Compressed Sensing with Embeding Negative-positive Transformation for Image Compression-encryption Applications

Bo Zhang, Zhixiang Zheng*, Luyao Guo, Gaokun Lin, Qiang Wang

Communication NCO Academy Army Engineering University Chongqing 40035, China

Abstract

Recently, compressed sensing (CS) cryptosystem has received a lot of interest. However, this cryptosystem is vulnerable to chosen-plaintext attack (CPA) because the CS sampling process is a linearity process. To solve this problem, we propose a novel CS-based cryptosystem by using negative-positive transformation (NPT) in this paper, which embeds a NPT operation in the CS sampling process. First, the image is pre-processed by using NPT operation. Then, the cipher image is re-encrypted by using CS. Last, the compressed ciphertext is quantized into bits. Since the introduction of NPT operation destroys the linearity of sampling process, our method can resist CPA. Compared with previous CS-based cryptosystems, the proposed cryptosystem has two advantages: 1) It achieves effective privacy protection against CPA; 2) It has better compression performance.

Keywords

Compressed sensing; chosen-plaintext attack; negative-positive transformation; image encryption.

1. INTRODUCTION

Compressed sensing (CS) has received a lot of attention recently [1], [2], which is capable of efficiently capturing and recovering a signal through a few of linear measurements. When CS was applied in secure applications, a secure CS (SCS) framework is proposed, where the measurement matrix is used as a key since the unauthorized user cannot recover the signal without the knowledge of the measurement matrix. However, when the entire measurement matrix is considered as a secret key, the storage space and transmission overhead for the key are too large. To overcome this difficulty, some pioneers proposed that we can generate the measurement matrix by chaotic functions [3-5], such as Logistic map [3], Skew tent map [4] and Logistic-Tent map [5]. The initial value which is utilized to generate the chaotic measurement matrix can be used as the key. This strategy saves the storage space and transmission overhead for the key significantly, which makes CS theory more attractive for secure applications.

In [6], the authors proved that SCS can guarantee the computation secrecy, since the adversary cannot figure out the right key by exhaustive searching in its key space. However, this cryptosystem fails to satisfy Shannon's perfect secrecy [7]. In this context, an achievable security metric for CS-based cryptosystem called asymptotic spherical security is defined in [8]. In [9], the authors demonstrated that only the energy information of the signal is obtained by the adversary who gets the CS samples. Therefore, it is recommended that the CS measurement vector is needed to be normalized before sending it into the channel.

In [10], the authors show that CS-based cryptosystem is vulnerable to known-plaintext attack (KPA). In [11], a quantitative analysis for the CS-based cryptosystem against KPA is performed, which shows that this cryptosystem can resist KPA if the adversary only collects one pair of the plaintext and the corresponding ciphertext. On this basis, some pioneers suggested that the CS-based cryptosystem should update the measurement matrix [12-14] for every signal.

ICCEIC2022@3rd International Conference on Computer Engineering and Intelligent Control
EMAIL: Email: sime0821@163.com (Zhixiang Zheng)

In order to use CS in multi-time-sampling (MTS) scenario, a novel CS-based cryptosystem by using negative-positive transformation (NPT) is proposed in this paper, which embeds a NPT operation [15] in the CS sampling process to achieve effective privacy protection against CPA. First, the image is pre-processed by using NPT operation. Then, the cipher image is re-encrypted by using CS. Last, the final compressed ciphertext is quantized into bits. Since the introduction of NPT operation destroys the linearity of sampling process, the proposed method can provide effective privacy protection against CPA. The proposed cryptosystem has two advantages. First, it achieves effective privacy protection against CPA. Second, it has better compression performance. The contribution of this paper is that a CS-based cryptosystem with embedding NPT operation is proposed, which can achieve effective privacy protection against CPA.

2. PRELIMINARIES

2.1. CS background

Consider a signal $\boldsymbol{x} \in R^N$, which can be represented as

$$\boldsymbol{x} = \boldsymbol{\varphi\theta}, \tag{1}$$

where $\boldsymbol{\varphi} \in R^{N\times N}$ is a basis matrix and $\boldsymbol{\theta} \in R^N$ is a coefficient vector.

