Neurocomputing 205 (2016) 472–480

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Embedding cryptographic features in compressive sensing

Yushu Zhang [a,b,c,*], Jiantao Zhou [b], Fei Chen [c], Leo Yu Zhang [b,c], Kwok-Wo Wong [d], Xing He [a], Di Xiao [e]

[a] Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, College of Electronic and Information Engineering, Southwest University, Chongqing 400715, China.
[b] Department of Computer and Information Science, Faculty of Science and Technology, University of Macau, Macau
[c] College of Computer Science and Engineering, Shenzhen University, Shenzhen 518060, China
[d] Department of Electronic Engineering, City University of Hong Kong, Kowloon, Hong Kong
[e] College of Computer Science, Chongqing University, Chongqing 400044, China

ARTICLE INFO

Article history:
Received 23 August 2015
Received in revised form
19 January 2016
Accepted 5 April 2016
Communicated by W.K. Wong
Available online 13 May 2016

Keywords:
Secure compressive sensing
Symmetric-key cipher
Parallel compressive sensing
Random permutation

ABSTRACT

Compressive sensing (CS) has been widely studied and applied in many fields. Recently, the way to perform secure compressive sensing (SCS) has become a topic of growing interest. The existing works on SCS usually take the sensing matrix as a key and can only be considered as preliminary explorations on SCS. In this paper, we firstly propose some possible encryption models for CS. It is believed that these models will provide a new point of view and stimulate further research in both CS and cryptography. Then, we demonstrate that random permutation is an acceptable permutation with overwhelming probability, which can effectively relax the Restricted Isometry Constant for parallel compressive sensing. Moreover, random permutation is utilized to design a secure parallel compressive sensing scheme. Security analysis indicates that the proposed scheme can achieve the asymptotic spherical secrecy. Meanwhile, the realization of chaos is used to validate the feasibility of one of the proposed encryption models for CS. Lastly, results verify that the embedding random permutation based encryption enhances the compression performance and the scheme possesses high transmission robustness against additive white Gaussian noise and cropping attack.

1. Introduction

Making use of the sparseness of natural signals, compressive sensing (CS) [6,15,9,8] unifies sampling and compression to reduce the data acquisition and computational load of the encoder, at the cost of a higher computational complexity at the decoder. If the CS framework can integrate with certain cryptographic features for simultaneous sampling, compression and encryption, its application areas can be extended to, for example, limited-resource sensor and video surveillance. It has been suggested in [8] that CS framework leads to an encryption scheme, where the sensing matrix can be considered as an encryption key. In recent years, there exist some pioneer works on secure compressive sensing (SCS) [25,24,20,12,31,1–5]. Rachlin and Baron [25] found that CS cannot achieve perfect secrecy but can guarantee computational secrecy. The definition of perfect secrecy [29] requires that the occurrence probability of a message conditioned on the cryptogram is equal to the *a priori* probability of the message, $P(X=x|Y=y)=P(X=x)$. Alternatively, the mutual information satisfies $I(X;Y)=0$. In contrast to perfect secrecy, computational secrecy relies on the difficulty in solving a hard computational problem (e.g. NP-hard) at the computation resources available to the adversary. Orsdemir et al. [24] investigated the security and robustness of employing a secret sensing matrix. They evaluated the security against brute force and structured attacks. The analyses indicate that the computational complexity of these attacks renders them infeasible in practice. In addition, this SCS method was found to have fair robustness against additive noise, making it a promising encryption technique for multimedia applications. Hossein et al. [20] also addressed the perfect secrecy problem for the scenario that the measurement matrix as a key is known to both the sender and the receiver. Similar results have been obtained, as reported in [25]. It is shown that the Shannon perfect secrecy is, in general, not achievable by such a SCS method while a weaker sense of perfect secrecy may be achieved under certain conditions. Agrawal and Vishwanath[1] employed the CS framework to establish secure physical layer communication over a Wyner wiretap channel. They showed that CS can exploit channel asymmetry so that a message that is encoded as a sparse vector is decodable with high probability at the receiver while it is impossible to decode with high probability by the eavesdropper.

* Corresponding author at: Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, College of Electronic and Information Engineering, Southwest University, Chongqing 400715, China.
E-mail address: yushuboshi@163.com (Y. Zhang).

http://dx.doi.org/10.1016/j.neucom.2016.04.053
0925-2312/

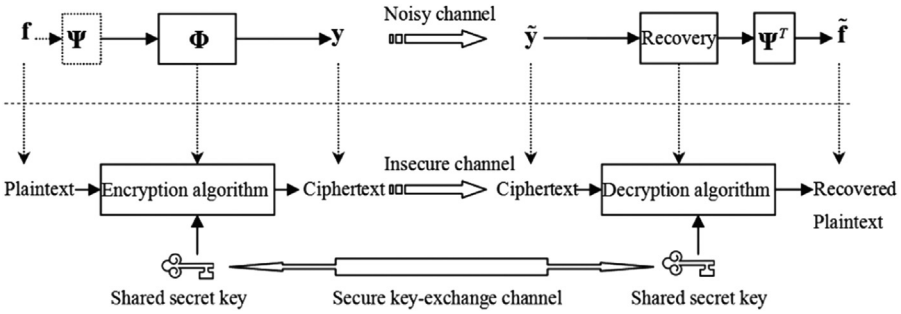

Fig. 1. The relationship between CS and symmetric-key cipher.

Dautov and Tsouri [12] proposed an encryption scheme where the sensing matrix is established using wireless physical layer security and linear feedback shift register with the corresponding *m*-sequences. It is shown that by using a Rician fading channel, the proposed scheme generates valid CS matrices while preventing access from an eavesdropper in close proximity to one of the legitimate participants. Cambareri et al. [4] designed a two-class information concealing system based on perturbing the measurement matrix, in which the first-class users can reconstruct the signal to its full resolution while the second-class ones are able to retrieve only a degraded version of the same signal. This two-class case is further extended to multiclass case in [5]. Yang et al. [31] extended the perfect secrecy criteria to measure the security in the information theory frame, which involve the plaintext sparsity feature and the mutual information of the ciphertext, key, and plaintext. Bianchi et al. [2,3] demonstrated that the attacker leverages random linear measurements which are generated by using Gaussian i.i.d. matrix and can only reveal the energy of the measurements for the signal. If the measurements are normalized, then the perfect secrecy is achievable.

This work contributes four aspects. First, associating CS with symmetric-key cryptography, we introduce possible encryption models for CS. Second, we demonstrate that random permutation is an acceptable permutation with overwhelming probability, which can effectively relax the Restricted Isometry Constant for parallel compressive sensing. Third, we design a secure parallel compressive sensing scheme based on random permutation. Results show that the embedding random permutation based encryption enhances the compression performance and the scheme possesses high transmission robustness against noise. The corresponding security analysis indicates that the proposed scheme can achieve the *asymptotic spherical secrecy*. In the end, this proposed scheme is implemented by chaos map to validate the feasibility of one of the proposed encryption models for CS.

The rest of this paper is organized as follows. The next section introduces some possible encryption models for CS. Section 3 demonstrates that random permutation is an acceptable permutation with overwhelming probability. By making use of random permutation, a secure parallel compressive sensing scheme followed by security analysis is designed in Section 4 and the realization of chaos in Section 5 to validate the feasibility of the proposed encryption models. Section 6 gives simulation results for the proposed encryption scheme. The last section concludes our work.

2. Some possible encryption models

Suppose an M-dimensional signal $\mathbf{f} \in \mathbb{R}^M$ is expressed as

$$\mathbf{f} = \sum_{i=1}^{M} x_i \boldsymbol{\psi}_i = \boldsymbol{\Psi}\mathbf{x}, \tag{1}$$

which means that $\mathbf{f}$ could be sparsely represented in a certain domain by the transform matrix $\boldsymbol{\Psi} := [\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots, \boldsymbol{\psi}_M]$ with each column vector $\boldsymbol{\psi}_i \in \mathbb{R}^M$, $i = 1, 2, \ldots, M$. We can say that $\mathbf{x}$ is exactly k-sparse if there are at most k non-zero coefficients in the $\boldsymbol{\Psi}$ domain. Instead of sampling $\mathbf{x}$ directly, we take a small number of CS measurements. Let $\boldsymbol{\Phi} := [\boldsymbol{\varphi}_1, \boldsymbol{\varphi}_2, \ldots, \boldsymbol{\varphi}_M]$ denote a $K \times M$ matrix with $K \ll M$. Then K non-adaptive linear samples $\mathbf{y}$ can be obtained by

$$\mathbf{y} = \boldsymbol{\Phi}\mathbf{f}. \tag{2}$$

The resultant CS measurements $\mathbf{y}$ are used for the recovery of the original signal by solving the following convex optimization problem

$$\min \|\mathbf{x}\|_1 \quad \text{s.t. } \mathbf{y} = \boldsymbol{\Phi}\boldsymbol{\Psi}\mathbf{x}$$
$$(\textit{or in noisy situation}: \ \|\boldsymbol{\Phi}\boldsymbol{\Psi}\mathbf{x} - \mathbf{y}\|_2 \le \varepsilon) \tag{3}$$

to obtain $\tilde{\mathbf{f}} = \boldsymbol{\Psi}\mathbf{x}$.

