A Parallel Image Encryption Method based on Compressive Sensing

R. Huang [a], K. H. Rhee [a,b], S. Uchida [a]

[a] *Graduate School of Information Science and Electrical Enginessing, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, Japan*

[b] *Department of IT Convergence and Application Engineering,Pukyong National University,599-1,Daeyeon 3-Dong,Nam-Gu,Busan 608-737,Korea*

corresponding author's Email: rong.huang01@gmail.com

Abstract: Recently, compressive sensing-based encryption schemes which combine sampling, compression and encryption together are proposed, in which the quantized measurements obtained from dimensionality reduction projection directly serve as the encrypted image. However, these types of encryption algorithms fail to resist against the chosen-plaintext attack. To enhance the security level, the block cipher structure consisting of scrambling, mixing, S-box and XOR with the chaotic lattice is designed to encrypt the quantized measurements. The two-dimensional coupled map lattice is employed as a spatiotemporal chaotic model, which enables implementing the block-wise XOR. Moreover, this block cipher structure works efficiently in the parallel computing environment. In particular, the communication unit exchanges data among the multiple processors and provides the collision-free property which is the precondition of optimal diffusion. The experimental results indicate that the proposed encryption algorithm not only achieves remarkable confusion, diffusion and sensitivity but also outperforms the existing parallel image encryption methods with respect to the compressibility and the encryption speed.

Keywords: compressive sensing, image encryption, parallel structure, chaotic model, optimal diffusion

Introduction

Background

Nowadays, multimedia data have been widely spread through the Internet. Since the private data are particularly vulnerable to eavesdropping during the data transmission, the confidentiality is required for such applications as Internet conference, Internet security camera, live TV, video-on-demand and telemedicine. Various data encryption standards like DES, AES, RSA and IDEA [1, 2] have been developed and widely used as a protection against illegal access to the private information. However, it is difficult to use them directly in multimedia data due to the following three reasons [3, 4]. First, the image size is always larger than that of text. The time consumption of image encryption and decryption is increased accordingly. Second, the correlation among adjacent pixels is not completely reduced by the conventional cryptography methods. The original image's contour is still visible in the encrypted image because considerable amount of perceptual redundancy has not been eliminated [3]. For example, the result image encrypted by AES directly (ECB mode) is shown in Fig.1(b). As can be seen, the encrypted image is still intelligible to some extent [5, 6]. Third, the exactness of recovered textual data is required while it is not always necessary for image decryption. In many applications, a recovered image preserving the semantics is acceptable. In addition, due to the bulky quantity of multimedia data, it is usually desired to compress prior to transmission especially when storage resources or transmission bandwidth is limited.

Related Work

Based on Compressive Sensing (CS) [7-9], the compression-combined encryption methods are proposed in [10-13]. Sampling and compression are combined together through a linear dimension reduction measurement process. Moreover, the randomness of measurement matrix renders the measurements unintelligible, which means that encryption can also be implemented synchronizing with sampling and compression.

Rachlin and Baron [10] demonstrate that, although the CS-based encryption scheme cannot achieve the perfect security, it is still meaningful owing to the high computational complexity of cracking. Orsdemir *et. al* [11] propose the notion of robust encryption. It means that the encrypted image is tolerant of some level of noise contamination. The security is analyzed in terms of brute force and structured attacks. They claim that the computational intractability makes the attacks infeasible in practice. Considering the unavoidable problem of packet loss during wireless transmission, Liu, Gao and *et. al* [12, 13] quantify the anti-packet loss ability of the CS-based encryption paradigm.

Parallel image encryption also has spurred a great deal of research activities. Mirzaei *et. al* [16] propose a parallel image encryption method in which the original image is first divided into four parts, then these sub-images are disordered. All pixels are permutated according to a total shuffling matrix. Gray value substitution is employed using the combined states of two chaotic systems, which works in parallel. However, this method lacks of diffusion mechanism. Zhou *et. al* [17] invent a parallel image encryption structure involving a well designed communication unit. Their method dissolves the intrinsic contradiction between parallelism and diffusivity. The experimental results exhibit that the full diffusion could be achieved after three rounds of encryption. Liao *et. al* [18] imitate the self-adaptive encryption [19] and propose a parallel method based on the property that waveform of a sin wave is sensitive to three parameters: amplitude, wavelength and distance. A similar communication unit is designed to exchange data among the processors. As a same result, three rounds of encryption are essential to achieving the full diffusion[1].

It should be noted that the signal reconstruction of CS-based method is an ill-posed problem, and results in heavy computational load on the recipient. We conclude that CS reduces the sampling rate at the expense of a complex reconstruction computing. The application of CS to Magnetic Resonance Image (MRI) has the potential for significant scan time reductions, with benefits for patients and health care economics [15]. This image encryption method designed under compressive sampling circumstance can play an important role to protect the privacy of MRI images when they are transmitted to other terminals for teleconsultation. We remark that the data integrity is significant in this application area because the artifacts or corrupted regions caused by transmission error may lead to misdiagnosis. In most cases, the small scaled contamination may be considered as lesions. Therefore, we analyze the ciphertext sensitivity and regard it as an authentication process.

Challenging Issues

The result image encrypted by the previous methods [10-13] does not leak any visual information indeed, whereas its security is not strong enough considering the basic security requirements, namely confusion, diffusion and sensitivity. We summarize four challenge issues and list them as follows.

[1] Liao *et. al* [18] claim that the full diffusion could be achieved even after the first round of encryption. However, their experiment for measuring the diffusion is not impartial. If one changes the original image pixel in the second quadrant, at least three rounds of encryption are required for achieving full diffusion. So the result provided in their paper might be the best case. It should be bear in mind that when measuring the security, only the worst boundary can be taken as a result.

(1) The confidentiality of the methods [10-13] merely survives against the ciphertext-only attack. However, on account of lacking diffusion process, its security is fragile with respect to the chosen-plaintext attack. The first challenging issue is how to enhance the security level.

(2) Block compressive sensing proposed in [20] suggests a highly efficient framework which allows parallel measuring. However, the existing encryption modes, like Cipher-Block Chaining (CBC) and Counter (CTR), have their own disadvantages. Although CBC mode can achieve good diffusion after several rounds of encryption, its serial structure becomes a barrier to the parallelism. In contrast, though CTR mode guarantees the parallelism, it is difficult to achieve full diffusion without a sophisticated design. Moreover, a natural error or an intentional change in the encrypted image causes error propagation within a partial region [21]. Yet, from the perspective of ciphertext sensitivity, the bit alteration should lead to a non-recognizable decrypted image [24]. The second challenging issue is how to ease this conflict to fulfill the full diffusion in the parallel structure.

(3) In general, to achieve a good diffusion result, the encryption algorithm must be iterated for several times. The repeated iteration operations undermine the computational efficiency. The third challenging issue is how to decrease the iteration rounds while retaining good diffusion performance.

(4) Additional requirements arise from the parallel structure. Specifically, the computation and communication load balance should be taken into account [25]. Since there are multiple processors working simultaneously, the total time overhead is determined by the processor which has the lowest unit throughput[2]. The fourth challenging issue is how to balance the workload so that all processors share equal unit throughput.

Our Contribution

In this paper, we propose a novel encryption scheme under compressive sampling circumstance working in the parallel structure. Contributions are highlighted as follows.

[2] Definition of unit throughput. Assume that the workload allocated to one processor is w, the processing capacity of this processor is c, then the unit throughput is defined by c/w.

(1) We design a two-stage encryption scheme. In the first stage, akin to the previous works [10-13], the linear measurement is implemented for compressively sampling the image. The second stage is designed as parallel structure in which the quantized measurements undergo permutation, substitution, block-wise exclusive-or (XOR) operation and a communication unit. In this way, the encryption scheme resists against the chosen-plaintext attack due to the achievement of full diffusion property.

(2) The communication unit carries out the collision-free data exchange which yields the full diffusion after only two rounds of encryption, namely optimal diffusion [25]. Furthermore, three conditions for achieving the optimal diffusion are summarized. They indicate that achievement of the optimal diffusion is independent of the aspect ratio of the original image.

(3) To avoid discussing the optimal scheduling problem, we assume that each processor has equivalent processing capacity. On the basis of this assumption, the unit throughput of each processor becomes same as long as the workload allocated to each processor is equal. This even distribution problem can be solved by adjusting the number of measurements of each block even if the original image has different aspect ratio.

The rest of the paper is organized as follows. Section 2 gives a brief introduction about compressive sensing. Security analysis on previous works [10-13] is elaborated in Section 3. Section 4 will be devoted to the description of the proposed encryption method. In Section 5, the numerical experimental results are given and the conclusion is presented in Section 6.

