IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 19, 2019, accepted January 28, 2019, date of publication February 5, 2019, date of current version March 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2897721

A Novel Image Encryption Scheme Based on Nonuniform Sampling in Block Compressive Sensing

LIYA ZHU[1], HUANSHENG SONG[2], XI ZHANG[3], MAODE YAN[1], LIANG ZHANG[1], AND TAO YAN[4]

[1]School of Electrics and Control Engineering, Chang'an University, Xi'an 710064, China
[2]School of Information Engineering, Chang'an University, Xi'an 710064, China
[3]School of Aeronautics and Astronautics Engineering, Air Force Engineering University, Xi'an 710038, China
[4]Aviation Maintenance School for NCO, Air Force Engineering University, Xinyang 464000, China

Corresponding author: Liya Zhu (lyzhu@chd.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572083, in part by the Natural Science Foundation of Shaanxi Province under Grant 2018JQ6017 and Grant 2018JM6023, in part by the Innovation Team Funds for the Central Universities of Chang'an University under Grant 300102328403, in part by the Fundamental Research Funds for the Central Universities of Chang'an University under Grant 300102328110 and Grant 300102328109, and in part by the School-Enterprise Cooperation Funds of CETC-27 under Grant 220032160348.

ABSTRACT This paper devotes to the image compression and encryption problems. We develop a novel hybrid scheme based on block compressive sensing. Concentrate on taking full advantage of the different frequency coefficients sparsity, the nonuniform sampling strategy is adopted to improve the compression efficiency. First, the discrete cosine transform coefficients matrices of blocks are transformed into vectors by zigzag scanning. The different frequency components are extracted in the front, middle, and back of vectors, respectively. Using the measurement matrices with different dimensions, the combination of low- and high-frequency components, together with the medium-frequency coefficients are compressed simultaneously. Second, the recombinational block measurements are re-encrypted by the permutation-diffusion framework. The logistic map is introduced for key stream generation. In order to accomplish a sensitive and effective cryptosystem, the control strategy for secret keys is employed. The simulation results indicate that the proposed scheme forms a high balance between reconstruction performance, storage and computational complexity, and hardware implementation. Moreover, the security analyses demonstrate the satisfactory performance and effectiveness of the proposed cryptosystem. The scheme can work efficiently in the parallel computing environment, especially for the images with medium and large size.

INDEX TERMS Block compressive sensing, image cryptosystem, logistic map, nonuniform sampling strategy.

I. INTRODUCTION

Image encryption is an efficient and imperative solution to ensure the image information security and withstand various attacks by the hacker. Some researchers investigated the encryption architectures for secure image transmission using DNA coding [1], asymmetric optical encryption [2], cellular automaton [3], etc. Because of the properties of chaotic system including ergodic and high sensitivity to initial conditions, some encryption algorithms chaos-based [4]–[7] were widely employed in the encryption process. Moreover, some researchers noticed the fact that noise-like or texture-like cipher images can easily catch hacker's attention and then be attacked, so the visually meaningful encryption schemes [8], [9] were proposed to avoid the security weakness.

Recently, some image encryption schemes based on compressive sensing (CS) have been proposed. In general, these cryptosystems were regarded as the solutions for image compression and encryption simultaneously. Essentially, CS encryption framework is the linear measurement process of plaintext, and it also determines the quality of decrypted image. It could provide a secret layer when the measurement matrix is kept secret. Although CS framework

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran Tariq.

can guarantee the computation secrecy [10], it is vulnerable to the chosen-plaintext attack because of the linearity [11]. In the pursuit of better security performance, some hybrid cryptosystems based on CS and conventional encryption methods were investigated, such as combining with double random phase encoding (DRPE) [12], [13], elementary cellular automata [14], visually meaningful ciphertext [15] and chaotic map [16]–[24], etc.

For the purpose of better compression and reconstruction performance, some algorithms were exploited in the CS procedure. In [17], Zhang *et al.* demonstrated the random permutation of sparse coefficients could effectively relax the restricted isometry property (RIP) for CS, and the reconstruction performance was enhanced around 2-6 dB at the same compression ratio. An image compression-encryption hybrid scheme based on the synthesis sparse model was proposed by Zhang *et al.* [22]. Via the overcomplete fixed dictionary and pixel-scrambling, the sparse representation could be obtained and re-encrypted. The simulation results validated a considerable compression performance with a good security. To decrease the data volume of encrypted image, 2D CS was employed in [23] and [24]. The plaint image was measured and encrypted twice via CS in two directions, so the encryption scheme could achieve better compression performance. In the abovementioned algorithms, CS framework was performed column by column, which was termed as parallel compressive sensing (PCS). However, the more computational time and memory storage are consumed as the dimension of image increasing.

To address this problem, a block compressive sensing (BCS) framework was proposed in [25]. The nonoverlapping blocks were represented in discrete cosine transform (DCT) or discrete wavelet transform (DWT) domain and compressed using the same size measurement matrices. Some compression-encryption algorithms based on BCS were proposed. For example, in [26], the image was first divided into some blocks, and then each block was encrypted with separate keys generated by linear feedback shift register (LFSR). The entropy encoding was performed as further security. Regrettably, more details and security analyses were not presented. In [27], the plain image blocks were measured, and the quantized measurement vectors were re-encrypted by Arnold scrambling, mixing, S-box and block-wise XOR operation in sequence. All these steps could be carried out efficiently in the parallel environment.

However, although the block cipher structure could reduce the compression complexity and improve the performance, the sparse characteristic of block coefficient was neglected due to the common uniform sampling in BCS process. A nonuniform sampling strategy in BCS was proposed by Zhou *et al.* [28]. The high-frequency component of DCT coefficients was measured by common CS and low-frequency component was not compressed. A significant increase in performance was observed but robustness was weakened in the meantime.

In this paper, a novel image compression-encryption hybrid scheme is presented, which consists of two primary stages with the first is BCS phase and the second is re-encryption procedure. We focus on improving the compression efficiency via the nonuniform sampling model. Unlike the proposed algorithm in [28], all frequency components are measured as different tactics to guarantee the robustness. Due to the "energy compaction" property of DCT, the coefficient matrix of each block is divided into three parts: the low-frequency component (LFC) located in the upper left corner, the high-frequency component (HFC) located in the lower right corner, and the relative "medium-frequency" component (MFC) filled in the middle. The combination of LFC and HFC, together with MFC are compressed simultaneously with the different compression ratios. In the following re-encryption procedure, the compressed blocks are re-encrypted by the typical permutation-diffusion algorithm to enhance the security performance. In the encryption scheme, logistic map is employed for key stream generation. One key is used for constructing the measurement matrix of BCS, and three keys are utilized in the forward diffusion, permutation and backward diffusion procedure, respectively.

Our contributions are as follows:

Firstly, the nonuniform sampling strategy in BCS phase can achieve the better performance by adjusting the parameters appropriately. Moreover, the identical measurement matrices are employed for different blocks, which is more suitable for parallel computing.

Secondly, the control strategy is introduced to solve the problem that cryptosystem is not sensitive to the BCS key. To be specific, one of re-encryption keys is controlled by the key of BCS. Numerical simulations and security analyses well validate the effectiveness and security of the proposed scheme.

The rest of the paper is organized as follows. Some fundamental knowledge is introduced in Section II. In Section III, the proposed encryption scheme is described. Simulation results are given in Section IV. Security performance analyses are presented in Section V. Finally, a brief conclusion is drawn in the last section.

II. FUNDAMENTAL KNOWLEDGE

A. BLOCK COMPRESSIVE SENSING

The CS is a popular algorithm based on sparse theory, and it can sample and compress the signal simultaneously. Suppose that a 1-D signal x with length of N can be represented as:

$$x = \sum_{i=1}^{N} \alpha_i \Psi_i = \Psi\alpha \tag{1}$$

where Ψ denotes the $N \times N$ orthogonal basis matrix and α is the transform coefficients of x in the Ψ domain. If there are K non-zero values, where $K \ll N$, x is termed as K-sparse. The linear measurement process by matrix Φ is denoted as:

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

where Φ is a measurement matrix with size of $M \times N$, y is a compressed vector with length of M, where $M \ll N$. Based

on Eqs. (1) and (2), the overall sampling process is as follows:

$$y = \Phi x = \Phi\Psi\alpha = \Theta\alpha \tag{3}$$

where Θ is the sensing matrix, it is the product of Φ and Ψ.

If x is K-sparse, in order to recover x from y correctly, Θ should satisfy the RIP condition [29]. The problem of estimating the sparse solution can be expressed as:

$$\min \ ||\alpha||_0 \quad s.t.\ y = \Phi\Psi\alpha \tag{4}$$

where $||\alpha||_0$ denotes the l_0-norm of α. This is a non-convex and NP-hard problem. It can be solved by converting a convex optimization problem [30], so Eq. (4) can be transformed to

$$\min \ ||\alpha||_1 \quad s.t.\ y = \Phi\Psi\alpha \tag{5}$$

Several reconstruction algorithms have been proposed such as matching pursuit (MP), orthogonal matching pursuit (OMP) [31], smoothed l_0 norm (SL_0) [32] and so on.

