A secure image permutation–substitution framework based on chaos and compressive sensing

Rui Zhang and Di Xiao

Abstract
Existing secure image acquisition works based on compressive sensing, viewing compressive sensing–based imaging system as a symmetric cryptosystem, can only achieve asymptotic spherical security denoting that the ciphertext only leaks information about the energy of plaintext. Thereby, compressive sensing–based secure image acquisition systems usually work in some scenarios of friendly attack, such as brute-force attack for the entire key space and ciphertext-only attack for the complete plaintext. In this article, a novel permutation–confusion strategy using chaos and compressive sensing is put forward to protect the privacy-crucial images from more threatening malicious attacks, including known-plaintext attack and chosen-plaintext attack. Security guarantee is provided by one-time random projection of compressive sensing, sample-level permutation, and bit-level substitution. It is noteworthy that double confidentiality is embedded in compressive sensing–based image acquisition process using the key-related measurement matrix and sparsifying basis and the randomness is improved. Simulation experiments and security analyses suggest that the proposed framework can achieve a high-level security and the performance of image reconstruction can be distinctly improved.

Keywords
Image security, compressive sensing, chaotic system, permutation, confusion

Date received: 29 November 2019; accepted: 24 February 2020

Handling Editor: Leo Zhang

Introduction
With the rapid development of multimedia technology, digital image has become an increasingly prevalent information carrier over the Internet. With the awakening of awareness that data are the treasure, personal privacy information contained in digital image is attracting more and more attention from malicious attackers. Image security is of great importance in both military and commercial fields. Fortunately, a large number of image-oriented privacy-preserving techniques are constantly emerging, for instance, image encryption, image digital signature, secret image sharing, and image information hiding. Image encryption is the most straightforward way.

In essence, all kinds of image encryption techniques aim at achieving both diffusion and confusion effects, which were identified as the two essential properties of a secure cipher by Shannon. Diffusion means the statistics redundancy of the plaintext is dissipated into the statistics of ciphertext, while confusion aims to break the connection between the ciphertext and the key. For an encryption algorithm with good diffusion, the ciphertext will change absolutely in a pseudo-random

Key Laboratory of Dependable Service Computing in Cyber Physical Society of Ministry of Education, College of Computer Science, Chongqing University, Chongqing, China

Corresponding author:
Di Xiao, Key Laboratory of Dependable Service Computing in Cyber Physical Society of Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, China.
Email: xiaodi_cqu@hotmail.com
manner when even one bit in the plain domain is changed. Confusion makes it difficult for attackers to reveal the key, though they hold numerous plaintext–ciphertext pairs generated by the same key. One of the simplest methods to achieve both diffusion and confusion is a permutation–substitution network. In general, permutation is to scramble the position of pixel or bit and substitution is to change pixel values in the field of image encryption.

Expect for the above image encryption techniques, some pioneering works tried to embed confidentiality feature in the process of compressed sampling. Compressed sampling (also called compressive sensing, CS), a merging sampling theory, is able to sample and compress simultaneously without the limit of Shannon–Nyquist sampling theorem and exactly reconstructs the original signal from very few measurements (samples) as long as the measurement matrix obeys some energy-preserving conditions. When CS is regarded as a symmetric cipher, the original signal, the reconstructed signal, and the measurement matrix are considered as the plaintext, the ciphertext, and the key, respectively. Accordingly, sampling and reconstruction process denote encryption and decryption process, respectively. From this point of view, CS has the potential of integrating sampling, compression, and encryption in the only one physical layer at a minimal cost. CS-based cipher works under a simple fact that it is computationally infeasible to recover the plaintext from the intercepted ciphertext without the complete knowledge of the corresponding measurement matrix. To avoid transmitting a large-scale measurement matrix, chaotic systems were suggested to produce the measurement matrix and the initial parameters (seed values) controlling a chaotic sequence were viewed as the shared key between the encoder and the decoder. It should be noted that CS-based cryptosystem is generally required to work under one-time pad, that is, the same measurement matrix is used only once. For reusing the key of CS-based cipher, Zhang et al. proposed a CS-based product cipher by embedding randomness in both measurement matrix and sparsifying basis. In view of the linearity of CS projection, CS-based cipher can achieve computational secrecy rather than information-theoretical secrecy. According to a latest research, attackers could not reveal any valuable information but the energy about the original signal from the noise-like measurements when the measurement matrix consists of the independent and identically distributed (i.i.d.) Gaussian entries. In light of this observation, it was suggested that normalizing all measurements and regarding the normalized measurements as the ciphertext would get a perfect version of CS-based cipher. The fact that CS-based cipher can achieve the asymptotic spherical security was defined by Cambareri et al.