Compressive Sensing Overview

Compressive Sensing (CS), also known as compressive sampling [7, 8], can sample a sparse or compressible signal at a rate below the Nyquist theorem required. It can be regarded as a signal acquisition and sparse vector recovery technique. Intuitively, most natural images are not simple in the spatial domain. Fortunately, the sparse representation of one original signal can be derived from decomposition algorithms such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or overcomplete basis transform [22]. Suppose x is a signal with length N. We deal with image data by first vectorizing it into one-dimension vector. For simplicity, assume that $\{\psi_i\}(i=1,\cdots,N)$ is a normal orthonormal basis in $\mathbb{R}^N$. Basis matrix with the ψ_i as columns is denoted by $\mathbf{\Psi}$. The decomposition coefficient s is the equivalent representation of x in $\mathbf{\Psi}$ domain. If only K entries of s are non-zero, where $K \ll N$, x is termed as K-sparse signal. The linear measurement process is expressed as:

$$y = \mathbf{\Phi}x = \mathbf{\Phi\Psi}s = \mathbf{\Theta}s \qquad (1)$$

This formula describes $M \times N$ inner products between x and M rows of measurement matrix $\mathbf{\Phi}$. The array $\mathbf{\Theta} = \mathbf{\Phi\Psi}$ can be called as sensor matrix. The asymmetric size of measurement matrix results in an ill-posed problem with respect to the reconstruction, which means equation (1) has infinitely many solutions. To simplify this problem, a necessary and sufficient condition has been proposed in [23], namely Restricted Isometry Property (RIP), which can be cast as follow:

$$(1-\delta_K)_2\|s\|_2 \le \|\mathbf{\Theta}s\|_2 \le (1+\delta_K)\|s\|_2$$

We loosely say that a matrix $\mathbf{\Theta}$ obeys the RIP of order K if δ_K is not too close to one. When this property holds, a steady solution can be obtained from this underdetermined system. In fact, we have a more intuitive equivalent condition, that is, the measurement matrix $\mathbf{\Phi}$ must be incoherent with basis matrix $\mathbf{\Psi}$. This related condition requires that the rows $\{\phi_i\}$ of $\mathbf{\Phi}$ cannot sparsely represent the columns $\{\psi_j\}$ of $\mathbf{\Psi}$ (and vice versa) [9]. In general, this requirement can be satisfied with overwhelming probability, when elements of measurement matrix $\mathbf{\Phi}$ are independent and identically distributed (i.i.d) random variables taking on their values from a Gaussian probability density function with mean zero and variance $1/N$ [8]. Meanwhile, the measurement data length M is restricted by the inequality below:

$$M \ge cK\log(N/K) \qquad (2)$$

where c is a small constant. The parameter M in formula (2) is one crucial factor of compression rate. Another one is quantization level.

The projection vector y obtained from equation (1) retain structure of the original signal. The recovery boils down to a convex optimization process:

$$\hat{s} = \operatorname{argmin}\|s'\|_1 \text{ subject to } s' = \mathbf{\Theta}y$$

In this paper, orthogonal matching pursuit (OMP) is adopted to reconstruct the original signal from the projection vector y. It is a reliable and efficient greedy algorithm whose computational complexity is $O(K \ln N)$ [27].

Security Analysis on CS-based Encryption Scheme

From the measurement process expressed in equation (1), we conclude that dimension reduction provides compression function and cipher property attributes to the randomness of measurement matrix. The sensor matrix $\mathbf{\Theta}$ is accounted a secure key and available for intended receivers through the secure channel. The unintelligible measurements are transmitted over the public channel. In previous works [10-13], the security analysis only concerns the computational complexity of brute force attack. However, that is not adequate if opponents have obtained temporary access to the encryption machinery. The following analysis shows its insecurity in terms of the chosen-plaintext attack.

Suppose that the sparse transform matrix $\mathbf{\Psi}$ equals an identity matrix I. The measurement vector y can be represented linearly by columns ϕ_i.

$$y = x_1\phi_1 + x_2\phi_2 +, \cdots, + x_N\phi_N$$

where x_i stands for i^{th} element of vector x. Likewise, the i^{th} column of $\mathbf{\Phi}$ is designated by ϕ_i.

Let $x^{[k]}$ denote a sparse vector in which only one entry is non-zero:

$$x^{[k]} = \begin{cases} x_i = 0 & i \neq k \\ x_i = 1 & i = k \end{cases} \qquad i = 1, \cdots, N$$

A plaintext set $X = \{x^{[k]} \mid k = 1, \cdots, N\}$ is constituted to perform the chosen-plaintext attack. One certain plaintext $x^{[k]}$ is encrypted, then the corresponding output $y^{[k]} = \mathbf{\Phi} x^{[k]} = \phi_k$ is obtained. To reveal the measurement matrix, he/she should sequentially execute N times encryption traversing all plaintext vectors in the set X. The measurement matrix is constructed by arraying the ciphertext set $Y = \{y^{[k]} \mid y^{[k]} = \mathbf{\Phi} x^{[k]}, k = 1, \cdots, N\}$ in sequence. We have $\mathbf{\Phi} = [\phi_1 \mid \phi_2 \mid \cdots \mid \phi_N] = [y^{[1]} \mid y^{[2]} \mid \cdots \mid y^{[N]}]$.

Performing the above chosen-plaintext attack, the CS-based encryption scheme can be broken by just using N plain-cipher pairs. In the following, we design an encryption scheme which not only enhances the security but also preserves the parallelism.

Our Proposed Enhancement Scheme

Encryption Scheme Configuration

This improved encryption scheme is composed of block linear measurement and parallel block cipher. Since the bulkiness of image data brings on an enormous measurement matrix, to address this problem, Gan [20] proposes the block compressive sensing which enables parallel measuring. One original image is first segmented into blocks and each block is measured by $\mathbf{\Phi}_B$. The complete block diagonal measurement matrix takes the following form:

$$\mathbf{\Phi} = \begin{bmatrix} \mathbf{\Phi}_B & & & \\ & \mathbf{\Phi}_B & & \\ & & \ddots & \\ & & & \mathbf{\Phi}_B \end{bmatrix}$$

To enhance the confidentiality, the quantized measurements are encrypted under the parallel structure. Compared with the previous works [10-13], the proposed method is more secure without severe reduction in efficiency performance. The encryption frame diagram is illustrated in Fig.2.

Key Schedule and Chaotic model

The 128-bit key $K = k_0, k_1, \cdots, k_{127}$ is divided into four 32-bit sub keys: $K_{\text{sub}}^j = k_{32j}, k_{32j+1}, \cdots, k_{32j+31} (j = 0,1,2,3)$. A four-tuple $\{z_{seed}, \hat{\mathbf{z}}_a, \hat{\mathbf{z}}_b, \hat{\mathbf{Z}}_{W \times H}\}$ is created using the key K. The floating-point number z_{seed} is used as the seed to generate the block Gaussian random matrix $\mathbf{\Phi}_B$. $\hat{\mathbf{z}}_a$ and $\hat{\mathbf{z}}_b$ are two quantized chaotic sequences of length L, while $\hat{\mathbf{Z}}_{W \times H}$ is a set of two-dimensional quantized chaotic lattices of size $W \times H$. The cardinality of this set is equal to L as well. In the following article, the approach to generating the four-tuple is described.

Four floating-point numbers are first calculated from equation (3) respectively, and regarded as the initial values of Logistic map as given in equation (4).

$$I^j = K_{\text{sub}}^j \Big/ \sum K_{\text{sub}}^j \qquad j = 0,1,2,3 \tag{3}$$

$$F(X_t^j) = \mu X_t^j (1 - X_t^j) \qquad j = 0,1,2,3 \ \ \& \ \ t = 0,1,2,\cdots \tag{4}$$

In equation (4), $\mu = 4$. The number of iteration t starts from 0, and the initial values are $X_0^j = I^j$. In order to improve the initial-value sensitivity, taking values is triggered after the equation (4) undergoes $t > t_0$ rounds of iteration. Here, the constant t_0 is preset to 100 empirically.

