
Fingerprinted and Encrypted Image

Figure 2. The architecture of JFE scheme

Step 1: Given a user fingerprint vector, permute the vector randomly, and then divide the permuted fingerprint vector into two parts: $X = X_1 + X_2$, where X_* denotes half of the vector, calculate the sum of both parts denoted by Sum_{X_1} and Sum_{X_2} respectively. Subtract these sums and multiply the total number of gray levels in the image to get Th, which is used to generate the initial value using MD5, MD5 is a widely used cryptographic hash function with a 128-bit hash value [40]. The MD5 hash value of Th is V^{Th}. According to the order of bits, we segment V^{Th} into eight 16-bit parts $V^{Th}{}_1$, $V^{Th}{}_2$,..., $V^{Th}{}_8$, and compute the values of these parts in decimal numbers. We can compute initial values x_0, y_0 and parameters u, η, which are viewed as the secret keys in this algorithm. Our encryption algorithm actually does have some of the following secret keys: (1) Initial values x_0 (Logistic map) and y_0 (PWLCM system); (2) Control parameters u (Logistic map) and η (PWLCM system).

$$x_0 = \frac{V^{Th}{}_1}{2^{16}}, \quad y_0 = \frac{V^{Th}{}_2}{2^{16}}, \quad u = 3.57 + \frac{V^{Th}{}_5}{2^{16}} \times 0.43, \quad \eta = \frac{V^{Th}{}_6}{2^{17}}$$

Step 2: Chaotic cellular automata for scrambling matrix generation. Adjacent coefficients in an image have a strong correlation. To scramble the image, this correlation needs to be reduced. We propose performing coefficient scrambling with the help of a number of generations of the GL. The universe of the GL is an infinite two-dimensional orthogonal grid of square cells, each of which is in one of two possible states, alive or dead. GL will add the diffusion property to the scrambling technique. At each step in time, the proposed scrambling matrix generation algorithm can be described as follows:

(1) Use logistic map to generate sequences ($x_1 x_2 \cdots x_{M\times N}$) respectively, where x_0 and u are given in advance as keys. Then we create a two-dimensional grids of cells G^0, as the seeds of GL by the sequences, the rule is that if the value of x_i is bigger than the mean value of the sequence, the corresponding cell is alive, else dead. Where G^0 is used to permute the DWT transformed coefficient matrixes; An $M \times N$ GL automaton is set up with an initial random configuration A_0, and is set to run for k generations, thus obtaining $\{A_1, A_2, ..., A_k\}$ matrices.

(2) Let I_G denote the original matrix, then getting the patches set of $\{Pl_1, Pl_2, ..., Pl_k\}$ in the original matrix.

(3) For every Pl_r in the patches set (for $r = 1, ..., m$). Let Pl_r denote the input image patch; Cp_r denotes the output scrambled matrix patches and A_1 is the first generation produced by the GL. Set row=1, col=1.

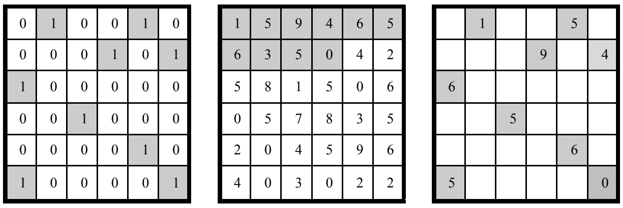
(4) For all (i, j) such that $A_1(i, j) = 1$, take the value of element P_e (row, col), put it in $Cp_r(i, j)$, and increment (row, col) with row-first order to point to the next objective in the input matrix.

(5) For $p = 2, ..., k$, for all i, j such that $A_p(i, j) = 1$ and $A_n(i, j) = 0$ (for $n = 1, ..., p-1$), take the value of element P_e (row, col), put it in $Cp_r(i, j)$, and increment (row, col) to point to the next objective.

(6) Take the gray value of the remaining objectives in Pl_r, and put them in row-first order in those $Cp_r(i, j)$ where, for all $p = 1, 2, ..., k$, $A_p(i, j) = 0$.