Recently, applying CS-based cipher to image encryption has attracted more and more attentions. Under the CS-based cipher model, CS-based imaging system can not only reduce the redundancy of image data but also provide some privacy-preserving properties to some extents. Chai et al. combined CS and steganography to generate a visually secure image. Zhang et al. proposed a scalable image encryption framework at different compression ratios, in which block CS works together with a Sobel edge detector and cascade chaotic maps. George and Pattathil produced the measurement matrix by utilizing multiple chaotic maps. Moreover, they proposed a method of constructing a random measurement matrix based on the linear feedback shift register (LFSR). Zhou et al. created a key-dependent measurement matrix using the circulant matrices and controlling the original row vectors of the circulant matrices with logistic map. Besides, they considered the partial Hadamard matrix as the measurement matrix controlled by chaotic map and the acquired measurements are further scrambled. Liu et al. combined CS and chaos to compress, fuse, and encrypt images simultaneously, in which the random measurement matrix is constructed from a logistic sequence and the acquired measurements are further fused by an adaptive-weighted fusion rule. For the purpose of alleviating the burden of information and communication systems, Zhou et al. proposed a simultaneous image encryption–compression scheme based on two-dimensional (2D) CS and hyperchaos.

In this article, we focus on how to design an image-oriented CS-based product cipher with the help of chaos. Considering that CS-based cipher is a lightweight cipher, we give a supplementary way to improve the security. Finally, a novel image sampling–compression–encryption framework is proposed for secure image acquisition, in which a high-level confidentiality is achieved through two approaches. One is that both the measurement matrix and sparsifying basis controlled by a same chaotic system are regarded as the shared secrets between the encoder and the decoder. Specifically, the elements of measurement matrix come from a chaotic sequence controlled by tent map, and the column vectors of a selected sparsifying basis are randomly permuted by leveraging the same tent map. Even having figured out either measurement matrix or sparsifying basis, attackers are still unable to reconstruct the original signal from CS measurements successfully. The other is that the captured data are further encrypted to breakout the linearity constraint of CS-based cipher by performing the sample-level permutation and the bit-level XOR, which are also manipulated.
by tent map. Obviously, diffusion and confusion effects can be easily achieved due to good pseudo randomness. In essence, the proposed imaging system is a two-layer cryptosystem consisting of CS-based cipher and chaos-based encryption.

The rest of this article is organized as follows. In section “Related works,” we briefly introduce some related knowledge about edge computing and CS-based cryptosystem and then point out some existing challenges in this field. In section “The proposed framework,” a double-secrecy encryption framework based on CS and chaos is proposed. Simulation experiments and analysis are given in section “Experimental results and security analyses.” Finally, conclusion is drawn in section “Conclusion.”

Related works

In this section, we introduce some fundamental knowledge about CS theory, chaos theory, and how to embed cryptographic feature in CS.

A brief review of CS

CS is an alternative to Shannon–Nyquist sampling when a signal is sparse or compressible. We denote a one-dimensional (1D) signal to be sampled as a column vector \( x = (x_1, x_2, \ldots, x_N)^T \). Assume that a transform basis \( \Psi = [\psi_1, \psi_2, \ldots, \psi_N] \) with size \( N \times N \) can provide a sparse representation for a 1D signal \( x \in \mathbb{R}^N \)

\[
    x = \sum_{i=1}^{N} s_i \psi_i = \Psi s \tag{1}
\]

where the column vector \( s \) contains only \( K \) non-zero entries. Thereby, \( x \) is said to be \( K \)-sparse in the sparsifying basis \( \Psi \). Fortunately, most natural images can be sparsely or compressively represented in a certain domain through some linear transforms, such as discrete wavelet transform (DWT) and discrete cosine transform (DCT). Note that a compressible signal can be transformed to be sparse after an overwhelming number of small coefficients in a certain domain are made to zeros.

In the CS framework, sampling and compression for a 1D signal \( x \) can be achieved simultaneously by a linear projection

\[
    y = \Phi s = \Phi \Psi^{-1} x \tag{2}
\]

where \( \Phi \) is a dimensionality-reducing measurement matrix with size \( M \times N (K < M = N) \) and \( y \in \mathbb{R}^M \) is the sensed measurement vector. Evidently, equation (2) does not have a unique solution. A significant achievement is that very few measurements contain all acquired information of recovering \( x \) exactly, since the measurement matrix \( \Phi \) obeys some energy-preserving guarantees.\(^{14-16} \)

In view of the sparsity, an instinctive method of reconstruction is to resolve the \( l_0 \) optimization problem

\[
    \hat{s} = \arg \min_{s} \|s\|_0 \quad \text{s.t.} \quad y = \Phi s \tag{3}
\]

\[
    \hat{x} = \Psi \hat{s}
\]

where \( \hat{s} \) and \( \hat{x} \) denote the approximate versions because of the lossy compression of CS. Unfortunately, equation (3) is a NP-hard problem.\(^{29} \)

Equation (3) can be relaxed as the \( l_1 \) optimization problem

\[
    \hat{s} = \arg \min_{s} \|s\|_1 \quad \text{s.t.} \quad y = \Phi s \tag{4}
\]

