Optics and Lasers in Engineering 98 (2017) 123–133

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes

Guiqiang Hu [a], Di Xiao [b,*], Yong Wang [c], Tao Xiang [b], Qing Zhou [b]

[a] School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[b] Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) of Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, China
[c] Key Laboratory of Electronic Commerce and Logistics of Chongqing, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

ARTICLE INFO

Keywords:
Optical image encryption
Compressive sensing
Double random phase encoding
Reality-preserving fractional cosine transform
Gyrator transform

ABSTRACT

Recently, a new kind of image encryption approach using compressive sensing (CS) and double random phase encoding has received much attention due to the advantages such as compressibility and robustness. However, this approach is found to be vulnerable to chosen plaintext attack (CPA) if the CS measurement matrix is reused. Therefore, designing an efficient measurement matrix updating mechanism that ensures resistance to CPA is of practical significance. In this paper, we provide a novel solution to update the CS measurement matrix by altering the secret sparse basis with the help of counter mode operation. Particularly, the secret sparse basis is implemented by a reality-preserving fractional cosine transform matrix. Compared with the conventional CS-based cryptosystem that totally generates all the random entries of measurement matrix, our scheme owns efficiency superiority while guaranteeing resistance to CPA. Experimental and analysis results show that the proposed scheme has a good security performance and has robustness against noise and occlusion.

1. Introduction

Compressive sensing (CS) has recently emerged as an efficient signal acquiring technique, which argues that the sparse signal can be faithfully reconstructed from a very small set of samples [1–3]. Namely, thanks to the CS sampling process, the signal acquisition and compression can be achieved simultaneously. Interestingly, the CS framework can be used for security purpose [4,5]. By respectively considering the original signal, the sampled measurements and the sensing matrix as the corresponding plaintext, the ciphertext and the key, the CS framework can be viewed as a symmetric cipher. Although it has been proven that the CS framework can achieve computational security under certain assumption [6,7], the energy information of the plaintext signal is inevitably leaked by the CS measurement [8]. Therefore, when exploiting the CS to protect the privacy of image in optical system, the well known optical technique double random phase encoding (DRPE) [9,10] is considered to be concatenate to the CS sampling process to overcome the abovementioned defect of energy information leakage. So far, several proposals adopted the combined CS-and-DRPE architecture [11–15]. This kind of approach has received great attention due to the following advantages. Firstly, CS is usually implemented in optical configuration, what makes the integration of CS and DRPE a very easy work. Secondly, the combination of the two cryptographic primitives (i.e., CS and DRPE) could enhance the security level of the integrated cryptosystem. What's more, the advantages of CS-based cryptosystem, such as compressibility, robustness, can be reserved in the combined CS-and-DRPE cryptosystem.

However, to ensure security, the schemes proposed in [11–15] must work in a "one-time-sampling" manner. Namely, the CS measurement matrix can never be reused, otherwise, the measurement matrix would be revealed by chosen-plaintext attack (CPA). The corresponding attack model will be given in Section 2.1. Based on this fact, many research communities investigate the ways to ensure resistance to CPA for CS-based cryptosystem [16–20]. For example, in [16], Huang et al. proposed a CS-based image encryption scheme that achieves CPA-security by adding some conventional block cipher components, which is not suitable for the optical circumstance. In [17], Fay presented a general model of refreshing the CS sensing matrix for every new signal by introducing the counter mode operation to the CS paradigm. In fact, our work is inspired by Fay's model, but in a very different configuration. In [18], Zhang et al. proposed to jointly quantize and diffuse the CS measurements so as to improve the security of the CS framework. In [19], Zhang et al. proposed a bi-level protected CS-based encryption model, where the measurement matrix is constructed to be non-RIP matrix so as to ensure the resistance to CPA. For more about

* Corresponding author.
E-mail address: xiaodi_cqu@hotmail.com (D. Xiao).

http://dx.doi.org/10.1016/j.optlaseng.2017.06.013
Received 29 October 2016; Received in revised form 16 June 2017; Accepted 16 June 2017
0143-8166/

the security issue of CS-based cryptosystem, interested readers may refer to [20] for a review of CS in information security.

In this paper, we aim to propose a CPA-resistant image encryption scheme under the CS-and-DRPE architecture. Specially, based on the observation that there are too much storage consumption and time consumption to generate a completely fresh CS measurement matrix for every new signal, we focus on how to design an efficient CS measurement matrix updating mechanism with low complexity. In our scheme, this is achieved by introducing the counter mode operation into the CS sampling process. In more detail, the measurement matrix updating is realized in an additionally confidential CS model, which exploits the data sparsity constraint of the CS reconstruction problem and the limited sparsifying property of reality-preserving discrete fractional cosine transform (RPFrCT) matrix. In this way, the measurement matrix updating is closely related to the secret sparse basis (i.e., the RPFrCT matrix) and can be achieved by altering the order of the RPFrCT matrix. Obviously, compared with the approach that updates the CS measurement matrix by totally generating all the random entries, our scheme is more efficient for practical applications. The numerical simulations demonstrate that the proposed scheme can achieve a remarkable security performance while maintaining the robustness against noise and occlusion.

