A joint image encryption and watermarking algorithm based on compressive sensing and chaotic map*

Xiao Di(肖 迪), Cai Hong-Kun(蔡洪坤), and Zheng Hong-Ying(郑洪英)†

Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) of Chinese Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, *China*

(Received 10 December 2014; revised manuscript received 7 January 2015; published online 10 April 2015)

In this paper, a compressive sensing (CS) and chaotic map-based joint image encryption and watermarking algorithm is proposed. The transform domain coefficients of the original image are scrambled by Arnold map firstly. Then the watermark is adhered to the scrambled data. By compressive sensing, a set of watermarked measurements is obtained as the watermarked cipher image. In this algorithm, watermark embedding and data compression can be performed without knowing the original image; similarly, watermark extraction will not interfere with decryption. Due to the characteristics of CS, this algorithm features compressible cipher image size, flexible watermark capacity, and lossless watermark extraction from the compressed cipher image as well as robustness against packet loss. Simulation results and analyses show that the algorithm achieves good performance in the sense of security, watermark capacity, extraction accuracy, reconstruction, robustness, etc.

Keywords: joint encryption and watermarking, compressive sensing, chaos, Arnold map

PACS: 05.45.–a, 05.45.Gg **DOI:** 10.1088/1674-1056/24/6/060505

1. Introduction

The development of the internet and multimedia technology results in the transmission of a large quantity of network multimedia data. The network multimedia security problem has received much attention. Generally, the security of the data is provided by encryption and watermarking.[1] Encryption aims at making the to-be-protected data unintelligible to any unauthorized user. Since chaos has high sensitivity to the initial value and unpredictability of system change, chaos-based security application has been widely studied in recent years.[2–4] Several chaos-based image encryption algorithms have been proposed in Refs. [5]–[7]. Watermarking helps us to hide the existence of the information, e.g. to hide the owner's identification information, authentication, etc.

Since the encryption and watermarking realize different functionalities, they can be combined together to protect both the confidentiality and the ownership/identification. Some applications like video conferencing, and military image/video transmission, etc., require confidentiality and integrity. In these mentioned applications where multimedia data are sensitive in nature and demand both confidentiality and integrity, a joint encryption and watermarking scheme is preferred. In Ref. [1], the proposed layered approach increases the overall system security by using the watermarking and encryption at the same time. Till now, some joint encryption and watermarking schemes have been proposed for multimedia data security.[8–13] These proposed designs are mostly based on partial encryption. In Ref. [13], the author pointed out that these types of methods cannot keep secure enough against replacement attacks and proposed a modified scheme for MPEG2 video encryption and watermarking.

In most network multimedia applications, compression is necessary for limited network traffic and storage space. In the last few years, compressive sensing (CS) has been developed with the superiority in reducing storage space and computation cost.[14–16] It has been used in the encryption and watermarking algorithm. In Ref. [17], Mayiami *et al*. proved that with the uniform distribution over source messages and specific restriction on the number of measurements, CS-based encryption can achieve the Shannon's definition of perfect secrecy. Zhang *et al*. proposed a CS-based encryption, in which the original image is encrypted as a set of coefficients by a secret orthogonal transform.[18] Liu *et al*. proposed an image encryption scheme with enhanced security and robustness against packet loss.[19] In addition, some CS-based watermarking algorithms have been proposed. In Ref. [20], a CS-based watermark algorithm embeds the secret information about the measurements by utilizing the relationships between measurements. It can be applied to lossy channels for data delivery, but the watermark extraction accuracy is not ideal. In Ref. [21], Veena *et al*. proposed a watermarking scheme in which both compressive sensing and the Arnold method are used. This scheme is computationally efficient, but the original image information is required in the watermark embedding process and the hidden information cannot be extracted before decrypting the

*Project supported by the Open Research Fund of Chongqing Key Laboratory of Emergency Communications, China (Grant No. CQKLEC, 20140504), the National Natural Science Foundation of China (Grant Nos. 61173178, 61302161, and 61472464), and the Fundamental Research Funds for the Central Universities, China (Grant Nos. 106112013CDJZR180005 and 106112014CDJZR185501).

†Corresponding author. E-mail: zhycqu@gmail.com

© 2015 Chinese Physical Society and IOP Publishing Ltd

original image.

The main motivation behind our proposed work is to design a joint encryption and watermarking algorithm for network multimedia security, which should have a high level of security and compressibility. Besides, the robustness against the packet loss during transmission and storage is also essential for the limited network traffic. The proposed method is robustness against the packet loss due to compressive sensing. In our algorithm, the Arnold map and compressive sensing are used for compression and encryption. The secret information is used for identification information, authentication, etc. The proposed algorithm allows watermarking the encrypted data without requiring the knowledge of the original image and extracting the hidden information before decrypting the original image. Experimental results and comparative analysis have proved the expected merits of the proposed scheme.

The remaining sections of this paper are organized as follows. In Section 2 the compressive sensing, chaos-based sensing matrix and Arnold transformation are described briefly. In Section 3 the joint encryption and watermarking scheme is proposed. In Section 4, the simulation results and analyses of the proposed algorithm are given. Finally, some conclusions are drawn from the present study in Section 5.