(7) Assume every Cp_r as a independent patch, steps 3, 4, and 5 are used to scramble these patches in the original grid.

Fig.3 (left) displays the first generation of the GL; living cells (cells in state 1) are shaded. Fig.3 (middle) shows the initial step of the algorithm to an matrix with 6×6 elements. Fig.3 (right) displays the scrambled matrix after applying step (3) of the algorithm. To recover the original matrix, the inverse of the scrambling algorithm must be executed, using as keys the initial random configuration A_0 and the number of iterations *ki*.



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. Encryption using CA. (left, first generation GL, middle, original patch, right, encrypted patch)

Step 3: For a compressed JPEG image, we calculate the one-level DWT coefficient matrix of the image from the block DCTs. Then we can get four sub-bands: the approximation coefficients LL, and the detailed coefficients HL, LH, HH. The low-frequency LL subband of the one-level DWT is a down-sampled image of the origin image. This process can reduce computational cost and lower complexity because most of the modified differences of all DWT coefficients are zero. Then, perform two-level DWT decomposition.

Step 4: The corresponding plain coefficients of the LL subband are put to the scrambling coefficient matrix according to the index matrix one by one.

Step 5: To protect content further, diffusion processes with the PWLCM map and SVD can enhance the resistance to attack. Using the PWLCM map to generate chaotic sequences $RP^J_{M\times N}=\{rp^J_1,rp^J_2,...,rp^J_{M\times N}\}$, then we can get the sequences $CP^J_{M\times N}=\{cp^J_1,cp^J_2,...,cp^J_{M\times N}\}$, cp_i =ceiling(fp_i), which is one-to-one correspondent with the coefficient sequence in DWT domain. The obtained chaotic sequence is arranged in the form of a matrix of dimension $M\times N$, which is denoted by CP^J, as a random matrix. Perform SVD on CP^J, we get $CP^J=U_{CP}V_{CP}V^T_{CP}$

Step 6: Deform all coefficients of each subband using orthonormal matrices U_{CPK} and V^T_{CPK}, as

$$I^{FE}=\begin{cases}U_{CP}I\,V^T_{CP}, M\leq N\\ V_{CP}I\,U^T_{CP}, M>N\end{cases}$$

Then, We can get the scrambled and fingerprinted image I^{JFE}.

V. Experiment results and security analysis

The performance of the proposed JFE technique is demonstrated using MATLAB platform on a computer having a Pentium(R) Dual-Core E5700 CPU and 2-GB RAM. We used eight types of test images with different spatial and frequency characteristics: Elena, Peppers, Airplane, Fishingboat , Baboon, and Watch. We set parameters x_0 =0.98968389485321, u =3.9978859364826, y_0 = 0.4576412939342, η =0.45967789391392. Fig. 4(a) shows the encrypted image. Fig. 4 (b) show the decrypted image with fingerprints under the correct key. From the results of our experiment, we can see it is difficult to recognize the original image from the encrypted one.

A. Perceptual Security

A good multimedia content encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute force attack infeasible. Generally, the encrypted image should be unintelligible for confidentiality. In the proposed scheme, the LL coefficients in DWT domain are encrypted by permutation via GL firstly. Then the scrambled values of coefficients are changed using SVD. The visual impact of the proposed encryption scheme is demonstrated in Fig.4(a). It is clear that all the encrypted images become noise-like images and are all actually unintelligible. Therefore, the proposed scheme indeed possessed high perceptual security.

B. Imperceptibility of the Fingerprint

The fingerprint is embedded in the image during the decryption process. In order to preserve visual quality, the fingerprint in the fingerprinted copy should be imperceptible and perceptually undetectable. Fig. 4(b) shows some experimental results of decrypted fingerprinted images. It can be observed that the quality of the fingerprinted image does not have any change observably.

C. Ability of resisting exhaustive attack

The total key space includes two processes of confusion and diffusion. Our encryption algorithm actually does have some of the following secret keys: (1) Initial values x_0 (Logistic map), y_0 (PWLCM system); (2) Parameters u (Logistic map), η (PWLCM system), k; (3) The iteration times R. The sensitivity to x_0, y_0, u and η is considered as 10^{-16} [41], The total key space is about $10^{16\times 4}=10^{64}$.This key space is large enough to resist the brute-force attack.