The seed $z_{seed} = F\left(X_{t_0+1}^0\right)$ directly takes the result after $t > t_0$ rounds of iteration. However, for obtaining quantized chaotic sequences/lattices, quantization algorithm should be designed in advance. A decimal $0.z_t^j(0)z_t^j(1)z_t^j(2)\cdots$ is quantized according to the equation (5).

$$\hat{z}_t^j = \operatorname{mod}\left(100 z_t^j(0) + 10 z_t^j(1) + z_t^j(2), 2^8\right) \tag{5}$$

where $z_t^j(0)$ stands for the decile of z_t^j, and the rest can be deduced by analogy. Then we have

$$\hat{\mathbf{z}}_a = \{\hat{z}_{t_0+1}^1, \hat{z}_{t_0+2}^1, \cdots, \hat{z}_{t_0+L}^1\}$$

$$\hat{\mathbf{z}}_b = \{\hat{z}_{t_0+1}^2, \hat{z}_{t_0+2}^2, \cdots, \hat{z}_{t_0+L}^2\}$$

About the set $\hat{\mathbf{Z}}_{W\times H}$, the two-dimensional Coupled Map Lattice (CML) [26] is utilized to generate quantized chaotic lattices, and the corresponding process can be divided into three steps: lattice initialization, lattice iteration and lattice quantization. The two-dimensional CML is a type of spatiotemporal chaos that is characterized by ergodicity, sensitive dependent on initial condition and random-like behaviors. In initialization, the chaotic sequence $z_{t_0+1}^3, z_{t_0+2}^3, \cdots, z_{t_0+W\times H}^3$ obtained from equation (4) shall be reshaped to a matrix of size $W \times H$. This initial lattice is denoted by $\mathbf{Z}_{W\times H}^0$. The lattice iteration process is represented by equation (6) and (7).

$$z_{ii,jj}^{n_c+1} = (1-\varepsilon) F\left(z_{ii,jj}^{n_c+1}\right) + \frac{1}{2}\varepsilon\left[F\left(z_{ii+1,jj}^{n_c}\right) + F\left(z_{ii,jj+1}^{n_c}\right)\right] \tag{6}$$

where function $F(\cdot)$ is the Logistic map which has been given in the equation (4). The parameter ε ranges in [0,1]. Moreover, the periodic boundary condition $z_{ii,jj+W}^{n_c} = z_{ii+H,jj}^{n_c} = z_{ii,jj}^{n_c}$ is satisfied.

$$z_{ii,jj}^{n_c+1} = \left(z_{ii,jj}^{n_c+1} + z_{ii+1,jj}^{n_c+1} \right) \bmod 1 \tag{7}$$

where $ii = 1, 2, \cdots, H$ and $jj = 1, 2, \cdots, W$ stand for the coordinates of current lattice. The enumerator n_c counts the times of iteration. In this stage, the same quantization method given in equation (5) is adopted. After n_c increases to L, the construction of the set $\hat{\mathbf{Z}}_{W\times H}$ is completed. By now, we have described the creation process of the four-tuple $\{z_{seed}, \hat{\mathbf{z}}_a, \hat{\mathbf{z}}_b, \hat{\mathbf{Z}}_{W\times H}\}$. These chaotic data are used in the following.

Encryption and Decryption Procedure

One block of the original image x_p is measured by block measurement matrix $\mathbf{\Phi}_B$ and y_p is the corresponding result. Note that subscript p indices the serial number of blocks. Each quantized measurement vector $\hat{y}_p$ undergoes following five processes: Arnold scrambling, Mixing [28], S-box, block-wise XOR operation and communication. Let R denote the number of iteration round. The procedure of encryption/decryption as well as parameter enactment is described hereinafter.

[Step 1]: Pretreatment. The original image is first divided into b blocks. We assume the size of each block is $\sqrt{N} \times \sqrt{N}$ and vectorize them into one-dimensional vectors in raster order. The p^{th} block's pixel vector with length N is labeled as x_p, where $p = 1, \cdots, b$. We just give the operation description of one certain block owing to the identical parallel structure.

[Step 2]: Measurement. Without loss of generality, $\mathbf{\Psi}$ is set to be discrete cosine transform (DCT). The measurement matrix of size $M \times N$ is created column by column using a Gaussian random sequence which is initialized by the seed $z_{t_0+p}^0$. The measurement vector y_p is derived from linear transform as given in equation (1).

[Step 3]: Quantization and Reallocation. Lloyd quantizer [29] is known as an optimal quantizer in the mean square error sense. This iterative algorithm is used to quantize the measurements y_p for a given 8-bit rate.

These quantized measurements are arrayed into a square block $\hat{\mathbf{Y}}_p$ of size $\sqrt{M} \times \sqrt{M}$ according to the inverse raster scanning. This square matrix is segmented into B blocks. The position of each block is expressed by a coordinate $(\mathbf{m},\mathbf{n})$, where $\mathbf{m},\mathbf{n} = 1,\cdots,\sqrt{B}$. To fulfill the collision-free data exchange in Step 8, a condition is attached. That is the size of $\hat{\mathbf{Y}}_{\mathbf{m},\mathbf{n}}$ should be $\sqrt{B} \times \sqrt{B}$, which means the number of elements of one block equals the number of blocks. Then, how to determine the parameters M, B, b becomes a serious issue. In Step 8, three conditions are summarized to handle this problem.

[Step 4]: Permutation. Arnold scrambling is commonly used to permutate the pixels' position or gray value as a pretreatment process. The original version can be recovered after undergoing period T iterations. In this scheme, for each block of size $\sqrt{B} \times \sqrt{B}$, we denote the coordinate of one quantized measurement as (m,n)[3]. The equation (8) is performed to scramble the elements of blocks $\hat{\mathbf{Y}}_{\mathbf{m},\mathbf{n}}$ in parallel, where $\mathbf{m},\mathbf{n} = 1,\cdots,\sqrt{B}$. The position moving of this pixel is shown as:

$$\begin{bmatrix} m' \\ n' \end{bmatrix} = \left\{ \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} \bmod\left(\sqrt{B}\right) \right\}^{t} \tag{8}$$

Thereinto $m, n, m', n' \in \left\{1, 2, \cdots, \sqrt{B}\right\}$, and t stands for the iteration time. Two parameter groups $a_1,\cdots,a_L$ and $b_1,\cdots,b_L$ are governed by the quantized chaotic sequence $\hat{\mathbf{z}}_a$ and $\hat{\mathbf{z}}_b$, respectively. Thus, for R rounds of parallel iterations, the length L should be $R{\cdot}B$.

[Step 5]: Mixing [28]. We define the XOR sum operation as $S = \hat{y}_{1,1} \oplus \hat{y}_{1,2} \oplus \cdots \oplus \hat{y}_{\sqrt{B},\sqrt{B}}$. Then, the output of mixing operation can be stated as $\left\{\hat{y}_{m,n} \oplus S \mid m = 1,\cdots,M; n = 1,\cdots,N\right\}$ to denote mixing manipulation.

[3] Here, (m,n) is the coordinate of one quantized measurement of a certain block, while $(\mathbf{m},\mathbf{n})$ stands for the position of a certain block.

One impressive property is that the alteration in a single element will affect all others. Another helpful property is $M\left(M\left(\hat{\mathbf{Y}}_{\mathbf{m},\mathbf{n}}\right)\right)=\hat{\mathbf{Y}}_{\mathbf{m},\mathbf{n}}$. These two properties indicate that the mixing operation can achieve full diffusion without an additional pseudorandom sequence.

[Step 6]: S-box Substitution. It is a basic component of block cipher algorithm which acts as a non-linear projection through table lookup. This unit provides confusion property which obscures the relationship between the key and the encrypted image. For the sake of simplicity, we employ a fixed 8×8 bits S-box from AES [30]. Let $S(\cdot)$ denote this substitution manipulation.

[Step 7]: Block-wise XOR. In the r^{th} round, the output is the result of XOR between its preceding round's result and two-dimensional quantized chaotic lattices.

$$\mathbf{C}_{\mathbf{m},\mathbf{n}}^{r}=\hat{\mathbf{Z}}_{\sqrt{B}\times\sqrt{B}}^{n_c}\bigoplus\mathbf{C}_{\mathbf{m},\mathbf{n}}^{r-1}\quad r=1,\cdots,R$$

The initial lattice is $\mathbf{C}_{\mathbf{m},\mathbf{n}}^{0}=S\left(M\left(\hat{\mathbf{Y}}_{\mathbf{m},\mathbf{n}}\right)\right)$.

[Step 8]: Communication. The communication unit can realize the collision-free data exchange which is equivalent to optimal diffusion [25]. We give the definition of optimal diffusion as follow.

Definition. [25] Suppose that each block contains B elements. After the r^{th} round of encryption, the effect of a single bit change in the original image has been spread over B^r elements.

Under block parallel operation mode, the conditions of the optimal diffusion are given below:

Condition. The optimal diffusion is achievable if the following two conditions are satisfied:

(1) After the r^{th} round encryption, the change in the value of an arbitrary element $c_{m,n}\in\mathbf{C}_{\mathbf{m},\mathbf{n}}^{r}$ impacts upon all other elements in the same block, where $m,n,\mathbf{m},\mathbf{n}\in\left\{1,\cdots,\sqrt{B}\right\}$.

(2) After the $(r+1)^{\text{th}}$ round encryption, the effect of $c_{m,n}$'s value change should make impact upon all elements which belong to $\mathbf{C}_{\mathbf{m},\mathbf{n}}^{r+1},\mathbf{m},\mathbf{n}=1,\cdots,\sqrt{B}$.