One of the central problems in CS framework is the selection of a proper measurement matrix $\boldsymbol{\Phi}$ satisfying the Restricted Isometry Property (RIP).

Definition 1 (*Candès and Tao [7]*). Matrix $\boldsymbol{\Phi}$ satisfies the Restricted Isometry Property of order s if there exists a constant $\delta_s \in [0, 1]$ such that

$$(1-\delta_s)\|\mathbf{x}\|_2^2 \le \|\boldsymbol{\Phi}\mathbf{x}\|_2^2 \le (1+\delta_s)\|\mathbf{x}\|_2^2 \tag{4}$$

for all s-sparse signals $\mathbf{x}$.

Candès and Tao [8] proposed that a matrix following the Gaussian or Bernoulli distribution satisfies RIP with overwhelming probability at sparsity $s \le O(K/\log M)$. The randomly selected Fourier basis also retains RIP with overwhelming probability, provided that the sparsity $s \le O\left(K/(\log M)^6\right)$.

The basic model of CS is shown in the upper half of Fig. 1, which includes two major aspects: measurements taking and signal recovery. From the perspective of symmetric-key cipher, measurements taking involves an encryption algorithm and signal recovery is associated with a decryption algorithm. The relationship between CS and symmetric-key cryptography indicates that some possible cryptographic features can be embedded in CS. To this end, we give some possible protection models for CS.

2.1. Embedding chaos in compressive sensing

For a random sensing matrix, its storage and transmission require a lot of space and energy. Thus, it is preferable to generate and handle the sensing matrix by one or more seed keys only. Yu et al. [32] proposed to construct the sensing matrix using chaotic sequence in a trivial manner and proved that the RIP of this kind of matrix is guaranteed with overwhelming probability, providing that the sparsity $s \le O(K/\log(M/s))$. They generated a sampled Logistic sequence $X(d, l, z_0)$, which has been regularized, with sampling distance d, length $l = K \times M$ and initial condition z_0. Then a matrix $\boldsymbol{\Phi}$ is created from this sequence column by column,

denoted as

$$\mathbf{\Phi}=\sqrt{\frac{2}{K}}\begin{pmatrix} z_0 & z_K & \cdots & z_{K(M-1)} \\ z_1 & z_{K+1} & \cdots & z_{K(M-1)+1} \\ \vdots & \vdots & \ddots & \vdots \\ z_{K-1} & z_{2K-1} & \cdots & z_{KM-1} \end{pmatrix} \tag{5}$$

where the scalar $\sqrt{2/K}$ is for normalization purpose. One can take the initial condition z_0 as a key, since different sensing matrices are obtained from different initial conditions. The adoption of chaos can further enhance the security due to its pseudo-random behavior and high sensitivity to the initial condition.

Frunzete et al. [18] further constructed the chaotic measurement matrix by introducing the one-dimensional skew tent map given by

$$z(k+1)=T[z(k);\mu]=\begin{cases}\dfrac{z(k)}{\mu}, & \text{if } 0<z(k)<\mu \\ \dfrac{1-z(k)}{1-\mu}, & \text{if } \mu\le z(k)<1\end{cases} \tag{6}$$

where the control parameter $\mu\in(0,1)$ and the initial state $z(0)\in(0,1)$. Unlike the Logistic map, the probability density function of skew tent map follows the uniform distribution, which has a higher strength in resisting statistical attacks in cryptographic applications.

2.2. Integrating optical imaging with compressive sensing

Romberg [28] proposed a universally efficient CS strategy, consisting of random waveform convolution and random time-domain subsampling. The signal $\mathbf{x}$ with a pulse h is randomly convoluted as $\mathbf{Hx}$, where

$$\mathbf{H}=M^{-1/2}\mathbf{F}^{*}\mathbf{\Sigma}\mathbf{F}. \tag{7}$$

The $\mathbf{F}$ represents the discrete Fourier matrix whose entries are

$$F_{\upsilon,t}=e^{-j2\pi(\upsilon-1)(t-1)/M},\quad 1\le\upsilon,t\le M. \tag{8}$$

The $\mathbf{\Sigma}$ is diagonal matrix whose nonzero entries are

$$\mathbf{\Sigma}=\begin{bmatrix}\varsigma_1 & 0 & \cdots & 0 \\ 0 & \varsigma_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \varsigma_M\end{bmatrix}, \tag{9}$$

where ς_υ are unit magnitude complex numbers with random phases as follows: $\varsigma_1=\pm1$ with equal probability; $\varsigma_{M/2+1}=\pm1$ with equal probability; $\varsigma_\upsilon=\exp(j\theta)$, where $2\le\upsilon<M/2+1$ and $\theta\in[0,2\pi]$ yields uniform distribution; $\varsigma_\upsilon=\varsigma^{*}_{M-\upsilon+2}$, i.e., the conjugate of $\varsigma_{M-\upsilon+2}$, where $M/2+2\le\upsilon<M$. After random convolution, random subsampling is performed by randomly choosing a small number of locations, or by breaking $\mathbf{Hx}$ into blocks and summarizing each block with a single randomized sum. These double random operations can be associated with double random phase encoding [26], which is the most classic optical encryption technique. Some cryptographic features can be embedded in random phases $\mathbf{\Sigma}$ and random subsampling. This simultaneously realizes optical sampling, compression and encryption. For example, such a framework has been designed in [40] with the architecture of double random masks, which is somewhat similar to double random phase encoding. Another heuristic investigation with respect to the integration of optical imaging and CS was given in [27], which demonstrated the possibility of achieving super-resolution with a single exposure by combining double random phase encoding and CS. Random phases can serve as keys to offer the security.

2.3. Diversity of measurement matrix

Do et al. [14] proposed a framework called structurally random matrix (SRM), defined as

$$\mathbf{\Phi}=\sqrt{\frac{K}{M}}\mathbf{DBR}, \tag{10}$$

where $\mathbf{R}\in\mathbb{R}^{M\times M}$ is either a uniform random permutation matrix or a diagonal random matrix whose diagonal entries R_{ii} are i.i.d. Bernoulli random variables with identical distribution $P(R_{ii}=\pm1)=\frac{1}{2}$. $\mathbf{B}\in\mathbb{R}^{M\times M}$ is an orthonormal matrix which is selected among popular fast computable transforms like DCT and $\mathbf{D}\in\mathbb{R}^{K\times M}$ represents a subsampling operator which selects a random subset of rows in the matrix $\mathbf{BR}$. The scalar coefficient $\sqrt{\frac{K}{M}}$ is chosen to normalize the transform so as to ensure that the energy of the measurement vector is almost close to that of the input signal. This SRM can serve as a secret due to the fact that the random permutation matrix $\mathbf{R}$ is a common technique in classic encryption schemes. For example, Zhang et al. [34] suggested a joint quantization and diffusion approach for the real-valued measurements based on the distribution of measurements of natural images sensed by structurally random ensemble. In addition, our work [36] also intended to design a robust coder for encrypted images over packet transmission networks based on SRM. Recently, Cambareri et al. [5] designed a novel multiclass encryption scheme based on perturbing the measurement matrix. The transmitter distributes the same encoded measurements to receivers with different privileges so that they are able to reconstruct the signal at various quality levels. Take the two-class situation as an example, the relationship between the two measurement matrices is formulated as

$$\mathbf{\Phi}^{(1)}=\mathbf{\Phi}^{(0)}+\Delta\mathbf{\Phi}, \tag{11}$$

where $\Delta\mathbf{\Phi}$ is an c-sparse perturbation matrix with entries

$$\Delta\Phi_{i,j}=\begin{cases}0, & (i,j)\notin C^{(0)} \\ -2\Delta\Phi_{i,j}, & (i,j)\in C^{(0)}\end{cases} \tag{12}$$

where $C^{(0)}$ is a subset of $c<KM$ entries chosen at random for each $\mathbf{\Phi}^{(0)}$ with density c/KM. A first-class user knowing the complete sampling matrix $\mathbf{\Phi}^{(1)}$ is able to exactly recover the signal while a second-class user only with the knowledge of $\mathbf{\Phi}^{(0)}$ is instead subject to an equivalent non-white noise term $\boldsymbol{\epsilon}=\Delta\mathbf{\Phi}\mathbf{x}$ because of the true sampling $\mathbf{y}=\mathbf{\Phi}^{(1)}\mathbf{x}$.