D. Resistance to statistical attack

1) The grey histogram analysis

Since, the proposed scheme is a rapid selective encryption in the compressed domain. Hence, the basic idea is to compare the histograms of the original and encrypted media. If the histograms of the encrypted images are fairly uniform and is significantly different from the histogram of the original one, then the encryption is said to be perfect. Fig. 4(c), (d) shows the grey-scale histograms. Comparing the two histograms we find that the pixel grey values of the original images are concentrated on some values, but the histograms of the encrypted images are significantly different from the histograms, and the histograms of the encrypted ones are very similar , which makes statistical attacks difficult.

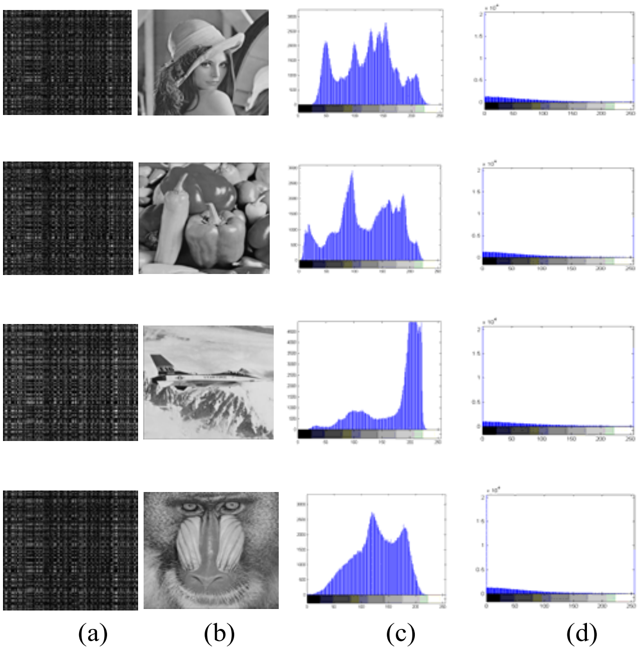


Figure 4. The experimental results : (a) the encrypted images, (b) the decrypted images with fingerprints, (c) the grey histogram of the original images, (d) the grey histogram of the encrypted images.

2) *Correlation coefficient analysis*

The correlation analysis says that a good encryption technique must break the correlation among the adjacent image pixels. We randomly select 2000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original image and the encrypted image. Fig.5(a), (b) show the correlation of two adjacent pixels in the original Lena image and its encrypted image. Fig.5(b) shows that the correlations of adjacent pixels in the encrypted image are greatly reduced.

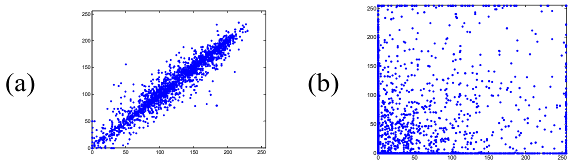


Figure 5. Correlation of two adjacent pixels

E. *Discussion of the encryption process*

We knew that the permutation process only enhances the unintelligibility of the encrypted image. Although single coefficient in 2-level LL subband permutation via GL can achieve better effect than 4 × 4 blocks in the 2-level LL subband permutation, however, the first method took 16 times as much as time that the latter took. In fact, the latter can get almost the same encryption effect that 4 × 4 blocks permutation in all subbands of 1-level DWT via GL could achieve, in this comparison, permutation performed only took 1/16 time that permutation in all subbands took. Therefore, 4 × 4 blocks permutation in the 2-level LL subband can get better performance than the others.

On the other hand, even if the chaotic map used in GL is cracked, the hacker still cannot decrypt the image since the random matrix key of diffusion in SVD encryption process remains secret. Fig.6 shows the comparison of when a diffusion process is and is not applied. It is clear that the diffusion process in the proposed scheme can enhance perceptual security. Therefore, if confidentiality is in high demand, the proposed method with diffusion can be applied. Otherwise, the encryption method with only permutation can be performed since only a rough sketch without details would be revealed, making the perceptual quality unacceptable.