2. Preliminary

2.1. Compressive sensing

Compressive sensing directly samples a sparse or compressible signal at a rate below Nyquist rate. A natural signal like a natural image generally has a sparse representation in the transform domain, such as discrete cosine transform (DCT) or discrete wavelet domain (DWT). We consider a one-dimensional (1D) natural signal s with length N and its transform coefficients x,

$$x = \Psi^{\mathrm{T}} s, \tag{1}$$

where Ψ is an $N \times N$ orthogonal transform matrix and called the sparse basis matrix. Generally, most of the coefficients in x are close to zero, and the relatively few large coefficients capture the principal information about the signal. We project x onto the second incoherent $M \times N$ $(M \ll N)$ matrix Φ and obtain the $M \times 1$ measurement vector,

$$y = \Phi x = \Phi \Psi^{\mathrm{T}} s. \tag{2}$$

We can recover the signal with high probability from y by solving a non-convex optimization problem $P0$.

$$(P0)\ \min ||\Psi^{\mathrm{T}} s||_0 \ \text{ s.t. } \ \Phi x = \Phi \Psi^{\mathrm{T}} s = y. \tag{3}$$

However, solving $P0$ is an NP-hard problem, which can be replaced by solving the linear programming problem $P1$.

$$(P1)\ \min ||\Psi^{\mathrm{T}} s||_1 \ \text{ s.t. } \ \Phi x = \Phi \Psi^{\mathrm{T}} s = y. \tag{4}$$

It has been proved that if measurement matrix Φ satisfies the restricted isometry property (RIP) then the optimization problem with restriction $(P0)$ should be always equivalent to its convex relaxation problem $(P1)$, which can be solved by the linear programming technique.[22] A matrix whose entries are independent and identically distributed random variables satisfies RIP with very high probability. In this paper, subspace pursuit (SP)[23] is adopted to reconstruct the original signal from these measurements y, which is a reliable and efficient algorithm.

2.2. Chaos-based sensing matrix

The sensing matrix used for CS is generated as follows.[24]

Firstly, generating a chaotic sequence $Z(d,k,z_0) = \{z_n, z_{n+d}, \ldots z_{kn+d}\}$ by sampling from the output sequence produced by the logistic map (5) with sampling distance d and initial condition z_0.

Let

$$z_{n+1} = \mu z_n (1 - z_n), \tag{5}$$

where μ is a positive constant. In our algorithm, $\mu = 4$. Let $x_k \in X(d,k,x_0)$ denote the regularization of $Z(d,k,z_0)$ as follows:

$$x_k = 1 - 2z_{n+kd}. \tag{6}$$

To construct the sensing matrix $A \in R^{M \times N}$, generate a sampled logistic sequence $X(d,k,x_0)$ with length $M \times N$, then create matrix A column by column with this sequence, write A as

$$A = \sqrt{2/M} \begin{pmatrix} x_0 & \cdots & x_{M(N-1)} \\ x_1 & \cdots & x_{M(N-1)+1} \\ \vdots & \ddots & \vdots \\ x_{M-1} & \cdots & x_{MN-1} \end{pmatrix}, \tag{7}$$

where the scalar $\sqrt{2/M}$ is for normalization, by choosing the sampling distance $d = 15$, then elements of sequence $X(d,k,x_0)$ are approximately independent and satisfy identical distribution, i.e., an independent and identical distribution (IID), and hence elements of matrix A are an (IID).

Theorem 1 Chaotic matrix $\Phi \in R^{M \times N}$ constructed according to Eq. (7) satisfies RIP for a constant $\delta > 0$ with an overwhelming probability, providing that $s \leq O(M/\log(N/s))$.

Theorem 1 has been proven in Ref. [24], which shows that when the sparse degree s is not bigger than a specific value, we can reconstruct the signal with an overwhelming probability by using sensing matrix Φ. In this paper, when the number of watermark data is less, the sparse degree is closer to the sparse degree of DCT coefficient matrix, which is sparse and is easy to find a suitable Φ to meet the conditions of Theorem 1. When a mass of watermark data are embedded,

the s will be closer to $W/2$ (W is the amount of watermark), the number N of all the signals is closer to W. In extreme conditions, the condition in theorem can be transformed into $s \leq O(M/\log(W/(W/2))) = O(M)$. That is to say, when sampling number M is bigger than s, we can reconstruct the signal by using the recovery algorithm of compressive sensing with an overwhelming probability. But, in this situation, the sampling number will be too big to lose the practical value.

2.3. Arnold map

We choose the two-dimensional Arnold map as the scrambling encryption of the image due to its briefness and good decentralization. The Arnold map finds application in the field of image encryption, digital watermarking, etc. The transform process realigns the pixel matrix by means of clipping and splicing. The two-dimensional (2D) Arnold map is given as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\, N) = \begin{bmatrix} 1 & u \\ v & uv+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\, N), \quad (8)$$

where (x,y) are the coordinates of the original image pixel, (x',y') are the coordinates of the scrambled image, N is the pixel number in the row and column coordinate of the image pixel, and u and v are positive integers, and $\det(A) = 1$. The transform alters the location of two pixels and if it is done several times will generate a scrambled image. Here, the parameter u, the parameter v, and the iteration number M can all be chosen as the secret keys.

3. Proposed algorithm

The block diagram of the proposed algorithm is shown in Fig. 1.

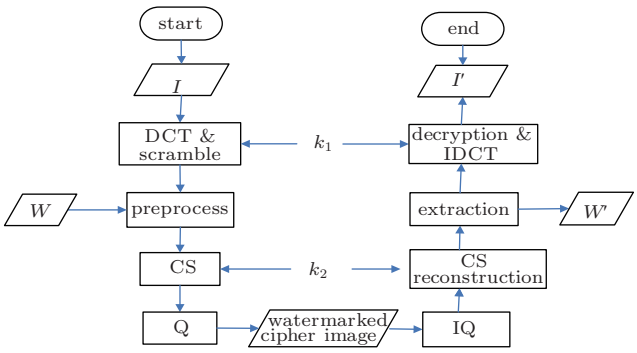


Fig. 1. (color online) Flow diagram of the proposed algorithm.

3.1. DCT and scrambling encryption

In order to use the compressive sensing, the original raw image should be converted into a sparse representation in some transform domain. In this paper, block discrete cosine transform (DCT) is applied to the original image $I(N \times N)$ to obtain the transform coefficient matrix X of the same size, and then X is scrambled through the Arnold map (the secret key k_1 is the parameters u, v and the iteration number). Finally, the scrambled DCT coefficient matrix X' is obtained. The scrambling process not only encrypts the data but also reduces the correlation of the coefficient matrix, which can efficiently enhance the reconstructed image quality.[25]

3.2. Pre-processing before watermark embedding

Nowadays, the average compressive sensing-based watermarking method embeds the watermark into the measurements after linear measurements or embeds the watermark in the sparse domain of the image before linear measurement, which will directly modify the information about the original image. To avoid this, we propose a novel embedding method to embed the watermark directly onto measurements in the linear measurement process. For this purpose, we should do some pre-processing.