Li et al. [21] introduced a deterministic construction of sensing matrix via algebraic curves over finite fields, which is a natural generalization of DeVore's construction [13] using polynomials over finite fields. The diversity of algebraic curves provides numerous choices for the sensing matrices, i.e., more choices of key in the encryption scheme, which may be valuable for the potential use of the sensing matrix for cryptographic purpose.

3. Random permutation meets parallel compressive sensing

Traditionally, a multidimensional signal needs to be reshaped into an 1D signal prior to sampling using CS. Nevertheless, such a transformation makes the required size of the sensing matrix dramatically large and increases the storage and computational complexity significantly. To solve this problem, Fang et al. proposed a novel solution [17,16], referred to as parallel compressive sensing (PCS), which reshapes the multidimensional signal into a 2D signal and samples the latter column by column with the same sensing matrix. Moreover, a so-called acceptable permutation can effectively relax the RIP for PCS.

Definition 2 (*Fang et al. [17]*). For a 2D sparse signal $\mathbf{X}$ with sparsity vector $\mathbf{s}=[s_1,s_2,\ldots,s_N]$ satisfying $\|\mathbf{s}\|_1=s$, where s_j is the sparsity level of the j-th column of $\mathbf{X}$, a permutation $\mathbf{P}(\bullet)$ is called acceptable for $\mathbf{X}$ if the Chebyshev norm of the sparsity vector of $\mathbf{P}(\mathbf{X})$ is smaller than $\|\mathbf{s}\|_\infty$ of $\mathbf{X}$.

When a 2D $\mathbf{s}$-sparse signal is exactly reconstructed by using PCS, a sufficient condition is given by the following lemma.

Lemma 1 (*Fang et al. [17]*). *Consider a 2D $\mathbf{s}$-sparse signal $\mathbf{X}$, if the RIP of order $\|\mathbf{s}\|_\infty$ holds for the sensing matrix $\mathbf{\Phi}$, i.e., $\delta_{2\|\mathbf{s}\|_\infty}<\sqrt{2}-1$, then $\mathbf{X}$ can be exactly reconstructed using PCS scheme.*

This lemma implies that with respect to PCS, the RIP requirement of the sensing matrix $\mathbf{\Phi}$ at a given reconstruction quality is related to $\|\mathbf{s}\|_\infty$. A zigzag-scan permutation is considered acceptable in relaxing the RIP condition before using the PCS [17], but it is tailored for the sparse signal following a layer model. Fang et al. further generalized the permutation as random permutation for the 2D sparse signal whose distribution is unknown in advance to enhance reconstruction performance for PCS [16]. Although random permutation was suggested in [17] and further exploited in [16], but a strict mathematic proof has not been revealed. In the following, we give a mathematic derivation. Assume that $\mathbf{P}(\bullet)$ is a random permutation operation, then $\mathbf{X}^*=\mathbf{P}(\mathbf{X})$, where $\mathbf{X}^*\in\mathbb{R}^{M\times N}$ is a permuted 2D signal with sparsity vector $\mathbf{s}^*$. Observing the relationship between random and acceptable permutations, we have the following theorem.

Theorem 1. *For a 2D sparse signal $\mathbf{X}$, if the distribution of the sparsity level in each column is not sufficiently uniform ($\|\mathbf{s}\|_\infty=\sigma\cdot\lceil\frac{s}{N}\rceil$, where σ is assumed to be not less than 2.72 but $\|\mathbf{s}\|_\infty\ll M$), then the random permutation $\mathbf{P}(\bullet)$ can be an acceptable permutation with overwhelming probability.*

Proof. If $\|\mathbf{s}^*\|_\infty\le\|\mathbf{s}\|_\infty$, i.e., $\Pr\{\mathbf{P}(\bullet)\ \textit{is acceptable}\}=0$, meaning that each column of $\mathbf{X}$ tends to have similar sparsity levels, $\mathbf{P}(\bullet)$ does not work. However, such an $\mathbf{X}$ has relaxed the RIP requirement for PCS without permutation. Thus, we consider the $\mathbf{X}$ where the distribution of the sparsity level in each column is not sufficiently uniform, which, more importantly, accords with the feature of a natural signal. Each element in $\mathbf{X}$ will be randomly located at any index of $\mathbf{X}^*$, that is, the transition of all the indices from $\mathbf{X}$ to $\mathbf{X}^*$ yields the uniform distribution. Each non-zero element of $\mathbf{X}$ appears in each column of $\mathbf{X}^*$ with equal probability $\frac{1}{N}$. This has a strong resemblance to the classical probability problem of s balls and N boxes. The probability is given by

$$\begin{aligned}&\mathrm{P}\{\mathbf{P}(\bullet)\ \textit{is acceptable}\}\\&\quad=\mathrm{P}\{\|\mathbf{s}^*\|_\infty<\|\mathbf{s}\|_\infty\}\\&\quad=1-\mathrm{P}\{\|\mathbf{s}^*\|_\infty\ge\|\mathbf{s}\|_\infty\}\\&\quad=1-\sum_{k=\|\mathbf{s}\|_\infty}^{M}\mathrm{P}\{\|\mathbf{s}^*\|_\infty=k\}.\end{aligned}$$

Let the incident Λ_1 be the occurrence of $\|\mathbf{s}^*\|_\infty=k$ and the incident Λ_2 be the occurrence of $\exists j,s_j^*=k$. If Λ_1 occurs, then Λ_2 must occur; not vice versa. It means that the cardinality of Λ_1 is not greater than that of Λ_2 and furthermore,

$$\mathrm{P}\{\|\mathbf{s}^*\|_\infty=k\}\le\mathrm{P}\{\exists j,s_j^*=k\}.$$

On the other hand, apparently,

$$\mathrm{P}\{\exists j,s_j^*=k+1\}\le\mathrm{P}\{\exists j,s_j^*=k\}.$$

Thus,

$$\begin{aligned}&\mathrm{P}\{\mathbf{P}(\bullet)\ \textit{is acceptable}\}\\&\quad\ge1-\sum_{k=\|\mathbf{s}\|_\infty}^{M}\mathrm{P}\{\exists j,s_j^*=k\}\\&\quad\ge1-(M-\|\mathbf{s}\|_\infty+1)\mathrm{P}\{\exists j,s_j^*=\|\mathbf{s}\|_\infty\}.\end{aligned}$$

Let $p=\frac{\|\mathbf{s}\|_1}{MN}=\frac{s}{MN}$.

$$\mathrm{P}\{\exists j,s_j^*=\|\mathbf{s}\|_\infty\}=\binom{M}{\|\mathbf{s}\|_\infty}p^{\|\mathbf{s}\|_\infty}(1-p)^{M-\|\mathbf{s}\|_\infty}.$$