According to the above two conditions, we design the communication unit in which any elements $\left\{c_{m,n}\middle|\left(1\top\ m,n\ \ \sqrt{B}\right)\&\left(m\neq\mathbf{m}\|n\neq\mathbf{n}\right)\right\}\in\mathbf{C}_{\mathbf{m},\mathbf{n}}$ are transmitted to other blocks $\mathbf{C}_{\mathbf{m}',\mathbf{n}'}$ and occupy the location $(\mathbf{m},\mathbf{n})$. From the above description, a necessary condition is exposed. That is the number of elements of one block should equal the number of blocks, mathematically, $M\cdot b/B=B$. Therefore, the parameters M,B,b should be chosen carefully according to the following three conditions. Firstly, M ▪ $4K$, which is the empirical version of formula (2) [27]. Secondly, $\sqrt{M}$, $\sqrt{B}$ and $\sqrt{b}$ must be integers. Thirdly, $B=\sqrt{M\cdot b}$. The first condition determines the compression ratio and the reconstruction quality. The compression ratio is defined as $\frac{M}{N}$. Moreover, these three conditions are independent of the original block's size N, which implies that the collision-free data change can be achieved regardless of the aspect ratio of the original image. Hence, the proposed encryption scheme is also applicable to the non-square images. For example, an original image of size 300×480 is segmented into $b=64$ blocks as shown in Fig.3. We fill in the blocks of different size with progressive grayscale. The appropriate M of each block is selected as 1024 and the compression ratio approximates to 0.4551.

Also, we conclude that when the above three conditions are satisfied, only two rounds of encryption are sufficient for achieving the full diffusion. In contrast, both Zhou's method [17] and Liao's method [18] need more than two rounds encryption. That is because their data exchange designing exists collision, thus resulting in the inefficient diffusion. In Fig.4, an example is given to clarify the collision-free data exchange process. In which, $M\cdot b=16$, $B=4$ and the size of sub-block is 2×2.

We can observe that through this free-collision data exchange process, the components of one sub-block are unpicked and separately placed to occupy one position of each sub-block.

The aforementioned description is the encryption process. The operations from step 4 to step 8 should be implemented iteratively for R rounds. In the last round of iteration, the communication unit can be skipped. The decryption procedures are composed of the inverse transformations of the encryption process and preformed in reverse order. The S-box should be replaced by corresponding inverse version.

It is worth noting that the parallel structure is still preserved during the decryption stage, which allows to implement the reconstruction algorithm OMP in parallel.

Security and Performance Evaluation

To evaluate the security and performance of an encryption algorithm, the resistance against a series of known attacks, such as brute-force attack, statistical attack and differential attack is generally investigated. In this section, security and performance evaluation includes reconstruction, key space analysis, statistical analysis, sensitivity analysis, information entropy analysis and efficiency analysis. Five different gray images with resolution 512×512 are selected as the original images. It should be mentioned that the proposed method is also applicable to the color images through the parallel encryption for each color channel.

(a) The “Lena” image, is a high-contrast image with sharp corners and textured area.

(b) The “Pepper” image, contains multiple separate plain areas with divergent shape. The distinct edges exist in the junction between two peppers.

(c) The “Baboon” image, contains a large textured area (the fur) and a homogeneous area (the face).

(d) The “Testpat” image, as illustrated in Fig.1(a), is a general test pattern that is comprised of a shrunken ``Lena" image and blocks with shades of progressive grayscale. Each block is padded by the monochromatic gray.

(e) The “Black” image, consists of black pixels and can be regarded as an all-zero matrix.

In the following, the test results of proposed method are compared with those of CS-based image encryption [10-13] and parallel image encryption [17, 18], respectively. We exclude the parallel method proposed in [16] from the comparison due to the inefficient diffusion mechanism.

Reconstruction

For directly comparing with the encrypted image illustrated in Fig.1(b), we first encrypt “Testpat” using the proposed method. The corresponding results are given in Fig.6(d). The original image is split into $b = 64$ blocks and each block contains $N = 4096$ pixels. The 128-bit length original key is set to $K = \left(0123456789\text{ABCDEF}0123456789\text{ABCDEF}\right)_{\text{hex}}$.

Large M offers the high quality reconstruction while small M leads to an aborted recovery. The appropriate step is set to be $M = 1024 = \frac{1}{4}N$, so the compression ratio is fixed to be 0.25. The reconstruction using the correct key has been depicted in Fig.6(a).

A peculiar problem to solutions of ill-posed equations is that the recovery is not exact but only approximate. In fact, the small degree of deterioration is beyond human's visual perception. We compute PSNR as the objective metric to evaluate the intelligibility of the reconstructed image. The calculation formulas are

$$\text{MSE} = \frac{1}{bN}\sum_{i=1}^{bN}(x_i - \hat{x}_i)^2$$

$$\text{PSNR} = 10 \times \lg\left(255^2/\text{MSE}\right)$$

The PSNR of Fig.6(a) is $31.2345\,\text{dB}$. Generally, when $\text{PSNR} > 30\text{dB}$, the quality of reconstruction is reckoned to be acceptable. Note that the issue that how to improve the reconstruction quality is not within the scope of our theme. So far, there exist too many reconstruction techniques to enumerate here. The prominent methods include orthogonal matching pursuit [27], Gradient pursuit [31], iterative shrinkage thresholding algorithm [32], FOCUSS [33] and SPARLS [34].

Space of the Key

The key used in the proposed encryption method is 128-bit length, with key space size $2^{128} \approx 3.4028 \times 10^{38}$, which can provide a sufficient security against the brute-force attack for ordinary business applications. In the case that the opponents possess exact knowledge about the key schedule, then they try to bypass by guessing the key and instead directly guess the 32-bit sub keys $K_{\text{sub}}^{j}, j = 0, \cdots, 3$. In that way, the opponents will exhaustively search $2^{32} \cdot 2^{32} \cdot 2^{32} \cdot 2^{32} = 2^{128}$ possible combinations, which indicates that the opponents still have to confront this extremely heavy work.

Statistical Analysis

To frustrate those attacks based on statistical analysis, the uniform distribution of encrypted image and low correlation between two adjacent encrypted pixels are demanded.

Histogram

The histogram of encrypted image is illustrated to characterize the randomness. Considering the trait of different images, we just post the histograms of “Lena”, “Testpat” and “Black” as well as the corresponding encrypted images in Fig.7. From the observation of the second column, the encrypted values inherit the Gaussian distribution property introduced by the measurement matrix. In contrast, the proposed method completely dissipates this Gaussian distribution replaced by a fairly uniform distribution as shown in the third column. It indicates that the proposed algorithm has a good ability of confusion and high resistance against the statistical attack [35].

Correlation of Two Adjacent Pixels

To evaluate the correlation between two adjacent pixels in vertical, horizontal and diagonal directions, we carry out the following procedure. Randomly select 2000 pairs of adjacent pixels from the original image and encrypted image, respectively. Let $\left(x_i, y_i\right)$ denote the i^{th} selected pair's pixel intensity. Each pair is regarded as a coordinate and placed in the rectangular coordinate system. Intuitively, as shown in the third column of Fig.8, the disordered distribution without the regular pattern indicates that the low correlation between two adjacent pixels. Same with the histogram test, we just show the test results of “Lena”, “Testpat” and “Black” as well as the corresponding encrypted images in Fig.8. We conclude the test in the horizontal direction and in the diagonal/vertical direction return similar results indeed. Moreover, the correlation is based on equation (9) and the results are listed in Table 1. These data demonstrate that the proposed method can result in one order of magnitude correlation reduction comparing with the outputs of methods [10-13].

$$r_{xy} = \frac{\left|\operatorname{cov}\left(x, y\right)\right|}{\sqrt{D\left(x\right)} \times \sqrt{D\left(y\right)}} \tag{9}$$

where x and y are gray-scale values of two adjacent pixels in the image. In numerical computation, the following discrete formulas are used:

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

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

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

Sensitivity Analysis

Sensitivity means that a slight change in one parameter results in a total different output. Good sensitivity is a basic requirement of an encryption method.

Key Sensitivity

Key sensitivity is defined as the degree of encrypted image's change caused by key's tiny change [3]. Fig.6(b) shows the decrypted image using the one-bit different key $\tilde{K}=\left(\mathrm{0123456789ABCDEF0123456789ABCDEE}\right)_{\mathrm{hex}}$.

The noise-like reconstruction result does not leak any perceptive information. Image “Testpat” is encrypted using K and $\tilde{K}$, respectively. The corresponding encrypted images and their difference image have been depicted in Fig.6(d) through Fig.6(f) for perceptual observation. In Table 2, we list the changing rate which is the percentage of different pixels between two cipher images encrypted by K and $\tilde{K}$, respectively. This result shows that even a slightly different key brings great changes in the encrypted image.