For two-dimensional image, BCS framework [25] was proposed by Gan *et al*. to decrease the computational cost and memory storage. Firstly, the image with size of $N \times N$ is divided into small non-overlapping blocks with size of $B \times B$. Secondly, the coefficient matrix in the Ψ domain is transformed into one-dimensional vector x, and the corresponding output vector y can be written as:

$$y_i = \Phi_B x_i \tag{6}$$

where x_i represents the vectorized signal of the i-th block through raster scanning. Φ_B is the measurement matrix with size of $n_B \times B^2$, where $n_B = \lfloor CR \times B^2 \rfloor$, CR represents the compression ratio. For the whole image, the equivalent sampling operator Φ is a block diagonal matrix taking the following form,

$$\Phi = \begin{bmatrix} \Phi_B & & & \\ & \Phi_B & & \\ & & \ddots & \\ & & & \Phi_B \end{bmatrix} \tag{7}$$

From above, one can see that a measurement matrix with size of $n_B \times B^2$ is stored, rather than a full $(CR \times N^2) \times N^2$ one. So BCS could save storage space. Besides, it could decrease the computation time and offer better reconstruction performance. However, there is a trade-off to determine the block dimension. It is worth noting that BCS will cause blocking artifacts in the partial block regions of reconstruction image, especially for the small block dimension or low compression ratio.

In the above measurement process, all the coefficients of block are measured by the same measurement matrix, which is regarded as uniform sampling. This model is simple but neglecting the sparsity of coefficients, which would affect the reconstruction performance. In this paper, similar to the JPEG compression process, the block DCT coefficient matrix is firstly transformed into vector by zigzag scanning, then LFC, MFC and HFC can be extracted in the front, middle and back of vector, respectively. LFC is the major factor influencing on recovery performance, however, it is not sparse. HFC is suitable to compress because of sparsity, but it have little or no effect on quality of reconstruction image.

If MFC and HFC are compressed, and LFC is transmitted directly, just like in [28], the performance of algorithm is optimal. But the problem of poor robustness is hard to be solved, especially for noise and cropping attack. If LFC is compressed as well, the performance of reconstruction would decrease because it is not sparse. To seek the balance between robustness and recovery performance, we try to combine LFC and HFC into the low & high-frequency component (LHFC), so it is sparse enough to be compressed. Base on this spot, the nonuniform sampling and reconstructing scheme of BCS is proposed. The flow chart of nonuniform sampling model is shown in Figure 1, and the detailed analyses of performance are described in Section IV.

B. LOGISTIC MAP

The chaotic system is often exploited in the image encryption process because it can generate the pseudorandom sequence and be sensitive to the initial value. The common chaotic system includes logistic map, tent map, Arnold map, hyper-chaotic system and so on. In this paper, logistic map is used to generate the pseudorandom sequence, and it is defined as:

$$x_{n+1} = \mu x_n (1 - x_n), \quad x_n \in (0, 1) \tag{8}$$

when the parameter $\mu \in [3.57, 4]$, the slight variation of initial value would yield dramatically different results, that to say, the system is chaotic.

C. PERMUTATION

Permutation is an image encryption algorithm which locations of pixels are shuffled with the gray values unchanged. In this paper, the modified permutation algorithm [33] based on Arnold map is adopted to save computation time. The process is described as follows:

(1) Resize the original image into 1-D vector;

(2) Assume $(1, j)$ is the initial coordinate position of pixel, according to Arnold map:

$$\begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} 1 \\ j \end{bmatrix} \tag{9}$$

we can get,

$$p = 1 + a \times j \tag{10}$$

$$q = b + (ab + 1) \times \mathrm{j} \tag{11}$$

(3) In Eq. (11), q is determined by two pseudorandom variables including b and $(ab+1)$. To scramble the 1-D vector using Arnold map, the pseudorandom variable $(ab + 1)$ can be regard as a new variable and still defined as a, that is:

$$q = b + a \times j \tag{12}$$

so the $(1, j)$ and $(1, q)$ pixels are swapped according to Eq. (12).

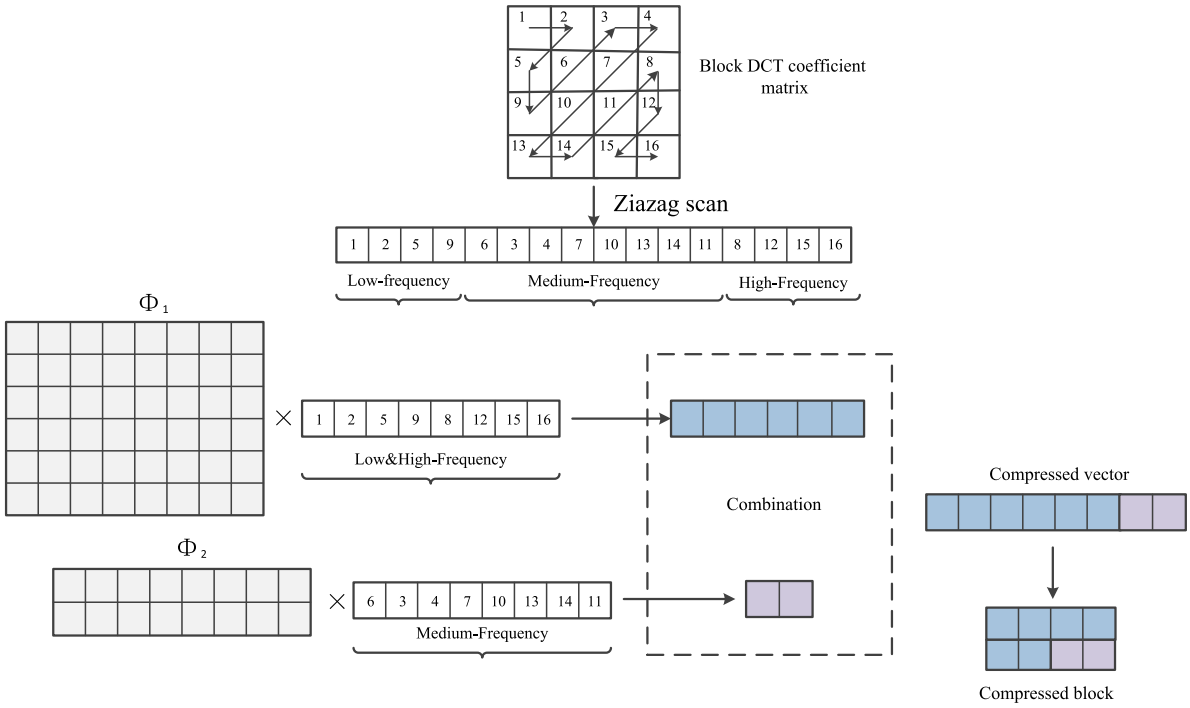


FIGURE 1. The flow chart of nonuniform sampling for block coefficient matrix.

(4) Resize the vector into the matrix. The pixels scrambling process is finished.

D. DIFFUSION

Diffusion is modifying the pixel values without changes of coordinate positions. In order to resist against the known-plaintext or chosen-plaintext attack, the diffusion is indispensable [11]. To enhance the effect of diffusion, in the paper, the diffusion process includes the forward and backward diffusion [33], which is described as follows:

(1) Forward diffusion: Modify the pixel values of plain vector sequentially from the first pixel to the last pixel according to:

$$C_i = (C_{i-1} + S_i + P_i) \ mod \ 256 \tag{13}$$

where C_i, C_{i-1}, S_i and P_i are the output cipher-pixel, the previous cipher pixel, key stream and the current plain pixel, respectively.

The corresponding inverse algorithm is Eq. (14)

$$P_i = (2 \times 256 + C_i - C_{i-1} - S_i) \ mod \ 256 \tag{14}$$

(2) Backward diffusion: Modify the pixel values sequentially from the last pixel to the first pixel according to:

$$C_i = (C_{i+1} + S_i + P_i) \ mod \ 256 \tag{15}$$

The corresponding inverse algorithm is Eq. (16):

$$P_i = (2 \times 256 + C_i - C_{i+1} - S_i) \ mod \ 256 \tag{16}$$

III. THE PROPOSED CRYPTOSYSTEM

A. ENCRYPTION PROCESS

The schematic of the proposed encryption scheme is illustrated in Figure 2. It consists of two primary procedures including BCS and re-encryption. All of chaotic sequences are generated from logistic map, and the initial values serve as the secret keys. The partial Hadamard matrix is selected as the measurement matrix because it can achieve the high reconstruction performance and be friendly to hardware. The encryption process is described as follows:

PREPARATION

Construct the measurement matrix controlled by secret key [23], the steps are as follows:

(1) Generate a chaotic sequence with length of $1000+z$ by logistic map, where k_1 is the initial value and z is the length of desired chaotic sequence, then discard the preceding 1000 values and obtain the sequence $s = [s_1, s_2, \ldots, s_z]$.

