Hindawi
Security and Communication Networks
Volume 2018, Article ID 1591206, 15 pages
https://doi.org/10.1155/2018/1591206

Research Article

A Novel Image Authentication with Tamper Localization and Self-Recovery in Encrypted Domain Based on Compressive Sensing

Rui Zhang, Di Xiao, and Yanting Chang

College of Computer Science, Chongqing University, Chongqing 400044, China

Correspondence should be addressed to Di Xiao; xiaodi_cqu@hotmail.com

Received 24 July 2017; Accepted 25 September 2017; Published 29 March 2018

Academic Editor: Yu-Dong Yao

This paper proposes a novel tamper detection, localization, and recovery scheme for encrypted images with Discrete Wavelet Transformation (DWT) and Compressive Sensing (CS). The original image is first transformed into DWT domain and divided into important part, that is, low-frequency part, and unimportant part, that is, high-frequency part. For low-frequency part contains the main information of image, traditional chaotic encryption is employed. Then, high-frequency part is encrypted with CS to vacate space for watermark. The scheme takes the processed original image content as watermark, from which the characteristic digest values are generated. Comparing with the existing image authentication algorithms, the proposed scheme can realize not only tamper detection and localization but also tamper recovery. Moreover, tamper recovery is based on block division and the recovery accuracy varies with the contents that are possibly tampered. If either the watermark or low-frequency part is tampered, the recovery accuracy is 100%. The experimental results show that the scheme can not only distinguish the type of tamper and find the tampered blocks but also recover the main information of the original image. With great robustness and security, the scheme can adequately meet the need of secure image transmission under unreliable conditions.

1. Introduction

With the rapid development of data storage and digital process, more and more digital information is transformed and transmitted over the Internet day by day, which brings people a series of security problems as well as convenience. For the openness of network, digital images are vulnerable to attack during the transmission over public network. Receivers often receive tampered images unconsciously. Therefore, unpredictable results occur. Especially for the fields such as governments, military, forensics, and electronic commerce, any slight attack will lead to serious consequences. Accordingly, people pay more and more attention to the protection of privacy information. The researches on digital image security, that is, image encryption, image data hiding, and image authentication, become more important than ever.

Image encryption technique scrambles the pixels of the image and decreases the correlation among the pixels, so that the encrypted image is hard to understand [1]. However, the encrypted image may arouse an attacker's attention to guess the secret behind encryption and seek various ways to crack or break the encrypted content, which heavily threatens the security of the original information. Data hiding technique focuses on embedding some significant information or authentication information into the original cover image based on the redundancy of cover image, which makes it difficult to detect the embedded information.

With the developments of techniques, people hope not only that the data can be delivered to receiver securely but also that the receiver can detect the integrity and authenticity of the received data, which thirsts for image authentication to detect whether the image is tampered and how it is tampered. Conventional authentication techniques belong to integrity authentication, which does not allow any slight change during data transmission and therefore is not suitable for image content authentication. Different from conventional authentication, content-based digital signature and watermarking technique can detect the range of tamper and judge whether

the tamper affects the real content of image. However, most of the existing digital signature and watermarking techniques can only detect the integrity of images or conduct image content authentication with no self-recovery ability or limited self-recovery ability. More and more application scenarios require not only exact tamper detection but also tampered content identification, tamper localization, and self-recovery. Take the transmission and storage of military and medical images as an example. The content owner often encrypts the images first for avoiding information leakage. The data hider embeds secret data in encrypted images. In the receiver side, secret data can be commendably extracted and can be employed to tamper detection, localization and original data recovery. In this way, data can be securely transmitted while the authentication of data integrity and authenticity also can be conducted, which has great practical significance.

In this paper, a novel image authentication with tamper localization and self-recovery for encrypted images is proposed. Firstly, the original image is transformed into Discrete Wavelet Transformation (DWT) domain and divided into important part, that is, low-frequency part, and unimportant part, that is, high-frequency part. Then, different parts are processed differently to realize different goals. Since the low-frequency part contains the main information of image, traditional chaotic encryption is employed in encryption stage so that the low-frequency part can be fully recovered in decryption stage. Then, for the high-frequency part, Compressive Sensing (CS) is used to conduct encryption so as to vacate space for watermark embedding. The scheme takes the processed content of original image as watermark, from which the characteristic digest values are then generated. The watermark is designed mainly for tamper recovery while the digest values are considered as the standard of tamper detection. Tamper recovery is based on block division and the recovery accuracy varies with the contents that are possibly tampered. If either the watermark or low-frequency part is tampered, the recovery accuracy is 100%. If both the watermark and low-frequency part are tampered, the recovery accuracy will decrease while the tampered degree increases. However, some existing pixel prediction techniques can be used to further improve the visual quality of recovered image. The experimental results show that the proposed scheme can not only distinguish the type of tamper and find the tampered image block but also recover the main information of the original image. With great robustness and security, the scheme can adequately meet the need of secure image transportation under unreliable conditions.

The rest of this paper is organized as follows. Section 2 briefly overviews the existing image data hiding and image authentication schemes. Section 3 lists some general knowledge about CS. Section 4 presents the proposed image authentication scheme. Experimental results are demonstrated in Section 5. Finally, we conclude in Section 6.

2. Related Works

Image encryption techniques, from traditional classical encryption algorithms, such as DES and AES, to chaotic novel encryption algorithms and joint encryption algorithms, such as [2], are designed to encrypt text and images. Data hiding techniques usually go with image encryption. The embedding domain can generally be plain domain or encrypted domain. For data hiding in plain domain, including both spatial domain and transform domain, the original image is watermarked first and then encrypted. The classical algorithms in spatial domain can be divided into LSB modification and substitution based algorithms [3], error expansion based algorithms [4], and histogram shifting based algorithms [5]. The classical algorithms in transform domain include discrete cosine transform (DCT) algorithms and discrete wavelet transformation (DWT) algorithms [6–11]. For data hiding in encrypted domain, also including both spatial domain and transform domain, the original image is first encrypted and then watermarked. Data hiding in spatial domain was conducted in [12–16], while authors of [17, 18] hide data in transform domain.

Image authentication techniques can be generally divided into integrity authentication and content authentication. For integrity authentication, any slight change of image is not allowed. For content authentication, the operations that do not influence the content features of image are acceptable. The two methods of image authentication are digital signature and digital watermarking.

So far, a large number of image authentication schemes with digital signature and digital watermarking have been proposed. References [19–21] focused on digital signature, which is sophisticated and has been employed in many applications, especially in electronic commerce. Digital watermarking can be divided into spatial domain schemes and transformation domain schemes. Spatial domain schemes include block-based fragile watermarking [22] and pixel significant bit based watermarking [23]. In [22], the cover image is divided into reversible blocks and irreversible blocks. Reversible blocks are employed to embed the feature information extracted from all the blocks, while irreversible blocks are used to extract the digest information of image. The scheme can accurately locate tampers and recover images with high quality. However, the scheme is quite complicated and cannot resist quantization attack. Moreover, the number of irreversible blocks cannot be more than that of reversible blocks. Otherwise, the scheme cannot realize reversible authentication. In [23] the 7 MSBs' checksum is computed of all the pixels in the original image, which is then embedded into the LSB of each pixel. Though the scheme is of practical value and is easy to implement, the security is extremely low and the scheme is subjected to LSB substitution attack.