First, the scrambled DCT coefficient matrix X' is divided into $(N/B)^2$ blocks of size $B \times B$. Meanwhile, the watermark of size W bits is also divided into$(N/B)^2$ segments and each segment has C bits ($C = WB^2/N^2$). Then each coefficient block is extended from $B \times B$ to $(B+b) \times B$ (the extended row number $b = \lceil C/B \rceil$). Finally, each segment of the watermark will be filled into the extended rows, and zeros would be padded in the remaining part if the extended rows cannot be filled with the watermark segment. Without loss of generality, a specific example is given in Fig. 2, where $N = 512$, $B = 32$, $b = 1$, and $C < B$, namely, the bit number of each watermark segment is less than that of the column for each coefficient block.

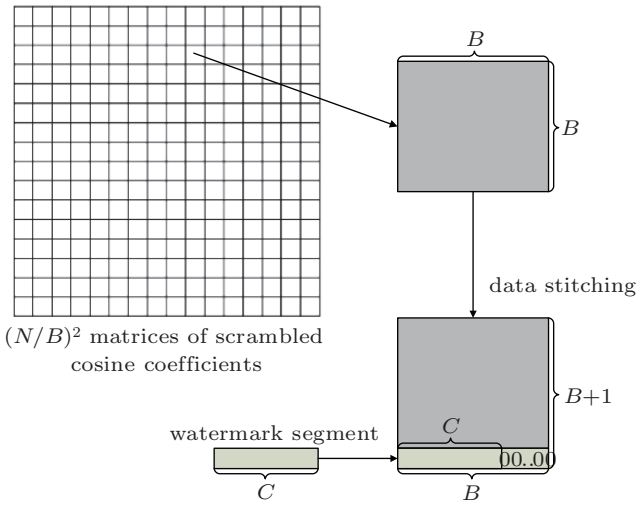


Fig. 2. (color online) Pre-processing of the DCT coefficients and watermark.

The watermark strength is denoted by α ($50 < \alpha < 500$), and the original value of the watermark and the value for filling are respectively denoted by w_0 and $\tilde{w}$. The watermark is adhered according to the following rules:

$$\begin{aligned} &\text{if } w_0 = 1, \quad \tilde{w} = \alpha \times 1, \\ &\text{if } w_0 = 0, \quad \tilde{w} = 0. \end{aligned} \quad (9)$$

When the processing is completed, we obtain $(N/B)^2$ matrices, each with a size of $(B+b)\times B$.

3.3. Compressive sensing and watermark embedding

All the matrices with a size of $(B+b)\times B$ make up a set of blocks with a size of $B_1 \times B_2$ ($B_1 = num \times (B+b)$, $B_2 = num \times B$, and num is a positive integer denoting the number of blocks for each sample). These blocks are converted into vectors x_i ($i = 1,2,\ldots,N^2/(B_1B_2)$) of size $B_1B_2 \times 1$. Then they are projected into some measurements, which can be represented by Eq. (10)

$$Ax_i, \quad i = 1,2,\ldots,N^2/(B_1B_2). \tag{10}$$

Here, A denotes the sensing matrix with a size of $m \times n$, $n = B_1B_2$, $0 < m \leq n$, y_i is a measurement with a size of $m \times 1$. The chaotic sequence-based sensing matrix A is used in this step. The secret key k_2, as the initial value of the chaotic map (5), will be used to generate the sensing matrix A and extract the watermark on the receiver side. Then, the quantified measurements will be transmitted to the receiver as the watermarked cipher image.

In this subsection, we realize the watermark embedding, compression, and further encryption at the same time by random projection.

3.4. Watermark extraction and decryption

After the watermarked cipher image is received, inverse quantification will be done. The secret key k_2 is needed in this procedure to generate the sensing matrix for signal recovery of compressive sensing. Then the receiver can reconstruct the content of the combined data, i.e., the scrambled DCT coefficients and watermark. The reconstructed data will be separated into the scrambled DCT coefficients and watermark as their prototypes.

For the extraction of the watermark, a fluctuation threshold T_e (generally $T_e = \alpha/2$) is set. For each value of the reconstructed watermark $\hat{w}$, let the extracted watermark be w' and one of the following conditions in Eq. (11) can be met

$$w' = \begin{cases} 1, & \text{if } \hat{w} < \alpha \pm T_e, \\ 0, & \text{if } \hat{w} < 0 \pm T_e, \\ \text{undefined}, & \text{otherwise.} \end{cases} \tag{11}$$

The unauthorized user without the secret key k_1 cannot obtain the original image, although the watermark has been extracted. Only the authorized user can decrypt the scrambled DCT coefficients by using k_1 and obtain the decrypted image.