An important precondition is that measurement matrix \( \Phi \) must satisfy restricted isometry property \((\text{RIP})\).\(^{14} \)

There are some typical matrices satisfying RIP, including Gaussian and Bernoulli measurement matrix with \( M \geq O(K \log(N/K)) \) rows.\(^{30} \)

Definition 1. A matrix \( \Phi \) with size \( M \times N \) is said to satisfy the RIP of order \( K \) if there exists a constant \( \delta_K \in (0, 1) \) such that\(^{14} \)

\[
    (1 - \delta_K) \| \omega \|_2^2 \leq \| \Phi \omega \|_2^2 \leq (1 + \delta_K) \| \omega \|_2^2 \tag{5}
\]

holds for any one \( K \)-sparse vector \( \omega \).

Chaotic encryption

In dynamical systems, chaos is extremely sensitive to initial conditions. Although the systems are deterministic, the sequences produced through iterating chaotic map show excellent pseudo randomness. Applying chaotic theory, the practice of cryptography has attracted much interest in the past 30 years, which utilizes the chaotic sequence to encrypt the plaintext. In view of its good randomness and large key space, thousands of chaotic encryption algorithms have been proposed, all of which take aim at a good diffusion–confusion effect by concealing the connection between ciphertext and plaintext as well as the used chaotic sequence. A common chaotic behavior is the tent map, which is defined as

\[
    z_{i+1} = T(z_i, \mu) = \begin{cases} 
    \frac{z_i}{\mu}, & \text{if } 0 < z_i < \mu \\
    1 - \frac{z_i}{\mu}, & \text{if } \mu < z_i < 1
    \end{cases} \tag{6}
\]

where \( i = \{0, 1, 2, \ldots\} \) and the parameters \( \{z_0, \mu\} \in (0, 1) \). Unlike the logistic map, the probability density function of tent map approximately follows the uniform distribution. Its great pseudo-random performance and high sensitivity to initial parameters make it...
almost impossible to find the real key by the exhaustive search to key space or guessing without a clue.

**CS-based cipher**

When viewed as a cryptosystem at the same time, CS-based information acquisition system can provide a certain level of confidentiality guarantee while compressively sampling. As shown in Figure 1, in the common framework of CS-based cipher, the original signal \( x \), the sensed measurements \( y \), and the measurement matrix \( \Phi \) is viewed as the plaintext, the ciphertext, and the key, respectively. In addition, \( \Phi \) needs to be updated frequently, even in a one-time setup, resulting from that it is not hard to figure out the fixed \( \Phi \) from the sufficient plaintext–ciphertext pairs.

To avoid transmitting the large-scale \( \Phi \), a practical solution is that the pseudo-random number generator (PRNG) is used to construct \( \Phi \) in the sense player and the initial parameters (seed values) controlling PRNG are viewed as the key known by only the encoder and the decoder. Recently, using chaotic systems to construct measurement matrix has drawn much attention. Yu et al.\(^\text{17}\) employed a logistic map to construct \( \Phi \) and proved that such a chaotic matrix may satisfy RIP with high probability. Frunzete et al.\(^\text{18}\) adopted tent map instead, which shows a higher strength of resisting statistical attacks in CS-based secure applications. Secure key exchange can be realized through two approaches. One is that the key is generated from the local agreed password. The other is that the key is secretly shared between the encoder and the decoder with the help of key-exchange protocols.

To avoid updating the key of CS-based cipher frequently, Zhang et al.\(^\text{19}\) provided a bi-level protected CS framework based on RIP-less theory,\(^\text{16,31}\) in which the measurement matrix is a key-controlled RIP matrix, \( \Psi \) is a key-related sparsifying basis, and \( \Phi \Psi^{-1} \) is a structural non-RIP matrix. To say the least, attackers have the potential of figuring out the non-RIP matrix \( \Phi \Psi^{-1} \) rather than reconstructing \( x \) through known-plaintext attack (KPA)\(^\text{32}\) and chosen-plaintext attack (CPA). Therefore, anyone intending to recover the plaintext \( x \) from the ciphertext \( y \) must hold the real keys of both \( \Phi \) and \( \Psi \).

**The proposed framework**

In this section, a double-secrecy encryption approach based on CS and chaos and an additional chaotic encryption are introduced in detail. Moreover, a novel sampling–compression–encryption framework is proposed to realize secure compressed imaging.

**Embedding double secrecy in one-time projection of CS**

As mentioned previously, one-time random projection of CS can perform image sampling, compression, and encryption simultaneously. Almost all CS-based cryptosystems work under a common framework, in which one-time measurement matrix \( \Phi \) generated by a key-controlled PRNG is viewed as the shared secret between the encoder and the decoder. Generally speaking, the security of the plaintext \( x \) mainly depends on the size of the key space and the credibility of the key management. The size of the key space is usually large enough to resist the brute-force attack when a chaotic sequence is used to construct \( \Phi \). The credibility of key management depends on the trust in the key holders, the key-exchange protocol, and the physical security. To improve the security of CS-based imaging system, we propose a dual-image encryption scheme without additional hardware cost.