(2) Sort the sequence s with the ascending order and get the new sequence s'.

(3) Search the values of sequence s in s', and get the corresponding index sequence $i = [i_1, i_2, \ldots, i_z]$.

(4) Construct the Hadamard matrix H with size of $d \times d(d \geq z)$, then group the corresponding row vectors of H into matrix Φ according to the index sequence i.

$$\Phi = [H\,(i_1, :)\,; H\,(i_2, :)\,; \ldots; H\,(i_z, :)]$$

where $H(i_z, :)$ denotes the i_z-th row vector of H.

So we can obtain the partial Hadamard matrix controlled by initial value k_1.

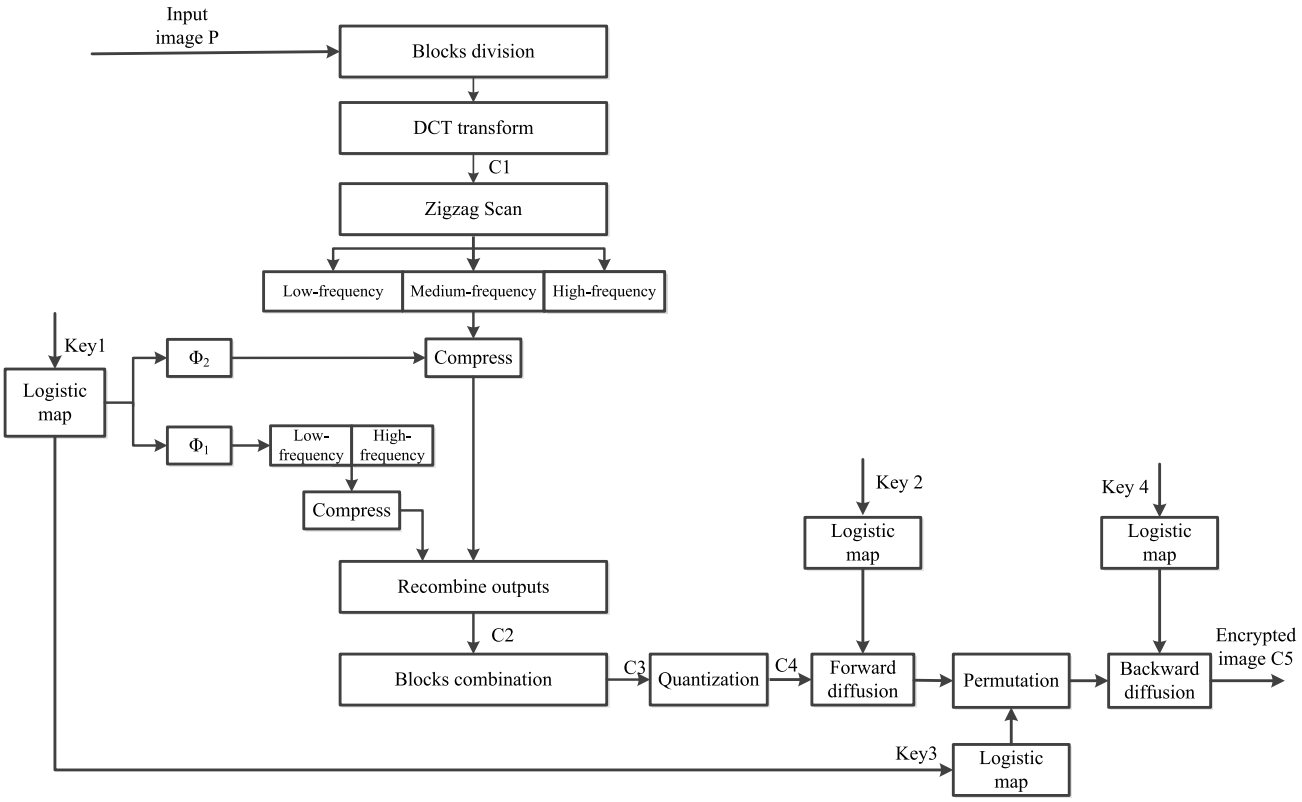


FIGURE 2. The schematic of the proposed encryption system.

Step 1: Divide the plain image $P(M \times N)$ into several non-overlapping blocks with size of $m \times n$, considering the limitation of partial Hadamard matrix, where one of the dimensions can be divisible by 4, and the other can be divisible by 2, 3 or 5.

Step 2: For each block, compression procedure is described as follows:

(1) Scan the DCT coefficient matrix $C1$ with zigzag order and get a one-dimension vector α.

(2) Partition the vector α into three parts including LFC, MFC and HFC according to the proper proportion. Combine LFC and HFC into the vector α_{LH}, and the MFC is named as α_M.

(3) Compress the vector α_{LH} and α_{M} using the corresponding measurement matrices, and recombine the outputs into a vector β.

(4) Resize the vector β into the matrix $C2$ with size of $m' \times n$, where $m' = round(m \times CR)$ and CR represents the average compression ratio for each block.

Step 3: Recombine these matrices together and obtain the matrix $C3$ with size of $M' \times N$, where $M' = round(M \times CR)$.

Step 4: Before re-encryption, we must perform the quantization process [20] which could convert the values of $C3$ within the range of [0, 255] by the linear mapping, and the auxiliary parameters $coff1$ and $coff2$ are defined as:

$$coff1 = \frac{255}{max - min} \tag{17}$$

$$coff2 = \frac{255 \times min}{max - min} \tag{18}$$

where max and min are the maximum and minimum value of the matrix $C3$, respectively. So we can obtain the matrix $C4$ according to Eq. (19).

$$c_{4i} = round(coff1 \times c_{3i} - coff2) \tag{19}$$

where c_{3i} and c_{4i} are the i-th elements of $C3$ and $C4$, respectively.

Step 5: Re-encryption procedure is described as follows:

(1) Resize the matrix $C4$ into a vector γ_1, then perform the forward diffusion process and obtain the vector γ_2, where the pseudorandom sequence is generated by logistic map with the initial value k_2.

(2) Scramble the pixels of γ_2 and obtain the vector γ_3 according to Eq. (12). The permutation order comes from the pseudorandom index sequence generated by logistic map with the initial value k_3.

(3) Perform the backward diffusion process using the initial value k_4, and obtain the vector γ_4, then resize the vector γ_4 into the matrix $C5$. This is just the final encrypted image.

B. DECRYPTION PROCESS

The decryption process is the inverse process of encryption. From the cipher image C, we can decrypt and reconstruct to get the plain image following the steps as below:

Step 1: Decrypt the cipher image as follows:

(1) Reshape C into a vector δ_1, then execute the inverse algorithm of backward diffusion according to Eq. (16) and obtain the vector δ_2.

(2) Perform the inverse permutation and get the vector δ_3.

(3) Execute the inverse algorithm of forward diffusion according to Eq. (14), and obtain the vector δ_4. Resize the vector δ_4 into the matrix $P1$.

Step 2: For $P1$, carry out the linear scaling according to Eq. (20) and obtain the matrix $P2$, where the parameters $coff1$ and $coff2$ are gotten from the sender.

$$p_{2i} = \frac{p_{1i} + coff\,2}{coff\,1} \tag{20}$$

Step 3: Divide the matrix $P2$ into several non-overlapping blocks with size of $m' \times n$.

Step 4: For each block, the reconstruction procedure is described as follows:

(1) Transform the block into vector ε, and then partition it into two parts ε_{LH} and ε_M according to the corresponding proportions.

(2) Reconstruct the LFC, MFC and HFC exploiting the corresponding measurement matrices.

(3) Recombine the different frequency components into a new vector, manipulate inverse zigzag order on it, and obtain matrix $P3$ with size of $m \times n$.

(4) Apply inverse discrete cosine transform to $P3$ and get the block image $P4$.

Step 5: Recombine the matrices $P4$ and obtain the matrix $P5$ with size of $M \times N$. This is just the decrypted image.

C. DISCUSSION

It is noteworthy that the relationship among secret keys. In Figure 2, k_1 is used for constructing the measurement matrix to compress the block DCT coefficients, k_2, k_3 and k_4 are used in the forward diffusion, permutation and backward diffusion procedure for the whole image, respectively. Assume these secret keys are independent of each other, which leads to a problem that the cryptosystem is not sensitive to k_1. For example, when the deviation 1×10^{-2} to k_1 in decryption system and others unchanged, the corresponding decrypted image is shown in Figure 3. It is obviously that outline of decrypted image can be identified. The reason is that the compression and reconstruction are performed within the limits of block, so the deviation of k_1 only causes the error propagation within the corresponding block of decrypted image, not spread to the whole image.