4. Simulation results and analysis

In this section, we utilize experimental results to demonstrate the proposed algorithm performance. All the grayscale images as well as true color images are suitable for the proposed method, provided that their widths and heights are integral multiples of block size B, respectively. Without loss of generality, the test images, including nature images, medical images, and texture images, are all grayscale images which have a fixed size of 512×512. Pseudo random binary sequences and a binary image of size 128×128 are used as the watermark in different experiments. In the pre-processing phase, the matrix X is divided into blocks with a size of $B \times B$ ($B = 8$). We investigate the relationship between the image reconstruction performance and the watermark strength and compressive ratio, and the influence of the watermark strength and compressive ratio on the watermark extraction accuracy. Block compressive sensing is used in the linear measurement step, with a block size of $B_1 \times B_2$ ($B_1 = 2(B+b), B_2 = 2B$).[26] The

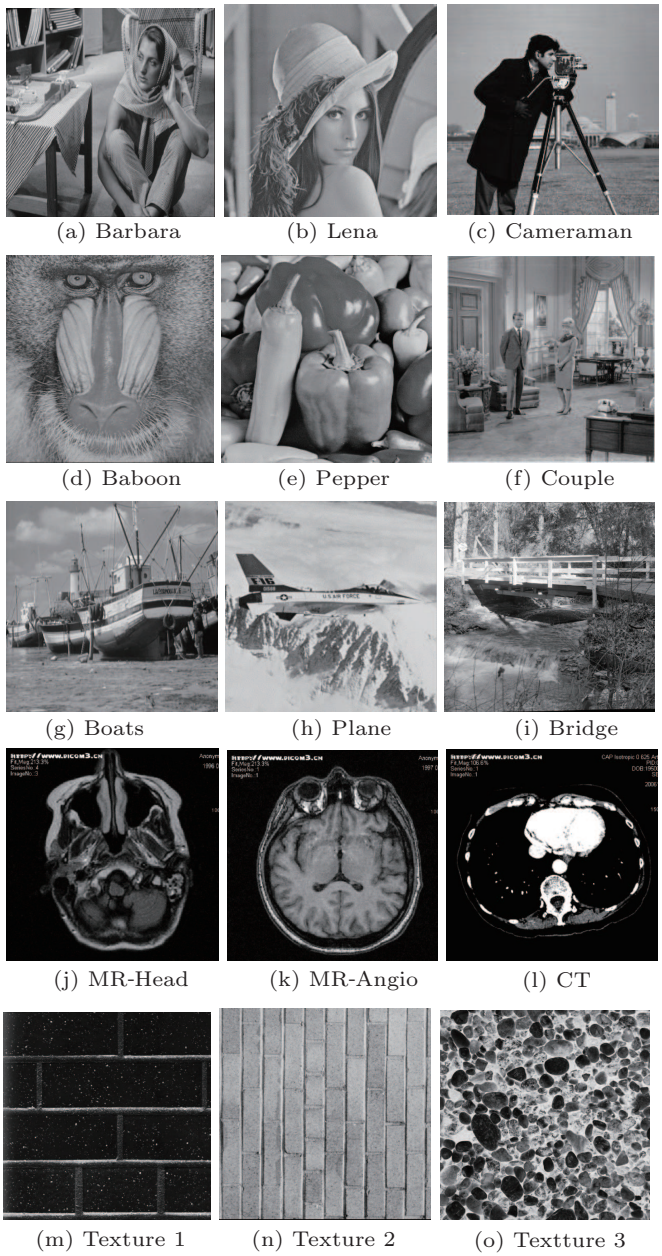


Fig. 3. Test images: (a)–(i) are nature images; (j)–(l) are medical images; (m)–(o) are texture images.

sensing matrices are generated by using a different secret key k_2. Simulations are performed on various test images shown in Fig. 3.

4.1. Security analysis

The security in the proposed algorithm is provided by the two parts, the scrambling process and the linear measurement step. The measurements as the watermarked cipher image are totally unintelligible and the attacker cannot obtain the watermark if the secret key k_2 is not leaked. Besides, only the authorized user with k_1 will obtain the decrypted image after extracting the watermark. In Ref. [27], Orsdemir *et al.* pointed out that the two possible attacks on compressive sensing-based encryption schemes for sparse signals are brute force attack and the attack based on symmetry and sparsity structure. The attack based on symmetry and sparsity structure is a more informed signal processing attack, which exploits the symmetry and sparsity structure inherent in compressive sensing. However, they have proved that the complexity of this structured attack is too high to be practical. Besides, in Ref. [16], Rachlin and Baron have analyzed the security of compressive sensing and demonstrated that CS-based encryption does not achieve Shannon's definition of perfect secrecy, but can provide a computational guarantee of secrecy (NP-hard problem). Even the attackers obtain the plaintext (the signal) and the ciphertext (the measurements), the high computational complexity makes it practically infeasible to deduce the secret key (the CS matrix). In the proposed algorithm, the DCT coefficients are scrambled for a primary security first, and then the linear measurement step provides a computational guarantee of secrecy. The overall security is improved by using two levels of encryption.

4.1.1. Key sensitivity analysis

Key sensitivity analysis is carried out to demonstrate the satisfactory security of the proposed scheme. In this experiment, we set the compression ratio $p = 0.89$. Figure 4(a) shows the watermarked cipher image 'Lena', figure 4(b) the decrypted image by using the right keys, figure 4(c) the original watermark, figure 4(d) the decrypted 'Lena' by using the wrong k_1, figure 4(e) the decrypted 'Lena' by using the wrong k_2, figures 4(f) and 4(g) demonstrate the extracted watermarks by using the wrong k_2 and the right k_2.

It is observed that the images decrypted with the wrong decryption keys do not give a clear view of the original image. This reflects high key sensitivity of the proposed encryption algorithm. A tiny change of the k_2 (from the right 0.3 to the wrong 0.30001) will cause a drastic change in the decrypted image, which shows high key sensitivity. Besides, the watermark cannot be extracted correctly, and the bit-correct rate (BCR) is only 50.003%. Security of the developed framework is evident from the achieved data confidentiality and high key sensitivity.