The sampling process of CS is a linear projection, i.e.,

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

where $\boldsymbol{\Phi} \in R^{M\times N}(M \ll N)$ is a measurement matrix and $\boldsymbol{y} \in R^M$ is the measurement vector of $\boldsymbol{x}$.

The signal recovery can be achieved from the measurement vector $\boldsymbol{y}$ by solving

$$\hat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}} \left\| \boldsymbol{\varphi}^{\mathrm{T}} \boldsymbol{x} \right\|_1 \text{ s.t. } \boldsymbol{y}=\boldsymbol{\Phi x}. \tag{3}$$

2.2. Chaotic measurement matrix

When CS is used in simultaneous compression-encryption applications, the measurement matrix can be generated by chaotic functions [3-5]. For example, Frunzete et al. [4] proposed to construct the measurement matrix $\boldsymbol{\Phi}$ by Skew tent map system:

$$z_{k+1} = T[z_k;\mu] = \begin{cases} z_k/\mu, & 0<z_k<\mu \\ 1\text{-}z_k/(1\text{-}\mu), & \mu \le z_k<1 \end{cases}, \tag{4}$$

where the control parameter $\mu \in (0,1)$ and the initial state $z_0 \in (0,1)$.

To construct the measurement matrix, iterate Skew tent map system governed by (4) to generate a chaotic sequence with length $L=M\times N$, then create the following chaotic matrix in a column-by-column manner with this sequence:

$$\boldsymbol{\Phi} = \sqrt{\frac{2}{M}} \begin{pmatrix} z_0 & z_M & \cdots & z_{MN-M} \\ z_1 & z_{M+1} & \cdots & z_{MN-M+1} \\ \vdots & \vdots & \ddots & \vdots \\ z_{M\text{-}1} & z_{2M\text{-}1} & \cdots & z_{MN-1} \end{pmatrix}, \tag{5}$$

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

2.3. Negative-positive transformation

NPT operation is a lightweight image encryption method which can be expressed by

$$\boldsymbol{Z}(i,j) = \begin{cases} \boldsymbol{X}(i,j), & \boldsymbol{R}(i,j)=0 \\ 255\text{-}\boldsymbol{X}(i,j), & \boldsymbol{R}(i,j)=1 \end{cases}, \tag{6}$$

where $\boldsymbol{X} \in R^{N\times N}$, $\boldsymbol{Z} \in R^{N\times N}$ and $\boldsymbol{R} \in R^{N\times N}$ are the original image, the cipher image and the random binary matrix, respectively. $\boldsymbol{X}(i,j)$, $\boldsymbol{Z}(i,j)$ and $\boldsymbol{R}(i,j)$ are the entries of $\boldsymbol{X}$, $\boldsymbol{Z}$ and $\boldsymbol{R}$ located in (i,j), respectively.

We can construct a random binary matrix by using Skew tent map system with two steps:

(1) Generate a chaotic matrix $\boldsymbol{A} \in R^{N\times N}$ with initial value $z_0 \in (0,1)$ by using Skew tent map system.

(2) Create a random binary matrix by using $\boldsymbol{A}$, which can be expressed by

$$\boldsymbol{R}(i,j) = \begin{cases} 1, & \boldsymbol{A}(i,j) \geq \text{median}(\text{vec}(\boldsymbol{A})) \\ 0, & \boldsymbol{A}(i,j) < \text{median}(\text{vec}(\boldsymbol{A})) \end{cases}, \tag{7}$$

where $\text{vec}(\cdot)$ reshapes a matrix into a vector and $\text{median}(\cdot)$ calculates the median.