Since transformation domain is suitable for the extraction of image features, the authentication methods often rest on wavelet transformation coefficients or cosine transformation coefficients. In [24], a watermark in the form of a visually meaningful binary pattern is used for tamper detection. One watermark bit is embedded into each DCT block by shifting a randomly selected coefficient to have a mapped value. Though the scheme works well in resisting some attacks, there is no tamper recovery capability. In [25], Hasan and Hassan proposed a robust self-embedding watermarking scheme for self-correction and a fragile watermarking scheme for sensitive authentication. The scheme can effectively detect and

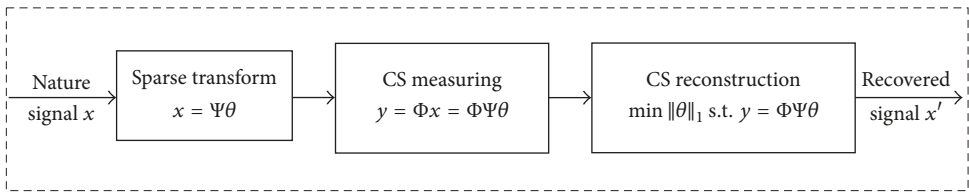


Figure 1: The framework of compressive sensing.

characterize changes and distinguish between malicious and normal manipulations and has autocorrection capabilities of local malicious alterations. In [26], a quantization and DCT based self-embedding fragile watermarking scheme with effective image authentication and restoration quality is proposed. The scheme used a small nonoverlapping block sized 2×2 to improve the accuracy of localization and can effectively remove the blocking artifacts. Unfortunately, the watermark data, which is embedded into three LSBs planes, may be destroyed by some image processing operations. In [27], Liu and Hu designed two watermarks from the low-frequency band of DWT domain and embedded the watermarks into the high-frequency bands. The scheme can resist the mild modifications of digital image and be able to detect and recover the malicious modifications precisely. In [28], the image features are extracted from the lowest-frequency coefficients of each block as the first embedded watermark and the orientation adjustment is then calculate based on the two-level wavelet coefficients in the middle-frequency subbands for image authentication. The scheme uses image feature and logo watermark as two different embedded watermarks and can realize image authentication and recovery of the tampered regions simultaneously. In [29] a semifragile and self-recoverable watermarking algorithm is proposed based on a group quantization and double authentication method. The scheme takes the generated authentication watermarks as information watermarks to reduce the amount of the embedding watermarks, enhances security by randomly permuting coefficients among a group, enhances robustness by embedding the watermarks in the largest coefficient inside a group, and employs the double authentication ring structure to effectively improve localization accuracy.

CS domain is another significant transformation domain, based on which image authentication schemes have sprung up. In [30], CS is employed to process watermark, which strengthens the security of watermark. However, due to the distortion during the process, the receiver cannot extract watermark exactly. In [31], CS is used to process watermarked image, which ensures the security of both watermark and cover image. However, the accuracy of watermark extraction is at risk. Some researchers have proved that hiding data in measurements is of strong robustness [32–37]. In [32, 33], Rachlin et al. showed the security and confidentiality of CS measurements. Without key and heuristic knowledge, attacker cannot infer the content of watermark from the measurements of encrypted image, which means that embedding watermark in CS measurements is feasible. In [34], the sender converts the original image into frequency domain with discrete wavelet transform (DWT), computes the measurements of encrypted image with compressive sensing measuring, and embeds watermark into the measurements. The watermarked encrypted image is then generated with CS reconstruction algorithm. However, only one measurement matrix is employed during the whole process, which is of huge computation and cannot resist large-scale noise attack. Moreover, the original image is needed for watermark extraction. Since the energy distribution of image is uneven and the embedding in energy-concentrated region will result in important information losing and destroying, it is better to embed watermark in energy-dispersed region.

CS based tamper authentication and recovery schemes for encrypted image can allow a certain compression ratio and effectively conduct tamper detection. The schemes can realize tamper content identification, or tamper localization or tamper recovery. However, the accuracy of tamper localization is not high and the above-mentioned three goals cannot be reached at the same time. In view of these insufficiencies, we propose a CS based image authentication scheme for the encrypted image jointly with tamper detection, localization, and recovery. The proposed scheme divides the image into important part and unimportant part and encrypts different parts with different encryption algorithms. For realizing tamper detection, localization, and recovery, the proposed scheme generates characteristic watermark from the original image and embeds the watermark into the compressive sensing measurements of the original image. The watermark is generated from the low-frequency part of DWT with CS. The reconstruction feature of CS is employed for tamper detection and recovery. And then the characteristic values extracted from watermark are considered as the tamper localization standard.

3. Compressive Sensing

In this section, we provide a brief introduction to CS. Compressive sensing, also known as compressive sampling or sparse sampling, is a new signal acquisition technology to capture and represent compressible signals at a rate significantly below the Nyquist rate. The original signals can be exactly or approximately reconstructed with a small number of measurements.

The general framework of compressive sensing, including sampling process in the encoder side and reconstruction process in the decoder side, is shown in Figure 1. Suppose that x is an $n \times 1$ natural signal which itself may or may not sparse in the canonical basis but is sparse or approximately sparse in an appropriate basis Ψ.

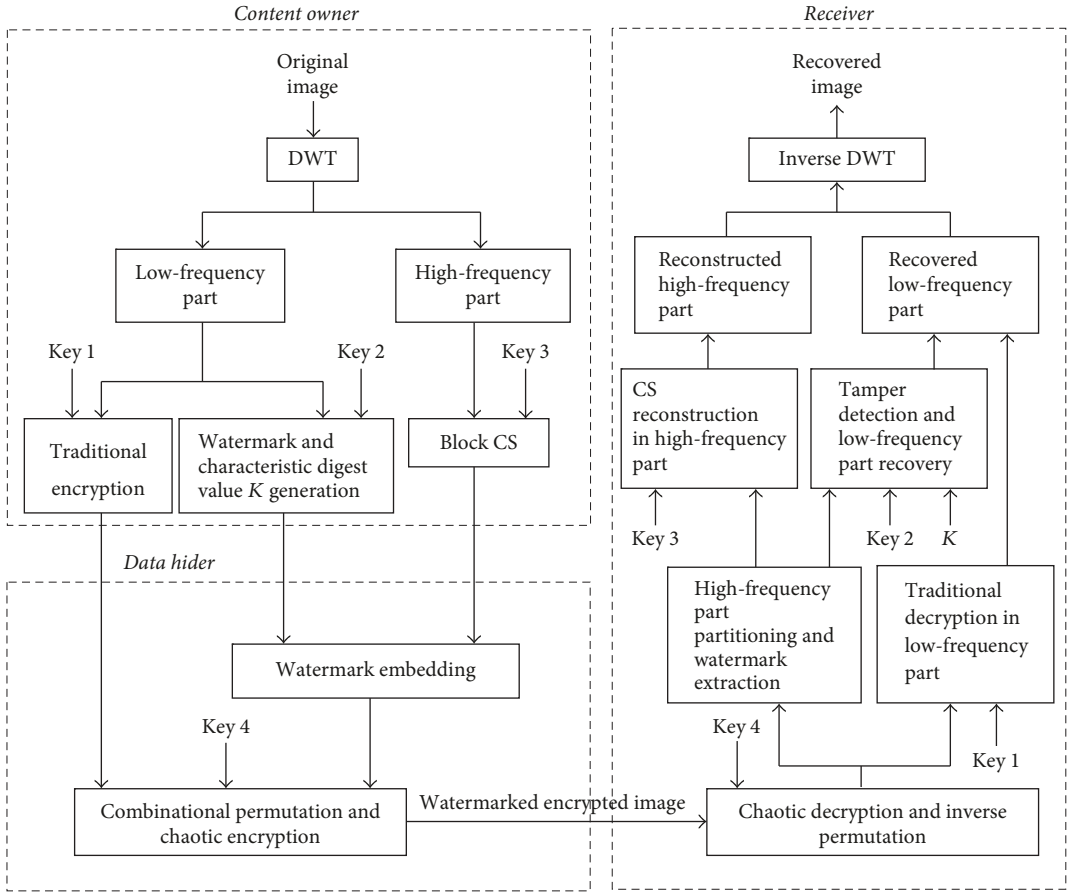


Figure 2: The general framework of the proposed scheme.