Due to the fact that $s\ll MN$ and then p is very small, we have

$$\binom{M}{\|\mathbf{s}\|_\infty}p^{\|\mathbf{s}\|_\infty}(1-p)^{M-\|\mathbf{s}\|_\infty}\approx\frac{\lambda^{\|\mathbf{s}\|_\infty}}{(\|\mathbf{s}\|_\infty)!}e^{-\lambda},$$

where $\lambda=pM=\frac{s}{N}$. $(\|\mathbf{s}\|_\infty)!$ can be calculated according to Stirling's approximation as follows

$$(\|\mathbf{s}\|_\infty)!\approx\sqrt{2\pi\|\mathbf{s}\|_\infty}\left(\frac{\|\mathbf{s}\|_\infty}{e}\right)^{\|\mathbf{s}\|_\infty},$$

hence,

$$\begin{aligned}&(M-\|\mathbf{s}\|_\infty+1)\mathrm{P}\{\exists j,s_j^*=\|\mathbf{s}\|_\infty\}\\&\quad\approx\frac{(M-\|\mathbf{s}\|_\infty+1)\lambda^{\|\mathbf{s}\|_\infty}e^{-\lambda}}{\sqrt{2\pi\|\mathbf{s}\|_\infty}(\|\mathbf{s}\|_\infty)^{\|\mathbf{s}\|_\infty}e^{-\|\mathbf{s}\|_\infty}}\\&\quad=\frac{(M-\|\mathbf{s}\|_\infty+1)}{\sqrt{2\pi\|\mathbf{s}\|_\infty}}\left(\frac{\lambda}{\|\mathbf{s}\|_\infty}\right)^{\|\mathbf{s}\|_\infty}e^{\|\mathbf{s}\|_\infty-\lambda}\\&\quad=\frac{\left(M-\sigma\lceil\frac{S}{N}\rceil+1\right)}{\sqrt{2\pi\sigma\cdot\lceil\frac{S}{N}\rceil}}\left(\frac{\lambda}{\sigma\cdot\lceil\frac{S}{N}\rceil}\right)^{\sigma\cdot\lceil\frac{S}{N}\rceil}e^{\sigma\cdot\lceil\frac{S}{N}\rceil-\lambda}\\&\quad\le\frac{\left(M-\sigma\lceil\frac{S}{N}\rceil+1\right)}{\sqrt{2\pi\sigma\cdot\lceil\frac{S}{N}\rceil}}\left(\frac{\lceil\frac{S}{N}\rceil}{\sigma\cdot\lceil\frac{S}{N}\rceil}\right)^{\sigma\cdot\lceil\frac{S}{N}\rceil}e^{\sigma\cdot\lceil\frac{S}{N}\rceil-\lambda}\\&\quad=\frac{\left(M-\sigma\lceil\frac{S}{N}\rceil+1\right)}{\sqrt{2\pi\sigma\cdot\lceil\frac{S}{N}\rceil}}\left(\frac{1}{\sigma}\right)^{\sigma\cdot\lceil\frac{S}{N}\rceil}e^{\sigma\cdot\lceil\frac{S}{N}\rceil-\lambda}\quad=C\cdot\left(\frac{e}{\sigma}\right)^{\|\mathbf{s}\|_\infty},\end{aligned}$$

where the constant $C=\frac{(M-\sigma\lceil\frac{S}{N}\rceil+1)}{\sqrt{2\pi\sigma\cdot\lceil\frac{S}{N}\rceil}e^{\lambda}}<M$. Generally, as long as $\|\mathbf{s}\|_\infty$ is large enough, it can guarantee $C\cdot\left(\frac{e}{\sigma}\right)^{\|\mathbf{s}\|_\infty}<1$. With the increase of $\|\mathbf{s}\|_\infty$, the value of $C\cdot\left(\frac{e}{\sigma}\right)^{\|\mathbf{s}\|_\infty}$ decreases exponentially and converges to zero. Therefore, the random permutation is able to be an acceptable permutation with overwhelming probability.

This completes the proof.□

4. Embedding random permutation in parallel compressive sensing

A block diagram of our approach is depicted in Fig. 2. The encoding process is mainly composed of two steps, random permutation and random measurement. A 2D signal $\mathbf{X}\in\mathbb{R}^{M\times N}$ is firstly reshaped into a 1D signal $\{x(i)\}_{i=1}^{MN}$, which is then performed by random permutation. The permuted signal $\{x^*(i)\}_{i=1}^{MN}$ is converted back to the 2D format $\mathbf{X}^*\in\mathbb{R}^{M\times N}$. After the permutation, the signal $\mathbf{X}^*$ is sampled column by column using a random matrix with i.i.d. entries from a subgaussian (Gaussian or Bernoulli) distribution $\mathbf{\Phi}$, i.e., $\mathbf{Y}^*[j]=\mathbf{\Phi}\mathbf{X}^*[j]$, where $\mathbf{Y}^*\in\mathbb{R}^{K\times N}$ and $\mathbf{X}^*[j]$ represents the jth column of $\mathbf{X}^*$. In the decoding phase, $\hat{\mathbf{X}}^*$ can be recovered from the received $\hat{\mathbf{Y}}^*$ and is then processed by the reverse permutation to derive the signal $\hat{\mathbf{X}}$ of interest, as shown in Fig. 2.

In what follows, we investigate the security of the proposed scheme embedding random permutation in PCS. Assume that Alice sends an encrypted message $\mathbf{Y}^*=\mathbf{\Phi}\mathbf{P}(\mathbf{X})=\mathbf{\Phi}\mathbf{X}^*$ to Bob, who decrypts the message by solving the following convex

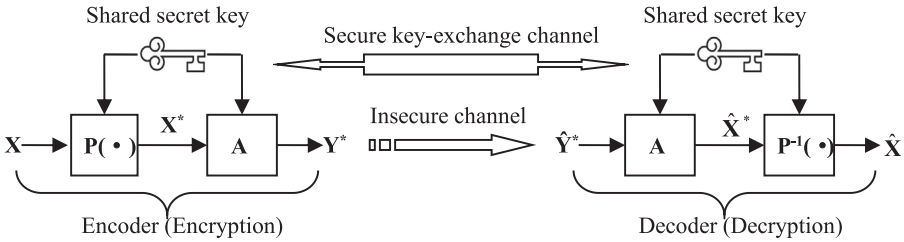

Fig. 2. A schematic diagram of the proposed approach.

optimization problem

$$\min \|\mathbf{X}^*[j]\|_1 \quad \text{s.t. } \mathbf{Y}^*[j] = \mathbf{\Phi}\mathbf{X}^*[j], \quad j \in [1, N] \tag{13}$$

and so $\mathbf{X} = \mathbf{P}^{-1}(\mathbf{X}^*)$. An eavesdropper, Eve, attempts to recover the plaintext $\mathbf{X}$ or the encryption keys $\mathbf{\Phi}$ and $\mathbf{P}(\bullet)$ after intercepting the ciphertext $\mathbf{Y}^*$.

4.1. Asymptotic spherical secrecy

Considering Shannon's definition of perfect secrecy that the probability of a message conditioned on the cryptogram is equal to the *a priori* probability of the message, the proposed scheme does not achieve perfect secrecy, as stated in Lemma 2.

Lemma 2. *Let X be a random variable, whose probability is $P_X(\mathbf{X}) > 0$, $\forall \mathbf{X} \in \mathbb{R}^{M\times N}$, and $\mathbf{\Phi}$ be a $K \times M$ measurement matrix. With respect to the encryption model $Y = \mathbf{\Phi}\mathbf{P}(X)$, we have $I(X;Y) > 0$, and so perfect secrecy is not achieved.*

Proof. We prove this lemma by contradiction. Apparently, $I(X;Y) > 0$ if and only if X and Y are statistically independent. In the context of $X = \mathbf{0}$, $Y = \mathbf{\Phi}\mathbf{P}(X) = \mathbf{\Phi}\mathbf{P}(\mathbf{0}) = \mathbf{\Phi}\cdot\mathbf{0} = \mathbf{0}$ and so $P_{Y|X}(Y = \mathbf{0}|X = \mathbf{0}) = 1$. On the other hand, only $\mathbf{X}$ in the null space of $\mathbf{\Phi}$ which is a new transform $\overline{\mathbf{\Phi}} = \mathbf{\Phi}\mathbf{P}(\bullet)$ are mapped to $Y = \mathbf{0}$; whereas, we have $P_Y(Y = \mathbf{0}) < 1$ due to the assumption that $P_X(\mathbf{X}) > 0$, $\forall \mathbf{X} \in \mathbb{R}^{M\times N}$. As a result, we conclude that $P_{Y|X}(Y = \mathbf{0}|X = \mathbf{0}) \neq P_Y(Y = \mathbf{0})$, meaning that X and Y are statistically dependent.