2.4. Threat model and security analysis

It has been proved that CS-based cryptosystem is vulnerable to CPA due to the linearity of the CS sampling process [10]. By making full use of the linearity of the CS sampling process, the adversary can easily obtain the secret measurement matrix. For example, if the adversary uses an artificial chosen plaintext $\boldsymbol{x}' = [1 \;\; 0 \;\; \cdots \;\; 0]^{\mathrm{T}}$ as the input of the CS-based cryptosystem, then the first column of measurement matrix is revealed. Therefore, we can conclude that the CS-based cryptosystem cannot provide effective privacy protection against CPA. The reason why this cryptosystem is vulnerable to CPA is due to the linearity of sampling process.

3. THE PROPOSED METHOD

In order to resist CPA, a novel CS-based cryptosystem by using NPT is proposed. The overall architecture of the proposed scheme is shown in Figure 1.

3.1. The CPA-resistance CS encoding

According to the discussion above, the CS-based crypto-system is vulnerable to CPA due to the linearity of the CS sampling process. To solve this problem, we embed a non-linear operation called NPT in the CS sampling process, which breaks its linearity. The main encoding steps include three steps.

Step 1: Use NPT operation to preprocess the 2D image before CS encoding

$$\boldsymbol{Z} = \mathrm{E}(\boldsymbol{X}), \tag{8}$$

where $\mathrm{E}(\bullet)$ denotes an image encryption function and $\boldsymbol{Z} \in R^{N\times N}$ is the cipher image of $\boldsymbol{X}$.

Specially, in this paper, we use NPT operation to realize the above encryption function. The NPT-based image encryption can be achieved by using (6), and the corresponding random binary matrix $\boldsymbol{R} \in R^{N\times N}$ is generated by using Skew tent map system with a secret key K_1.

Step 2: Use CS to compress and re-encrypt the cipher image simultaneously.

In order to simplify the encoder, we use parallel CS (PCS) to sample the cipher image. It contains two sub-steps.

(1) Construct a chaotic measurement matrix $\boldsymbol{\Phi} \in R^{M\times N}$ by using Skew tent map system with another secret key K_2.

(2) Sample the cipher image by using $\boldsymbol{\Phi}$

$$\boldsymbol{y}_i = \boldsymbol{\Phi}\boldsymbol{z}_i, \tag{9}$$

where $\boldsymbol{z}_i \in R^{N\times 1}$ is i-th column of $\boldsymbol{Z}$ and $\boldsymbol{y}_i \in R^{M\times 1}$ is the measurement vector of $\boldsymbol{z}_i$.

For the whole intermediate ciphertext, the above sample process can be expressed by

$$\boldsymbol{Y} = \boldsymbol{\Phi}\boldsymbol{Z}, \tag{10}$$

where $\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, ..., \boldsymbol{y}_N] \in R^{M\times N}$ is the final compressed ciphertext.

Step 3: $\boldsymbol{Y}$ is quantized into bits by using scalar quantization (SQ).

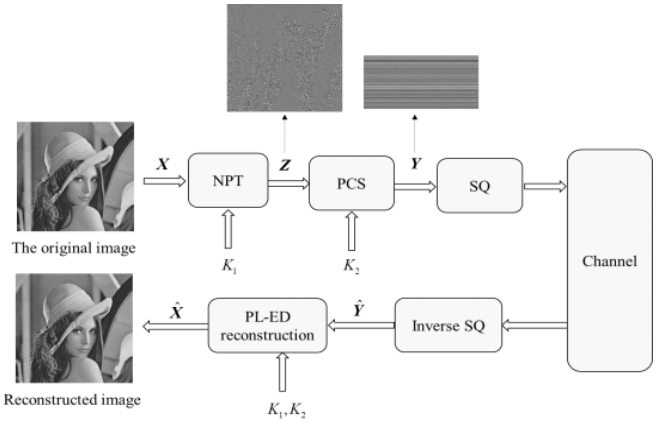


Figure 1. The proposed scheme.

3.2. Image reconstruction

When the recipient receives the keys (e. g., K_1 and K_2), the random binary matrix $\boldsymbol{R}$ and the chaotic measurement matrix $\boldsymbol{\Phi}$ will be exactly generated. Now we will study CS reconstruction problem in this subsection.