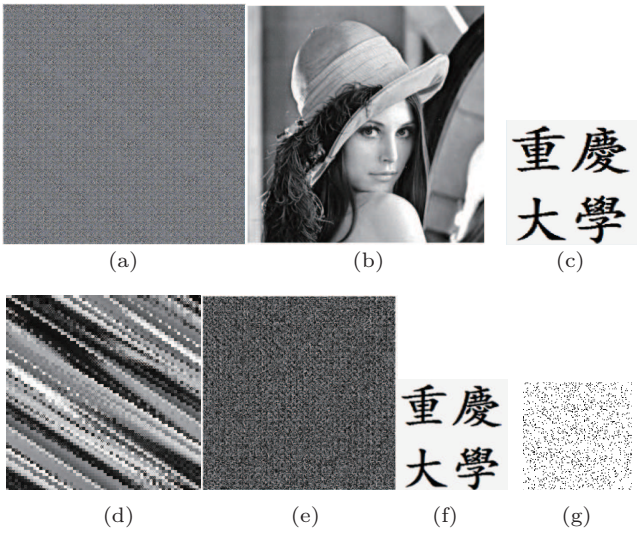


Fig. 4. Key sensitivity analyses on the proposed system: (a) the watermarked cipher image 'Lena', (b) the decrypted image by using the right keys, (c) the original watermark, (d) the decrypted 'Lena' by using the wrong k_1, (e) the decrypted 'Lena' by using the wrong k_2; (f) and (g) demonstrate the extracted watermarks by using the right k_2 and the wrong k_2.

4.1.2. Correlation coefficient analysis

We randomly select 1000 pairs of adjacent pixels (in vertical, horizontal, and diagonal directions) from the plain image and encrypted 'Lena', and calculate the correlation coefficients of two adjacent pixels according to the following formula:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{12}$$

where

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2.$$

Table 1 shows the results of correlation coefficients of the original 'Lena' and the encrypted 'Lena' by using the proposed method and other chaotic cryptosystems. The result indicates that the correlation of two pixels of the encrypted image is small. A comparison with other chaotic cryptosystems shows that the encryption effect is good.

Table 1. Correlation coefficients of the original image and the encrypted image among different algorithms.

Correlation	Vertical	Horizontal	Diagonal
Plain image (Fig. 3(b))	0.9410	0.9271	0.9821
Encrypted image (Fig. 4(a))	0.0051	–0.0078	0.0260
Encrypted image in Ref. [6]	–0.0035	–0.0574	0.0578
Encrypted image in Ref. [7]	–0.0318	–0.0965	0.0362

4.2. Watermark extraction accuracy

In this paper, the watermark with the DCT coefficient is projected into the measurements in the linear measurements step. The existing reconstruction algorithms of compressive

sensing are approximate recovery of the original signal, i.e., a process of getting the optimal solution. The watermark extraction accuracy will increase with the growth of the watermark strength (α), which is proved by the experimental results in Fig. 5. Here watermark quantity is 32768 bits.

From Fig. 5, it is clearly seen that the BCR improves continuously with the growth of α for different compression ratios. When α is bigger than 100, we can precisely extract the watermark even with compression ratio $p = 0.44$. We may draw the conclusion from Fig. 5 that watermark extraction accuracy is affected by both the compression ratio and the watermark strength. The bigger the compression ratio and the watermark strength, the greater the watermark extraction accuracy is. However, the watermark strength cannot increase infinitely, for the oversize watermark strength will seriously affect the reconstruction performance. We investigate the reconstruction performance and the relevant factors in the next subsection.

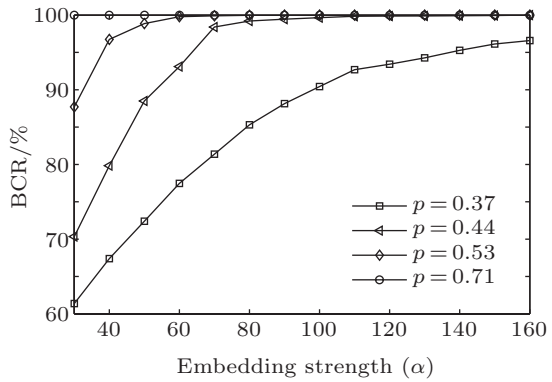


Fig. 5. BCRs versus embedding strength for different compressive ratios.

4.3. Reconstruction performance and the related factors

In our algorithm, we first extend the data in the preprocessing step, and adhere the watermark to the extended spaces. Then we compress the data in the linear measurement step. If the compressing operation is bypassed, the total data size is larger than the original one. But in practice, compression is required to save the bandwidth. In this experiment, the watermark size is 32768 bits and the watermark strength $\alpha = 100$. We know that the quality of the reconstructed image is affected by the compression ratio. The higher the compression ratio, the better the reconstructed image is.

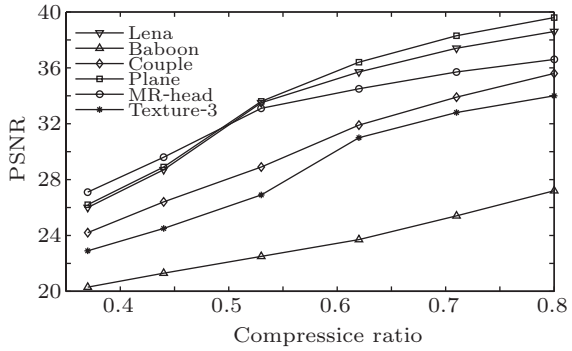


Fig. 6. PSNRs versus compression ratio for six images.