By the RIP, $\mathbf{Y}$ provides information about the norm of $\mathbf{X}$. The fact that the l_2-norm of a vector can be considered as its energy has been utilized by Cambareri et al. [5] in introducing the notion of asymptotic spherical secrecy for CS encoding in which the measurement matrix serves as a key.□

Definition 3 (*Asymptotic spherical secrecy, Cambareri et al. [5]*). Let $\mathbf{x}^{(n)} = (x_0, x_1, \ldots, x_n) \in \mathbb{R}^n$ be a plaintext sequence of increasing length n and $\mathbf{y}^{(n)}$ be the corresponding ciphertext sequence. Assume that the power of the plaintext is positive and finite, i.e.,

$$W_{\mathbf{x}} = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} x_k^2, \quad 0 < W_{\mathbf{x}} < +\infty. \tag{14}$$

A cryptosystem is said to have asymptotic spherical secrecy if

$$f_{Y^{(n)}|X^{(n)}}(\mathbf{y}, \mathbf{x}) \underset{\mathcal{D}}{\to} f_{Y^{(n)}|W_{\mathbf{x}}}(\mathbf{y}), \tag{15}$$

where $\underset{\mathcal{D}}{\to}$ denotes the convergence in distribution as $n \to \infty$.

This definition implies that it is impossible for Eve to infer the plaintext $\mathbf{x}$ but its power from the statistical properties of the random measurements $\mathbf{y}$. Although not achieving perfect secrecy, the proposed scheme satisfies asymptotic spherical secrecy.

Theorem 2 (*Asymptotic spherical secrecy of the proposed scheme*). *Let*

(1) $\mathbf{X}^{(n)} = (X_{ij}) \in \mathbb{R}^{M\times N}$ *be a bounded-value plaintext with power* $0 < W_{\mathbf{X}} < +\infty$, *defined as* $W_{\mathbf{X}} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{M} \sum_{j=1}^{N} X_{ij}^2$, *where* $n = MN$;

(2) $\mathbf{X}^{*(n)} = \mathbf{P}\left(\mathbf{X}^{(n)}\right) = \left(X_{ij}^*\right) \in \mathbb{R}^{M\times N}$ *with power* $W_{\mathbf{X}^*} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij}^*\right)^2$;

(3) $\mathbf{Y}^{(n)} = (Y_{ij}) \in \mathbb{R}^{K\times M}$ *be the corresponding ciphertext, where* $Y_{ij} = \sum_{k=1}^{M} \Phi_{ik} X_{kj}^*$. *As* $n \to \infty$, *we have*

$$Y_{ij} \underset{\mathcal{D}}{\to} N(0, MW_{\mathbf{X}}/K). \tag{16}$$

Proof. Permutation does not affect the power and thus $W_{\mathbf{X}^*} = W_{\mathbf{X}}$. After the random permutation, the energy is approximately uniformly distributed to each column of $\mathbf{X}^{*(n)}$. In other words, the power of each column converges to that of the whole plaintext in distribution, i.e.,

$$\frac{1}{M} \sum_{k=1}^{M} \left(X_{ij}^*\right)^2 \underset{D}{\to} \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij}^*\right)^2 = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{M} \sum_{j=1}^{N} X_{ij}^2 = W_{\mathbf{X}}. \tag{17}$$

We calculate

$$\mathbf{E}\left[Y_{ij}^2\right] = \mathbf{E}\left[\left(\sum_{k=1}^{M} \Phi_{ik} X_{kj}^*\right)^2\right] = \frac{1}{K} \sum_{k=1}^{M} \left(X_{kj}^*\right)^2 \underset{\mathcal{D}}{\to} \frac{M}{K} W_{\mathbf{X}}, \tag{18}$$

thereby yielding the result stated in Theorem 2.□

5. The realization of chaos

Chaos technique has widely used in designing some encryption models [22,23,39,11,10,37]. In order to validate the feasibility of the proposed encryption models at first, we utilize chaos to implement the proposed scheme embedding random permutation in PCS. The whole process is under the control of the skew tent chaos map with four keys, μ, $z(0)$, μ' and $z'(0)$.

5.1. Generate the permutation order

There are a number of classic methods in realizing the permutation operation $\mathbf{P}(\bullet)$ from one or more keys using chaos, some of which are stated as follows:

Straightforward transform: Use 2D chaotic transforms such as Arnold map to directly project the indices of the 2D signal, e.g., [35].

Matrix rotation: Employ chaotic sequence to construct the rotation matrix acting on 1D signal, e.g., [38].

Index sorting: Sort the chaotic sequence to generate the index matrix, applying to the indices of the 1D signal, e.g., [30].

Here, we apply the method "index sorting" to perform the permutation. According to [30], a permutation sequence is produced using the skew tent map by the following steps:

(a) Set the keys μ and $z(0)$ to iterate the skew tent map $MN+m$ times, then discard the first m values to get rid of the transient effect.
(b) Sort the remaining MN values $\{z(i)\}_{i=m+1}^{m+MN}$ to obtain $\{\overline{z}(i)\}_{i=m+1}^{m+MN}$.
(c) Search the values of $\{z(i)\}_{i=m+1}^{m+MN}$ in $\{\overline{z}(i)\}_{i=m+1}^{m+MN}$, and store the corresponding indices $\{Index(i)\}_{i=1}^{MN}$.

Apparently, $\{Index(i)\}_{i=1}^{MN}$ indicates an order of the integers from 1 to MN. The above steps have been widely used to generate the permutation order in image encryption schemes. However, the complexity $\mathcal{O}(n^2\log n)$ is high. A novel algorithm, whose complexity is only $\mathcal{O}(n\log n)$, was designed in [33]. The procedures are:

(a) Initialize a flag sequence $\{flag(k)\}_{k=1}^{MN}$ and a permutation sequence $\{Index(k)\}_{k=1}^{MN}$ to 0 and set $i=1$.
(b) Calculate $z(k+1)=T[z(k);\mu]$ and $\chi=\lceil MN\times z(k+1)\rceil$.
(c) If $flag(\chi)=0$, then set $Index(i)=\chi$, $flag(\chi)=1$ and $i=i+1$; otherwise, go to Step b.
(d) If $i<MN$, go to Step b.

5.2. Construct the measurement matrix

Following the idea of [18], the chaotic measurement matrix which approximately obeys Gaussian distribution is constructed by the following steps:

(a) Define the chaotic sequence $\Delta(d,k,\mu',z'(0)):=\{z'(n+i\times d)\}_{i=0}^{k}$, which is extracted from the chaotic sequence generated by the skew tent map with sampling distance d and keys μ' and $z'(0)$.
(b) Introduce a new transform $\{\vartheta(k)\}_{k=0}^{KM-1}=\{-2\times\Delta(d,k,\mu',z'(0))+1\}|_{k=KM-1}$.
(c) Create the measurement matrix column by column using the sequence $\{\vartheta(k)\}_{k=0}^{KM-1}$, as given by

$$\mathbf{\Phi}=\sqrt{\frac{2}{K}}\begin{pmatrix}\vartheta(0) & \cdots & \vartheta(KM-K)\\ \vdots & \ddots & \vdots\\ \vartheta(K-1) & \cdots & \vartheta(KM-1)\end{pmatrix} \tag{19}$$

where the scalar $\sqrt{2/K}$ is used for normalization.

5.3. Computational secrecy

Cryptosystems relying on computation-secrecy such as RSA are practical and widely used. In contrast to information theoretic secrecy which is an ideal encryption requirement, computational secrecy allows the ciphertext possessing complete or partial plaintext information, which is common. This ensures that for Eve to recover the plaintext from the ciphertext without the correct key is equivalent to solving a computational problem that is assumed to be extremely difficult (e.g., NP-hard). In the proposed scheme, $\mathbf{X}$ is a 2D sparse signal with sparsity $\mathbf{s}$. If a wrong key μ, $z(0)$, μ' or $z'(0)$, which is almost identical to the correct key, is used by Eve in attempting to recover $\mathbf{X}$, the result is unsuccessful due to the high key sensitivity. Moreover, the unsuccessful recovery of the signal using a wrong key can also be justified by the following theorem.