By taking the NPT-based image encryption into consideration, we can recover image by solving

$$\hat{\boldsymbol{X}} = \arg\min_{\boldsymbol{X}} \left\| \boldsymbol{\Psi X \Psi}^{\mathrm{T}} \right\|_1 \text{ s.t.} \boldsymbol{Y} = \boldsymbol{\Phi} \mathrm{E}(\boldsymbol{X}) , \tag{11}$$

where $\boldsymbol{\Psi} \in R^{N \times N}$ is a wavelet basis matrix.

The above problem can be solved by using projected Landweber with embedding decryption (PL-ED) algorithm [14]. The detailed steps are summarized below.

Input: $\boldsymbol{\Phi} \in R^{M \times N}$, $\boldsymbol{Y} \in R^{M \times N}$, $\boldsymbol{\Psi} \in R^{N \times N}$, $\varepsilon \in R^{+}$, $C_{\max} \in Z^{+}$, and λ is a factor which controls the convergence speed.

Initialization: $n = 0$; $\hat{\boldsymbol{Z}}_{(0)} = \boldsymbol{\Phi}^{\mathrm{T}} (\boldsymbol{\Phi \Phi}^{\mathrm{T}})^{-1} \boldsymbol{Y}$, where $\hat{\boldsymbol{Z}}_{(0)}$ is the initial estimation of $\boldsymbol{Z}$; $\hat{\boldsymbol{X}}_{(0)} = \mathrm{E}^{-1}(\hat{\boldsymbol{Z}}_{(0)})$, where $\mathrm{E}^{-1}(\cdot)$ is the decryption function and $\hat{\boldsymbol{X}}_{(0)}$ is the initial estimation of $\boldsymbol{X}$.

Stop condition

$$\frac{1}{N} \left\| \hat{\boldsymbol{X}}_{(n)} - \hat{\boldsymbol{X}}_{(n-1)} \right\|_F \le \varepsilon \text{ or } n > C_{\max} .$$

Iteration

While the stop condition is not satisfied.

Step 1: Bivariate shrinkage [16]. It includes three sub-steps.

(1) Dual-tree discrete wavelet transform (DDWT) [17]:

$$\hat{\boldsymbol{D}}_{(n)} = \boldsymbol{\Psi} \hat{\boldsymbol{X}}_{(n)} \boldsymbol{\Psi}^{\mathrm{T}} .$$

(2) Bivariate shrinkage:

$$\bar{\boldsymbol{D}}_{(n)} = \mathrm{Th}(\hat{\boldsymbol{D}}_{(n)}, \lambda) ,$$

where $\mathrm{Th}(\bullet)$ is a denotes a bivariate shrinkage operation and λ is a control factor. The bivariate shrinkage operation can set the coefficients with small absolute value to zero. Therefore, after bivariate shrinkage, we can obtain a sparse solution. The reader can refer to [16] for more details about bivariate shrinkage function.

(3) Inverse DDWT: $\bar{\boldsymbol{X}}_{(n)} = \boldsymbol{\Psi}^{\mathrm{T}} \bar{\boldsymbol{D}}_{(n)} \boldsymbol{\Psi}$.

Step 2: Update the iterative guess by projection operation.

(1) Encryption: $\bar{\boldsymbol{Z}}_{(n)} = \mathrm{E}(\bar{\boldsymbol{X}}_{(n)})$.

(2) Projection: $\tilde{\boldsymbol{Z}}_{(n)} = \bar{\boldsymbol{Z}}_{(n)} + \boldsymbol{\Phi}^{\mathrm{T}} (\boldsymbol{\Phi \Phi}^{\mathrm{T}})^{-1} (\boldsymbol{Y} - \boldsymbol{\Phi} \bar{\boldsymbol{Z}}_{(n)})$.

(3) Decryption: $\hat{\boldsymbol{X}}_{(n+1)} = \mathrm{E}^{-1}(\tilde{\boldsymbol{Z}}_{(n)})$.

Step 3: Update the index: $n = n + 1$.