Plaintext Sensitivity

Plaintext sensitivity is to test the influence of changing a single pixel in the original image on the cipher pixels [3]. Since linear measurement process of compressive sensing plays a role in sampling data, in this situation, the quantized measurements $\tilde{\mathbf{Y}}$ are regarded as “plain image”. We deem that this test approach is reasonable. Because the security strength of the second encryption stage must be not stronger than that of entire cryptosystem, in this case, we modify one bit of $\tilde{\mathbf{Y}}$ in arbitrary position, then calculate the number of pixel change rate (NPCR) and the unified average changing intensity (UACI) which are defined by equation (10) and equation (11), respectively.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times M} \times 100\% \tag{10}$$

$$\mathrm{UACI} = \frac{1}{M \times M}\left[\sum_{i,j} \frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right] \times 100\% \tag{11}$$

where the symbol C_1 and C_2 denote the encrypted images whose corresponding “plain images” have only one bit difference.

The average experimental results of five selected images are listed in Table 3, showing the influence of round on the diffusion performance. For image encryption algorithm with satisfactory property of diffusion, the values of NPCR and UACI are close to 0.9961 and 0.3346, respectively [36]. Comparing with Zhou's algorithm [17] and Liao's algorithm [18], the proposed method can achieve the full diffusion so that NPCR and UACI values are large enough to the ideal encryption system after only two rounds of iteration. The above results manifest the achievement of collision-free data exchange and optimal diffusion. We exclude the CS-based image encryption methods [10-13] from the comparison due to the inefficient diffusion mechanism. The resistance against the chosen-plaintext attack is endowed owing to this full diffusion property.

Ciphertext Sensitivity

Ciphertext sensitivity is a measurement to authenticate the data integrity and generally expected from cryptographic techniques [24]. As mentioned in the second item of challenging issues, CTR mode enables implementing encryption in parallel and resisting against the chosen-plaintext attack by using non-repeating counters. However, it is distinct that each block is independent and a bit-flip error in some block of encrypted image only causes an error propagation within the corresponding block of the original image. In the proposal, the dependencies among blocks are built by the communication unit. If the encrypted image is obtained from two or more rounds of encryption, one bit change in the encrypted image leads to a non-recognizable decrypted image. The proposed method takes the data integrity seriously and is appropriate for the private teleconsultation. The same measurement NPCR and UACI are used for exhibiting the ciphertext sensitivity. The average values of five selected images are listed in Table 4. Here, it should be noted that the optimal value of UACI becomes close to 0.25 due to the Gaussian distribution property of the quantized measurements.

Avalanche Criterion

The avalanche criterion is known as a test about the changing rate, which measures the percentage of the changed bits in the encrypted image when one bit alteration in the original image occurs. In the ideal case, this value should be exactly equal to 50%. The test results comparison with the existing methods are listed in Table.5. It can be seen that the changing rate in our method is extremely close to the ideal case and comparable with the existing methods.

Information Entropy Analysis

Information entropy can be used to characterize the uncertainty and it is calculated by $H(C)=\sum P(C_{i,j})\log_2(1/C_{i,j})$. For a gray image, if the 2^8 values appear with equal probability, the entropy $H(C)$ reaches the maximum value 8. The entropy of encrypted image is tested under different rounds. From Table 6, the entropy $H(C)$ is close to the maximum value 8, which implies that the encrypted image has good confusion property.

Efficiency analysis

This scheme enhances the security of the previous works [10-13] in the relatively high-efficiency mode. There are four mainly contributing factors:

(1) Compressive sensing directly captures a compressed signal representation without going through the intermediate stage of acquiring Nyquist rate samples.

(2) In the second encryption stage, the manipulated target is the dimension reduction quantized measurements.

(3) Parallel structure allows the users to encrypt/decrypt blocks simultaneously.

(4) Optimal diffusion. After only two rounds of encryption, full diffusion can be achieved.

The Table 7 compares the encryption time of the proposed scheme with those of two existing parallel image encryption methods [17, 18]. For each algorithm, the encryption is implemented iteratively until the full diffusion property is achieved. Considering that multiply processors work in parallel, the essential assumption is that each processor possesses the equivalent processing capacity. The time counter is triggered from the image sampling stage. All experiments are performed using MATLAB R2010b on a personal computer with a 1.8 GHZ Athlon Dual-Core Processor, 2 GB memory and 120 GB harddisk capacity. The encryption time results in Table 7 indicate that the proposed scheme outperforms both Zhou's method and Liao's method with respect to the encryption speed.

Conclusion

In this paper, we investigate the weakness of CS-based encryption schemes which fails to resist against the chosen-plaintext attack. Hence we propose a parallel image encryption scheme under the compressive sampling circumstance to enhance the security and performance. We design a block cipher structure that consists of scrambling, mixing, S-box and block-wise XOR with chaotic lattice. We obtain collision-free data exchange and optimal diffusion by considering well-designed communication unit in the algorithm. The proposed scheme has the ability of resistance to the chosen-plaintext attack and outperforms the existing parallel image encryption with respect to the compressibility and the encryption speed. We confirm the security and performance enhancement through the experimental results.

Reference

[1] S. A. Vanstone, A. J. Menezes, and P. C. Oorschot (1999) Handbook of Applied Cryptography. Boca Raton, FL: CRC Press.

[2] R. A. Mollin (2006) An Introduction to Cryptography. Boca Raton, FL: CRC Press.

[3] S. G. Lian (2008) Multimedia Content Encryption. Boca Raton, FL: CRC Press.

[4] C. P. Wu and C. C. J. Kuo (2000) Fast Encryption Methods for Audiovisual Data Confidentiality. In Proceedings of SPIE, pp: 284-295.

[5] A. A. Shtewi, B. E. M. Hasan, and A. E. F. Hegazy (2010) An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems. International Journal of Computer Science and Network Security, 10(2) 226-232.

[6] M. Grangetto, E. Magli, and G. Olmo (2006) Multimedia Selective Encryption by Means of Randomized Arithmetic Coding. IEEE Transactions on Multimedia, 8(5) 905-917.

[7] E. J. Cand`es, J. Romberg, and T. Tao (2006) Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Frequecny Information. IEEE Transactions on Information Theory, 52(2) 489-509.

[8] D. L. Donoho (2006) Compressive Sensing. IEEE Transactions on Information Theory, 52(4) 1289-1306.

[9] R. G. Baraniuk (2007) Compressive Sensing. IEEE Signal Processing Magazine, 24(4) 118-121.

[10] Y. Rachlin and D. Baron (2008) The Secrecy of Compressed Sensing Measurements. In 46th Annual Allerton Conference on Communication, Control and Computing, September, pp: 813-817.

[11] A. Orsdemir, H. O. Altun, G. Sharma, and M. F . Bocko (2008) On the Security and Robustness of Encryption via Compressed Sensing. In IEEE Military Communications Conference, pp: 1-7.

[12] D. H. Liu, G. M. Shi, D. H. Gao, and M. Gao (2009) A Robust Image Encryption Scheme over Wireless Channels. In International Conference on Wireless Communications & Signal Processing, pp: 1-6.

[13] D.H. Gao, D. H. Liu, Y. Q. Feng and F. P. Yu (2010) A Robust Image Transmission Scheme for Wireless Channels Based on Compressive Sensing. In ICIC'10 Proceedings of the Advanced intelligent computing theories and applications, pp: 334-341.

[14] L. Yu, J. P. Barbot, G. Zhang, and H. Sun (2010) Compressive Sensing with Chaotic Sequence. IEEE Signal Processing Letters, 17(8) 731-734.

[15] M. Lustig, D. L. Donoho, J. M. Santos, and J. M. Pauly (2008) Compressed Sensing MRI. IEEE Transactions on Signal Processing, 25(2) 72-82.

[16] O. Mirzaei, M. Yaghoobi and H. Irani (2011) A New Image Encryption Method: Parallel Sub-Image Encryption with Hyper Chaos. Nonlinear Dynamics,DOI: 10.1007/s11071-011-0006-6.

[17] Q. Zhou, K. Wong and X. F. Liao etc (2008) Parallel Image Encryption Algorithm based on Discretized Chaotic Map. Chaos Solitons & Fractals}, 38, 1081-1092.

[18] X. F. Liao, S. Y. Lai and Q. Zhou (2010) A Novel Image Encryption Algorithm based on Self-Adaptive Wave Transmission. Signal Processing, 90, 2714-2722.

[19] C. Gang, Z. X. Yu (2005) A Self-Adaptive Algorithm on Image Encryption. Journal of Software, 119(11) 1974-1982.

[20] L. Gan (2007) Block Compressed Sensing of Natural Images. In 15th International Conference on Digital Signal Processing, pp: 403-406.

[21] H. Lipmaa, P. Rogoway and D. Wagner (2000) CTR-Mode Encryption, Comments to NIST concerning ASE Modes of Operations.