Most of existing CS-based ciphers are based on the fact that the decoding process is doomed to failure.
when there is no information about \( \Phi \). In other words, embedding cryptographic feature in the process of CS decoding rests only on the measurement matrix and sparsifying basis \( \Psi \) is generally considered to be public. According to a latest study, \(^{19} \Psi \) can be transformed into an equivalent form \( \Psi' \) through random permutation.

**Definition 2.** \( \Psi \) and \( \Psi' \) are two equivalent sparsifying bases (i.e. \( \Psi = \Psi' = x, \| s \|_0 = \| s \|_1 = K \) if\(^9 \)

\[
\Psi = \Psi' \mathbf{P}
\]  

(7)

where \( \mathbf{P} \) is a random permutation matrix. Such a random permutation matrix can be generated using the tent map by the following steps:

- **Step 1.** Initialize the permutation matrix \( \mathbf{P} \) to an identity matrix with size \( N \times N \).
- **Step 2.** Iterate the tent map with the key \( k_p = \{ t_0, \mu^3 \} \) to generate a chaotic sequence \( \{ C^1_i \} \) \(_{i=1}^{2N} \).
- **Step 3.** Calculate \( \{ C^1_i \} \) \(_{i=1}^{2N} = \{ C^2_i \} \) \(_{i=1}^{MN} \).
- **Step 4.** Divide the acquired integer sequence \( \{ C^1_i \} \) \(_{i=1}^{2N} \) into two sequences \( \{ C^1_i \} \) \(_{i=1}^{N} \) and \( \{ C^2_i \} \) \(_{i=1}^{N} \).
- **Step 5.** Exchange the \( C^1_i \) \(_{i=1}^{N} \) th column (or row) and the \( C^2_i \) \(_{i=1}^{N} \) th column (or row) in \( \mathbf{P} \).
- **Step 6.** Repeat Step 5 until \( i \) iterates through \( \{1, 2, \ldots, N\} \).

Obviously, random permutation matrix \( \mathbf{P} \) is directly related with the key \( k_p \) of a chaotic system. It means that the permuted sparsifying basis \( \Psi' \) would be endowed with the cryptographic feature to some extent when \( k_p \) is shared only between the encoder and the decoder.

Tent map has been proved to be suitable for constructing measurement matrix \( \Phi \). Accordingly, a certain level of confidentiality provided by chaos can be embedded in process of CS decoding. Such a measurement matrix \( \Phi \) can be generated using the tent map by the following steps:

- **Step 1.** Initialize the measurement matrix to a null matrix \( \Phi \) with size \( M \times N \).
- **Step 2.** Iterate the tent map with the key \( k_b = \{ t_0, \mu^2 \} \) to generate a chaotic sequence \( \{ C^2_i \} \) \(_{i=1}^{MN} \).
- **Step 3.** Calculate \( \{ C^2_i \} \) \(_{i=1}^{MN} = \{ C^4_i \} \) \(_{i=1}^{MN} \).
- **Step 4.** Construct \( \Phi \) column-by-column using the regularized sequence \( \{ C^4_i \} \) \(_{i=1}^{MN} \), as follows

\[
\Phi = \sqrt{\frac{2}{M}} \begin{pmatrix}
C^1_1 & C^1_2 & \cdots & C^1_{2M} \\
C^2_1 & C^2_2 & \cdots & C^2_{2M} \\
\vdots & \vdots & \ddots & \vdots \\
C^4_1 & C^4_2 & \cdots & C^4_{2M}
\end{pmatrix}
\]  

(8)

where the scalar \( \sqrt{2/M} \) is for normalization.

It is not hard to come to a conclusion that transmitting the two keys, \( k_b \) and \( k_p \), secretly by a secure auxiliary channel or key-exchange protocol can provide such a CS-based cipher with double confidentiality.

**Chaotic permutation–substitution encryption**

As mentioned previously, CS-based cipher can only provide a computational guarantee of secrecy and the energy of the plaintext \( x \) can be revealed through the cryptanalysis on the ciphertext \( y \). Such security constriction is rooted in the linearity of CS. To improve the secrecy of the acquired data, some chaos-based strong encryption methods, including sample-level permutation and bit-level XOR, are used after CS-based secure compressed imaging. Note that CS measurement \( y \) is considered to be public, so it should be quantized in advance. Here, we use a standard uniform quantizer \( Q(\cdot) \) with levels 256 to transform \( y \) into a binary format \( y^b = Q(y) = [y_{b1}, y_{b2}, \ldots, y_{bM}] \), where \( y^b \) is an integer vector in the interval \([0, 255]\).