End while.

Output: the recovered image $\hat{\boldsymbol{X}} = \hat{\boldsymbol{X}}_{(n)}$.

3.3. Security analysis

In this part, we will verify that the proposed CS-based cryptosystem can achieve effective privacy protection against CPA. Combine (8) and (10), we can see that the sampling process for $\boldsymbol{X}$ can be expressed by

$$\boldsymbol{y} = \boldsymbol{\Phi}\mathrm{E}(\boldsymbol{X}), \tag{12}$$

According to (12), we can see that the CS sampling process for $\boldsymbol{X}$ can be regarded as a non-linear operation. Since the linearity of the CS encoding process is destroyed, our method can resist CPA. To demonstrate this, let us consider an example.

Example 1: Suppose the size of the image is 4×4, the sampling ratio is set to be 0.5, and the secret matrix $\boldsymbol{\Phi}$ can be expressed by $\boldsymbol{\Phi} = \left[\boldsymbol{\Phi}_{:,1} \quad \boldsymbol{\Phi}_{:,2} \quad \boldsymbol{\Phi}_{:,3} \quad \boldsymbol{\Phi}_{:,4}\right]$, where $\boldsymbol{\Phi}_{:,i} \in R^{2\times 1}$ is the i-th column of $\boldsymbol{\Phi}$. Assume that the random binary matrix is

$$\boldsymbol{R} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}. \tag{13}$$

Now, we demonstrate that the adversary cannot reveal the secret measurement matrix when NPT operation is embedded in the CS encoding process. In order to reveal the first column of the measurement matrix, the adversary use the cryptosystem to encrypt an artificial chosen plaintext

$$\boldsymbol{X}' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{14}$$

Obviously, for traditional CS-based cryptosystems, if this artificial chosen plaintext is used, the first column of the measurement matrix is revealed. However, in the proposed method, we embed a NPT operation in the CS sampling process. Before sampling the artificial chosen plaintext, the plaintext is encrypted by using NPT operation. After NPT-based encryption, we can obtain the intermediate ciphertext

$$\boldsymbol{Z} = \begin{bmatrix} 254 & 0 & 255 & 0 \\ 255 & 255 & 0 & 255 \\ 0 & 255 & 255 & 0 \\ 255 & 0 & 0 & 255 \end{bmatrix}. \tag{15}$$

Then, the intermediate ciphertext is sampled by using PCS. The first column of the final ciphertext can be expressed by

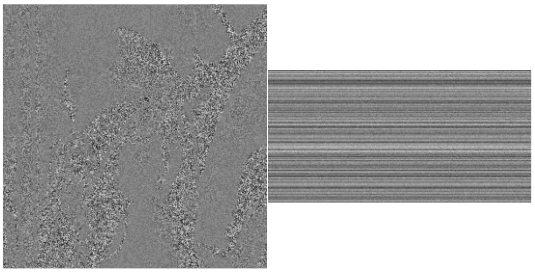
$$\boldsymbol{y}_1' = 254\boldsymbol{\Phi}_{:,1} + 255\boldsymbol{\Phi}_{:,2} + 255\boldsymbol{\Phi}_{:,4}. \tag{16}$$

According to (16), we can see that the first column of final ciphertext is still a combination of columns. Since the adversary does not know which columns are involved in computing, he cannot figure out the secret measurement matrix. In conclusion, since the linearity of the CS encoding process is destroyed by embedding NPT operation, our proposed method can achieve effective privacy protection against CPA.

4. SIMULATION RESULTS

4.1. Encryption performance

First, the encryption performance is evaluated by subjective evaluation. Lena image (512×512) is used in the experiment. The bit size for each CS measurement is 8. The cipher image and the final compressed ciphertext are presented in Figure 2. It can be seen that the cipher image leaks some outline information of the original image. The main reason is that NPT operation is a lightweight encryption method, which cannot protect image privacy perfectly when it is used separately. To enhance the security performance, CS is used to re-encrypt the intermediate cipher image. After CS-based encryption, the final cipher image masks the content of the image perfectly, which means that our method can provide visual privacy protection for 2D images. Furthermore, the size of the compressed ciphertext is far less than that of the plaintext, which means the image is encrypted and compressed by using the proposed method at the same time.