[22] B. A. Olshausen and D. J. Field (1997) Sparse Coding with an Overcomplete Basis Set: A Strategy Employed by V1. Vision Research, 37(23):3311-3325.

[23] E. J. Cand`es and T. Tao (2005) Decoding by Linear Programming. IEEE Transactions on Information Theory, 51(12) 4203-4215.

[24] J. M. K. Mastan, G. A. Sathishkumar and K. B. Bagan (2011) A Color Image Encryption Technique Based on a Substitution-Permutation Network. In Advances in Computing and Communications, 193(5) 524-533.

[25] Q. Zhou, Y. Hu, and X. F. Liao (2010) Analysis of the Diffusion Property of Image Encryption Algorithm in Block-and-Permutation Mode and Its Implementation. Journal of Electronics \& Information Technology (in Chinese), 32(8) 2015-2018.

[26] S. Wang, J. Kuang, and J. Li etc (2002) Chaos-based Communication in a Large Community. Physics Review, 66(6) 1-4.

[27] J. A. Tropp and A. C. Gilbert (2007) Signal Recovery from Random Measurements via Orthogonal Matching Pursuit. IEEE Transactions on Information Theory, 53(12) 4655-4666.

[28] Q. Zhou, K. Wong, and X. F. Liao etc (2008) Parallel Image Encryption Algorithm based on Discretized Chaotic Map. Chaos, Solitons & Fractals, 38(4) 1081-1092.

[29] S. Lloyd (1982) Least squares quantization in PCM. IEEE Transactions on Information Theory, 28(2) 129-137.

[30] ``Specification for the Advanced Encryption Standard", \url{http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf}, 2001.

[31] T. Blumensath and M. E. Davies (2008) Gradient Pursuits. IEEE Transactions on Signal Processing, 56(6) 2370-2382.

[32] J. Bioucas and M. Figueiredo (2007) A New TwIST: Two-Step Iterative Shrinkage/Thresholding Algortihms for Image Restoration. IEEE Transactions on Image Processing, 16(12) 2992-3004.

[33] I. F. Gorodnitsky and B. D. Rao (1997) Sparse Signal Reconstruction from Limited Data Using FOCUSS: A Re-Weighted Norm Minmization Algorithm. IEEE Transactions on Signal Processing, 45(3) 600-616.

[34] B. Babadi, N. kalouptsidis and V. Tarokh (2010) SPARLS: The Sparse RLS Algorithm. IEEE Transactions on Signal Processing, 58(8) 4013-4025.

[35] P. Fei, S. S. Qiu and L. Min (2005) An Image Encryption Algorithm based on Mixed Chaotic Dynamic Systems and External Keys. In IEEE Internation Conference Communic Circuits & Systems, pp: 1135-1139.

[36] Y. Wu, J. P. Noonan and S. Agaian (2011) NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology: Journal of Selected Areas in Telecommunications, 2(4) 31-38.

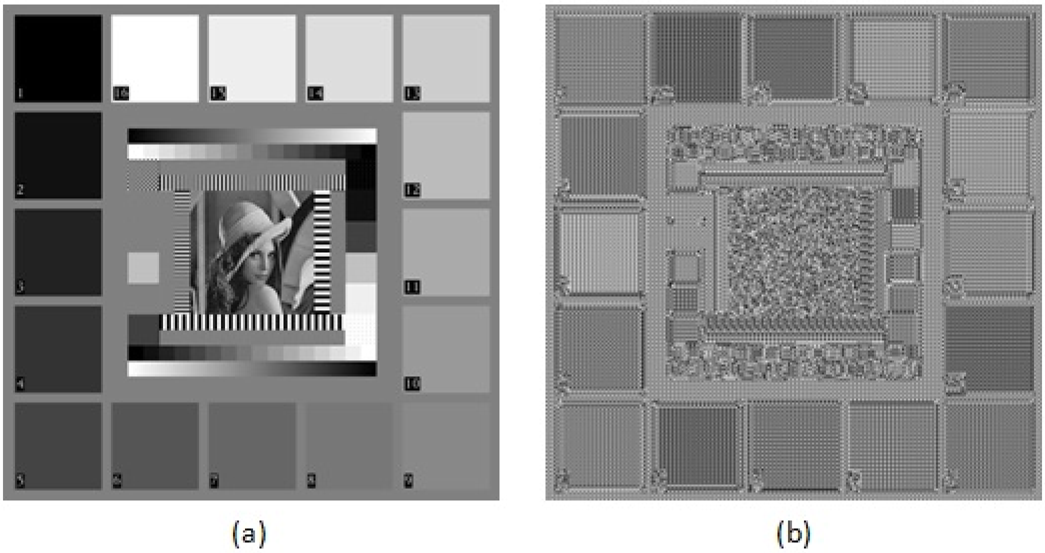


Fig.1 Application of the AES to original image (a) and its corresponding encrypted image (b).

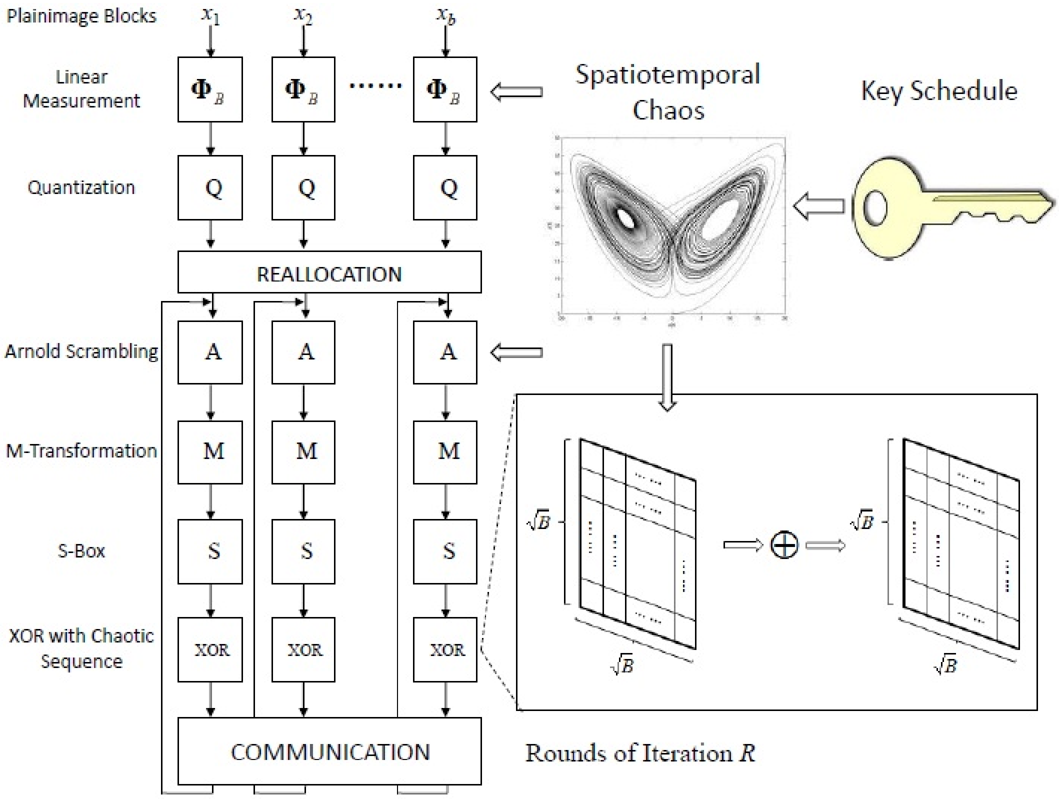


Fig.2 Frame diagram of the proposed encryption scheme structure.