Theorem 3 (*Rachlin and Baron [25]*). *Let* $\mathbf{\Phi}$ *and* $\tilde{\mathbf{\Phi}}$ *be* $K\times M$ *Gaussian matrices with entries generated by different keys. Let* $\mathbf{x}$ *be* s*-sparse and* $\mathbf{y}=\mathbf{\Phi x}$. *When* $\tilde{s}\geq s+1$, *the* l_0 *or* l_1 *optimization used will yield an* $\tilde{s}$*-sparse solution with probability one.*

On the contrary, once an s-sparse solution is obtained using some keys, Eve easily realizes that it must be the correct key. Computational secrecy can be achieved if Eve is computationally bounded; otherwise, the cryptanalysis will succeed. However, in practical applications, the keys should be at least 2^{64} bits and are updated periodically to resist brute-force attack.

Every communication requires altering the session keys, which can be securely transmitted. For instance, they are encrypted by public-key encryption algorithms such as RSA. Apparently, it can resist the potential attacks including known-plaintext attack, chosen-plaintext attack and chosen-ciphertext attack. It is also impossible for the attacker to cryptanalyze the proposed approach using cipher-only attack, since analyzing the encoded data, having a smaller amount than the original data, to retrieve the original data without knowing the secret measurement matrix is an NP-hard question.

6. Simulation

For simulation purpose, an image can be considered as a 2D signal, which is sparsified by 2D discrete cosine transform (DCT2) to obtain a 2D sparse signal $\mathbf{X}$. The best s-term approximation is acquired by keeping the s largest DCT2 coefficients and setting the remaining to zeros. Random permutation and Gaussian matrix are generated by using MATLAB code. Four images of size 512×512, Peppers, Lena, Boat and Baboon, are used in the simulations. The basis pursuit algorithm in the CVX optimization toolbox [19] is employed to realize the PCS reconstruction. Apart from the basis pursuit, other reconstruction algorithms can also be used. The reconstruction performance is evaluated by peak signal-to-noise ratio (PSNR).

6.1. Compressibility

The encoded (or encrypted) image can have various sizes depending on the compression ratio (CR), i.e., the ratio of the number of measurements to the total number of entries in the DCT2 coefficient matrix. Fig. 3 shows four encoded images of the

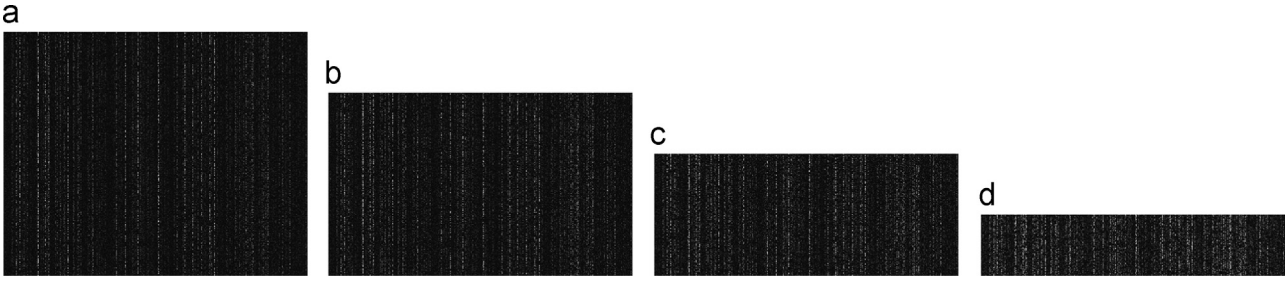

Fig. 3. Four encoded images at different CRs. (a) $CR=0.8$; (b) $CR=0.6$; (c) $CR=0.4$; (d) $CR=0.2$.

original Peppers image corresponding to $CR = 0.8, 0.6, 0.4, 0.2$. In order to investigate the effect of encryption on *CR*, we plot PSNR versus *CR* for different images with/without encryption in Fig. 4, where "E" represents introducing random permutation encryption while "N" means not introducing, which refers to the case that a 2D sparse signal is sampled column by column using the same measurement matrix drawn from Gaussian ensembles. As observed from Fig. 4, random permutation helps to improve the PSNR of all images by around 2–6 dB at the same *CR*. In other words, at the same PSNR, random permutation encryption makes *CR* smaller. This is due to the fact that random permutation can relax the RIP for 2D sparse signals with high probability in PCS, as justified by Theorem 1.

6.2. Robustness

Introducing encryption into PCS makes it still possess high reconstruction robustness, even for a small amount of encoded data. This can be visually verified by the four decoded images shown in Fig. 5. The decoded (or decrypted) images contain most of the visual information of the original images, even at $CR = 0.2$. A significant requirement in the transmission process is the robustness of a coding system (or cryptosystem) against imperfection such as additive white Gaussian noise (AWGN) and cropping attack (CA). These two capabilities are quantified in Table 1 for the Peppers image. In particular, the encoded images at different *CR*s are affected by these imperfections and the PSNRs of the corresponding decoded images are calculated. Additive white Gaussian noise yields zero-mean normal distribution with variance 1 while the cropping attack cuts one-eighth of the encoded image at the upper left corner. Observing Γ_3 and Γ_4, or Γ_5 and Γ_6 from Table 1, we can see that at a channel with both AWGN and CA, random permutation encryption improves the PSNR at the same *CR*. By individually comparing the variation trends of $\Gamma_2-\Gamma_1$, $\Gamma_4-\Gamma_3$ and $\Gamma_6-\Gamma_5$, the tendency is that the smaller the *CR*, the greater the improvement. In addition, vertically contrasting these three rows of data reveals that PSNR improvements are similar with and without AWGN (or CA). Thus, we come to the conclusion that the proposed approach possesses a strong robustness against AWGN and CA. It is worth mentioning that similar results are obtained using other images. In addition, to test the sensitivity of the four keys for the chaos realization, a tiny perturbation of 10^{-16} is added, respectively, and the decoded images are depicted in Fig. 6. Their indistinguishability justifies the high key sensitivity of the proposed approach. In fact, this is guaranteed by the inherent property of chaos, i.e., high sensitivity to initial conditions. The key space is at least 2^{64}.

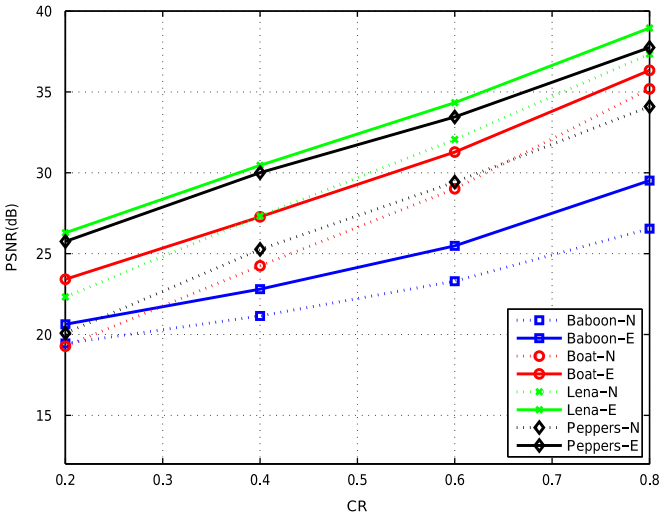

Fig. 4. PSNR versus *CR* for different images with/without random permutation encryption.

7. Conclusion

This paper is firstly dedicated to the design of some encryption models for SCS. Some connections between CS and symmetric-key cipher are analyzed. Next, random permutation is verified to be able to efficiently relax the RIP condition with high probability. Furthermore, an encryption scheme for PCS has been proposed. Simulations using images as 2D signals show that at the same compression ratio, random permutation encryption improves the PSNR by 2–6 dB for all images. For a channel suffered from both additive white Gaussian noise and cropping attack, it still improves the PSNR when the compression ratio is fixed. It is found that the proposed approach possesses a high robustness against additive white Gaussian noise and cropping attack. Security analysis indicates that the asymptotic spherical secrecy is achievable. The implementation of chaos validates the feasibility of the proposed encryption models for CS.

Table 1
PSNR of different settings at various *CR*s.