$$x = \Psi\theta, \tag{1}$$

where θ is k sparse; that is, there are exactly $k \ll n$ nonzero components. For the sampling process, measurements y can be computed through multiplying an $m \times n$ ($m \ll n$) measurement matrix Φ by x.

$$y = \Phi x, \tag{2}$$

where y, an $m \times 1$ sample vector, contains most useful information of x. Φ satisfies the restricted isometry property (RIP) of a certain order [38]. Then the sparse θ signal can be directly sampled via the following equation:

$$y = \Phi x = \Phi\Psi\theta. \tag{3}$$

For the reconstruction process, the signal x can be reconstructed from measurements y by solving an l_1 minimization problem.

$$\begin{aligned} \widehat{\theta} = \arg\min \quad & \theta_1 \\ \text{s.t.} \quad & y = \Phi\Psi\theta \\ & \widehat{x} = \Psi\widehat{\theta}, \end{aligned} \tag{4}$$

where $\widehat{x}$ is the recovered signal.

To the best of our knowledge, if the entries of matrix Φ are generated from a Gaussian distribution with zero mean and variance, Φ is a RIP matrix with overwhelming probability. In this paper, such a Gaussian distribution is employed to generate compressive sensing matrix. Moreover, the DWT is adopted to make the original signal sparse.

4. The Proposed Scheme

As illustrated in Figure 2, the proposed scheme mainly involves three parties: content owner, data hider, and receiver. The content owner generates watermark and characteristic digest values from the original image and encrypts the original image. When receiving the encrypted image and watermark, the data hider embeds the watermark into the encrypted image and transmits the watermarked encrypted image to the receiver. With relevant keys, the receiver can easily decrypt the watermarked encrypted image and conduct tamper detection, tamper localization, and image recovery.

4.1. Image Encryption and Watermark Embedding. In this stage, the content owner first encrypts the original image and generates the watermark to be embedded. Then the data hider conducts watermark embedding into the encrypted image. The framework is illustrated in Figure 3.

4.1.1. Image Encryption and Watermark Generation. Suppose that the original image is a gray scale image I.

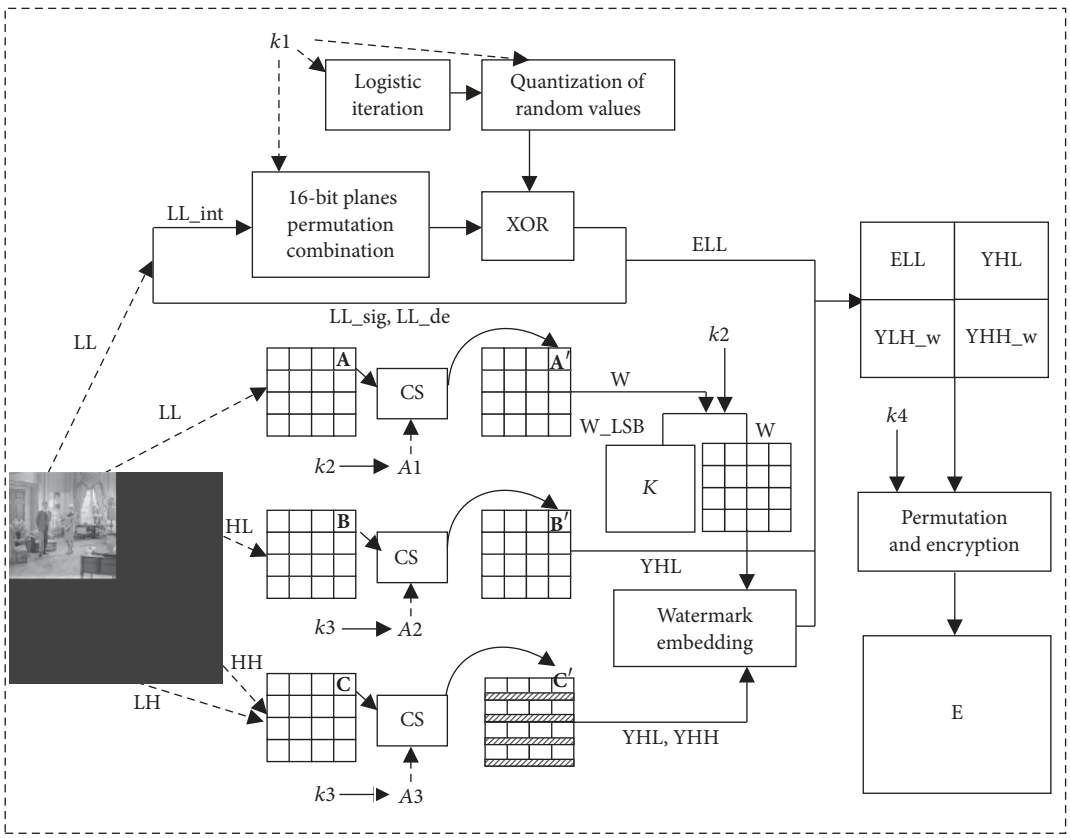


Figure 3: The framework of encryption and watermark embedding.

Step 1. The content owner decomposes the original image I with DWT and gets low-frequency part LL and high-frequency parts HL, LH, and HH. For further processing, the low-frequency part is considered as the important part while the high-frequency parts are deemed as the unimportant parts.

Step 2. There are two operations for important part LL. One is traditional image encryption. The other is watermark generation and characteristic digest value generation with direct block division and compressive sensing.

(A) Traditional Image Encryption with Arnold Scrambling and Logistic Map

(1) Separate out sign matrix LL_sig, absolute integer matrix LL_int, and decimal matrix LL_de from LL. Conduct $t1$ times Arnold scrambling to the 16-bit planes of LL_int, respectively, and then the scrambled bit panes are reassembled. The periodicity of Arnold scrambling $y1$ and the iterations $t1$ are part of the private key $k1$.

(2) According to another part of the private key $k1$, the initial values $(x0, y0)$, and a big integer P, use Logistic map to generate a random sequence with the size as LL_int, multiply it by the big integer P, and then perform modular 65536 operation.

(3) XOR the generated pixels and the random numbers to get the encrypted low-frequency integer matrix ELL_int, which is then reassembled with the sign matrix LL_sig and decimal matrix LL_de to form the encrypted low-frequency part ELL.

(B) Watermark Generation. The watermark generated from LL with block compressive sensing in this proposed scheme is designed for tamper authentication and recovery. Therefore, the size of measurement matrix should be the same as that of block. Watermark is generated as follows.

Divide LL into nonoverlapping blocks with the size of $a \times a$. Generate chaotic measurement matrix $A1$ with the seed private key $x2$. Here a and $x2$ are part of the private key $k2$. For each block, reshape it into one-dimensional vector through Zig-Zag scanning. Then each vector is measured to get the measurement value. All the measurement values are combined to form the measurement watermark matrix W. Since the watermark will be used for low-frequency recovery, the compression ratio is set to 1 for reducing distortion.

(C) Characteristic Digest Value Generation. Characteristic digest value is generated through watermark processing, which will be used for image authentication in the coming stage. Since it is transmitted via secure channel, it can be employed for tamper authentication and localization.

Take the absolute value of W as an integer matrix. Transform each element of the matrix into 16-bit sequence

with 0 and 1, which is then permuted with the private key t. Pick out the LSB plane from the 16-bit planes to form W_LSB. Compress it with run-length encoding. Then it is considered as the characteristic digest value K and transmitted to the receiver side together with other private keys.