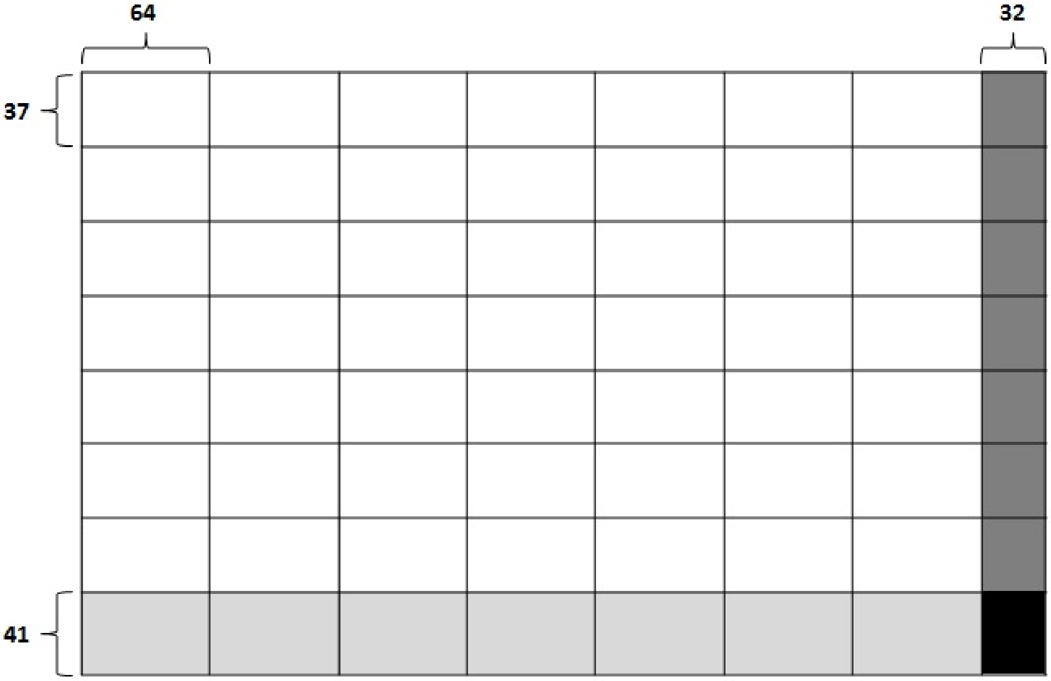
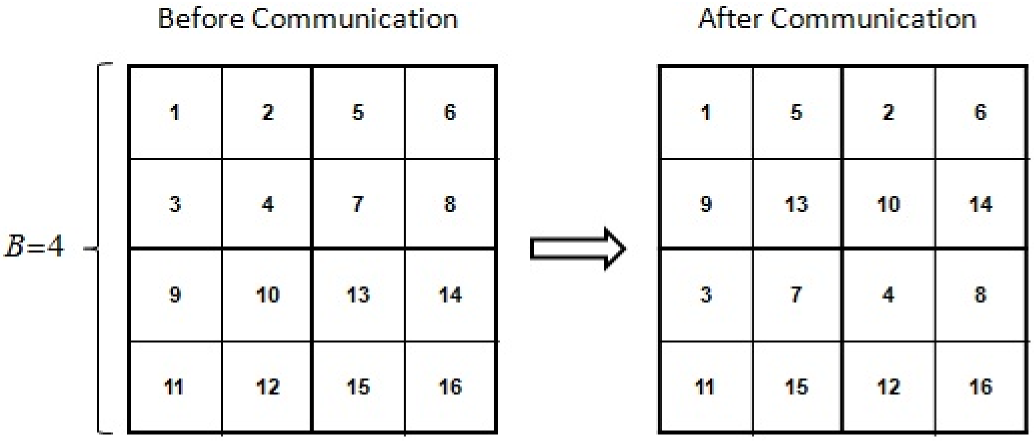


Fig.3 An example for non-square image.



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

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

Fig.4 An example for communication process.

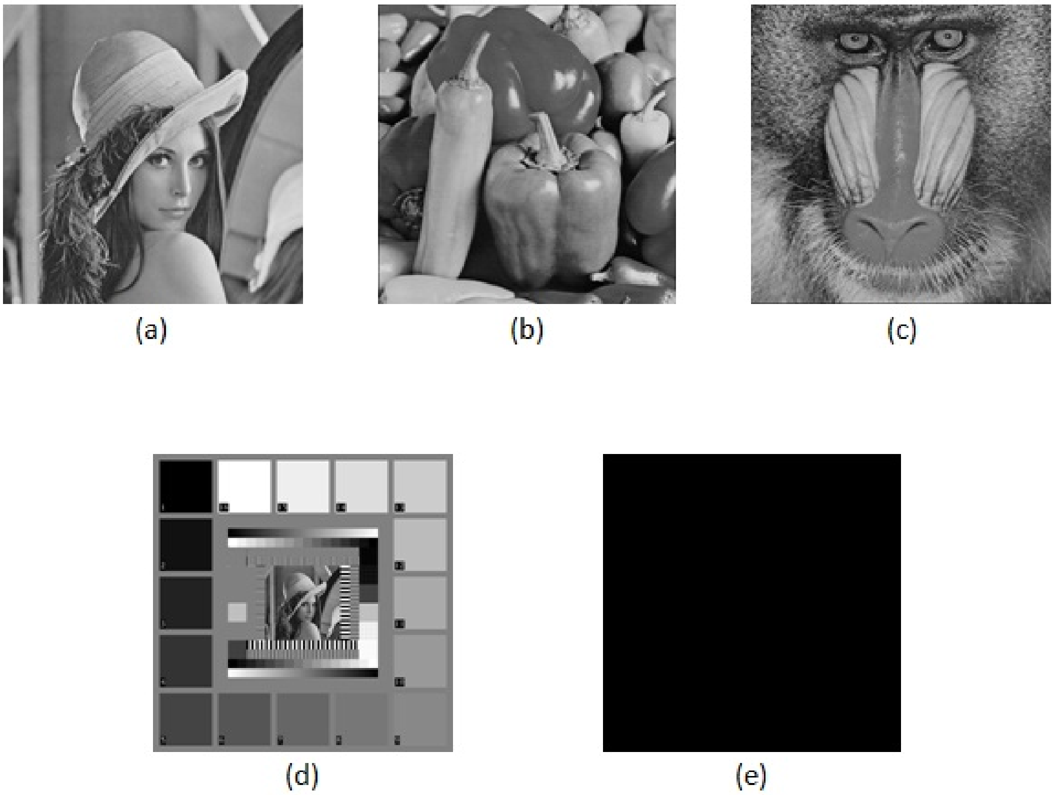


Fig.5 Five selected original images. (a) Lena; (b) Pepper; (c) Baboon; (d) Testpat; (e) Black.

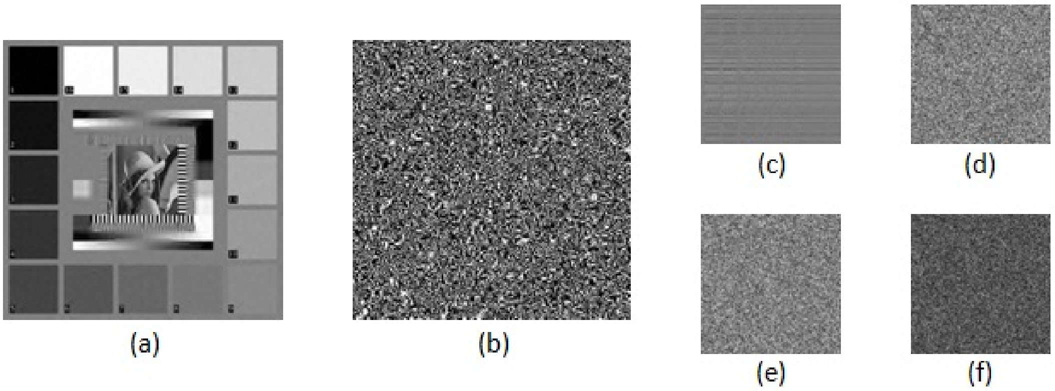
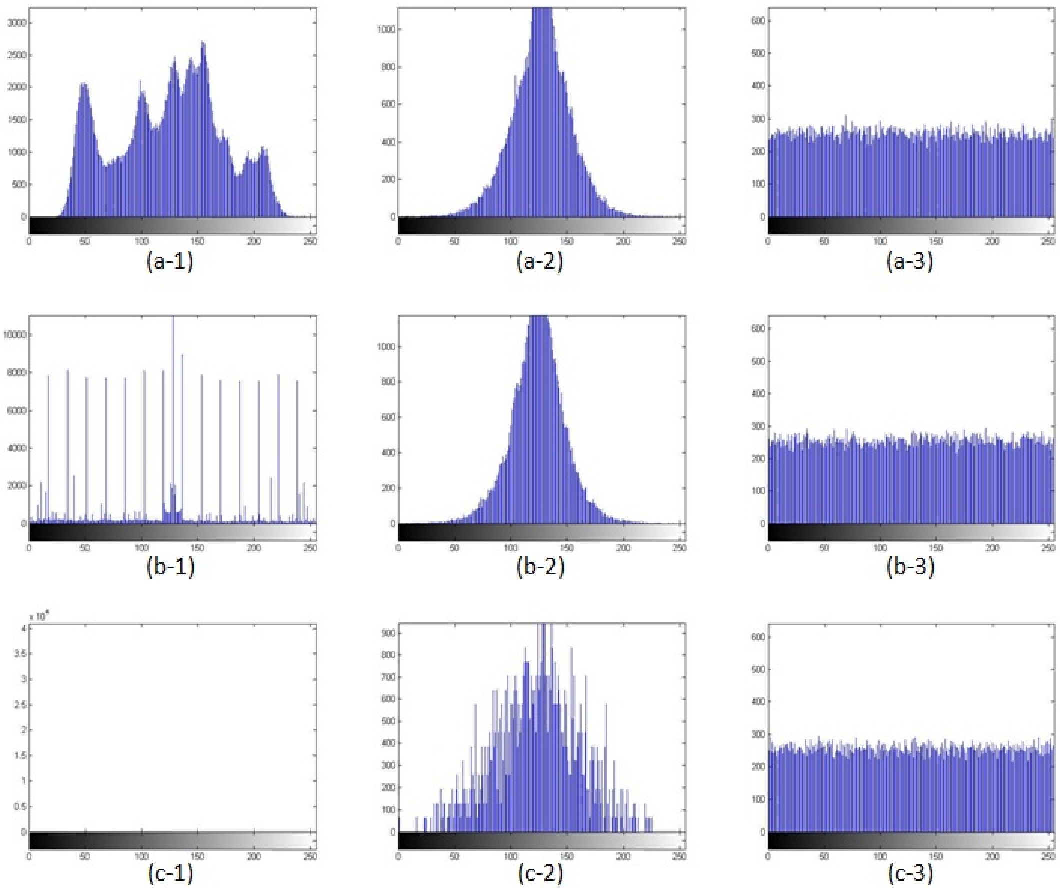