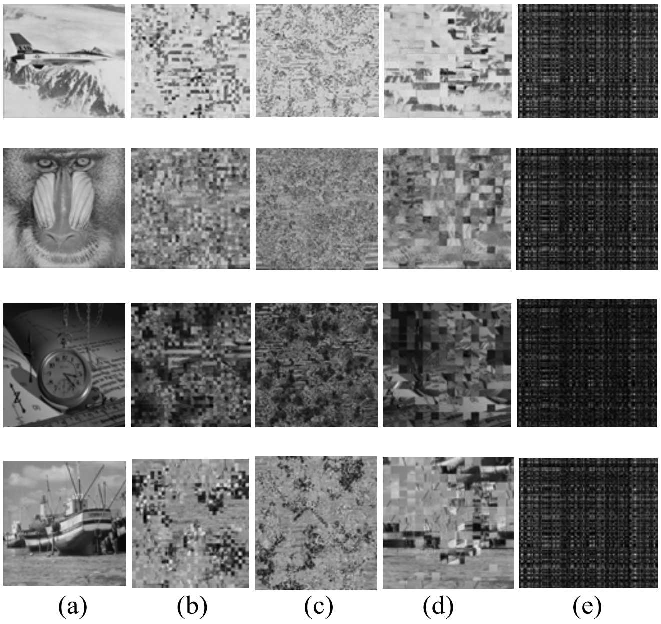


Figure 6. Evaluation of the encryption process. (a) Original images, (b) 4 × 4 blocks in the 2-level LL subband permutation via GL, (c) Single coefficient in 2-level LL subband permutation via GL, (d) Permutated 4 × 4 blocks in all subbands of 1-level DWT via GL respectively, (e) image encryption with permutation on 2-level LL subband via GL and diffusion using SVD distortion.

F. *Encryption Efficiency*

1) *Comparative Analysis*

This subsection presents a comparative analysis of the proposed technique with the existing state of art. The considered technique is a joint encryption/watermarking algorithm for verifying medical image presented by D. Bouslimi et al.[42]. The authors have suggested the merging of a stream cipher algorithm (RC45) and watermarking approaches. However, the stream cipher algorithm for encryption still has a high time complexity according to the abundant data in images. On the other hand, watermarking and encryption are conducted in the spatial domain. The approach is inefficient because a large amount of time is spent on the inter-conversion between the DCT coefficients and spatial pixel data. The proposed algorithm is able to overcome the aforementioned weaknesses by incorporating chaotic map with CA and SVD in the compressed domain. It is evident that the chaotic maps are very sensitive to their initial seed. Therefore, a slight change in the initial seed will cause the significant change in their final value. Furthermore, the proposed technique is perceptually efficient. The use of orthogonal matrices obtained by SVD produces a nonlinear process for the encryption of LL subbands. Another benefit of using the SVD is that it ensures the matrices used in encryption are invertible so that the inverse process will perfectly reconstruct the subbands. This proves an improvement by the proposed technique over the existing watermarking and encryption technique.

2) *Time efficiency*

In the case of multimedia distribution in social networks, if a technique requires a huge amount of time to encrypt/decrypt a image, then it is not considered a feasible technique. Therefore, the time efficiency of the proposed technique is evaluated in this subsection. In the proposed technique, the time efficiency is depicted in Table 1. These experiments are run on a computer having a Pentium(R) Dual-Core E5700, and with MATLAB 7.1 version. From the table, it is clear that time taken for the encryption process is completed in 0.9 s or so. Therefore, we can say that the proposed JFE scheme is time efficient , and it can provide security services within strict time deadlines to users.