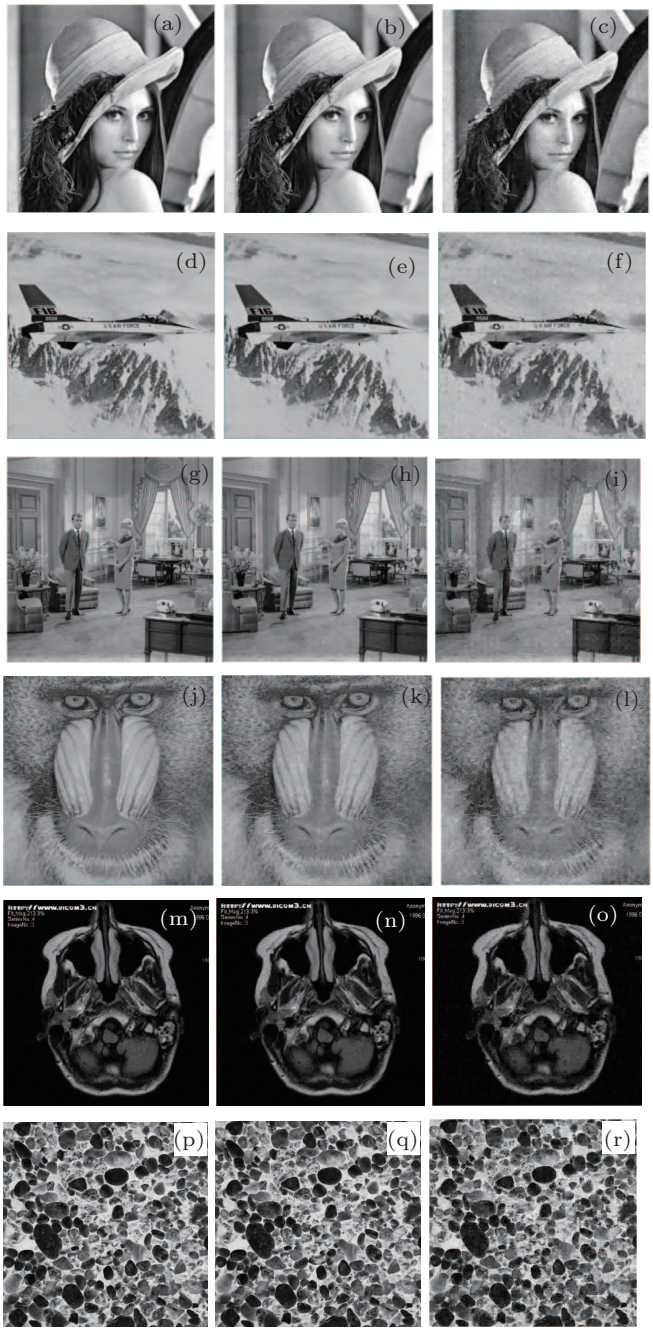


Fig. 7. The reconstructed images under different compressive ratios: (a) reconstructed Lena ($p = 0.80$, PSNR = 38.1 dB); (b) reconstructed Lena ($p = 0.53$, PSNR = 34.2 dB); (c) reconstructed Lena ($p = 0.37$, PSNR = 26.2 dB); (d) reconstructed Plane ($p = 0.80$, PSNR = 39.5 dB); (e) reconstructed Plane ($p = 0.53$, PSNR = 34.4 dB); (f) reconstructed Plane ($p = 0.37$, PSNR = 25.2dB); (g) reconstructed Couple ($p = 0.80$, PSNR = 34.8 dB); (h) reconstructed Couple ($p = 0.53$, PSNR = 30.0 dB); (i) reconstructed Couple ($p = 0.37$, PSNR = 23.2 dB); (j) reconstructed Baboon ($p = 0.80$, PSNR = 27.2 dB); (k) reconstructed Baboon ($p = 0.53$, PSNR = 22.7 dB); (l) reconstructed Baboon ($p = 0.37$, PSNR = 20.1 dB); (m) reconstructed MR-head ($p = 0.80$, PSNR = 36.6 dB); (n) reconstructed MR-head ($p = 0.53$, PSNR = 33.1 dB); (o) reconstructed MR-head ($p = 0.37$, PSNR = 27.1 dB); (p) reconstructed Texture image 2 ($p = 0.80$, PSNR = 34.0 dB); (q) reconstructed Texture image 2 (p =0.53, PSNR = 29.9 dB); (r) reconstructed Texture image 2 ($p = 0.37$, PSNR = 22.9 dB).

To verify the results, objective evaluation is performed by using peak signal-to-noise ratio (PSNR). Figure 6 shows PSNRs of the reconstructed images for different compression ratios when six test images of Lena, Couple, Plane, Baboon, MR-head, and Texture-3 are used as the original images. From Fig. 6, we can see that the smoother the original image, the better the reconstructed image is. The reason is that the smoother original image has better sparsity. Figure 7 shows the reconstructed images by using four different original images for different compression ratios.

From the previous subsection, we know that we still can precisely extract the watermark without high watermark strength when a high compression ratio is adopted. In this subsection, we investigate the relationships between the reconstructed image quality and the watermark strength for $p = 0.37$ and $p = 0.27$. Figures 8 and 9 show the reconstructed Lena images, respectively, with $p = 0.37$ and $p = 0.27$ for different watermark strengths.

From Fig. 8, in a range from 50 to 500, the increase of the watermark strength will not produce a serious decline in the reconstructed image with $p = 0.37$. The PSNRs of the reconstructed images fluctuate within a certain range. However, a serious decline in the reconstructed image quality will be generated by increasing the watermark strength with $p = 0.27$ as shown in Fig. 9.



Fig. 8. For compressive ratio $p = 0.37$, the reconstructed Lena images with $\alpha = 50$, 200, 350, 500 and their PSNRs 26.8, 26.9, 26.5, and 26.7 (dB)

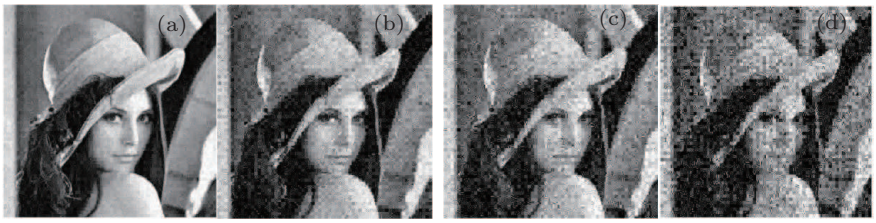


Fig. 9. For compressive ratio $p = 0.27$, the reconstructed Lena images respectively with $\alpha = 50$ (a), 200 (b), 350 (c), 500 (d) and their PSNR = 24.0 (a), 17.4 (b), 15.2 (c), and 11.9 (d) (dB).

We can conclude that compression ratio and watermark strength will have an effect on the reconstructed image quality. In the proposed method, the trade-off between the watermark extraction accuracy and the reconstructed image quality will be considered when compression ratio is relatively low.