To overcome this problem, we try to achieve the goal that the errors of each block can be propagated to the whole image. A feasible solution is to adopt the control strategy, specifically, one key of re-encryption is controlled by the BCS key. In the proposed cryptosystem, the secret keys are set as four random values from 0 to 1. Considering the output of logistic map also meet the above requirements, similar to Eq. (8), k_3 (or k_2, k_4) can be defined as:

$$k_3 = \mu k_1 (1 - k_1) \tag{21}$$

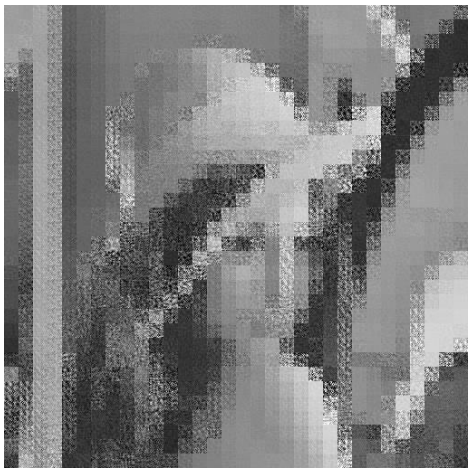


FIGURE 3. The decrypted image with the wrong k_1 when all keys are independent.

In this way, the key of re-encryption would vary as the BCS key changing.

IV. SIMULATION RESULTS

In this section, four different images with size of 512×512 pixels: Lena, Pepper, Barbara and Baboon are served as plain images. All the experiments in this paper are conducted in a personal computer with Core i7-6700 CPU @2.90GHz, 8GB RAM. Software Version: MATLAB 2016a. Assume the proportions of LFC, MFC and HFC are defined as p_1, p_2 and p_3, respectively. For the whole image, the average compression ratio (CR) can be calculated by:

$$CR = (p_1 + p_3) \times cr_1 + p_2 \times cr_2 \tag{22}$$

where cr_1 and cr_2 are corresponding compression ratios of LHFC and MFC.

In the simulation, the parameters of chaotic system are $k_1 = 0.23, k_2 = 0.94, k_4 = 0.61, \mu = 3.99$, respectively. The parameters of BCS are $p_1{:}p_2{:}p_3 = 5{:}6{:}5$, $cr_1 = 12/16$, $cr_2 = 1/12$ and the block size is 16×16. According to Eq. (22), $CR = 0.5$. In the reconstruction process, SL_0 algorithm is employed.

In order to evaluate the quality of decrypted images, the peak signal to noise ratio (PSNR) is introduced as follows:

$$\mathrm{PSNR} = 10\log_{10}(\frac{255^2}{MSE}) \tag{23}$$

where MSE denotes the mean square error, and it is defined as:

$$\mathrm{MSE} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (R(x, y) - I(x, y))^2 \tag{24}$$

where $R(x, y)$ and $I(x, y)$ represent the recovery image and input image, respectively.

The simulation results are shown in Figure 4, where the plain images, the corresponding histograms of plain images, the corresponding cipher images, the corresponding histograms of cipher images and the decrypted images are listed

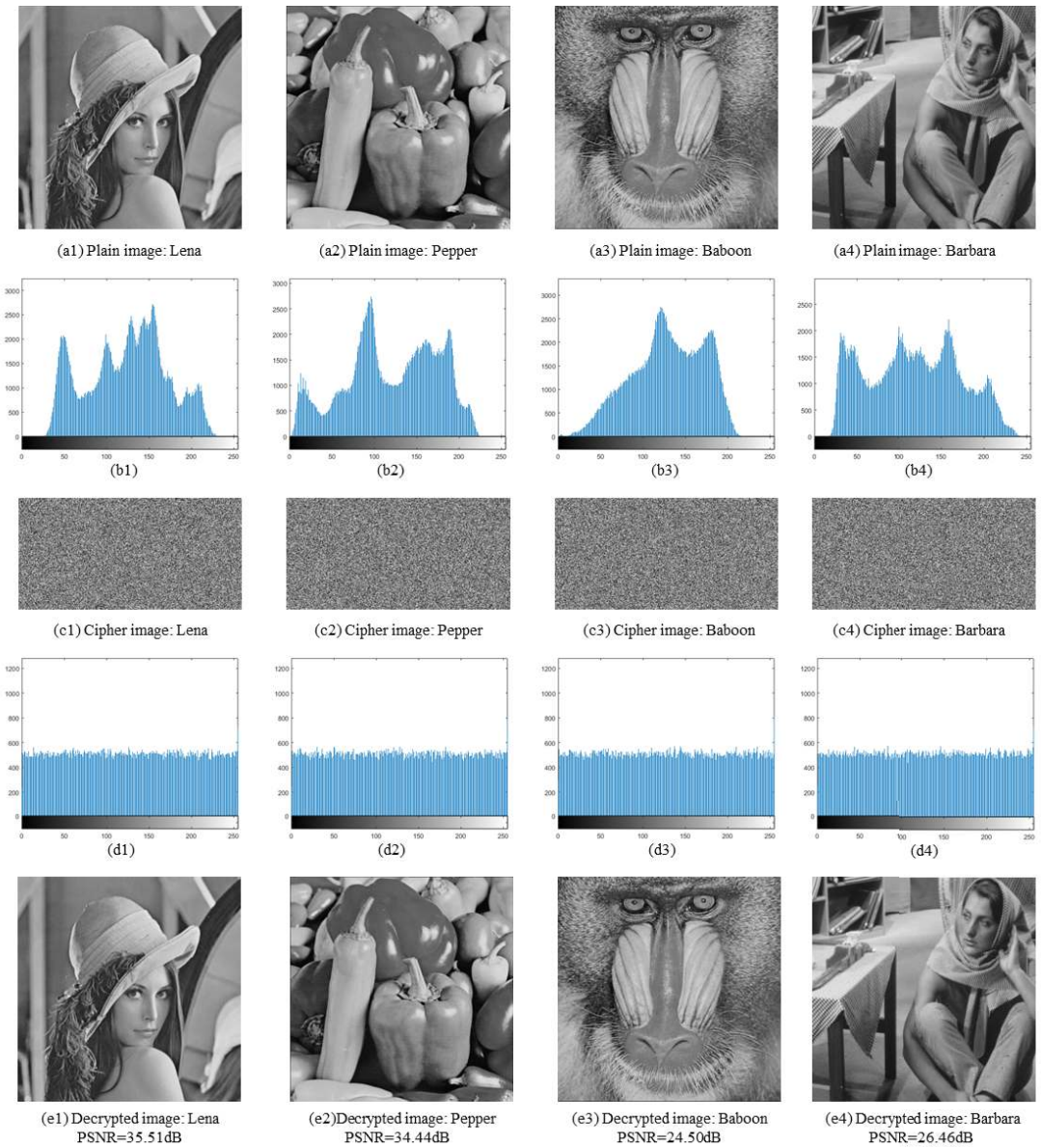


FIGURE 4. Simulation results: (a1)-(a4) are four plain images, (b1)-(b4) are the corresponding histograms of plain images, (c1)-(c4) are the corresponding cipher images, (d1)-(d4) are the corresponding histograms of cipher images, (e1)-(e4) are the corresponding decrypted images, respectively.

from the first to fifth row, respectively. The results indicate the validity of proposed cryptosystem.

A. THE EFFECT OF DIFFERENT PARAMETERS ON RECONSTRUCTION PERFORMANCE

In the nonuniform sampling scheme, the quality of recovery image is affected by such factors: the energy contributions of different frequency components and the corresponding compression ratios. In order to obtain the recovery image with higher quality, the parameters of Eq. (22) should be set up suitably. In general, cr_1 should be larger than cr_2 because the human eyes are more sensitive to low-frequency than medium and high-frequency components. The proportions of different frequency components should be established properly considering the characteristic of image. In Table 1, the corresponding PSNR values of four images with different parameters are listed.

From the table, one can note that the reconstruction performance of image Lena, Pepper and Baboon decline as cr_1 decreasing, when the proportions are fixed. In another aspect, PSNR values of above three images increase as the LHFC proportion increasing, when cr_1 is fixed. But the opposite results can be indicated from the image Barbara. One possible reason is that there are plenty of tiny square and rhombic blocks in the image Barbara, however, MFC has the largest effect on the blocks edge reconstruction process. So we should adjust parameters in accordance with the specific

TABLE 1. PSNR values of recovery images with different frequency components and compression ratios (CR = 0.5).

Proportions of different frequency components			Compression ratios		PSNR(dB)			
p_1	p_2	p_3	cr_1	cr_2	Lena	Pepper	Baboon	Barbara
5/16	6/16	5/16	12/16	1/12	35.51	34.44	24.50	26.46
5/16	6/16	5/16	11/16	3/16	34.57	33.77	23.82	27.07
5/16	6/16	5/16	10/16	7/24	33.43	33.04	23.23	27.85
5/16	8/16	3/16	12/16	1/4	34.51	33.70	23.89	28.12
5/16	8/16	3/16	11/16	5/16	33.93	33.28	23.60	28.78
5/16	8/16	3/16	10/16	3/8	33.00	32.41	23.12	29.05

TABLE 2. Computation times with different cryptosystems (Time unit: *s*, CR = 0.5).