Table 1. TIME EFFICIENCY

Images	Lena	Peppers	Airplane	Baboon	watch	Fishingboat
Time(s)	1.02	0.92	0.90	0.92	0.92	0.90

VI. CONCLUSION

The traditional JFE methods don’t consider the relationship between users and resource-constrained mobile devices, therefore then cannot be applied to secure multimedia sharing for resource-constrained mobile social network because of the tremendous scale of social network and the limited resources that mobile devices have. In this paper, the first JFE method based on CA and SVD in the DWT transform domain for mobile social network to deal with the issues of JPEG images sharing and traitor tracing is proposed. The experiment results and algorithm analyses show that the new algorithm possesses a large key space and can resist brute-force, and statistical attacks. Our methods does not require a great deal of computation time in comparison with full decoding because the proposed algorithm can transform JPEG images into DWT domain directly. Therefore, the efficiency is desirable, our algorithm is meant to be a good candidate to ensure the security of JPEG images distribution. Above all, the proposed scheme can continually protect decrypted content from being illegally distributed by an authorized member. Therefore, by the proposed JFE mechanisms the risk of the illegal distribution of authorized users can be reduced. The fundamental goal of our research has been to provide a useful synthesis of social network analysis for the field of secure JPEG images sharing for mobile social network.

ACKNOWLEDGMENT

This work is supported by NSF of China Grants (61370092, 61370223), Natural Science Foundation of Hubei Province of China (No.2015CFB236, No.2014CFB188), and Youth innovation team project in Hubei Provincial Department of Education (No.T201410).

REFERENCES

[1] P. Belimpasakis and A. Saaranen, "Sharing with people: a system for user-centric content sharing," *Multimedia Syst.* , vol. 16, pp. 399-421, 2010.

[2] J. Dittmann, P. Wohlmacher, and K. Nahrstedt, "Using cryptographic and watermarking algorithms," *IEEE Multimedia* vol. 8, pp. 54-65, 2001.

[3] S. Lian and X. Chen, "Traceable content protection based on chaos and neural networks," *Applied Soft Computing,* vol. 11, pp. 4293-4301, 2011.

[4] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solitons Fractals,* vol. 21, pp. 749-761, 2004.

[5] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos Solitons Fractals,* vol. 35, pp. 408-419, 2008.

[6] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos,* vol. 16, pp. 2129-2151, 2006.

[7] J. Guo, P. Zheng, and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain," *Journal of Visual Communication and Image Representation,* vol. 30, pp. 125-135, 2015.

[8] A. Qureshi, D. Megías, and H. Rifà-Pous, "Framework for preserving security and privacy in peer-to-peer content distribution systems," *Expert Systems with Applications,* vol. 42, pp. 1391-1408, 2015.

[9] C. Ye, Z. Xiong, Y. Ding, G. Wang, J. Li, and K. Zhang, "Joint fingerprinting and encryption in hybrid domains for multimedia sharing in social networks," *Journal of Visual Languages & Computing,* vol. 25, pp. 658-666, 2014.

[10] M. Li, D. Xiao, Y. Zhang, and H. Liu, "Attack and improvement of the joint fingerprinting and decryption method for vector quantization images," *Signal Processing,* vol. 99, pp. 17-28, 2014.

[11] B. Czaplewski and R. Rykaczewski, "Matrix-based robust joint fingerprinting and decryption method for multicast distribution of multimedia," *Signal Processing,* 2014.

[12] T. Xiang, C. Yu, and F. Chen, "Secure MQ coder: An efficient way to protect JPEG 2000 images in wireless multimedia sensor networks," *Signal Processing: Image Communication,* vol. 29, pp. 1015-1027, 2014.

[13] R. Gupta and S. Jain, "A review on watermarking techniques for compressed encrypted images," in *Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014 International Conference on*, 2014, pp. 10-13.

[14] W. Wang, "Team-and-role-based organizational context and access control for cooperative hypermedia environments," in *Proceedings of the tenth ACM Conference on Hypertext and hypermedia: returning to our diverse roots: returning to our diverse roots*, 1999, pp. 37-46.

[15] S. K. Chang, G. Polese, M. Cibelli, and R. Thomas, "Visual authorization modeling in e-commerce applications," *IEEE Multimedia,* vol. 10, pp. 44-54, 2003.