It should be noted that since the characteristic digest value is generated through taking a bit plane from the blocks of watermark W which originates from low-frequency part with compressive sensing, the characteristic digest value can only detect whether the watermark or low-frequency part is tampered and then find out the tampered blocks.

Step 3. For the unimportant part, that is, high-frequency parts HL, LH, and HH, different compressive sensing operation will be employed to ensure the reasonability of watermark embedding and the invariance of image size before and after encryption.

(A) For HL. Divide HL into nonoverlapping blocks with the size of $a \times a$. Reshape each block into one-dimensional vector with the same method. Generate a measurement matrix $A2$ with the private key $x3$. Then each block is measured to get a measurement value, which is then transformed and combined as the measurement value matrix YHL with compression ratio of 1.

(B) For LH and HH. Divide LH and HH into nonoverlapping blocks with the size of $a \times a$. Reshape each block into one-dimensional vector with the same method. Generate a measurement matrix $A3$ with the private key $x4$. Then each block is measured to get a measurement value, which is then transformed as the blocked measurement value matrices YLH and YHH with compression ratio of 0.5. The vacant positions are filled up with 0. Here, half of space in LH and HH after compression is vacated for watermark. Moreover, a, $x3$, and $x4$ are part of $k3$.

4.1.2. Watermark Embedding. Watermark is made up of measurement values and will be embedded into the measurement values of high-frequency part. Therefore, it not only makes watermark localization and extraction convenient but also reduces the error rate of watermark extraction. After being embedded, the watermark and other elements in high-frequency part show the same distribution features of encrypted data so that it is difficult to distinguish whether watermark is embedded.

Step 1. Separate each watermark block into two parts, that is, the upper part and the lower part. The size of each part is $a/2 \times a$. Embed these two parts into the corresponding positions of YLH and YHH, respectively, which have been filled up with "0." After watermark embedding, YLH_w and YHH_w are generated and then combined with YHL to form the watermarked high-frequency part.

Step 2. Reassemble the low-frequency part and the high-frequency part. Generate a random sequence using Logistic map with the private key $(x1, y1)$. Combine this sequence and the watermarked encrypted image with XOR operation. Then perform $t2$ times Arnold scrambling to the resultant matrix to get the final watermarked encrypted image E. Here, iteration cycle $y2$ and iteration times $t2$ and $(x1, y1)$ are part of the private key $k4$.

4.2. Watermark Extraction and Image Decryption. In this section, all the operations will be done by the receiver. As illustrated in Figure 4, the process can be divided into four stages, that is, watermark extraction, image decryption, tamper validation, and tamper localization and recovery.

4.2.1. Watermark Extraction. After receiving the watermarked encrypted image, the receiver first decrypts the image and then extracts the watermark from the image. The watermark extraction process is the inverse process of embedding.

Step 1. The receiver first separates $(x1, y1)$ from $k4$. Generate a chaotic random sequence using Logistic map with $(x1, y1)$. Then pick up iteration cycle $y2$ and iteration times $t2$. Perform $y2 - t2$ times Arnold scrambling to the watermarked encrypted image E. Perform XOR operation between this scrambled image and the generated chaotic random sequence and then divide it into low-frequency part ELL_RE and watermarked high-frequency part.

Step 2. Divide the watermarked high-frequency part into three parts, that is, YHL_RE, YLH_w_RE, and YHH_w_RE, which are then further divided into nonoverlapping blocks. From the first block of YLH_w_RE and YHH_w_RE, take the lower part of the corresponding block to get a watermark block and put it into the corresponding block position of the watermark extraction matrix W_RE. When the processing of all the blocks finishes, the watermark is fully extracted. Moreover, the high-frequency part after watermark extraction will change into YLH_RE and YHH_RE.

The extracted watermark is mainly used for tamper verification. Without tamper, a high quality image will be directly reconstructed after decryption. When tamper occurs, the characteristic digest value will be generated and then compared with the transmitted characteristic digest value for tamper localization and recovery.

4.2.2. Image Decryption

(A) Low-Frequency Part Decryption

(1) Separate out the sign matrix ELL_sig_RE, the absolute integer matrix ELL_int_RE, and the decimal matrix ELL_de_RE from ELL_RE. Take the initial value $(x0, y0)$ and the big integer P out of the key $k1$. Generate a random sequence using Logistic map with the same length as ELL_int_RE. Multiply it by the big integer P and then perform modular 65536 operation. Conduct XOR operation between the resultant sequence and the pixels of ELL_int_RE.

(2) Take the periodicity of Arnold scrambling $y1$ and the iterations $t1$ out of the key $k1$. Divide the integer part of the low frequency after XOR operation into 16-bit planes. Perform $y1 - t1$ times Arnold scrambling to

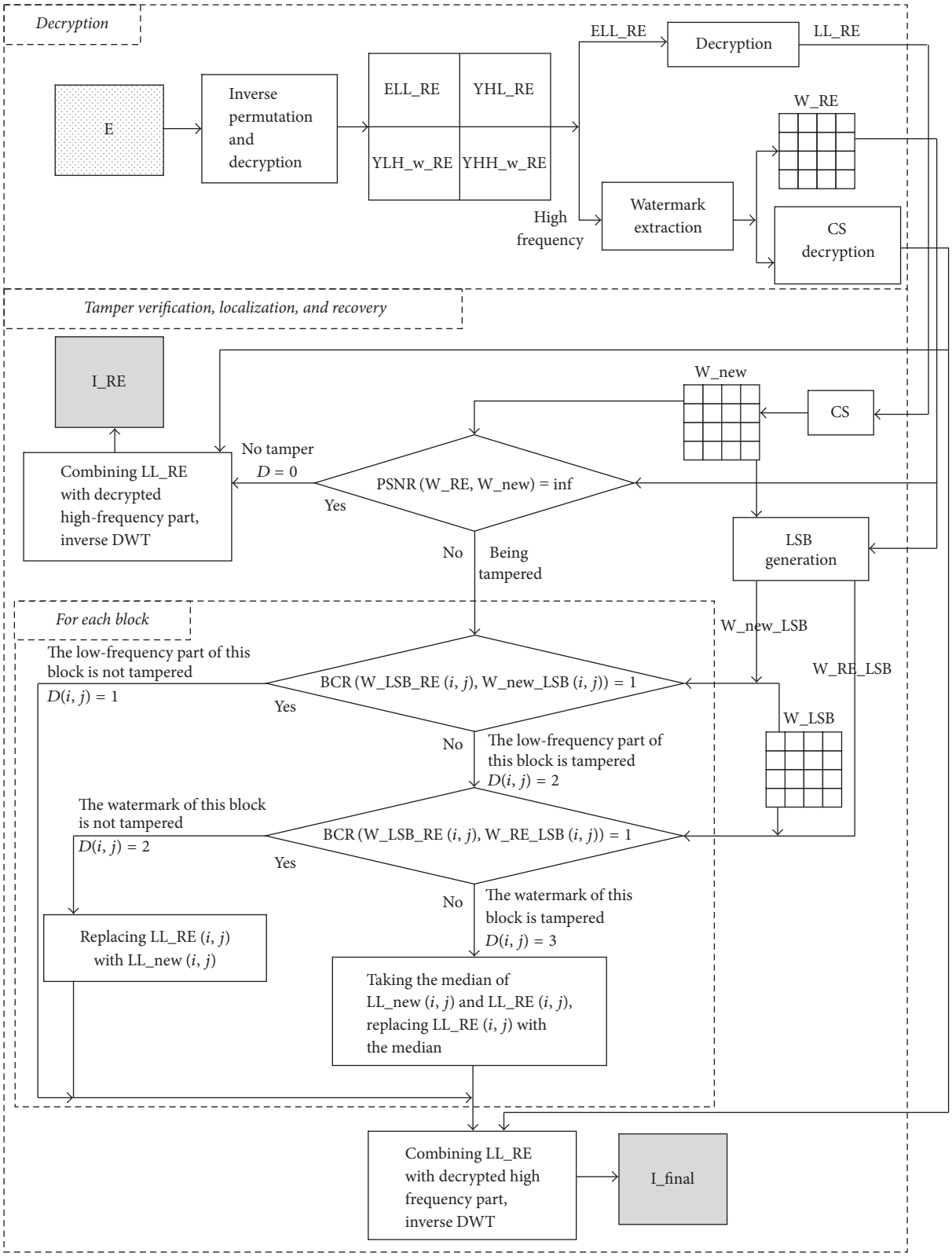


Figure 4: Watermark extraction, image decryption, tamper verification, and tamper localization and recovery.

these 16-bit planes, respectively, and then reassemble the scrambled bit panes to get the decrypted integer part of the low frequency LL_int_RE.