Image	Algorithm	Computation time for sender			Computation time for receiver			PSNR
		Compression	Encryption	Total	Decryption	Reconstruction	Total	(dB)
Lena 256×256	BCS:8×8	0.2140	0.0261	0.2401	0.0274	0.6309	0.6583	29.64
	BCS:16×16	0.2120	0.0267	0.2387	0.0255	0.8261	0.8516	29.45
	PCS	0.0091	0.0258	0.0349	0.0285	1.0240	1.0525	26.12
Lena 512×512	BCS:8×8	0.6465	0.0876	0.7341	0.0875	2.4147	2.5022	34.91
	BCS:16×16	0.6432	0.0878	0.7310	0.0871	2.8980	2.9851	35.51
	PCS	0.0184	0.0919	0.1103	0.0885	8.4035	8.4920	29.96

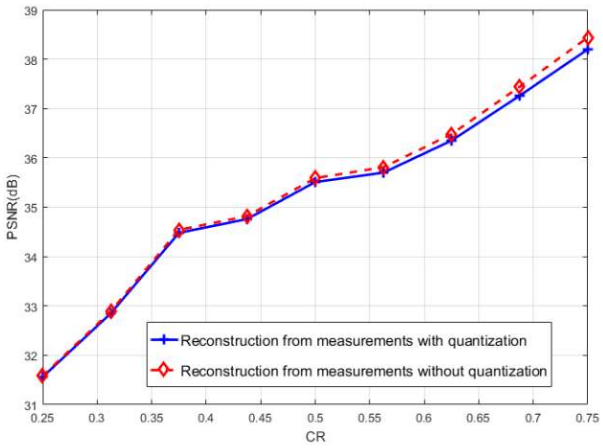


FIGURE 5. Reconstruction performance of the encryption schemes with and without quantization.

characteristics of image so as to obtain the recover image with high quality.

B. ASSESSMENT OF RECONSTRUCTION DISTORTION BY QUANTIZATION

It is well known that CS would lead to the image distortion. In the proposed scheme, the quantization step is adopted before re-encryption, which would lead to the further distortion of image. To evaluate the influence of the measurement quantization on the image distortion, we investigate the difference between the reconstruction performance of schemes with quantization and without quantization. The 512 × 512 Lena is served as the original image and the results are plotted in Figure 5. Due to the robustness property of BCS framework, the average loss in PSNR is around 0.1 dB. Especially for the low compression ratios, the losses are even negligible. Thus the reconstruction distortion caused by quantization is perfectly acceptable.

C. TIME COMPLEXITY ANALYSIS

For the purpose of processing the natural images in real time, the encryption and decryption procedure should be implemented as soon as possible. To estimate the time consumption of encryption scheme accurately, the simulation is carried out for 100 times, and average computation times of different size images with different block dimensions are listed in Table 2. For comparison purpose, we also list the computation time of PCS framework.

Table 2 indicates that: (1) For sender, the compression process accounts for 86 percent of total time when BCS framework is adopted. The compression procedure of PCS is performed much faster than that of BCS because the matrix multiplication is operated only one time. Regardless of BCS or PCS, the times of encryption and decryption grow longer with the size of image increasing because the whole image is re-encrypted. The time-consumption of cryptosystem derives from the workload of chaotic map iteration [34, 35]. (2) For receiver, the reconstruction process costs more than 95 percent of total time. Especially for 512 × 512 image, the reconstruction time of PCS framework is much longer than that of BCS. Because the reconstruction process is seeking the optimal solution, and the dimension of measurement matrix is larger, the more time is consumed. The similar conclusion has been confirmed in [19]. If the parallel model is employed, the compression and reconstruction time of BCS will decrease significantly.

D. SELECTION OF REASONABLE BLOCK DIMENSION

For the encryption scheme based on BCS, the large block dimension would offer better reconstruction performance,

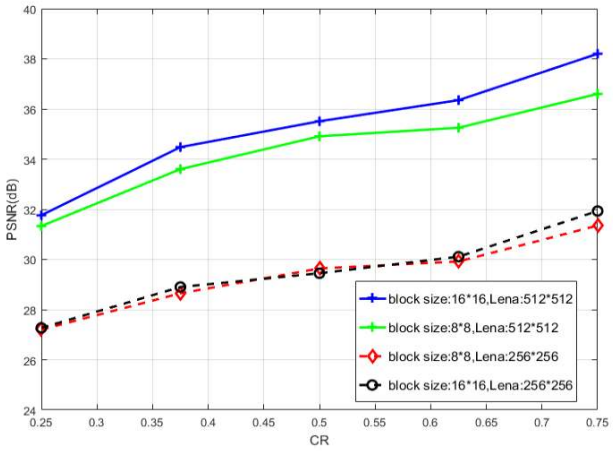


FIGURE 6. Reconstruction performance of the encryption schemes with different block dimensions.

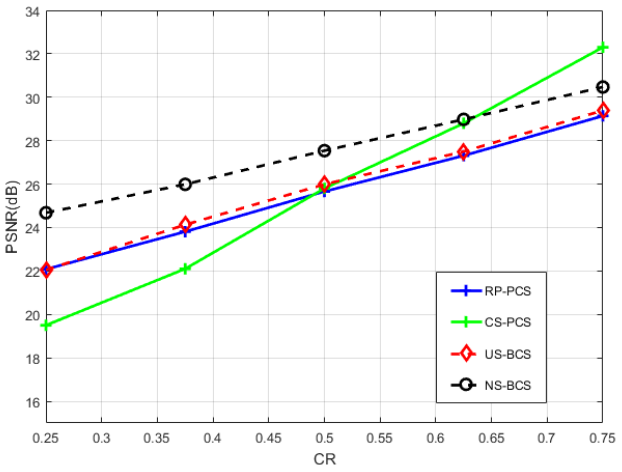


FIGURE 7. Reconstruction performance of the different CS schemes.

whereas require more memory in storage and more implementation time, so there is a trade-off to determine the block dimension. If the size of block is set as 32×32, the vectorization processing would cost much more reconstruction time, so we only employ 8×8 and 16×16 block dimensions in the simulation, and the corresponding PSNR values are plotted in Figure 6.

For the small image with 256×256, we can achieve the roughly equal performance adopting block dimensions 8×8 and 16×16, due to the less computation time, the selection of block dimension 8×8 should be reasonable. For the medium image with 512×512, the scheme adopting block dimension 16×16 would improve the PSNR values by around 0.3-1.6 dB at the same *CR*. Taking into account the reconstruction performance and efficiency, the selection of the block dimension 16×16 should be optimal.

E. COMPARISONS WITH OTHER TYPICAL IMAGE ENCRYPTION SCHEMES

In CS framework, the image compression and recovery performance is influenced by some factors including the measurement matrix, the sparse basis and reconstruction algorithm. So the absolutely fair comparison is difficult to execute. In this section, the proposed scheme based on nonuniform sampling in BCS (NS-BCS) by tuning parameters are compared with other three cryptosystem, including the scheme based on uniform sampling in BCS (US-BCS) framework, the random permutation for PCS (RP-PCS) proposed in [17] and the chaotic system for PCS (CS-PCS) proposed in [20]. The test image is Lena (256×256) and the reconstruction algorithm is adopted as OMP. The sparse representations of image are DCT except for DWT in CS-PCS. The performance is directly cited from the source report [20] or calculated by the corresponding algorithm (RP-PCS and US-BCS). The simulation results are plotted in Figure 7.

From the figure, we can see that the recovery performance via US-BCS and RP-PCS algorithms are roughly equal. The result demonstrates that random permutation in PCS can effectively relax the RIP to enhance the reconstruction performance equal to US-BCS. However, the NS-BCS framework helps to improve the PSNR values by around 2 dB at the same *CR*. This due to the nonuniform sampling model could make the best of different frequency coefficients sparsity. In another aspect, these three algorithms can achieve the better reconstruction performance than CS-PCS when $CR < 0.5$, but the latter can reconstruct the image with a higher precision as *CR* increasing. The cause might be that DWT is the optimal sparse representation for signals with large scale. Synthesize the above comparison results, the proposed cryptosystem based on US-BCS could achieve better recovery performance than other typical encryption schemes, especially for the low compression ratios.

V. SECURITY PERFORMANCE ANALYSES

In this section, some security performance including key space, key sensitivity, plaintext sensitivity, statistical analyses and robustness analyses are discussed. In the simulation, the block dimension is 16×16, $CR = 0.5$, and other parameters are the same as what listed in Section IV.

A. KEY SPACE

According to the suggestion of [36], the key space of a good encryption scheme should be larger than 2^{100} to resist the brute-force attack. In the proposed cryptosystem, the independent secret keys are k_1, k_2 and k_4. According to the IEEE floating-point standard [37], the precision of double-precision number is about 10^{-15}, so the total key space can be calculated by

$$\text{Key space} = 10^{15} \times 10^{15} \times 10^{15} = 10^{45} \approx 2^{149} \quad (25)$$

Obviously, the key space of proposed scheme is large enough to prevent the exhaustive searching.