Fig.6 Reconstruction and key sensitivity test. The “Testpat” image is regarded as original image. (a) Decrypted image using K; (b) Decrypted image using $\tilde{K}$; (c) Encrypted image obtained from [10-13]; (d) Encrypted image using K; (e) Encrypted image using $\tilde{K}$; (f) Difference between encrypted image (d) and (e).



(a-1) (a-2) (a-3)

(b-1) (b-2) (b-3)

(c-1) (c-2) (c-3)

Fig.7 Histogram test. The first column lists the histograms of original images. The second and third columns list the histograms of encrypted images obtained from the methods [10-13] and the proposed method, respectively. The original test images are “Lena”, “Testpat” and “Black” from top to bottom in turn.

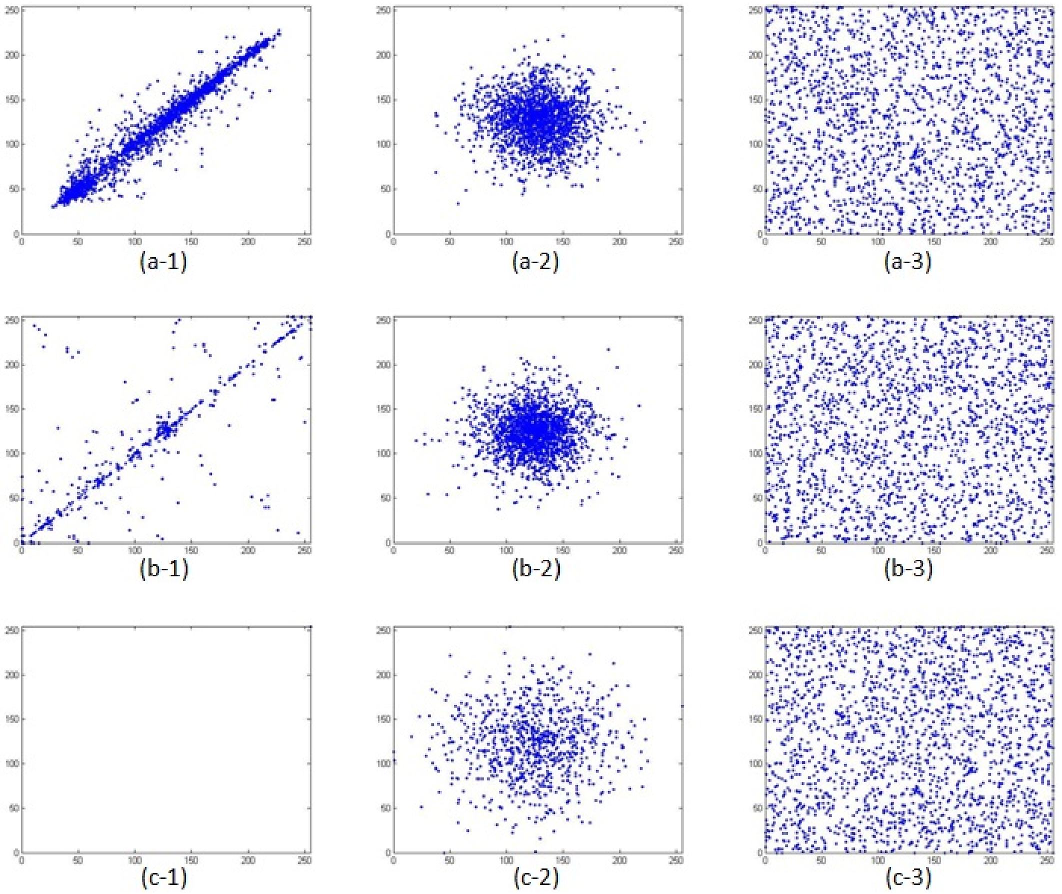


Fig.8 Correlation test. The first column lists the test results of original images. The second and third columns list the test results of encrypted images obtained from the methods [10-13] and the proposed method, respectively. The original test images are "Lena", "Testpat" and "Black" from top to bottom in turn.

Tab.1 Correlation Coefficient of Adjacent Pixels

Image Name	Direction	Test Results		
		Original Image	Encrypted Image in [10-13]	Encrypted Image in this proposal
Lena	Horizontal	0.9719	0.0215	0.0033
	Vertical	0.9850	0.0808	0.0009
	Diagonal	0.9593	0.0176	0.0058
Pepper	Horizontal	0.9771	0.0205	0.0007
	Vertical	0.9792	0.0737	0.0007
	Diagonal	0.9654	0.0174	0.0035
Baboon	Horizontal	0.8636	0.0213	0.0014
	Vertical	0.7519	0.0784	0.0011
	Diagonal	0.7213	0.0174	0.0045

Testpat	Horizontal	0.8748	0.0160	0.0015
	Vertical	0.9041	0.0731	0.0011
	Diagonal	0.8075	0.0194	0.0027
Black	Horizontal	∞	0.0214	0.0008
	Vertical	∞	0.0837	0.0046
	Diagonal	∞	0.0187	0.0039

Tab.2 Key Sensibility at Different Rounds

Image Name	Round	Changing Rate	Image Name	Round	Changing Rate
Lena	1	0.9965	Testpat	1	0.9972
	2	0.9971		2	0.9975
Pepper	1	0.9972	Black	1	0.9972
	2	0.9967		2	0.9973
Baboon	1	0.9974			
	2	0.9980			

Tab.3 NPCR and UACI Performance for Measuring the Plaintext Sensitivity

Round	Test Item	Zhou’s Method [17]	Liao’s Method [18]	Proposed Method
1	NPCR	0.0039	7.629×10^{-6}	0.0038
	UACI	0.0014	8.976×10^{-8}	0.0013
2	NPCR	0.2500	1.526×10^{-5}	0.9979
	UACI	0.0846	2.094×10^{-7}	0.3348
3	NPCR	0.9961	0.9957	0.9965
	UACI	0.3357	0.3351	0.3359
4	NPCR	0.9962	0.9974	0.9962
	UACI	0.3331	0.3342	0.3354

Tab.4 NPCR and UACI Performance for Measuring the Ciphertext Sensitivity

Round	Test Item	Zhou’s Method [17]	Liao’s Method [18]	Proposed Method
1	NPCR	0.0038	0.4981	0.0039
	UACI	0.0013	0.1412	0.0016
2	NPCR	0.2500	0.7471	0.9922

	UACI	0.0646	0.2147	0.2445
3	NPCR	0.9961	0.9960	0.9962
	UACI	0.2581	0.2868	0.2589
4	NPCR	0.9961	0.9960	0.9959
	UACI	0.2547	0.2868	0.2599

Tab.5 Avalanche Criterion

Round	Zhou’s Method [17]	Liao’s Method [18]	Proposed Method
1	0.0017	2.861×10^{-6}	0.0018
2	0.1248	3.815×10^{-6}	0.5016
3	0.5007	0.5003	0.4997
4	0.4996	0.5001	0.5004

Tab.6 Entropy Test

Image Name	Round	H(C)	
		Method [10-13]	Proposed Method
Lena	1	6.8048	7.9973
	2	6.6765	7.9971
Pepper	1	6.8567	7.9974
	2	6.7091	7.9975
Baboon	1	6.8661	7.9971
	2	6.7909	7.9973
Testpat	1	6.6694	7.9972
	2	6.5629	7.9975
Black	1	7.2538	7.9969
	2	7.1185	7.9973

Tab.7 Encryption Time (unit: second)

Zhou’s Method [17]	Liao’s Method [18]	Proposed Method
0.729	0.510	0.317