Permutation is to scramble the position of CS measurements, which is done by putting them in a random order. A random index sequence \( \{ C^1_i \} \) \(_{i=1}^{M} \) can be generated using tent map with the succeeding steps:

- **Step 1.** Initialize a flag sequence \( \{ F^M_i \} \) \(_{i=1}^{M} \) and an index sequence \( \{ C^3_i \} \) \(_{i=1}^{M} \) to 0, and set the key \( k_p = \{ t_0, \mu^3 \} \) and \( i = j = 1 \).
- **Step 2.** Calculate \( z^3 = T(z_i^3, \mu^3) \) and \( \eta = [M \times z_i^3] \), and then set \( j = j + 1 \).
- **Step 3.** If \( F_i = 0 \), set \( C^3_i = \eta, F_i = 1, \) and \( i = i + 1 \).
- **Step 4.** Repeat Steps 2 and 3 until \( i > M \).

Therefore, a scrambled measurement vector \( y_c \) can be generated by the following transformation

\[
y_c = f_p(y, k_p) = [y_1, y_2, \ldots, y_M]
\]  

(9)

where \( f_p(\cdot) \) is a permutation function. Equation (9) means to reorder the sensed data according to the random indexes.

Substitution is further considered to change the statistical property. For a good confusion effect, substitution operation is done by performing the bitwise XOR operation between \( y' \) and a chaotic sequence. Such a chaotic sequence \( \{ C^1_i \} \) \(_{i=1}^{M} \) can be generated using tent map by the following steps:

- **Step 1.** Initialize a sequence \( \{ C^4_i \} \) \(_{i=1}^{M} \) to 0 and set the key \( k_s = \{ t_0, \mu^4 \} \).
- **Step 2.** Iterate the tent map to generate a chaotic sequence \( \{ C^4_i \} \) \(_{i=1}^{M} \in (0, 1) \).
Step 3. Calculate \( \{C_i^{M-1}\} = \{|C_i^j \times 10^{14}|\mod (255)\}_{i=1}^{M} \).

The chaotic sequence \( \{C_i^j\} \) controlled by the key \( k_i \) can be used to encrypt \( y' \) according to the following transformation

\[
y'' = f_i(y', k_i) = [y'_1 \oplus C_i^1, y'_2 \oplus C_i^2, \ldots, y'_M \oplus C_i^M]
\]

where the acquired \( y'' \) is regarded as the ciphertext to be transmitted through the public channels.

The proposed sampling–compression–encryption framework

The proposed CS-based double-secrecy cipher can provide a certain level of security guarantee, which can be implemented in the sense player of a low-cost information acquisition system. When there is a requirement for high confidentiality, some additional strong encryption methods need to be employed. Here, as shown in Figure 2, a sampling–compression–encryption framework is further proposed for secure image acquisition, whose security is guaranteed by the built-in CS-based cipher and the chaotic encryption.

Assume that the signal to be sampled is a gray image \( X \) with size \( N \times N \) and the corresponding sparse coefficient matrix is \( S \in \mathbb{R}^{N \times N} \), that is, \( S = \Psi X \Psi^T \), where \( \Psi \) is a fixed orthogonal DWT matrix. The random permutation matrix \( P \in \mathbb{I}_{2^N \times 2^N} \) and measurement matrix \( \Phi \in \mathbb{I}_{1 \times N} \) are constructed from two chaotic sequences \( \{C_i^j\}_{i=1}^{2^N} \) and \( \{C_i^{M-1}\} \) controlled by the keys \( k_p \) and \( k_s \). According to the above research, \( X = \Psi^T S \Psi = (\Psi \Phi)^T S (\Psi \Phi) \), \( \|S\|_0 = \|S\|_0 \). The proposed double-secrecy encryption (encoding) process can be implemented by the following one-time projection

\[
Y = \Phi \cdot (P\Psi) \cdot X \cdot (P\Psi)^T = \Phi \cdot P \cdot \Psi X \Psi^T \cdot P^T
\]

where \( Y \in \mathbb{I}_{M \times N} \) is the acquired measurements matrix. Obviously, the above process is controlled by two chaotic behaviors, resulting in double confidentiality.

When \( Y \) could not meet a high requirement of confidentiality, the proposed chaotic encryption based on confusion–diffusion mechanism needs to be further employed. Before it starts, \( Y \) must be vectorized and quantized, that is, \( y^b = Q(\text{Vec}(Y)) \). Two chaotic sequences \( \{C_i^j\}_{i=1}^{2^N} \) and \( \{C_i^{M-1}\} \) controlled by the keys \( k_p \) and \( k_s \) are used to implement the following permutation–substitution transformation

\[
y'' = f_i(f_p(y^b, k_p), k_s)
\]

Obviously, the whole sampling–compression–encryption process \( X \to y'' \) is controlled by the four keys \( \{k_p, k_s, k_p, k_s\} \) and is composed of CS-based lightweight encryption and chaotic encryption. Therefore, theoretically speaking, the proposed secure image acquisition framework can achieve a high-level confidentiality.