[16] M. Giordano and G. Polese, "Visual Computer-Managed Security: A Framework for Developing Access Control in Enterprise Applications," *IEEE Software,* vol. 30, pp. 62-69, 2013.

[17] D. Bouslimi, G. Coatrieux, and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images," *Comput Meth Programs Biomed,* vol. 106, pp. 47-54, 2012.

[18] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," *IEEE Signal Processing Magazine,* vol. 30, pp. 87-96, 2013.

[19] A. Subramanyam and S. Emmanuel, "Robust watermarking of compressed JPEG images in encrypted domain," 2011, pp. 37-57.

[20] A. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust Watermarking of Compressed and Encrypted JPEG2000 Images," *IEEE Trans. Multimedia* vol. 14, pp. 703-716, 2012.

[21] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proc. IEEE,* vol. 92, pp. 918-932, 2004.

[22] C. Y. Lin, P. Prangjarote, L. W. Kang, W. L. Huang, and T. H. Chen, "Joint fingerprinting and decryption with noise-resistant for vector quantization images," *Signal Processing,* 2012.

[23] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," *IEEE Transactions on Information Forensics and Security,* vol. 5, pp. 480-491, 2010.

[24] C. H. Yuen and K. W. Wong, "A chaos-based joint image compression and encryption scheme using DCT and SHA-1," *Applied Soft Computing,* vol. 11, pp. 5092-5098, 2011.

[25] S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system," *Chaos, Solitons & Fractals,* vol. 40, pp. 2509-2519, 2009.

[26] C. P. Wu and C. C. J. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Transactions on Multimedia,* vol. 7, pp. 828-839, 2005.

[27] C. Ye, H. Ling, F. Zou, and C. Liu, "Secure content sharing for social network using fingerprinting and encryption in the TSH transform domain," in *Proceedings of the 20th ACM international conference on Multimedia*, 2012, pp. 1117-1120.

[28] S. Wolfram, "A new kind of science," *Wolfram Media,* 2002.

[29] S. Wolfram, "Theory and applications of cellular automata," 1986.

[30] A. Adamatzky, *Game of life cellular automata*: Springer, 2010.

[31] H. Shen, X. Cheng, K. Cai, and M. B. Hu, "Detect overlapping and hierarchical community structure in networks," *Physica A,* vol. 388, pp. 1706-1712, 2009.

[32] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory* vol. 44, pp. 1897-1905, 1998.

[33] G. Tardos, "Optimal probabilistic fingerprint codes," *J. ACM* vol. 55, p. 10, 2008.

[34] C. Ye, H. Ling, F. Zou, and Z. Lu, "A new fingerprinting scheme using social network analysis for majority attack," *Telecommunication Systems,* vol. 54, pp. 315-331, 2013.

[35] B. J. Davis and S. H. Nawab, "The relationship of transform coefficients for differing transforms and/or differing subblock sizes," *IEEE Transactions on Signal Processing,* vol. 52, pp. 1458-1461, 2004.

[36] L. Wang, H. Ling, F. Zou, and Z. Lu, "Real-Time Compressed-Domain Video Watermarking Resistance to Geometric Distortions," *IEEE Multimedia,* vol. 19, pp. 70-79, 2012.

[37] S. G. Mallat, "A theory for multiresolution signal decomposition: the wavelet representation," *IEEE Trans. Pattern Anal. Mach. Intell. ,* vol. 11, pp. 674-693, 1989.

[38] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proceedings of the IEEE,* vol. 92, pp. 918-932, 2004.

[39] S. Wolfram and M. Gad-el-Hak, "A new kind of science," *Applied Mechanics Reviews,* vol. 56, p. B18, 2003.

[40] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications,* vol. 59, pp. 3320-3327, 2010.

[41] M. K. Khan, J. Zhang, and K. Alghathbar, "Challenge-response-based biometric image scrambling for secure personal identification," *Future Generation Computer Systems,* vol. 27, pp. 411-418, 2011.

[42] D. Bouslimi, G. Coatrieux, and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images," *Computer Methods and Programs in Biomedicine,* vol. 106, pp. 47-54, 2012.