(a) (b)

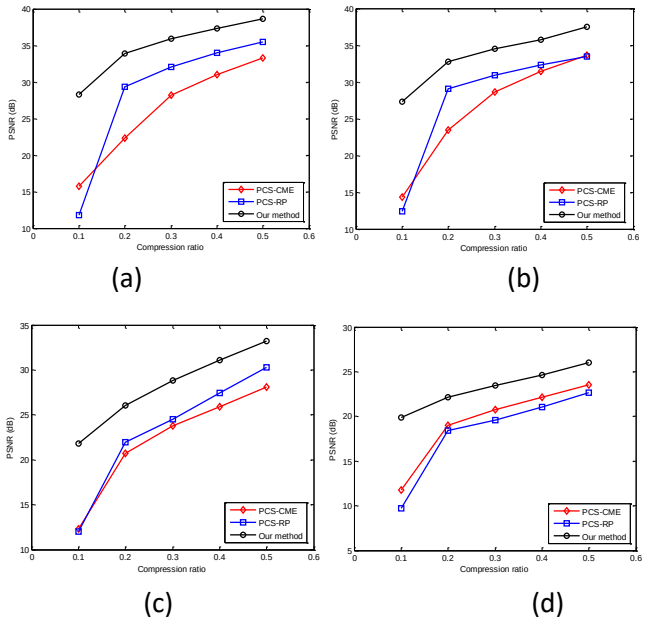
Figure 2. Encryption performance evaluation. (a) the cipher image; and (b) the final compressed ciphertext.

Now, the security performance is evaluated by key space analysis. According to [18], the key space for a good encryption scheme is suggested to be larger than 2^{100} to achieve effective privacy protection against brute-force attack. In the proposed method, the separate keys are K_1 and K_2. Based on the floating-point standard [19], the precision of double-precision number is about 10^{-15}, so the key space of our method is

$$Key\ space = 10^{15} \times 10^{15} = 10^{30} \approx 2^{100}, \tag{17}$$

which is larger enough to resist the brute-force searching.

4.2. Compression performance



(a) (b)

(c) (d)

Figure 3. PSNR results for different CS-based methods. (a) Lena; (b) Peppers; (c) Barbara; and (d) Mandrill.

In this section, we evaluate the compression performance of the proposed method and compare it with two schemes, including PCS with counter mode encryption (PCS-CME) proposed in [5] and PCS with random permutation (PCS-RP) proposed in [13]. Four gray images (512×512) is used in this test. Each CS measurement is quantized into 8 bits. For all schemes, we do not add entropy coder after the quantization with the purpose of simplifying the encoder. For PCS-RP scheme, orthogonal matching pursuit (OMP) [20] algorithm is applied to reconstruct the image. For PCS-CME scheme, we use smoothed projected Landweber (SPL) [21] algorithm to reconstruct the original image. The PSNR (in dB) versus compression ratio for different methods is showed in Figure 3. It can be seen from the figure that our method can obtain remarkable gain in comparison with the other two schemes. For instance, when compression ratio equals to 0.1, for Lena image, the gain of our method is more than 12 dB. The reconstructed images are displayed in Figure 4. It can be seen that our method has better visual quality than the other two schemes.

Figure 4. Reconstructed Lena under compression rate with 0.25. (a) the original image; (b) PCS-RP (26.84 dB); (c) PCS-RP (26.78 dB); and (d) our method (PSNR= 34.98 dB).

5. Conclusions

In this paper, a novel CS-based cryptosystem by using NPT operation is proposed, which embeds a NPT operation in the sampling process to achieve effective privacy protection against CPA. Compared with previous CS-based cryptosystems, the proposed cryptosystem has two advantages: 1) It achieves effective privacy protection against CPA; 2) It has better compression performance.