CR	0.2	0.4	0.6	0.8
PCS–N($=\Gamma_1$)	20.0800	25.2575	29.4243	34.0949
PCS–E($=\Gamma_2$)	25.7507	30.0071	33.4539	37.7431
$\Gamma_2-\Gamma_1$	5.6707	4.7496	4.0296	3.6482
PCS–AWGN–N($=\Gamma_3$)	20.0899	25.2382	29.3072	33.0931
PCS–AWGN–E($=\Gamma_4$)	25.7405	29.9143	33.0547	35.8942
$\Gamma_4-\Gamma_3$	5.6506	4.6761	3.7475	2.8011
PCS–CA–N($=\Gamma_5$)	19.3763	24.6003	28.8997	33.5010
PCS–CA–E($=\Gamma_6$)	25.1834	29.4669	33.0240	37.3011
$\Gamma_6-\Gamma_5$	5.8071	4.8666	4.1243	3.8001

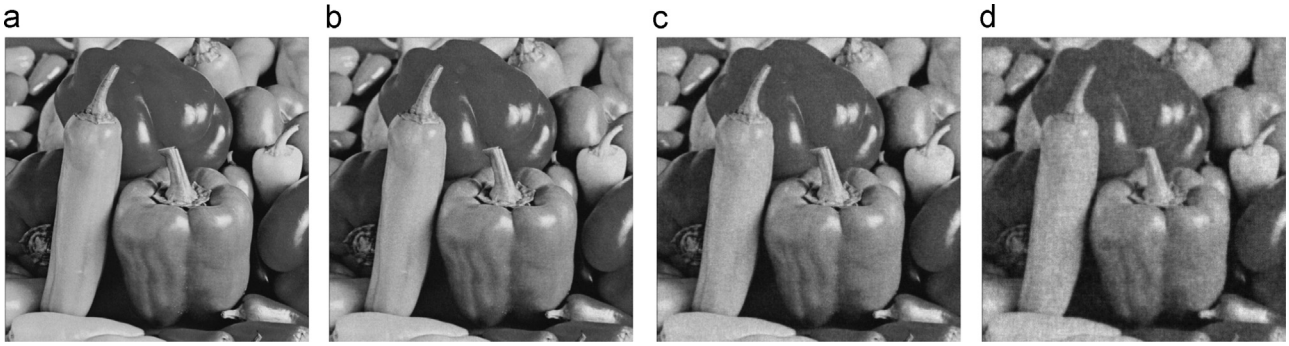

Fig. 5. Four decoded images corresponding to the four encoded images in Fig. 3 at various *CR*s. (a) $CR = 0.8$; (b) $CR = 0.6$; (c) $CR = 0.4$; (d) $CR = 0.2$.

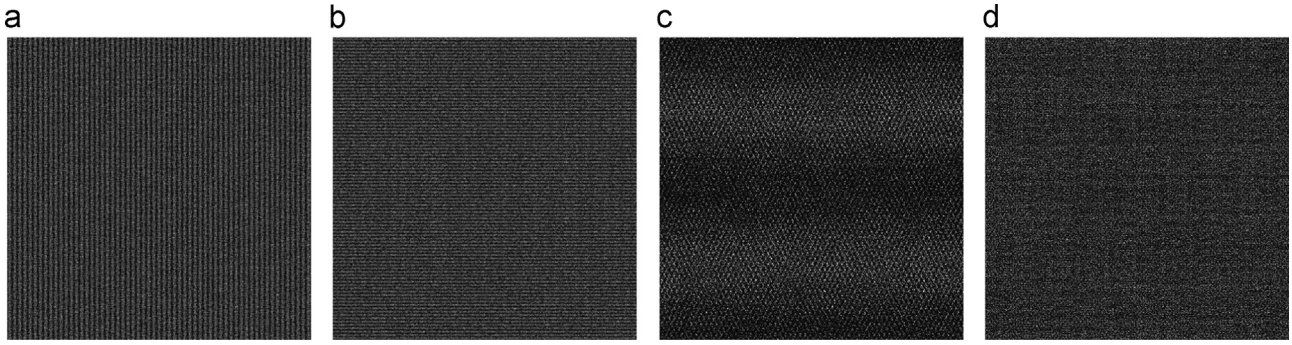

Fig. 6. The test of key sensitivity ($CR=0.2$). (a) $z(0)=0.33+10^{-16}$; (b) $\mu=0.63+10^{-16}$; (c) $z'(0)=0.73+10^{-16}$; (d) $\mu'=0.28+10^{-16}$.

Acknowledgments

The work was funded by the National Natural Science Foundation of China (Grant Nos. 61502399, 61402547, 61502314, 61403313, 61572089), the Natural Science Foundation Project of Chongqing CSTC (Grant No. cstc2015jcyjA40039), the Fundamental Research Funds for the Central Universities (Grant No. XDJK2015C077), the Macau Science and Technology Development Fund (Grant Nos. FDCT/009/2013/A1, FDCT/046/2014/A1) and the Research Committee at University of Macau (Grant Nos. MRG007/ZJT/2015/FST, MRG021/ZJT/2013/FST, MYRG2014-00031-FST, MYRG2015-00056-FST).