(3) Combine LL_int_RE with ELL_sig_RE and ELL_de_RE to form the decrypted image of the low frequency LL_RE.

(B) High-Frequency Part Decryption. According to the private key k_3, reconstruct each block of YHL_RE, YLH_RE, and YHH_RE with compressive sensing to get the recovered HL_RE, LH_RE, and HH_RE.

(C) Image Decryption. Combine LL_RE with HL_RE, LH_RE, and HH_RE. Perform inverse DWT to get the recovered image I_RE.

4.3. Tamper Detection, Localization, and Recovery

4.3.1. Tamper Detection. Since the low-frequency part contains the important information of image and the high-frequency part contains the unimportant information of image, the former is encrypted with traditional encryption algorithm while the latter is processed with CS. Due to the lossy compression of CS, it cannot perfectly recover the original image. Therefore, the low-frequency part should be recovered as completely as possible. Watermark is generated from the low-frequency part with CS, the sensibility of which can be used for tamper detection. Moreover, watermark is embedded into the high-frequency part. For the reversibility of watermark embedding, watermark is mainly used for tamper verification and recovery in low-frequency part. Generated from watermark and transmitted via secure channel, the characteristic digest value can be used for tamper localization that occurred to the watermark.

Based on the above theoretical analysis, three kinds of tampers may happen to the watermarked encrypted image during the transmission in the channel, that is, tamper with watermark, tamper with low-frequency part, and tamper with both low-frequency part and watermark.

(A) Data Preprocessing

(1) Firstly, generate a new watermark matrix W_new from the decrypted LL_RE.

(2) Secondly, recover a new image of low-frequency part LL_new from the extracted watermark W_RE.

(B) Comparison betweenW_RE and W_new

(1) If PSNR(W_RE, W_new) = Inf, W_RE is exactly the same as W_new, which means that LL_RE and W_RE are correctly recovered. Therefore, I_RE is the very image that has been correctly recovered. No tamper occurs.

For LL_RE, its related operations include traditional encryption and decryption, which are reversible. So it can be correctly recovered unless tamper occurs. If the low-frequency part is tampered, the decrypted LL_RE will vary and the newly generated watermark W_new will change. If the watermark is tampered, the extracted watermark W_RE will vary. Since these two are the same, it is believed that no tamper occurs and the low-frequency part LL_RE is correct.

(2) If PSNR(W_RE, W_new) $\neq$ Inf, the low-frequency part or the watermark is tampered. Tamper localization and tamper recovery are needed.

If the low-frequency part is partly tampered, the decrypted LL_RE will vary and the newly generated watermark W_new will change. If the watermark is tampered, the extracted watermark W_RE will vary. Under these circumstances, accurate tamper localization will greatly contribute to the recovery of image.

4.3.2. Tamper Localization and Recovery. When a tamper is detected, a comparison between the characteristic digest values generated from the extracted watermark and the one transmitted via a secure channel is needed for tamper localization, tamper content authentication, and tamper recovery. This process runs on each block. The blocks without tamper remain unchanged.

(A) Data Preprocessing

(1) Generate new characteristic digest values W_new_LSB from the watermark W_new.

(2) Generate new characteristic digest values W_RE_LSB from the extracted watermark W_RE.

(3) Suppose that D is a zero matrix with the same size as the watermark block number. Take D as tamper localization matrix. If the watermark block (i, j) is tampered, then $D(i, j) = 1$. If the low-frequency part block (i, j) is tampered, then $D(i, j) = 2$. If both the watermark block (i, j) and the low-frequency part block (i, j) are tampered, then $D(i, j) = 3$. If no tamper occurs, $D(i, j) = 0$.

(B) Tamper Localization and Recovery. Compare W_LSB with W_RE_LSB and W_new_LSB, respectively, for tamper localization. Since they are all generated directly or indirectly from the low-frequency part LL after block division and W_LSB is transmitted to the receiver side after being coded with run-length encoding, they are suitable for tamper localization.

(1) Start from the first block. For the block (i, j), take the elements W_LSB(i, j), W_RE_LSB(i, j), and W_new_LSB(i, j) from W_LSB, W_RE_LSB, and W_new_LSB, respectively.

(2) Compare W_LSB(i, j) with W_RE_LSB(i, j) and W_new_LSB(i, j), respectively:

$$s = \mathrm{BCR}\left(\mathrm{W\_LSB}\left(i, j\right), \mathrm{W\_RE\_LSB}\left(i, j\right)\right), \quad (5)$$

$$t = \mathrm{BCR}\left(\mathrm{W\_LSB}\left(i, j\right), \mathrm{W\_new\_LSB}\left(i, j\right)\right). \quad (6)$$

(a) If $s \neq 1$ and $t = 1$, it is believed that the recovered watermark W_new(i, j) of this block is correct, which means

Table 1: The PSNRs of watermarked encrypted images.

Image	Couple	Lena	Pepper	Milkdrop	Lake	Baboon	Airfield	Plane
PSNR (dB)	22.49	22.36	23.53	23.64	22.45	24.71	23.51	23.46

Table 2: Correlation coefficients of the watermarked encrypted images.

	Couple	Lena	Pepper	Milkdrop	Lake	Baboon	Airfield	Plane
Horizontal	0.0017	0.0072	−0.0040	0.0080	0.0001	−0.0027	−0.0049	0.0084
Vertical	0.0002	0.0019	−0.0022	0.0005	−0.0020	−0.0021	−0.0061	0.0039
Diagonal	−0.0027	−0.0074	−0.0036	−0.0007	0.0053	0.0009	0.0003	0.0069

that there is no tamper occurring in this low-frequency part block LL_RE(i, j). The extracted watermark block W_RE(i, j) is tampered; $D(i, j) = 1$. The low-frequency part block LL_RE(i, j) can remain unchanged.

(b) If $s = 1$ and $t \neq 1$, it is believed that the extracted watermark block W_RE(i, j) is correct while the newly generated watermark W_new_LSB(i, j) is incorrect, which means that the low-frequency part is tampered; $D(i, j) = 2$. Then replace LL_RE(i, j) with LL_new(i, j) which is recovered from W_RE(i, j).

(c) If $s \neq 1$ and $t \neq 1$, it is believed that both the extracted watermark and the low-frequency part of this block are tampered; $D(i, j) = 3$. Then replace LL_RE(i, j) with LL_mid(i, j) which is the median of LL_RE(i, j) and LL_new(i, j).

(d) Perform the above operations to each block successively. And finally tamper localization and recovery can be realized.

(C) Combine LL_RE with HL_RE, LH_RE, and HH_RE. Then inverse DWT can help to get the final recovered image I_final.

(D) If both the extracted watermark and the low frequency were tampered, some existing pixel prediction techniques [39–41] with full use of spatial correlation can be employed to further improve the visual quality of the recovered image I_final.