B. KEY SENSITIVITY

An efficient encryption scheme should be sensitive to the secret keys. If a tiny difference between decryption and

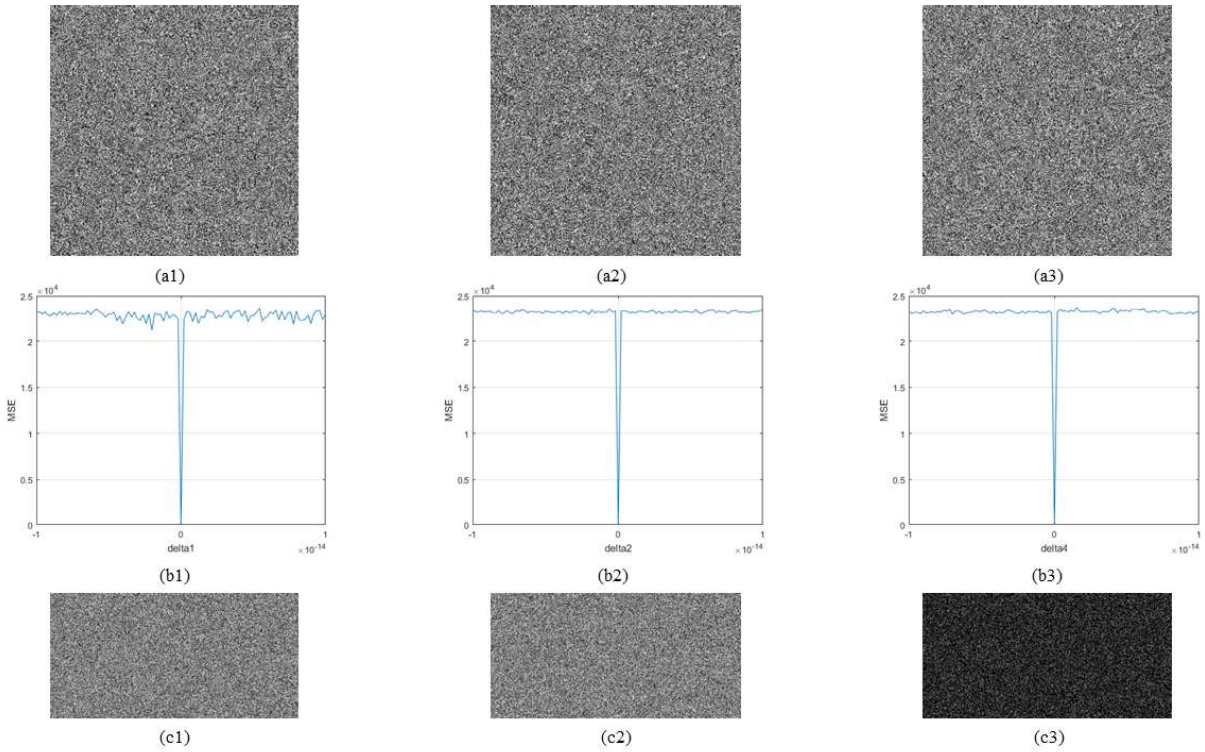


FIGURE 8. Decrypted images with (a1) $\Delta 1 = 10^{-14}$; (a2) $\Delta 2 = 10^{-14}$; (a3) $\Delta 4 = 10^{-14}$; MSE curves with (b1) k1 + Δ1; (b2) k2 + Δ2; (b3) k4 + Δ4; Encrypted Lena with (c1) k1 = 0.23, k2 = 0.94, k4 = 0.61; (c2) k1 = 0.23 + 10^{-14}, k2 = 0.94, k4 = 0.61; (c3) differential image between (c1) and (c2).

encryption keys, the decrypted image should be distorted greatly. On the other hand, if the encryption keys change slightly, the encrypted images should show a significant difference.

1) KEY SENSITIVITY FOR DECRYPTION

In the proposed cryptosystem, k_1, k_2 and k_4 are three independent keys, and k_3 is controlled by k_1. Assume one secret key of decryption changes slightly 10^{-14} with others unchanged, the corresponding decrypted images are shown in Figure 8. (a1)-(a3), and the MSE curves for deviations are shown in Figure 8. (b1)-(b3), where the Δ_1, Δ_2 and Δ_4 are the corresponding deviations from correct keys, respectively. It is obvious that the decrypted images using the keys with a tiny change cannot provide any perceptive information. So the decryption system is sensitive to the secret keys.

2) KEY SENSITIVITY FOR ENCRYPTION

Assume one secret key of encryption system changes slightly 10^{-14} with others unchanged, the corresponding encrypted images are shown in Figure 8. (c1) and (c2), the difference of two encrypted images is shown in Figure 8. (c3). The results illustrate that a slight change of key can lead to the significant changes of encrypted images. So the encryption system is sensitive to the keys.

From the above results, the proposed cryptosystem is sensitive enough to the secret keys.

C. PLAINTEXT SENSITIVITY

Plaintext sensitivity is to test the influence of changing a single pixel in the original image on the cipher pixels. Two plain images with slight difference are encrypted by the same key, and the corresponding cipher images are compared each other. If there are not many differences between the corresponding cipher images, the cryptosystem has no great plaintext sensitivity, it generally could not resist against the known-plaintext or chosen-plaintext attack. In order to calculate the difference of two cipher images, the number of pixels' change rate (NPCR) and the unified average changing intensity (UACI) [38] are defined by Eq. (26) and (27), respectively.

$$\mathrm{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \quad (26)$$

where,

$$\mathrm{D}(\mathrm{i},\mathrm{j}) = \begin{cases} 1, & I_1(i,j) \neq I_2(i,j) \\ 0, & I_1(i,j) = I_2(i,j) \end{cases}$$

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|I_1(i,j) - I_2(i,j)|}{255} \times 100\% \quad (27)$$

where the symbol $I_1(i,j)$ and $I_2(i,j)$ denote the pixel values located at grid (i,j) in the images I_1 and I_2 with size of M × N,

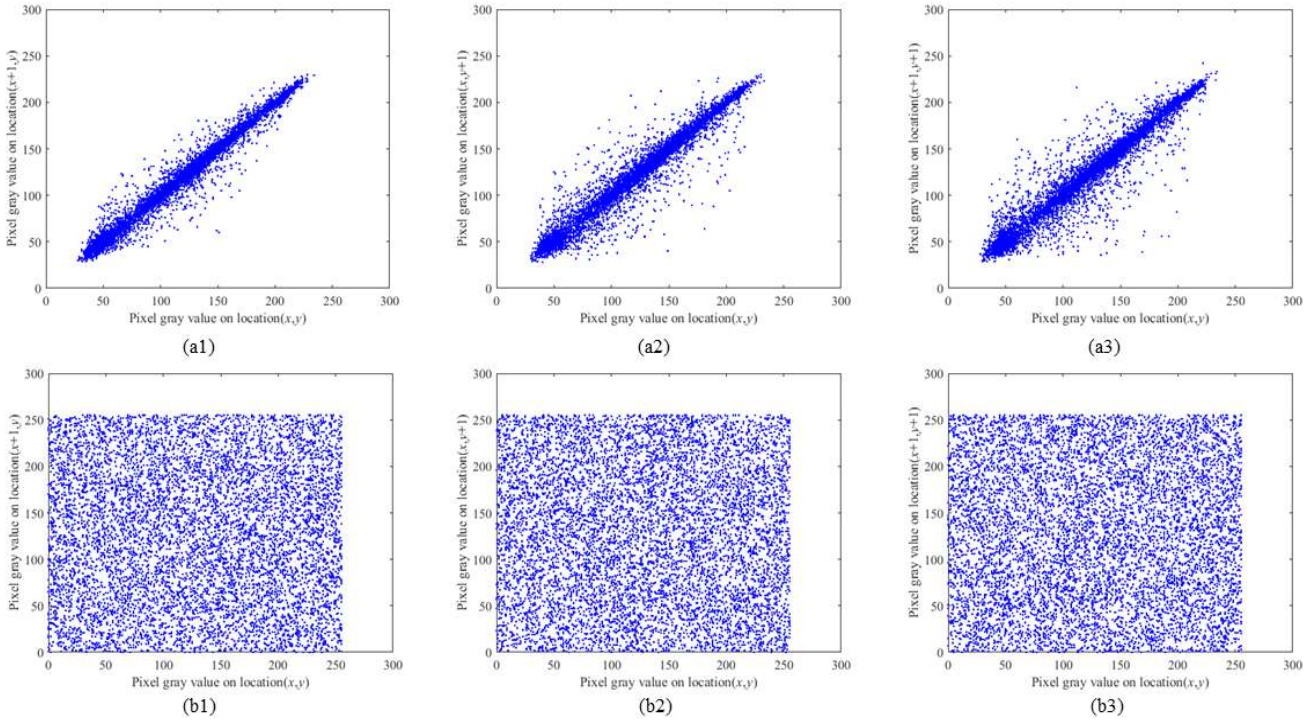


FIGURE 9. Correlation distributions of two adjacent pixels: (a1)-(a3) are correlation distributions of plain image in horizontal, vertical and diagonal directions, (b1)-(b3) are correlation distributions of cipher image in horizontal, vertical and diagonal directions, respectively.