References

[1] Shweta Agrawal, Sriram Vishwanath, Secrecy using compressive sensing, in: Proceedings of the IEEE Information Theory Workshop (ITW), Paraty, October 2011, pp. 563–567.
[2] Tiziano Bianchi, Valerio Bioglio, Enrico Magli, On the security of random linear measurements, in: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, May 2014, pp. 3992–3996.
[3] Tiziano Bianchi, Valerio Bioglio, Enrico Magli, Analysis of one-time random projections for privacy preserving compressed sensing, IEEE Trans. Inf. Forensics Secur. 11 (2) (2016) 313–327.
[4] Valerio cambareri, Javier Haboba, Fabio Pareschi, Riccardo Rovatti, Gianluca Setti, Kwok-Wo Wong, A two-class information concealing system based on compressed sensing, in Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Beijing, May 2013, pp. 1356–1359.
[5] Valerio Cambareri, Mauro Mangia, Fabio Pareschi, Riccardo Rovatti, Gianluca Setti, Low-complexity multiclass encryption by compressed sensing, IEEE Trans. Signal Process. 63 (May (9)) (2015) 2183–2195.
[6] Emmanuel J. Candès, Justin Romberg, Terence Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information, IEEE Trans. Inf. Theory 52 (February (2)) (2006) 489–509.
[7] Emmanuel J. Candès, Terence Tao, Decoding by linear programming, IEEE Trans. Inf. Theory 51 (December (12)) (2005) 4203–4215.
[8] Emmanuel J. Candès, Terence Tao, Near-optimal signal recovery from random projections: universal encoding strategies?, IEEE Trans. Inf. Theory 52 (December (12)) (2006) 5406–5425.
[9] Emmanuel J. Candès, Michael B. Wakin, An introduction to compressive sampling, IEEE Signal Process. Mag. 25 (March (2)) (2008) 21–30.
[10] Fei Chen, Kwok-wo Wong, Xiaofeng Liao, Tao Xiang, Period distribution of generalized discrete Arnold cat map, Theor. Comput. Sci. 552 (2014) 13–25.
[11] Jianyong Chen, Junwei Zhou, Kwok-Wo Wong, A modified chaos-based joint compression and encryption scheme, IEEE Trans. Circuits Syst. II: Express Briefs 58 (2) (2011) 110–114.
[12] Ruslan Dautov, Gill R. Tsouri, Establishing secure measurement matrix for compressed sensing using wireless physical layer security, in: Proceedings of the International Conference on Computer Networks & Communications (ICNC), San Diego, CA, January 2013, pp. 354–358.
[13] Ronald A. DeVore, Deterministic constructions of compressed sensing matrices, J. Complex. 23 (August–December (4)) (2007) 918–925.
[14] Thong T. Do, Lu Gan, Nam H. Nguyen, Trac D. Tran, Fast and efficient compressive sensing using structurally random matrices, IEEE Trans. Signal Process. 60 (January (1)) (2012) 139–154.
[15] David L. Donoho, Compressed sensing, IEEE Trans. Inf. Theory 52 (April (4)) (2006) 1289–1306.
[16] Hao Fang, Sergiy A. Vorobyov, Hai Jiang, Permutation enhanced parallel reconstruction for compressive sampling, in: Proceedings of the 6th International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), Mexico, December 13–16, 2015, pp. 1–10.
[17] Hao Fang, Sergiy A. Vorobyov, Hai Jiang, Omid Taheri, Permutation meets parallel compressed sensing: how to relax restricted isometry property for 2D sparse signals, IEEE Trans. Signal Process. 62 (January (1)) (2014) 196–210.
[18] Madalin Frunzete, Lei Yu, J. Barbot, Adriana Vlad, Compressive sensing matrix designed by tent map, for secure data transmission, in: Proceedings of the IEEE Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), Poznan, September 2011, pp. 1–6.
[19] Michael Grant, Stephen Boyd, Yinyu Ye, Cvx: Matlab software for disciplined convex programming, 2008.
[20] S. Amir Hossein, A.E. Tabatabaei, Natasa Zivic, Security analysis of the joint encryption and compressed sensing, in: Proceedings of the 20th Telecommunications Forum (TELFOR), Belgrade, November 2012, pp. 799–802.
[21] Shuxing Li, Fei Gao, Gennian Ge, Shengyuan Zhang, Deterministic construction of compressed sensing matrices via algebraic curves, IEEE Trans. Inf. Theory 58 (August(8)) (2012) 5035–5041.
[22] Qiuzhen Lin, Kwok-Wo Wong, Jianyong Chen, An enhanced variable-length arithmetic coding and encryption scheme using chaotic maps, J. Syst. Softw. 86 (5) (2013) 1384–1389.
[23] Oi-Yan Lui, Kwok-Wo Wong, Jianyong Chen, Junwei Zhou, Chaos-based joint compression and encryption algorithm for generating variable length ciphertext, Appl. Soft Comput. 12 (1) (2012) 125–132.
[24] Adem Orsdemir, H. Oktay Altun, Gaurav Sharma, Mark F. Bocko, On the security and robustness of encryption via compressed sensing, in: Proceedings of the IEEE Military Communications Conference (MILCOM), San Diego, CA, November 2008, pp. 1–7.
[25] Yaron Rachlin, Dror Baron, The secrecy of compressed sensing measurements, In: Proceedings of the 46th Annual Allerton Conference on Communication, Control and Computing, Urbana-Champaign, IL, September 2008, pp. 813–817.
[26] Philippe Refregier, Bahram Javidi, Optical image encryption using input plane and fourier plane random encoding, in: SPIE, International Society for Optics and Photonics, San Diego, CA, United States, April 1995, pp. 62–68.
[27] Yair Rivenson, Adrian Stern, Bahram Javidi, Single exposure super-resolution compressive imaging by double phase encoding, Opt. Express 18 (July (14)) (2010) 15094–15103.
[28] Justin Romberg, Compressive sensing by random convolution, SIAM J. Imaging Sci. 2 (November (4)) (2009) 1098–1128.
[29] Claude E. Shannon, Communication theory of secrecy systems, Bell Syst. Techn. J. 28 (October (4)) (1949) 656–715.
[30] Xingyuan Wang, Lin Teng, Xue Qin, A novel colour image encryption algorithm based on chaos, Signal Process. 92 (April (4)) (2012) 1101–1108.
[31] Zuyuan Yang, Wei Yan, Yong Xiang, On the security of compressed sensing based signal cryptosystem, IEEE Trans. Emerg. Top. Comput. 3 (September (3)) (2015) 363–371.
[32] Lei Yu, Jean Pierre Barbot, Gang Zheng, Hong Sun, Compressive sensing with chaotic sequence, IEEE Signal Process. Lett. 17 (August (8)) (2010) 731–734.
[33] Leo Yu Zhang, Xiaobo Hu, Yuansheng Liu, Kwok-Wo Wong, Jie Gan, A chaotic image encryption scheme owning temp-value feedback, Commun. Nonlinear Sci. Numer. Simul. 19 (October (10)) (2014) 3653–3659.
[34] Leo Yu Zhang, Kwok-Wo Wong, Yushu Zhang, Qiuzhen Lin, Joint quantization and diffusion for compressed sensing measurements of natural images, in: Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon, May 2015, pp. 2744–2747.
[35] M.-R. Zhang, G.-C. Shao, K.-C. Yi, T-matrix and its applications in image processing, Electron. Lett. 40 (25) (2004) 1583–1584.
[36] Yushu Zhang, Kwok-Wo Wong, Leo Yu Zhang, Wenying Wen, Jiantao Zhou, Xing He, Robust coding of encrypted images via structural matrix, Signal Process.—Image Commun. 39 (November) (2015) 202–211.
[37] Yushu Zhang, Di Xiao, Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform, Opt. Lasers Eng. 51 (4) (2013) 472–480.

[38] Yushu Zhang, Di Xiao, An image encryption scheme based on rotation matrix bit-level permutation and block diffusion, Commun. Nonlinear Sci. Numer. Simul. 19 (January (1)) (2014) 74–82.
[39] Yushu Zhang, Di Xiao, Yonglu Shu, Jing Li, A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations, Signal Process.—Image Commun. 28 (3) (2013) 292–300.
[40] Yushu Zhang, Leo Yu Zhang, Exploiting random convolution and random subsampling for image encryption and compression, Electron. Lett. 51 (October (20)) (2015) 1572–1574.

Yushu Zhang received the Ph.D. degree in Computer Science and Technology from Chongqing University, Chongqing, China, in December 2014. During 2014, he had been a Research Associate at City University of Hong Kong. Since January 2015, he has been an Associate Professor at School of Electronics and Information Engineering, Southwest University, China. At present, he is a Post-doctoral Fellow at University of Macau. His research interests include multimedia coding and security, compressive sensing security, and secure signal processing through lossy channel.

Jiantao Zhou is currently an Assistant Professor with the Department of Computer and Information Science, Faculty of Science and Technology, University of Macau. He received the B.Eng. degree from the Department of Electronic Engineering, Dalian University of Technology, Dalian, China, in 2002, the M.Phil. degree from the Department of Radio Engineering, Southeast University, Nanjing, China, in 2005, and the Ph.D. degree from the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong, in 2009. He held various research positions at the University of Illinois at Urbana-Champaign, the Hong Kong University of Science and Technology, and the McMaster University. His research interests include multimedia security and forensics, and high-fidelity image compression. He was a co-author of a paper that received the Best Paper award in the IEEE Pacific-Rim Conference on Multimedia (PCM) in 2007.

Fei Chen joined College of Computer Science and Engineering at Shenzhen University, China, as a lecturer in 2015. He received a Ph.D. degree in Computer Science and Engineering at The Chinese University of Hong Kong, and a M.S. and B.Eng. degrees in Computer Science and Engineering at Chongqing University, China. He visited the Distributed Systems Group at Vienna University of Technology in 2014; he also interned at the Database Team of the Alibaba Group in 2013, and the State Key Laboratory of Information Security of the Chinese Academy of Science in 2009. His research interests include information and network security, data protection and privacy.

Leo Yu Zhang received both his Bachelor's degree and Master's degree in Computational Mathematics from Xiangtan University in 2009 and 2012, respectively. From 2012 to 2013, he worked at the State Grid Electric Power Research Institute of China as a development engineer. Currently, he is pursuing his Ph.D. degree from the Department of Electronic Engineering, City University of Hong Kong, Hong Kong. His research interests include multimedia security and compressive sensing.

Kwok-Wo Wong received the B.Sc. degree in Electronic Engineering from the Chinese University of Hong Kong and the Ph.D. degree from the City University of Hong Kong, where he is currently an Associate Professor in the Department of Electronic Engineering. His current research interests include chaos, cryptography, and neural networks. He has published more than 100 papers in 25 international mathematics, physics, and engineering journals in the fields of nonlinear dynamics, cryptography, neural networks, and optics. He is a senior member of the IEEE. He is also a chartered engineer and a member of the Institution of Engineering and Technology (IET).

Xing He received the B.S. degree in Mathematics and Applied Mathematics from the Department of Mathematics, Guizhou University, Guiyang, China, in 2009, and Ph.D. degree in Computer Science and Technology from Chongqing University, Chongqing, China, in 2013. Currently, he is an Associate Professor at the School of Electronics and Information Engineering, Southwest University, Chongqing, PR China. From November 2012 to October 2013, he was a Research Assistant with the Texas A&M University at Qatar, Doha, Qatar. His research interests include neural networks, bifurcation theory, optimization method, smart grid, nonlinear dynamical system

Di Xiao received the Ph.D. degree in Computer Software and Theory from Chongqing University, Chongqing, China, in 2005. From 2006 to 2008, he has done postdoctoral research at Chongqing University. From 2008 to 2009, he has been a visiting scholar funded by the Chinese government at the Department of Computer Science, New Jersey Institute of Technology, USA. Currently, he is a professor at College of Computer Science, Chongqing University, China. His research interests include image processing, chaos based cryptography, image and graphics watermarking, etc. He is a member of IEEE and ACM.