(a) With the help of the tamper localization matrix D, the tampered blocks and their neighboring blocks can be easily found out.

(b) For all the pixels in the tampered block, pixel prediction will begin from the tampered pixels with most nontampered neighboring pixels. If two or more neighboring blocks were tampered, theses blocks can be taken as an integrated whole to select the prediction beginning pixel. The predicted pixels can be used as nontampered pixels for next predictions.

(c) Apply corresponding pixels prediction algorithms to further improve the visual quality of image. Without loss of generality, the method in [41] is selected in this paper. After prediction, an improved image will be obtained.

5. Experimental Results and Performance Analysis

The test image set of this proposed scheme consists of 8 standard test images of size 512 × 512, that is, Couple, Lena, Peppers, Milkdrop, Lake, Baboon, Airfield, and Plane, shown in Figure 5.

5.1. Image Quality Analysis

(A) Watermarked Encrypted Image Quality. In the proposed scheme, the watermark is generated from the low-frequency part of cover image with CS and then is embedded into the encrypted high-frequency part. After encryption and permutation, the original image and watermark cannot be seen from the watermarked encrypted image any more. That is to say, the watermark and original image are well masked. Table 1 shows that the PSNR of different encrypted images are all below 25 dB. According to Table 2, the correlation coefficients of eight test images after encryption and data embedding are all close to 0. For the watermarked encrypted images, as shown in Figure 6, one can see nothing related to the original image and cannot distinguish whether a watermark is embedded into this image.

(B) Recovered Image Quality. In this proposed scheme, the encryption key and embedding key are employed during the process of image encryption and watermark embedding. Moreover, the high-frequency part is encrypted with CS while the low-frequency part is encrypted with traditional encryption algorithms. When the encrypted image is not tampered, the distortion of the recovered image only results from the reconstruction of high-frequency part with CS. Since other operations are all reversible and the watermark extraction is also reversible, the quality of the recovered image with correct keys and without tamper is reasonably high.

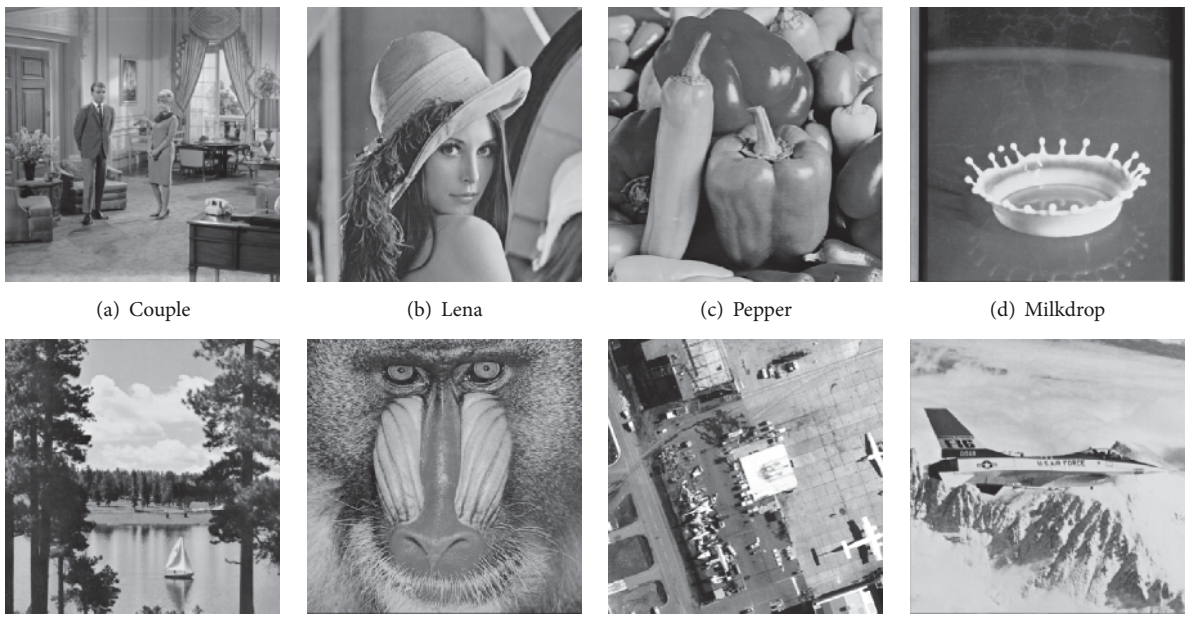
5.2. Image Authentication Performance Analysis. The watermark is generated from the low-frequency part with CS in order to perform accuracy tamper detection with the sensibility of CS and CS measurements.

Firstly, data preprocessing is done:

(1) Conduct inverse DWT of the decrypted LL_RE and the decrypted high-frequency part to get the recovered image I_RE.

(2) According to the extracted watermark W_RE, recover the low-frequency part LL_new. Conduct inverse DWT of LL_new and the decrypted high-frequency part to get recovered image I_new.

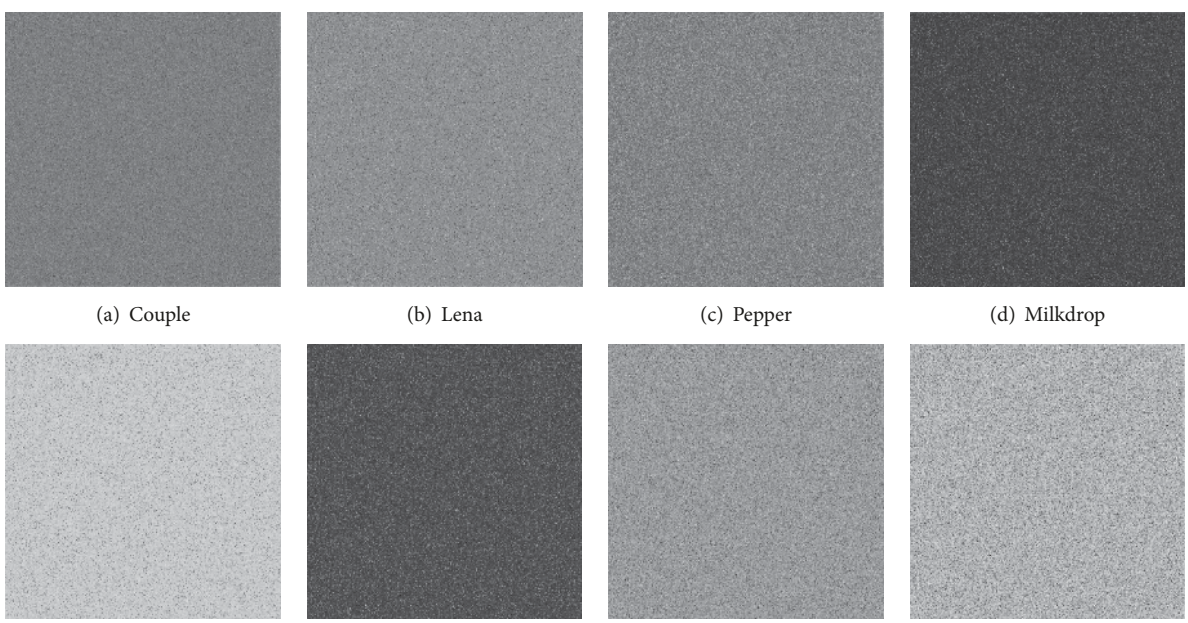
(3) According to the tamper detection and recovery method, recover the low-frequency part LL_RE.



(a) Couple (b) Lena (c) Pepper (d) Milkdrop

(e) Lake (f) Baboon (g) Airfield (h) Plane

Figure 5: The test images.