4.4. Watermarking capacity analysis

In our method the watermark is not directly embedded in the spatial or transform domain, which is different from that in other watermarking algorithms. The pre-processed watermark and transformation coefficient are projected into the measurements in steps of linear measurements. Before this, the watermark is stored independently of the DCT coefficients. So the watermark quantity can be subjected to no constraints. However, the watermark quantity cannot be infinite by considering the increased data size and the quality of the reconstructed image. The trade-off between the watermark quantity and the quality of the reconstructed image should be considered in practice.

Table 2. Reconstruction performances under different watermark quantities.

Watermark quantity (bits)	32768	65535	98304	131072
Compression ratio	0.89	0.80	0.72	0.67
	PSNR/dB			
Lena	39.7	37.4	33.2	27.3
Plane	40.2	37.9	33.3	27.9
Couple	36.5	33.9	30.0	25.2
Baboon	28.5	27.9	24.6	21.0

A larger number of experiments have been done to study the influence of watermark quantity on the quality of the reconstructed image. In this subsection, we fix the sampling number in the sampling process, and make the size of the cipher image equal to the original image. Table 2 shows the PSNRs of the reconstructed images with different watermark quantities for four original images. From Table 2, we can see

that more watermark quantity will cause lower PSNR, with sampling number fixed. But in the field of network multimedia data security, the watermarking capacity of the proposed method is already enough.

4.5. Robustness against packet loss and distortion

In this subsection, we discuss the effectiveness of our scheme when the received cipher image is incomplete or affected by noise, namely the anti-packet loss performance and the robustness against distortion. We encrypt and watermark the test images using the new scheme. Simulations are performed on the test images in Fig. 3. However, for the limitation of space in this paper, only the results for 'Lena' image are illustrated here.

From Figs. 10(a)–10(d), it is clear that we can still extract an understandable watermark even if the received cipher image is incomplete. Figures 10(d)–10(h) show the decrypted images for different packet loss ratios. The authorized user can still decrypt an understandable plain-image even though the received cipher image is incomplete. These experiments indicate that the proposed method has the robustness against packet loss.

From Fig. 11, the ability to resist the distortion of the ciphered image is analyzed. Although it cannot ensure the exact recovery of the original image and accurate exaction of the watermark, an understandable reconstructed image can be obtained and an understandable watermark can be extracted. This indicates that the proposed method has robustness against distortion.

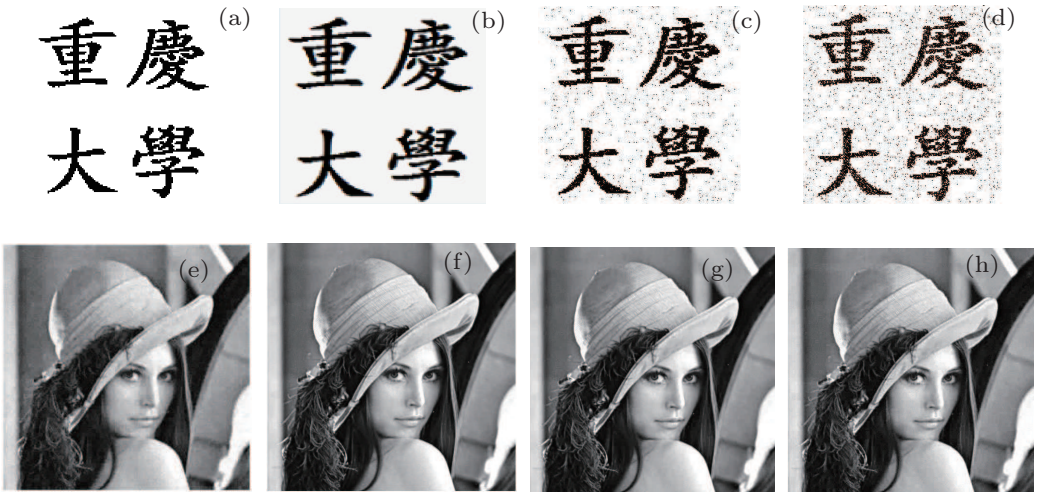


Fig. 10. Watermark extractions for different packet loss ratios: (a) the extracted watermark without packet loss; (b) the extracted watermark with 10% packet loss; (c) the extracted watermark with 30% packet loss; (d) the extracted watermark with 50% packet loss; (e) the decrypted image without packet loss (PSNR = 39.7 dB); (f) the decrypted image with 10% packet loss (PSNR = 37.9 dB); (g) the decrypted image with 30% packet loss (PSNR = 34.6 dB); (h) the decrypted image with 50% packet loss (PSNR = 31.2 dB).

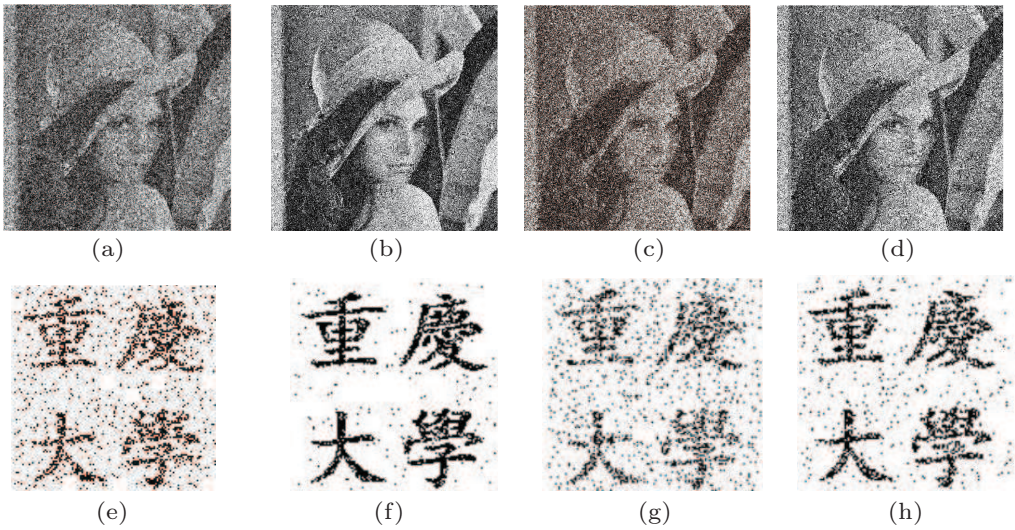


Fig. 11. Decrypted images and the extracted watermarks when the ciphered image is affected by noise: (a) 1% Gauss noise; (b) 1% salt and pepper noise; (c) 2% Gauss noise; (d) 2% salt and pepper noise; (e) 1% Gauss noise; (f) 1% salt and pepper noise; (g) 2% salt and pepper noise; (h) 2% salt and pepper noise.