Experimental results and security analyses

In this section, several simulations are implemented by MATLAB 2016b in Window 7 to demonstrate the high security of the proposed framework. A standard 512 \times 512 Lena image is considered as the test image, which can be sparsely represented by 2D discrete

![Figure 2. The proposed framework.](image)
wavelet transformation (DWT2). Without loss of generality, the compression ratio is set to 0.5 and the orthogonal matching pursuit (OMP) algorithm is utilized to reconstruct the original image. Based on the tent map, the keys \( k_C = f_{0:45, 0:60} \) and \( k_F = f_{0:50, 0:55} \) are used to construct the permutation matrix \( P \) and the measurement matrix \( F \), respectively, and the keys \( k_p = f_{0:55, 0:50} \) and \( k_s = f_{0:60, 0:45} \) are used to perform the permutation operation \( f_P \) and the substitution operation \( f_s \), respectively. For a more intuitive result, the ciphertexts are still expressed in the image format. The original image, the CS-based encrypted image, the finally encrypted image, and the decrypted image are shown in Figure 3(a)–(d), respectively.

**Figure 3.** (a) The original image, (b) the CS-based encrypted image, (c) the finally encrypted image, and (d) the decrypted image (PSNR = 32.56).

**Figure 4.** The histograms of different images: (a) the original image, (b) the CS-based encrypted image, and (c) the finally encrypted image.

Histogram analysis

In the field of image processing, the histogram of an image normally refers to a histogram of the pixel values. The histogram of image is an important statistical characteristic, which is usually considered as an approximation of the density function. Generally speaking, an ideal image encryption algorithm has the ability to realize that the encrypted image would not reveal any statistical feature of the original image.

The histogram of the original image, the encrypted image, and the decrypted image are shown in Figure 4. Obviously, the pixel values of the finally encrypted image well distribute in the interval \([0, 255]\), which stands for an excellent encrypted result. However, the pixel values of the CS-based encrypted image approximately follow Guassian distribution, which is not accidental, resulting from a fact that CS measurements follows sub-Guassian distribution. It can be therefore said that the proposed privacy-preserving framework can conceal the statistical characteristic of the plaintext well.

Correlation analysis

After encryption process is performed, an obvious space correlation for the neighboring pixels in a natural image always appears, which is a kind of meaningful information in some privacy-preserving scenarios. Hence, it is very crucial for an image encryption
algorithm to avoid leaking the correlation. There is a mathematical definition of the correlation coefficient, $Cor$, used to assess the correlation between two adjacent pixels, which is expressed as follows

\[
Cor(X) = \frac{\sum_{i=1}^{m} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{m} (x_i - E(x))^2} \sqrt{\sum_{i=1}^{m} (y_i - E(y))^2}}
\]

where $x_i$ and $y_i$ are the two randomly selected pixel values of test image $X$, $m$ is the selected pixel pairs, and $E(\cdot)$ means to compute the mean value.

In our experiments, 2000 pairs of adjacent pixels are selected randomly from the original image, the CS-based encrypted image, and the finally encrypted image in the horizontal, vertical, and diagonal directions. As shown in Table 1, any two adjacent pixels in the original images are tightly correlated with each other but the correlation coefficients of the finally encrypted image are close to 0 in all directions. A more intuitive experimental result is shown in Figure 5. In general, CS-based encryption does well in only the vertical and diagonal directions but does not work in the horizontal direction. And the correlation is completely broken up after chaotic encryption is performed.

### Key sensitivity analysis

In the proposed encryption framework, four chaotic sequences related with four keys $\{k_p, k_q, k_s, k_t\}$ are generated by utilizing the tent map, $k_q$ and $k_t$ controlling measurement matrix and sparsifying basis, respectively, used to finish the CS-based sampling, compression, and encryption. $k_p$ and $k_s$ are used to finish the proposed chaotic encryption. Theoretically, anyone who would like to recover the original image (plaintext) $X$ must hold all the above keys at the same time. What is known to us is that chaotic system is extremely sensitive to the input initial parameters (viewed as a key). Here, it will demonstrate how difficult for an attacker to get these real keys without any prior knowledge.

In our experiments, a seemingly tiny change $10^{-15}$ takes place in every key, and then these changed key are used to recover the original image. Note that only one key is changed in every experiment. As shown in Figure 6(a)–(c), the decrypted images can not reveal any meaningful information once one key is false. Figure 6(d) denotes that the decryption (reconstruction) algorithm cannot work completely after the bitwise XOR operation is performed. Here, we emphasize a conclusion that the proposed image encryption scheme can not only flexibly meet the different levels of security requirement but also be considered as a multi-party management system by distributing the four keys to several authorized individuals.

### Attack analysis

**Brute-force attack.** Brute-force attack means that an attacker tries to guess the possible keys and uses them for decryption. In the proposed framework, a chaotic system is used to perform CS-based sampling–compression–encryption, sample-level permutation, and bit-level substitution operations. The above key-sensitivity test intuitively demonstrates that the whole key space is large enough to make brute-force attack infeasible, which is therefore said to be computational secrecy.