6.ACKNOWLEDGMENT

This work was supported by the Project Supported by Graduate Student Research and Innovation Foundation of Chongqing, China (Grant No. CYB22063). Zhixiang Zheng (sime0821@163.com) is the corresponding author of this paper.

7.REFERENCES

[1] D. L. Donoho, "Compressed sensing," *IEEE Trans. on Information Theory*, vol. 52, no. 4, pp. 1289-1306, 2006.

[2] R. G. Baraniuk, "Compressive sensing," *IEEE Signal Processing Magazine*, vol. 24, no. 4, pp. 118-121, 2007.

[3] L. Yu, J. P. Barbot, G. Zheng, and H. Sun, "Compressive sensing with chaotic sequence," *IEEE Signal Processing Letters*, vol. 17, no. 8, pp.731-734, 2010.

[4] M. Frunzete, L. Yu, J. Barbot, et al., "Compressive sensing matrix designed by tent map, for secure data transmission," *in Proc. of IEEE Signal Processing Algorithms, Architectures, Arrangements, and Applications*, pp. 1-6, 2011.

[5] G. Hu, D. Xiao, Y. Wang, et al., "An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications," *Journal of Visual Communication and Image Representation*, vol. 44, pp. 116-127, 2017.

[6] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," *in Proc. of 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 813-817, 2008.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[8] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Lowcomplexity multiclass encryption by compressed sensing," *IEEE Trans. on Signal Processing*, vol. 63, no. 9, pp. 2183-2195, 2015.
[9] T. Bianchi, V. Bioglio, and E. Magli, "Analysis of one-time random projections for privacy preserving compressed sensing," *IEEE Trans. On Information Forensics and Security*, vol. 11, no. 2, pp. 313-327, 2016.
[10] L. Y. Zhang, K. W. Wong, Y. Zhang, et al., Bi-level protected compressive sampling, *IEEE Trans. on Multimedia*, vol. 18, no. 9, pp. 1720-1732 , 2016.
[11] V. Cambareri, M. Mangia, F. Pareschi, et al., "On known-plaintext attacks to a compressed sensing-based encryption: Aquantitative analysis," *IEEE Trans. on Inf. Forensics Security*, vol. 10, no. 10, pp. 2182-2195, 2015.
[12] R. Fay, "Introducing the counter mode of operation to compressed sensing based encryption," *Information Processing Letters*, vol. 116, no. 4, pp. 279-283, 2016.
[13] Y. S. Zhang, J. Zhou, F. Chen, "Embedding cryptographic features in compressive sensing," *Neurocomputing*, vol. 205, pp. 472-480, 2016.
[14] B. Zhang, D. Xiao, M. D. Wang, and J. Liang, "Privacy-preserving compressed sensing for image simultaneous compression-encryption ap-plications," *in Proc. of 2021 IEEE Data Compression Conference*, 2021, pp. 283-292.
[15] B. Zhang, D. Xiao, and Y. Xiang, "Robust coding of encrypted images via 2D compressed sensing," *IEEE Trans. on Multimedia*, vol. 23, pp. 2656-2671, 2021.
[16] L.S. Endur, I. W. Selesnick, "Bivariate shrinkage functions for wavelet-based denoising exploiting interscale dependency," *IEEE Trans. on Signal Processing*, vol. 50, no. 11, pp. 2744-2756, 2002.
[17] J. Yang, Y. Wang, W. Xu ,et al., "Image coding using dual-tree discrete wavelet transform," *IEEE Trans. on Image Processing*, vol. 17, no. 9, pp. 1555-1569, 2008.
[18] G. Alvarez, and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006.
[19] IEEE Standard for Binary Floating-Point Arithmetic, *IEEE Standard* 754, 1985.
[20] S. Mun and J. E. Fowler, "Block compressed sensing of images using directional transforms," *in Proc. of IEEE Conference on Image Processing (ICIP)*, pp. 3021-3024, 2009.
[21] J. Tropp, and A. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. on Information Theory*, vol. 53, no. 12, pp. 4655-4666, 2007.