5. Comparative analysis

Compared with the separate encryption algorithms in Refs. [5]–[7], the proposed algorithm has no advantage in the execution time, for the utilization of CS will need matrix computation with high complexity. The proposed algorithm features the combination between encryption and watermarking functionalities.

Besides, compared with other joint encryption and watermarking algorithms in Refs. [9] and [12] in terms of compressible cipher image size, flexible watermark capacity, lossless watermark extraction from the compressed cipher image, and robustness against packet loss, only the proposed algorithm can achieve all the four desired characteristics as shown in Table 3.

Table 3. Comparison of our proposed algorithm with other algorithms.

Method	Lian[9]	Teneja'[12]	Proposed
Compressible cipher image size	×	√	√
Flexible watermark capacity	×	×	√
Lossless watermark extraction from the compressed cipher	×	×	√
Robustness against packet loss	×	×	√

6. Conclusions

In this paper, a novel joint image encryption and watermarking algorithm is presented. The algorithm is based on compressive sensing and a chaotic map. The proposed method possesses some characteristics as follows. (i) Cipher image size is compressible and watermark capacity can be flexibly adjusted according to the need. (ii) The watermark can be extracted precisely even if the cipher image is compressed. Both compressive sensing and Arnold transformation are used for high security. (iii) Both the watermark and cipher image are robust against packet loss. (iv) It is secure. Thus, it has high potential to be adopted for network multimedia security application.

References

[1] Cox I J, Doërr G and Furon T 2006 *Digital Watermarking* (Berlin/Heidelberg: Springer) pp. 1–15

[2] Wang X Y and Teng L 2012 *Chin. Phys. B* **21** 020504

[3] Tong X J, Wang Z and Zuo K 2012 *Chin. Phys. B* **21** 020506

[4] Xiao D and Xie Y J 2013 *Acta Phys. Sin.* **62** 240508 (in Chinese)

[5] Liu H J and Wang X Y 2010 *Comput. Math. Appl.* **59** 3320

[6] Liu H J and Wang X Y 2011 *Opt. Commun.* **284** 3895

[7] Wang X Y, Teng L and Qin X 2012 *Signal Processing* **92** 1101

[8] Khan M I, Jeoti V, Malik A S and Khan M F 2011 *Proceedings of the 17th Asia-Pacific Conference on Communications*, October 2–5, 2011, Sabah, Malaysia, p. 816

[9] Lian S G, Liu Z X, Zhen R and Wang H L 2006 *Opt. Eng.* **45** 080510

[10] Lian S, Liu Z, Ren Z and Wang H 2007 *IEEE T. Circ. Syst. Vid.* **17** 774

[11] Cancellaro M, Battisti F, Carli M, Boato G, De Natale F G B and Neri A 2008 *Proc. SPIE, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X* **6819** 68191C

[12] Taneja N, Bhatnagar G, Raman B and Gupta I 2013 *Multimedia Tools Appl.* **67** 593

[13] Lian S G 2009 *Multimedia Tools Appl.* **43** 91

[14] Donoho D L 2006 *IEEE Trans. Inf. Theory* **52** 1289

[15] Li X, Qin S Y 2011 *IET Image Process.* **5** 141

[16] Rachbin Y, and Baron D 2008 *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, September 23–26, 2008, UIUC, Illinois, USA, p. 813

[17] Mayiami M R, Seyfe B and Bafghi H G 2010 arXiv: 1011.3985 [cs.IT]

[18] Zhang X P, Ren Y L, Feng G R and Qian Z X 2011 *Proceedings of the Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, October 14–16, 2011, Dalian, China, p. 222

[19] Liu D H, Shi G M, Gao D H and Gao M 2009 *Proceedings of the International Conference on Wireless Communications & Signal Processing*, November 13–15, 2009, Nanjing, China, p. 1

[20] Huang H C, Chang F C, Wu C H and Lai W H 2012 *Proceedings of the Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, July 18–20, 2012, Piraeus, Greece, p. 223

[21] Veena V K, Jyothish Lal G, Vishnu Prahu S, Sachin Kumar S and Soman K P 2012 *Proceedings of the International Conference on Machine Vision and Image Processing*, December 14–15, 2012, Taipei, China, p. 105

[22] Candès E J and Wakin M B 2008 *IEEE Signal Process. Mag.* **25** 21

[23] Dai W and Milenkovic O 2009 *IEEE Trans. Inf. Theory* **55** 2230

[24] Yu L, Barbot J P, Zheng G and Sun H 2010 *IEEE Signal Proc. Lett.* **17** 731

[25] Gao Z R, Xiong C Y, Zhou C and Wang H X 2011 *Proceedings of the International Conference on Multimedia and Signal Processing*, May 14–15, 2011, Guilin, China, p. 321

[26] Gan L 2007 *Proceedings of the International Conference on Digital Signal Processing*, July 1–4, 2007, Cardiff, UK, p. 403

[27] Orsdemir A, Altun H O, Sharma G and Bocko M F 2008 *Proceedings of the Military Communications Conference*, November 16–19, 2008, San Diego, USA, p. 1