**Ciphertext-only attack.** Ciphertext-only attack (COA) means that an attacker tries to get some valuable information about the plaintext only from the ciphertext. The security of the proposed framework depends on two kinds of privacy-preserving operations, including CS-based encryption and chaotic permutation–substitution encryption. In view of the linearity of CS projection, an interesting security feature of the CS-based cryptosystem under COA is the asymptotic spherical secrecy, meaning that any two different plaintexts with the same power keep approximately indistinguishable from their ciphertext. Such a property is attributed to the energy-preserving guarantee of RIP. In the proposed framework, the chaos-based bitwise XOR operation (substitution) can break the energy-preserving property such that attackers would not reveal any valuable information through COA.

**KPA and CPA.** As for the standalone CS-based cryptosystem, at least $N$ independent plaintext–ciphertext pairs ($512 \times 512$ pairs for $512 \times 512$ Lena image) are

---

**Table 1.** Correlation coefficients.

| Different images                | Directions | Horizontal | Vertical  | Diagonal |
|---------------------------------|------------|------------|-----------|----------|
| The original image              |            | 0.9687     | 0.9830    | -0.0191  |
| The CS-based encrypted image    |            | 0.9855     | -0.0618   | 0.0041   |
| The finally encrypted image     |            | 0.9570     | -0.0485   | 0.0052   |

CS: compressive sensing.
Figure 5. Correlations between two adjacent pixels selected from different images in the different directions. The original image, CS-based encrypted image, and finally encrypted image in the (a) horizontal direction, (b) vertical direction, and (c) diagonal direction.

Figure 6. The decrypted image using a false key: (a) $k_b + 10^{-15}$, (b) $k_v + 10^{-15}$, (c) $k_p + 10^{-15}$, and (d) $k_s + 10^{-15}$.
needed to figure out the used measurement matrix. Only when the measurement matrix is reused multiple times the attackers are likely to reveal the plaintext from the intercepted ciphertext through CS reconstruction algorithm. But in the proposed framework, the final ciphertext approximately completely loses the feature of measurements such that there is no energy-preserving guarantee. Besides, the keys controlling $F$ and $C$ would be frequently updated. Hence, attackers are not able to get both the used $F$ as well as $C$ and the energy information of the plaintext, meaning a failure under KPA or CPA scenario.

**Comparison**

In this part, the superiority of the proposed framework is demonstrated by comparing it with some existing works. First, we present some potential attack types in this field, including attack type I: brute-force attack to the whole key space or guess at possible measurement matrices, attack type II: reveal the energy information of plaintext by COA, and attack type III: calculate the used measurement matrix by KPA or CPA. Then, we analyzed their resistance to the above attack types. Finally, their security levels are given in Table 2. CS-based sampling–compression–encryption framework, in which single chaos or multiple chaotic map(s) is used to construct measurement matrix, is a lightweight cipher. The bi-level protected CS framework is a prominent work but still could not get rid of the linear relationship between plaintext and ciphertext. In Zhou et al. and Liu et al., some additional privacy-preserving methods are integrated with CS-based cipher to enhance the confidentiality, but their confusion–diffusion effects are still not outstanding. In the proposed framework, not only is CS-based cipher embedded with double secrecy but also sample-level permutation and bit-level substitution (XOR operation) are used to guarantee a great confusion–diffusion effect.

**Conclusion**

In this article, it is pointed out that CS-based image acquisition systems have the potential to perform sampling, compression, and encryption simultaneously. Besides, how to design the CS-based cipher is deeply studied from two feasible view points, that is, the key-dependent measurement matrix and the key-related sparsifying basis. Moreover, we employ a chaotic system to realize a CS-based cipher with double confidentiality. Considering that CS measurements cannot provide an adequate guarantee of confidentiality, an intrinsic weakness of CS-based cipher, an additional encryption approach based on chaos, and diffusion–confusion mechanism have been proposed. Combining the CS-based double-secrecy cipher with the permutation–substitution encryption, we proposed a novel sampling–compression–encryption framework for secure image acquisition. Based on the simulation experiments and analyses, it is therefore said that the proposed framework achieves a high-level security.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Chongqing Research Program of Basic Research and Frontier Technology (Grant No. cstc2017jcyjBX0008), the Chongqing Postgraduate Education Reform Project (Grant No. yjg183018), and the Chongqing University Postgraduate Education Reform Project (Grant No. cquyjg18219).

**ORCID IDs**

Rui Zhang https://orcid.org/0000-0002-4233-1858

Di Xiao https://orcid.org/0000-0002-6958-5807

**References**

1. Guan Z-H, Huang F and Guan W. Chaos-based image encryption algorithm. *Phys Lett A* 2005; 346(1): 153–157.
2. Lu CS and Liao HYM. Structural digital signature for image authentication: An incidental distortion resistant scheme. *IEEE T Multimedia* 2003; 5(2): 161–173.
3. Moulin P and O’Sullivan J. Information-theoretic analysis of information hiding. IEEE T Inf Theory 1999; 49(3): 563–593.