(a) Couple (b) Lena (c) Pepper (d) Milkdrop

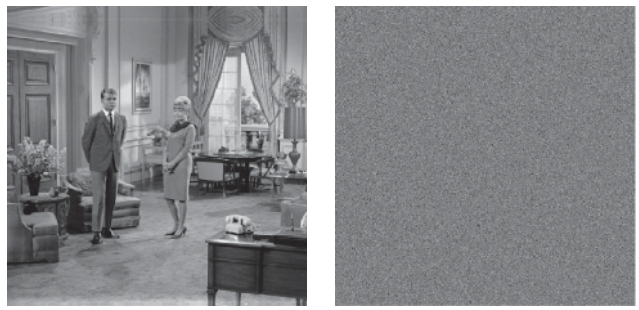
(e) Lake (f) Baboon (g) Airfield (h) Plane

Figure 6: The watermarked encrypted images.

Conduct inverse DWT of LL_RE and the decrypted high-frequency part to get tamper recovered image I_final.

In this experiment, tamper simulation is to replace the elements of some rows with 1. Figures 7–10 show the tamper localization and recovery effects when the low-frequency part or watermark is tampered. Without loss of generality, image Couple is taken as an example. Figure 7 shows the original image and watermarked encrypted image.

Figure 8 shows the tamper localization matrix, recovered image, and tamper recovered image when the low-frequency part is tampered. As can be seen, when a low-frequency part block of the watermarked encrypted image is tampered, the corresponding element of tamper localization matrix D will be changed into 2. The directly decrypted image, shown in (b), is damaged. However, since the watermark is not tampered, the recovered low-frequency part LL_new is correct and the quality of decrypted image I_new is



(a) (b)

Figure 7: The original image I (a) and the watermarked encrypted image E (b).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
5	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
9	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
10	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

(a)

(b) I_RE (c) I_new (d) I_final

Figure 8: The effect of tamper detection and recovery when low frequency is tampered.

fine, shown in (c). In other words, the proposed tamper recovery algorithm can identify that the low-frequency part is tampered and then will replace corresponding tampered block with right watermark block to get the final image I_final, shown in (d).

Figure 9 shows the tamper localization matrix, recovered image, and tamper recovered image when the watermark is tampered. As can be seen, when the watermark of a block in watermarked encrypted image is tampered, the corresponding element of tamper localization matrix D will be changed into 1. Since the low-frequency part of this block is not tampered, there is no modification to be done and it can be directly decrypted to get a good quality image I_RE, shown in (b). But since the watermark is tampered, the recovered low-frequency part LL_new is incorrect and the quality of the decrypted image I_new is damaged, shown in (c). In other words, the proposed tamper recovery algorithm can identify that the watermark is tampered and then conduct

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

(a)

(b) I_RE

(c) I_new

(d) I_final

Figure 9: The effect of tamper detection and recovery when watermark is tampered.

recovery operations to get the image I_final, shown in (d).

Figure 10 shows the tamper localization matrix, recovered image, and tamper recovered image when both the low-frequency part and the watermark are tampered. As can be seen, when both the low-frequency part and the watermark of a block in watermarked encrypted image are tampered, the corresponding element of tamper localization matrix D will be changed into 3. For the low-frequency part of this block is tampered, the directly decrypted image, shown in (b), is damaged. Since the watermark is tampered, the recovered low-frequency part LL_new is incorrect and the quality of decrypted image I_new is damaged, shown in (c). In other words, the proposed tamper recovery algorithm can identify that both the low-frequency part and the watermark of this block are tampered, then replaces LL_RE with the median of LL_RE and LL_new, and finally decrypts the image to get a relatively high quality image I_final, shown in (d). With pixel prediction techniques, the visual quality of I_final can be further improved. As shown in (e), though tampered traces still can be seen by the naked eye the heavily tampered blocks have been well improved.

In general, the proposed scheme has better tamper verification and recovery effects on this kind of local tampers. The smaller the block size is, the more accurate the tamper localization is.

5.3. Image Security Analysis. In the proposed scheme, image encryption and watermark embedding are alternate, and encryption key and embedding key are mutually bounded, which make the scheme secure. Moreover, the scheme can resist cropping attacks to a certain extent. Take Lena as an example to get the recovered images from the watermarked encrypted images with different cropping strengths. As can be seen in Table 3, when the watermarked encrypted image is cropped within a certain range, the directly recovered image and the image recovered from watermark will be affected in different degrees. However, for the image recovered with the proposed tamper recovery scheme, its PSNR will be the better one of the former two recovered images.

6. Conclusions

In this paper, we propose a novel tamper verification and recovery scheme for encrypted images with CS. After DWT, the original image can be divided into important part, that is, low-frequency part, and unimportant part, that is, high-frequency part. The watermark and characteristic digest value

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
5	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
9	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
10	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

(a)

(b) I_RE

(c) I_new

(d) I_final

(e) I_improved

Figure 10: The effect of tamper detection and recovery when watermark and low frequency are tampered.

Table 3: PSNR and NC of the recovered images through the different proportion of cropping attacks.

Cropping ratio	PSNR (dB)			NC		
	I_RE	I_new	I_final	I_RE	I_new	I_final
0	36.41	36.38	36.41	0.9987	0.9984	0.9987
1/64	34.51	33.58	34.47	0.9971	0.9921	0.9969
1/32	32.79	32.17	32.70	0.9943	0.9914	0.9986
1/16	30.90	29.51	30.09	0.9830	0.9247	0.9555
1/8	29.47	28.24	28.45	0.9797	0.9144	0.9390
1/4	28.11	26.86	27.04	0.9687	0.8166	0.8531

are generated from the low-frequency part with block CS. The characteristic digest value will be encoded and then transmitted via secure channel together with private keys. The watermark is designed mainly for tamper recovery and is embedded into the high-frequency part processed with CS. The receiver can employ the extracted watermark and characteristic digest value to perform accurate tamper detection, localization, and recovery. Theoretical analysis and experimental simulations show that in an unreliable environment the proposed scheme is robust and secure against moderate attacks, such as cropping attacks. Moreover, the tampered blocks can be accurately and effectively found out with tamper localization matrix and the tampered image can be well recovered. Comparing with the existing image

authentication algorithms, the proposed scheme can simultaneously implement tamper verification, tamper content identification, tamper localization, and tamper recovery. With great robustness and security, the scheme can adequately meet the need of secure image transmission under unreliable conditions.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was funded by the National Natural Science Foundation of China (Grant nos. 61572089, 61502399, and 61633005), the Natural Science Foundation of Chongqing Science and Technology Commission (Grant nos. cstc2017jcyjBX0008, cstc2014jcyjA40030, and cstc2015jcyjA40039), the project supported by Graduate Student Research and Innovation Foundation of Chongqing (Grant no. CYB17026), the Chongqing Higher Education Reform Projects (Grant no. 153012), and the Fundamental Research Funds for the Central Universities (Grant nos. 106112017CDJQJ188830 and 106112017CDJXY180005).

References

[1] A. S. Rajput, N. Mishra, and S. Sharma, "Towards the growth of image encryption and authentication schemes," in *Proceedings of the 2013 2nd International Conference on Advances in Computing, Communications and Informatics, ICACCI 2013*, pp. 454–459, Mysore, India, August 2013.

[2] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools and Applications*, vol. 75, no. 11, pp. 6303–6319, 2016.

[3] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proceedings of the IEEE International Conference Image Processing (ICIP '94)*, vol. 2, pp. 86–90, Austin, Tex, USA, November 1994.

[4] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[5] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits & Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[6] S. Singh, T. J. Siddiqui, R. Singh, and H. V. Singh, "DCT-domain robust data hiding using chaotic sequence," in *Proceedings of the 2011 International Conference on Multimedia, Signal Processing and Communication Technologies, IMPACT 2011*, pp. 300–303, Aligarh, India, December 2011.