TABLE 3. NPCR and UACI performance for measuring the plaintext sensitivity.

	Lena	Barbara	Baboon	Boat	Desired value
NPCR	99.6061%	99.6000%	99.6034%	99.5973%	99.6094%
UACI	33.4150%	33.3242%	33.4643%	33.4401%	33.4635%

respectively. According to [38], for image encryption scheme with satisfactory property of diffusion, the values of NPCR and UACI should be close to 99.6094% and 33.4635%, respectively.

In the simulation, P_1 and P_2 denote two plain images with one bit difference, C_1 and C_2 are the corresponding cipher images, the NPCR and UACI values of C_1 and C_2 are calculated. To eliminate the randomness, the experiment is carried out for 100 times, and the average results of four selected images are listed in Table 3. One can see that the values of NPCR and UACI are all close to the desired value. The results illustrate that the proposed cryptosystem has great plaintext sensitivity to withstand the known-plaintext and chosen-plaintext attacks.

D. STATISTICAL ANALYSES

1) HISTOGRAM

As an important statistical feature of image, histogram is often adopted to evaluate the performance of encryption scheme. The frequency of each gray level should be fairly uniform in distribution to resist the statistical attack. In Figure 4,

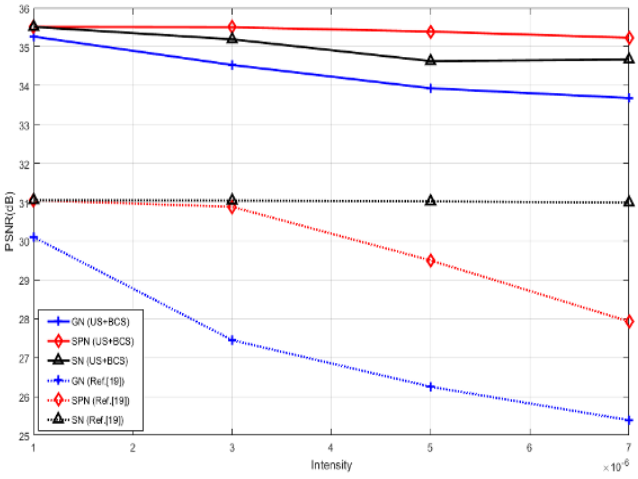


FIGURE 10. PSNR values of decrypted images when the cipher images are contaminated by the different noises.

the histograms of plain images and cipher images are plotted in the second and fourth row, respectively. As can be seen, the histograms of cipher images are nearly uniform, which illustrate the encryption algorithm is effective.

2) CORRELATION COEFFICIENT OF TWO ADJACENT PIXELS

The correlation coefficient of two adjacent pixels is another important statistical feature of image. For a meaningful image, there is a strong correlation between adjacent pixels in horizontal, vertical and diagonal directions. On the contrary,

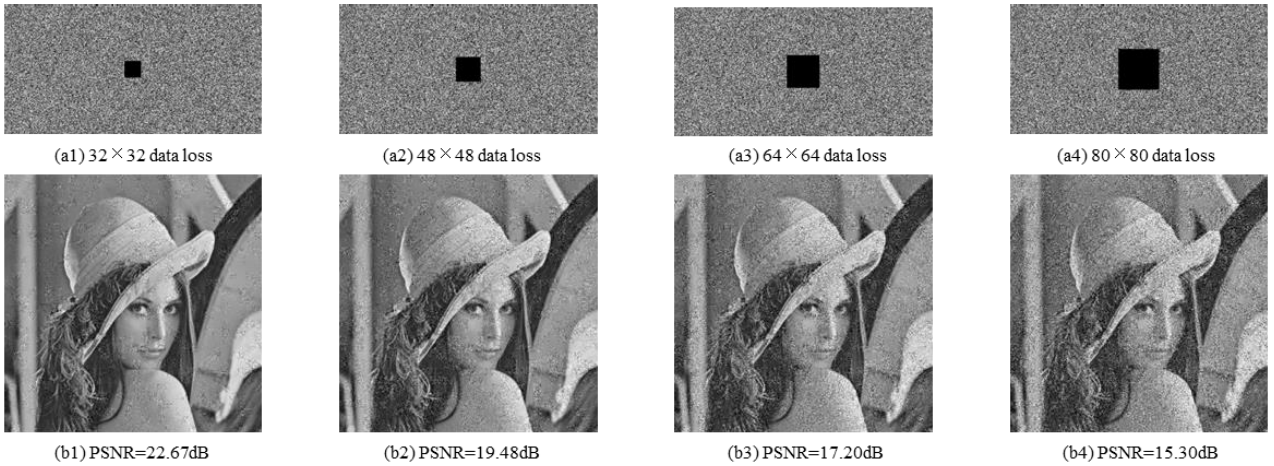


FIGURE 11. Results of cropping attacks: from (a1)-(a4) are cropping attacks using masks with varying pixels sizes, (b1)-(b4) are the corresponding decrypted images from (a1)–(a4), respectively.

TABLE 4. Correlation coefficients of adjacent pixels.

	Horizontal	Vertical	Diagonal
Lena	0.9858	0.9713	0.9614
Ref. [14]	0.0037	0.0018	0.0011
Ref. [20]	0.0036	0.0012	0.0005
Ref. [21]	0.0018	0.0014	0.0034
Ref. [24]	0.0042	-0.0043	0.0163
Proposed scheme	-0.0016	0.0010	-0.0015

there should be a weak correlation between adjacent pixels of cipher images. The correlation coefficient r_{xy} is defined as follows:

$$r_{xy} = \frac{\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))}{\sqrt{(\sum_{i=1}^{N} (x_i - E(x))^2)(\sum_{i=1}^{N} (y_i - E(y))^2)}} \quad (28)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \text{ and } E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i, \quad (29)$$

where x_i and y_i are gray-level values of the selected adjacent pixels, and N is the number of sample pixels.

In the simulation, 8000 pairs of adjacent pixels are selected randomly to calculate r_{xy} in three directions. The comparison results with [14], [20], [21], [24] are listed in Table 4, meanwhile the distribution of r_{xy} are plotted in Figure 9. As demonstrated in Table 4, the proposed scheme owns superiority in horizontal and vertical directions. From the figure, one can see that the regular distributions become disordered. The similar results verify that the strong correlations between adjacent pixels of plain image are weakened effectively by the proposed encryption algorithm.

E. ROBUSTNESS ANALYSES

1) NOISE ATTACK

It is inevitable that encrypted images are affected by all kinds of noises during the image transmission. Noises will add difficulties in recovering the plain image. So the robustness of the proposed cryptosystem against noise attack is considered here. For a fair comparison with the scheme based on PCS framework [19], the simulation is carried out with the same parameters. The original image is Lena (512×512), $CR = 0.5$ and SL_0 algorithm is employed in the construction process. The cipher image Lena is contaminated by different noises including gaussian noise (GN), salt & pepper noise (SPN) and speckle noise (SN), and the normalized noise intensities are set as 0.000001, 0.000003, 0.000005 and 0.000007, respectively. The evaluation results of [19] and proposed scheme are plotted in Figure 10.

From the figure, we can see that: (1) GN has the largest effect on the proposed scheme in three types of noises, the PSNR values are changing from 35.26 dB to 33.68 dB when the noise intensity changes from 0.000001 to 0.000007. The same conclusion can be drawn from [19]. (2) The proposed encryption scheme has the strongest capability to resist SPN, as the PSNR values remain approximately constant when the noise intensity changes. Meanwhile, it has a certain ability to resist SN attack, and the PSNR values vary from 35.51 dB to 34.67 dB (3) Comparing with the encryption scheme of [19] based on PCS, the NS-BCS framework could improve the construction performance around 4-8 dB while for the same noise type and intensity.

In conclusion, the above results illustrate the proposed cryptosystem has good robustness to noise attacks.

2) CROPPING ATTACK

The robustness of a cryptosystem against cropping attack is a significant requirement in image transmission. That is means the valuable information can be recovered effectively from the decrypted images under the influence of data loss. In the simulation, four cropping masks with different sizes are selected, which are shown in Figure 11. (a1)-(a4), and the corresponding decrypted images are illustrated in Figure 11. (b1)-(b4). With the data loss size varying from 32 × 32 to 80 × 80, the PSNR values of reconstruction images are changing from 22.67 dB to 15.30 dB. Thus the proposed cryptosystem could resist the local cropping attack to a certain degree.