The rest of this paper is organized as follows. In the next section, some preliminaries are given. The proposed scheme is described in Section 3. In addition, experimental results and security analyses are given in Section 4. The last section concludes this paper.

2. Preliminaries

2.1. Compressive sensing

The CS framework involves a sampling process and a reconstruction process. Considering a 1D sparse signal $\mathbf{v} = [v_1, v_2, \ldots, v_N]^T$ to be sampled, the CS sampling process is done by a non-adaptive linear projection $\mathbf{y} = \mathbf{\Phi v}$, where $\mathbf{\Phi} \in R^{M\times N}(M < N)$ is the measurement matrix, and $\mathbf{y} \in R^M$ is the measurement vector. The CS theory states that if $\mathbf{\Phi}$ satisfies the restricted isometry property (RIP) of a certain order, the sparse signal $\hat{\mathbf{v}} = [\hat{v}_1, \hat{v}_2, \ldots, \hat{v}_N]^T$ can be recovered from $\mathbf{y}$ by solving an l_1-minimization problem defined as follows,

$$\hat{\mathbf{v}} = \arg\min \|\mathbf{v}\|_1 \ s.t.\ \mathbf{y} = \mathbf{\Phi v}. \tag{1}$$

It is worth noting that when applying CS to 2D image with bulk data size, sampling the whole image as a stacked vector under conventional CS framework may result in a dramatically large sized measurement matrix and a large scale reconstruction problem, which is often expensive in practice. To reduce the storage and computational complexity, one of the common solutions is to exploit the parallel CS [21] paradigm, where the 2D image is sampled and reconstructed column by column independently. More precisely, considering an image of 2D matrix $\mathbf{X} \in R^{N\times N}$, let $\mathbf{x}_i \in R^N$ denote the i-th column of $\mathbf{X}$, and $\mathbf{\Phi} \in R^{M\times N}$ be the measurement matrix. Then, the sampling process of parallel CS can be expressed as

$$\mathbf{y}_i = \mathbf{\Phi x}_i, \ (\mathbf{y}_i \in R^M, \ i = 1, \ldots, N). \tag{2}$$

In this way, the whole measurement is represented as $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N]$. Moreover, since real image data is rarely sparse, an $N\times N$ sparse representation basis $\mathbf{\Psi}$ that is incoherent with the measurement matrix is often required to transform the image into sparse signal, i.e., $\mathbf{s}_i = \mathbf{\Psi}^{-1}\mathbf{x}_i$. In this way, the sparse signal can be reconstructed by the following l_1-minimization problem defined as follows,

$$\hat{\mathbf{s}}_i = \arg\min \|\mathbf{s}_i\|_1 \quad s.t. \quad \mathbf{y}_i = \mathbf{\Phi x}_i = \mathbf{\Phi\Psi s}_i = \mathbf{A s}_i, \ (i = 1, \ldots, N), \tag{3}$$

where $\mathbf{A} = \mathbf{\Phi\Psi}$ is referred as the sensing matrix. After reconstructing the sparse signal $\mathbf{S} = [\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_N]$, where $i = 1, \ldots, N$, image data can be recovered via $\hat{\mathbf{x}}_i = \mathbf{\Psi}\hat{\mathbf{s}}_i$, and then the entire reconstructed image is formed as $\hat{\mathbf{X}} = [\hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2, \ldots, \hat{\mathbf{x}}_N]$.

Note that the conventional parallel CS paradigm with measurement matrix re-using is vulnerable to CPA. As analyzed in cryptanalysis [22], adversary has access to an encryption oracle that encrypts arbitrary plaintext to obtain the corresponding ciphertext. Considering the encryption process of parallel CS sampling process $\mathbf{y}_i = \mathbf{\Phi x}_i$, where $i = 1, \ldots, N$. If the adversary asks the encryption oracle to encrypt an artificial chosen plaintext $\mathbf{x'}_i = [0, \ldots, 0, 1_i, 0, \ldots, 0]^T$ by $\mathbf{y'}_i = \mathbf{\Phi x'}_i$, then the i-th column of $\mathbf{\Phi} \in R^{M\times N}$ could be revealed, since it is equivalent to the corresponding ciphertext $\mathbf{y'}_i$. By repeating the above process from the first column to the last column, the whole secret measurement matrix could be revealed. Hence, we can conclude that the parallel CS-based cryptosystem with a fixed measurement matrix is not secure against CPA.

Furthermore, the concatenation of DRPE followed by CS would not change the vulnerability mentioned above, since the DRPE technique is also found to be vulnerable to CPA [23–25]. In this case, adversary can treat the DRPE process as a matrix multiplication. Thus, the abovementioned CPA is still feasible to crack the DRPE-combined scheme. The similar cryptanalysis work had already been proposed in [19] (detailed cracking process can be found in Section II. C of [19]).