4. Shannon C. Communication theory of secrecy systems. Bell Syst Tech J 1948; 28(4): 656–715.

5. Heys HM and Tavares SE. Substitution–permutation networks resistant to differential and linear cryptanalysis. J Cryptol 1996; 9(1): 1–19.

6. Wang X-Y, Chen F and Wang T. A new compound mode of confusion and diffusion for block encryption of image based on chaos. Commun Nonlinear Sci 2010; 15(9): 2479–2485.

7. Zhang Y and Xiao D. An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Commun Nonlinear Sci 2014; 19(1): 74–82.

8. Chen J-X, Zhu Z-L, Fu C, et al. An efficient image encryption scheme using lookup table-based confusion and diffusion. Nonlinear Dynam 2015; 81(3): 1151–1166.

9. Rachlin Y and Baron D. The secrecy of compressed sensing measurements. In: Proceedings of the 2008 46th Allerton conference on communication, control, and computing, Urbana, IL, 23–26 September 2008, pp.813–817. New York: IEEE.

10. Orsdemir A, Altun HO, Sharma G, et al. On the security and robustness of encryption via compressed sensing. In: Proceedings of the 2008 IEEE military communications conference, San Diego, CA, 16–19 November 2008, pp.1–7. New York: IEEE.

11. Donoho DL. Compressed sensing. IEEE T Inf Theory 2006; 52(4): 1289–1306.

12. Candès EJ and Wakin MB. An introduction to compressive sampling. IEEE Signal Process Mag 2008; 25(2): 21–30.

13. Candès EJ, Romberg J and Tao T. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE T Inf Theory 2006; 52(2): 489–509.

14. Baraniuk R, Davenport M, DeVore R, et al. A simple proof of the restricted isometry property for random matrices. Constr Approx 2008; 28(3): 253–263.

15. Candès EJ and Tao T. Near-optimal signal recovery from random projections: universal encoding strategies? IEEE T Inf Theory 2006; 52(12): 5406–5425.

16. Kueng R and Gross D. Ripless compressed sensing from anisotropic measurements. Linear Algebra App 2014; 441: 110–123.

17. Yu L, Barbot JP, Zheng G, et al. Compressive sensing with chaotic sequence. IEEE Signal Process Lett 2010; 17(8): 731–734.

18. Frunzete M, Yu L, Barbot JP, et al. Compressive sensing matrix designed by tent map, for secure data transmission. In: Proceedings of the signal processing algorithms, architectures, arrangements, and applications conference, Poznan, 29–30 September 2011, pp.1–6. New York: IEEE.

19. Zhang LY, Wong KW, Zhang Y, et al. Bi-level protected compressive sampling. IEEE T Multimedia 2016; 18(9): 1720–1732.

20. Bianchi T, Bioglio V and Magli E. Analysis of one-time random projections for privacy preserving compressed sensing. IEEE T Inf Foren Sec 2016; 11(2): 313–327.

21. Cambareri V, Mangia M, Pareschi F, et al. Low-complexity multiclass encryption by compressed sensing. IEEE T Signal Process 2015; 63(9): 2183–2195.

22. Chai X, Gan Z, Chen Y, et al. A visually secure image encryption scheme based on compressive sensing. Signal Process 2017; 134: 35–51.

23. Zhang Y, Zhou J, Chen F, et al. A block compressive sensing based scalable encryption framework for protecting significant image regions. Int J Bifurcat Chaos 2016; 26(11): 1650191.

24. George SN and Pattathil DP. A novel approach for secure compressive sensing of images using multiple chaotic maps. J Optics 2014; 43(1): 1–17.

25. George SN and Pattathil DP. A secure LFSR based random measurement matrix for compressive sensing. Sens Imag 2014; 15(1): 85.

26. Zhou N, Zhang A, Zheng F, et al. Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. Opt Laser Technol 2014; 62: 152–160.

27. Zhou N, Pan S, Cheng S, et al. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing. Opt Laser Technol 2016; 82: 121–133.

28. Liu X, Mei W and Du H. Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos. Opt Commun 2016; 366: 22–32.

29. Candès EJ and Tao T. Decoding by linear programming. IEEE T Inf Theor 2005; 51(12): 4203–4215.

30. Mendelson S, Pajor A and Tomczak-Jaegermann N. Uniform uncertainty principle for Bernoulli and sub-Gaussian ensembles. Constr Approx 2008; 28(3): 277–289.

31. Candès EJ and Plan Y. A probabilistic and ripless theory of compressed sensing. IEEE T Inf Theory 2011; 57(11): 7235–7254.

32. Cambareri V, Mangia M, Pareschi F, et al. On known-plaintext attacks to a compressed sensing-based encryption: a quantitative analysis. IEEE T Inf Foren Sec 2015; 10(10): 2182–2195.