VI. CONCLUSIONS

In this paper, an image cryptosystem based on nonuniform sampling in BCS for simultaneous encryption and compression is proposed. The simulation results indicate that the proposed scheme can save storage space, reduce the computation time and enhance the reconstruction performance. Comprehensive analyses show that security performance is satisfactory. The proposed cryptosystem is a compression-encryption hybrid solution which can work efficiently, especially for the medium and large images. In the simulation, the parameters of BCS are set up as a matter of experience, so it is difficult to draw a generic rule for different types of images. In the following work, we will investigate the adaptive learning algorithm [39] according to the statistical characteristic of images for general applicability.

ACKNOWLEDGEMENT

The authors would like to thank editors and the anonymous reviewers for their valuable suggestion to improve the quality of this paper. We would like to express appreciation to Ms. Z. Tang, Mr. H. Wang, Mr. X. Xu, and Ms. X. Wang for their suggestion or other help in various aspects.

REFERENCES

[1] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Process*, vol. 125, pp. 187–202, Aug. 2016.

[2] Y. Wang, C. Quan, and C. J. Tay, "Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm," *Opt. Lasers Eng.*, vol. 78, pp. 8–16, Mar. 2016.

[3] P. Ping, F. Xu, and Z. J. Wang, "Image encryption based on non-affine and balanced cellular automata," *Signal Process.*, vol. 105, pp. 419–429, Dec. 2014.

[4] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, Apr. 2014.

[5] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dyn.*, vol. 81, pp. 511–529, Jul. 2015.

[6] W. Zhang, H. Yu, Y.-I. Zhao, and Z.-I. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Process*, vol. 118, pp. 36–50, Jan. 2016.

[7] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Process*, vol. 113, pp. 104–112, Aug. 2015.

[8] L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," *Inf. Sci.*, vol. 324, pp. 197–207, Dec. 2015.

[9] W. Wen, Y. Zhang, Y. Fang, and Z. Fang, "Image salient regions encryption for generating visually meaningful ciphertext image," *Neural Comput. Appl.*, vol. 29, pp. 653–663, Feb. 2018.

[10] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, VA, USA, Sep. 2008, pp. 813–817.

[11] L. Y. Zhang, K.-W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Trans. Multimedia*, vol. 18, no. 9, pp. 1720–1732, Sep. 2016.

[12] X. Liu, Y. Cao, P. Lu, X. Lu, and Y. Li, "Optical image encryption technique based on compressed sensing and arnold transformation," *Optik-Int. J. Light Electron Opt.*, vol. 124, no. 24, pp. 6590–6593, Dec. 2013.

[13] G. Hu, D. Xiao, Y. Wang, T. Xiang, and Q. Zhou, "Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes," *Opt. Lasers Eng.*, vol. 98, pp. 123–133, Nov. 2017.

[14] T. Chen, M. Zhang, J. Wu, C. Yuen, and Y. Tong, "Image encryption and compression based on Kronecker compressed sensing and elementary cellular automata scrambling," *Opt. Laser Technol.*, vol. 84, pp. 118–133, Oct. 2016.

[15] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process*, vol. 134, pp. 35–51, May 2017.

[16] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Opt. Laser Technol.*, vol. 62, pp. 152–160, Oct. 2014.

[17] Y. Zhang *et al.*, "Embedding cryptographic features in compressive sensing," *Neurocomputing*, vol. 205, pp. 472–480, Sep. 2016.

[18] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," *Nonlinear Dyn.*, vol. 84, no. 4, pp. 2333–2356, Jun. 2016.

[19] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process*, vol. 148, pp. 124–144, Jul. 2018.

[20] G. Hu, D. Xiao, Y. Wang, and T. Xiang, "An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications," *J. Vis. Commun. Image Represent.*, vol. 44, pp. 116–127, Apr. 2017.

[21] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Opt. Laser Technol.*, vol. 99, pp. 238–248, Feb. 2018.

[22] Y. Zhang, B. Xu, and N. Zhou, "A novel image compression–encryption hybrid algorithm based on the analysis sparse representation," *Opt. Commun.*, vol. 392, pp. 223–233, Jun. 2017.

[23] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform," *Opt. Commun*, vol. 343, pp. 10–21, May 2015.

[24] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.

[25] L. Gan, "Block compressed sensing of natural images," in *Proc. 15th Int. Conf. Digit. Signal Process.*, Cardiff, U.K., Jul. 2007, pp. 403–406.

[26] V. Athira, S. N. George, and P. P. Deepthi, "A novel encryption method based on compressive sensing," in *Proc. Int. Mutli-Conf. Automat., Comput., Commun., Control Compressed Sens.*, Kottayam, India, Mar. 2013, pp. 271–275.

[27] R. Huang, K. H. Rhee, and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 71–93, Sep. 2014.

[28] C. Zhou, C. Xiong, R. Mao, and J. Gong, "Compressed sensing of images using nonuniform sampling," in *Proc. 4th Int. Conf. Intell. Comput. Technol. Automat.*, Shenzhen, China, Mar. 2011, pp. 483–486.

[29] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[30] E. J. Candes, "Compressed sampling," in *Proc. Int. Congr. Math.*, Madrid, Spain, 2006, pp. 1433–1452.

[31] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, Dec. 2007.

[32] H. Mohimani, M. Babaie-Zadeh, and C. Jutten, "A fast approach for overcomplete sparse decomposition based on smoothed ℓ^0 norm," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 289–301, Jan. 2009.

[33] Y. Zhang, "Digital image encryption system," in *Chaotic Digital Image Cryptosyste*. Beijing, China: Tsinghua Univ. Press, 2016, pp. 55–60.

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

[35] K.-W. Wong, B. S.-H. Kwok, and C.-H. Yuen, "An efficient diffusion approach for chaos-based image encryption," *Chaos, Solitons Fractals*, vol. 41, pp. 2652–2663, Sep. 2009.

[36] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[37] *IEEE Standard for Binary Floating-Point Arithmetic*, IEEE Standard 754, 1985.

[38] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidiscipl. J. Sel. Areas Telecommun.*, vol. 4, no. 2, pp. 31–38, Apr. 2011.

[39] R. Lai, J. Guan, Y. Yang, and A. Xiong, "Spatiotemporal adaptive nonuniformity correction based on BTV regularization," *IEEE Access*, vol. 7, pp. 753–762, 2019.

LIYA ZHU was born in Suzhou, Anhui, China, in 1980. He received the B.S. degree in navigation engineering and the M.S. degree in information and communication engineering from the Avionic Engineering Institute, Air Force Engineering University, Xi'an, China, in 2002 and 2007, respectively.

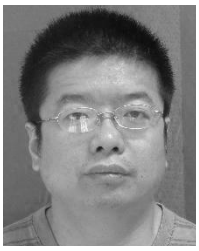
He is currently pursuing the Ph.D. degree with the School of Information Engineering, Chang'an University, Xi'an. His research interests include compressive sensing, image processing, and information security.

HUANSHENG SONG was born in Inner Mongolia in 1964. He received the B.S. and M.S. degrees in communication and electronic systems and the Ph.D. degree in information and communication engineering from Xi'an Jiaotong University, Xi'an, China, in 1985, 1988, and 1996, respectively.

He is currently a Professor with the School of Information Engineering, Chang'an University, Xi'an. His current research interests include image processing and recognition and intelligent transportation systems.

XI ZHANG was born in Heilongjiang, China, in 1979. He received the B.S. degree in navigation engineering and Ph.D. degree in information and communication engineering from the Avionic Engineering Institute, Air Force Engineering University, Xi'an, China, in 2002, and 2007, respectively.

He is currently an Associate Professor with the School of Aeronautics Engineering, Air Force Engineering University. His research interests include radar signal processing and information countermeasure.



MAODE YAN was born in Shaanxi, China, in 1974. He received the B.S., M.S., and Ph.D. degrees from the School of Marine Science and Technology, Northwestern Polytechnical University, Xi'an, China, in 1996, 1999, and 2001, respectively.

He is currently a Professor with the School of Electronics and Control Engineering, Chang'an University, Xi'an. His research interests include networked control systems, vehicle platoon modeling and control, robots and their formation control, and embedded systems and applications.

LIANG ZHANG was born in Baotou, Inner Mongolia, China, in 1983. He received the B.S. degree in information engineering, in 2005, the degree from the College of Electronic Science and Engineering, National University of Defense Technology, Changsha, China, and the M.S. degree in information and communication engineering, in 2008.

He is currently an Engineer with the School of Electronics and Control Engineering, Chang'an University, Xi'an, China. His research interests include cyberspace security and remote-sensing information processing.

TAO YAN was born in Minquan, Henan, China, in 1979. He received the B.S. degree in navigation engineering, in 2002, the M.S. and Ph.D. degrees in information and communication engineering, in 2005 and 2008, respectively, and the degree from the Avionic Engineering Institute, Air Force Engineering University, in 2008.

He is currently a Lecturer with the Aviation Maintenance School for NCO, Air Force Engineering University, Xinyang, China. His research interests include source encoding, FEC, joint channel coding modulation, and data link technology.