[7] C. C. Lin and P. F. Shiu, "High capacity data hiding scheme for dct-based images," *Journal of Information Hiding & Multimedia Signal Processing*, vol. 1, no. 3, 2010.

[8] Y. K. Lin, "High capacity reversible data hiding scheme based upon discrete cosine transformation," *Journal of Systems & Software*, vol. 85, no. 10, pp. 2395–2404, 2012.

[9] H. Liu, J. Liu, J. Huang, D. Huang, and Y. Q. Shi, "A robust DWT-based blind data hiding algorithm," *Proceedings - IEEE International Symposium on Circuits and Systems*, vol. 2, pp. 672–675, 2002.

[10] H.-Y. Huang and S.-H. Chang, "A lossless data hiding based on discrete Haar wavelet transform," in *Proceedings of the 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, 10th IEEE Int. Conf. Scalable Computing and Communications, ScalCom-2010*, pp. 1554–1559, Bradford, UK, July 2010.

[11] F. Li, Q. Mao, and C. C. Chang, "Reversible data hiding scheme based on the Haar discrete wavelet transform and interleaving prediction method," *Multimedia Tools & Applications*, pp. 1–20, 2017.

[12] Z. Qian, X. Zhang, Y. Ren, and G. Feng, "Block cipher based separable reversible data hiding in encrypted images," *Multimedia Tools & Applications*, vol. 75, no. 21, pp. 13749–13763, 2016.

[13] T. C. Lu, C. C. Chang, and Y. H. Huang, "High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting," *Multimedia Tools & Applications*, vol. 72, no. 1, pp. 417–435, 2014.

[14] X. P. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[15] X. P. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.

[16] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, 2012.

[17] T.-C. Lin and C.-M. Lin, "Wavelet-based copyright-protection scheme for digital images based on local features," *Information Sciences*, vol. 179, no. 19, pp. 3349–3358, 2009.

[18] G. S. Kalra, R. Talwar, and H. Sadawarti, "Adaptive digital image watermarking for color images in frequency domain," *Multimedia Tools & Applications*, vol. 74, no. 17, pp. 6849–6869, 2014.

[19] H.-P. Chen, X.-J. Shen, and W. Wei, "Digital signature algorithm based on hash: Round function and self-certified public key system," in *Proceedings of the 1st International Workshop on Education Technology and Computer Science, ETCS 2009*, pp. 618–624, Hubei, China, March 2009.

[20] C. Wang and X. Zhuang, "A watermarking scheme based on digital images' signatures," in *Proceedings of the 2nd International Conference on Multimedia Technology, ICMT 2011*, pp. 125–127, Hangzhou, China, July 2011.

[21] R. Kaur and A. Kaur, "Digital signature," in *Proceedings of the Turing 100 - International Conference on Computing Sciences, ICCS 2012*, pp. 295–301, Phagwara, India, September 2012.

[22] Q. Gu and T. Gao, "A new image authentication based on reversible watermarking algorithm," in *Proceedings of the 7th World Congress on Intelligent Control and Automation, WCICA'08*, pp. 2727–2731, Chongqing, China, June 2008.

[23] S. Walton, "Information authentication for a slippery new age," *Dr. Dobbs Journal*, vol. 20, no. 4, pp. 18–26, 1995.

[24] M. Al Baloshi and M. E. Al-Mualla, "A DCT-based watermarking technique for image authentication," in *Proceedings of the 2007 IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2007*, pp. 754–760, Amman, Jordan, May 2007.

[25] Y. M. Y. Hasan and A. M. Hassan, "Tamper detection with self-correction hybrid spatial-DCT domains image authentication technique," in *Proceedings of the ISSPIT 2007 - 2007 IEEE*

International Symposium on Signal Processing and Information Technology, pp. 369–374, Giza, Egypt, December 2007.

[26] D. Singh and S. K. Singh, "DCT based efficient fragile watermarking scheme for image authentication and restoration," *Multimedia Tools & Applications*, vol. 76, pp. 1–25, 2015.

[27] H. Liu and Y. Hu, "A wavelet-based watermarking scheme with authentication and recovery mechanism," in *Proceedings of the International Conference on Electrical and Control Engineering, ICECE 2010*, pp. 323–326, Wuhan, China, June 2010.

[28] L.-J. Wang and M.-Y. Syue, "Image authentication and recovery using wavelet-based multipurpose watermarking," in *Proceedings of the 2013 10th International Joint Conference on Computer Science and Software Engineering, JCSSE 2013*, pp. 31–36, Maha Sarakham, Thailand, May 2013.

[29] C. L. Li, A. H. Zhang, Z. F. Liu, L. Liao, and D. Huang, "Semi-fragile self-recoverable watermarking algorithm based on wavelet group quantization and double authentication," *Multimedia Tools & Applications*, vol. 74, no. 23, pp. 10581–10604, 2015.

[30] G. Valenzise, M. Tagliasacchi, S. Tubaro, G. Cancelli, and M. Barni, "A compressive-sensing basedwatermarking scheme for sparse image tampering identification," in *Proceedings of the 2009 IEEE International Conference on Image Processing, ICIP 2009*, pp. 1265–1268, Cairo, Egypt, November 2009.

[31] V. K. Veena, G. Jyothish Lal, S. Vishnu Prabhu, S. Sachin Kumar, and K. P. Soman, "A robust watermarking method based on Compressed Sensing and Arnold scrambling," in *Proceedings of the 2012 International Conference on Machine Vision and Image Processing, MVIP 2012*, pp. 105–108, Taipei, Taiwan, December 2012.

[32] Y. Rachlin and R. D. Baron, "The secrecy of compressed sensing measurements," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 813–817, IEEE, Urbana, Ill, USA, September 2008.

[33] S. A. Hossein, A. E. Tabatabaei, and N. Zivic, "Security analysis of the joint encryption and compressed sensing," in *Proceedings of the 20th Telecommunications Forum (TELFOR '12)*, pp. 799–802, Belgrade, Serbia, November 2012.

[34] G. F. Chen, S. X. Guo, Y. Li, and L. Li, "Digital image watermark algorithm based on compressive sensing," *Modern Electronics Technique*, vol. 35, no. 13, pp. 98–104, 2012.

[35] H.-C. Huang, F.-C. Chang, C.-H. Wu, and W.-H. Lai, "Watermarking for compressive sampling applications," in *Proceedings of the 2012 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2012*, pp. 223–226, Piraeus, Greece, July 2012.

[36] J. S. Pan, W. Li, C. S. Yang, and L. J. Yan, "Image steganography based on subsampling and compressive sensing," *Multimedia Tools & Applications*, vol. 74, no. 21, pp. 9191–9205, 2015.

[37] H. C. Huang and F. C. Chang, "Robust image watermarking based on compressed sensing techniques," *Journal of Information Hiding & Multimedia Signal Processing*, vol. 5, no. 2, pp. 275–285, 2014.

[38] E. J. Candes, "The restricted isometry property and its implications for compressed sensing," *Comptes Rendus Mathematique*, vol. 346, no. 9, pp. 589–592, 2008.

[39] M. Fallahpour, "Reversible image data hiding based on gradient adjusted prediction," *IEICE Electronics Express*, vol. 5, no. 20, pp. 870–876, 2008.

[40] M. Li, D. Xiao, Z. Peng, and H. Nan, "A modified reversible data hiding in encrypted images using random diffusion and accurate prediction," *ETRI Journal*, vol. 36, no. 2, pp. 325–328, 2014.

[41] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," *Journal of Visual Communication & Image Representation*, vol. 28, pp. 21–27, 2015.