Intuitively, to address the abovementioned security issue, a straight forward solution is to update the measurement matrix for every new signal. Therefore, the updating mechanism of measurement matrix becomes a critical issue for secure use of CS paradigm.

2.2. Reality-preserving fractional cosine transform

Reality-preserving fractional cosine transform (RPFrCT) [26] is a parameterized transform derived from the discrete cosine transform (DCT), whose transform matrix of size $N\times N$ can be expressed as

$$\mathbf{C} = \frac{1}{\sqrt{N}}\varepsilon_k \cos\left(2\pi\frac{(2n+1)k}{4n}\right), \tag{4}$$

where is $n = 0, \ldots, N-1$, $k = 0, \ldots, N-1$, $\varepsilon_0 = 1$ and $\varepsilon_k = \sqrt{2}$ for $k > 0$. Moreover, the matrix $\mathbf{C}$ can be expressed as the form of

$$\mathbf{C} = \mathbf{U\Lambda U}^*, \tag{5}$$

where "$*$" denotes matrix conjugate transposition, $\mathbf{U} = [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_N]$ consists of N orthonormal eigenvectors, $\mathbf{\Lambda} = diag(\lambda_0, \ldots, \lambda_{N-1})$ is the diagonal matrix with element $\lambda_n = \exp(j\phi_n)$, $n = 0, \ldots, N-1$.

Thus, the discrete fractional cosine transform (DFrCT) matrix of order α can be defined as the form of

$$\mathbf{C}_\alpha = \mathbf{U\Lambda}^\alpha\mathbf{U}^*, \tag{6}$$

where $\mathbf{\Lambda}^\alpha$ is the α-th power of $\mathbf{\Lambda}$.

In our scheme, we implement the RPFrCT matrix by following the way proposed in [19]. More precisely, the implementation procedure can be described as follows:

Step 1: Construct a DFrCT matrix $\mathbf{C}_\alpha$ of size $N/2\times N/2$.

Step 2: Construct a RPFrCT matrix $\mathbf{R}_\alpha$ as the form $\mathbf{R}_\alpha = \begin{bmatrix}\mathrm{Re}(\mathbf{C}_\alpha), & -\mathrm{Im}(\mathbf{C}_\alpha)\\ \mathrm{Im}(\mathbf{C}_\alpha), & \mathrm{Re}(\mathbf{C}_\alpha)\end{bmatrix}$, where $\mathrm{Re}(x)$ and $\mathrm{Im}(x)$ return the real and imaginary part of compact value x, respectively.

After that, the RPFrCT on a 1D real signal $\mathbf{v} = [v_1, v_2, \ldots, v_N]^T$ of length N can be achieved via $\mathbf{y} = \mathbf{R}_\alpha\mathbf{v}$. The derivation about the reason can be summarized as follows:

At first, assuming the length N of signal $\mathbf{v}$ is even, thus, we can construct a complex signal as the form of $\tilde{\mathbf{v}} = [v_1 + jv_{1+N/2}, v_2 + jv_{2+N/2}, \ldots, v_{N/2} + jv_N]^T$. Then, a DFrCT can be achieved by using the DFrCT matrix $\mathbf{C}_\alpha$ of size $N/2\times N/2$, i.e., $\tilde{\mathbf{y}} = \mathbf{C}_\alpha\tilde{\mathbf{v}}$. In this way, it holds that

$$\mathbf{y} = \mathbf{R}_\alpha\mathbf{v} = \begin{bmatrix}\mathrm{Re}(\mathbf{C}_\alpha), & -\mathrm{Im}(\mathbf{C}_\alpha)\\ \mathrm{Im}(\mathbf{C}_\alpha), & \mathrm{Re}(\mathbf{C}_\alpha)\end{bmatrix}\cdot\begin{bmatrix}\mathrm{Re}(\tilde{\mathbf{v}})\\ \mathrm{Im}(\tilde{\mathbf{v}})\end{bmatrix} = \begin{bmatrix}\mathrm{Re}(\mathbf{C}_\alpha)\mathrm{Re}(\tilde{\mathbf{v}}) - \mathrm{Im}(\mathbf{C}_\alpha)\mathrm{Im}(\tilde{\mathbf{v}})\\ \mathrm{Im}(\mathbf{C}_\alpha)\mathrm{Re}(\tilde{\mathbf{v}}) + \mathrm{Re}(\mathbf{C}_\alpha)\mathrm{Im}(\tilde{\mathbf{v}})\end{bmatrix}$$
$$= \left[\mathrm{Re}(\tilde{\mathbf{y}}), \mathrm{Im}(\tilde{\mathbf{y}})\right]^T$$

Therefore, the reality-preserving transform is achieved by the above implementation.