J. Vis. Commun. Image R. 44 (2017) 116–127

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications ☆

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

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

ARTICLE INFO

Article history:
Received 10 September 2016
Revised 25 November 2016
Accepted 17 January 2017
Available online 24 January 2017

Keywords:
Compressive sensing
Cryptography
Image compression
Image encryption
Parallel processing

ABSTRACT

Recently, using compressive sensing (CS) as a cryptosystem has drawn attention due to its compressibility and low-complexity during the sampling process. However, when applying such cryptosystem to images, how to protect the privacy of the image while keeping efficiency becomes a challenge. In this paper, we propose a novel image coding scheme that achieves combined compression and encryption under a parallel compressive sensing framework, where both the CS sampling and the CS reconstruction are performed in parallel. In this way, the efficiency can be guaranteed. On the other hand, for security, the resistance to chosen plaintext attack (CPA) is realized with the help of the cooperation between a nonlinear chaotic sensing matrix construction process and a counter mode operation. Furthermore, the defect of energy information leakage in CS-based cryptosystem is also overcome by a diffusion procedure. Experimental and analysis results show the scheme achieves effectiveness, efficiency and high security simultaneously.

1. Introduction

Compressive sensing (CS) has recently emerged as an efficient signal acquiring framework, which is known to unify sampling and compression in a simple linear projection step [1–3]. CS sampling process of a sparse signal $\mathbf{x}$ is done by a matrix multiplication, i.e., $\mathbf{y} = \mathbf{Ax}$, where $\mathbf{A}$ is the sensing matrix, and $\mathbf{y}$ is the measurement vector. Interestingly, if $\mathbf{A}$ is random, this random linear projection can provide not only compression but also some notion of security. The equivalences between CS and a private cryptosystem can be defined as: the signal $\mathbf{x}$ is the plain text, the measurement vector $\mathbf{y}$ is the cipher text and the sensing matrix $\mathbf{A}$ is the secret key. In this way, the encoding process can be viewed as an encryption function, and the decryption can be achieved by solving an optimization problem (see Section 3.1). The CS-based cryptosystem has some inherent advantages. Firstly, the low cost of CS sampling process makes the CS-based cryptosystem very suitable for low-complexity restricted system. Secondly, during the CS sampling process, compression and encryption can be jointly guaranteed by a simple matrix multiplication operation. It is worth mentioning that the combined compression and encryption of CS sampling is an appealing option for real-world communications [4]. For instance, considering the telemedicine circumstance, the patients' sensitive information needs to be encrypted for privacy protection. At the same time, it is also necessary to compress the multimedia data to reduce the storage space and bandwidth of the secure transmission system. Apparently, in such scenario, both the encryption requirement and the compression requirement can be simultaneously fulfilled by the CS sampling process. Therefore, the CS-based cryptosystem shows great potential in the secure communication of digital data [5–9].

Although promising, applying the CS-based cryptosystem to image with bulk data size remains challenging. Two issues are confronted: efficiency and security. On the one hand, for efficiency consideration, sampling the whole vector-reshaped image under conventional CS framework may require a dramatically large sized sensing matrix, which is often unreliable in practice. Fortunately, a good solution referred as parallel CS [10] can address the efficiency issue, where the 2D image is sampled column by column by using the same sensing matrix. In this way, the storage and computational complexity can be reduced significantly, since both sampling and reconstruction are conducted in parallel. Therefore, the approach of parallel CS is commonly used to represent the image date for its high efficiency [10–12]. On the other hand, for security consideration, it has been proven that the CS-based cryptosystem is computational security under brute-force attack and ciphertext only attack (COA), since the systematical searching in its key space is computationally infeasible [13,14]. However, the re-use of sens-

☆ This paper has been recommended for acceptance by M.T. Sun.

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

http://dx.doi.org/10.1016/j.jvcir.2017.01.022
1047-3203/

ing matrix in the parallel CS framework would make the chosen plaintext attack (CPA) feasible. The security analysis and potential attack model of CS-based cryptosystem will be given in detail in Section 3.2. Moreover, it is stated in [15] that the ciphertext measurements of CS-based cryptosystem leak information about the plaintext energy. Based on this fact, Bianchi et al. suggested normalizing the measurement vector to achieve a higher security level. However, for decryption, the information of measurement energy must be transmitted over an auxiliary classical cryptography protected channel, which restricts its application. To sum up, how to design a secure CS-based image cryptosystem while maintaining the efficiency for practical use is a challenging work.

In this paper, we aim to design an efficient parallel CS-based image compression-encryption coding scheme that ensures resistance to CPA, so as to address the abovementioned efficiency issue and the security issue simultaneously. Specially, based on the fact that chaotic sequence can be employed to construct the CS sensing matrix [16,17], we exploit the pseudo-random behavior and sensitivity of chaotic system to protect the secret of the CS sensing matrix. In addition, a counter mode operation is embedded in the construction of chaotic sensing matrix to implement a CPA-resistance CS sampling process. Furthermore, based on the observation that the defect of energy information leakage in CS-based cryptosystem would restrict the application of image privacy protection (see Section 4.2), a diffusion procedure governed by chaotic system is added to the CS sampling process. The numerical simulations demonstrate that the proposed scheme achieves a remarkable security performance under some crucial security criterions.

The rest of this paper is organized as follows. In the next section, related works are overviewed. The parallel CS preliminaries and a threat mode are given in Section 3. The proposed scheme is described in Section 4. In addition, experimental results and security analyses are given in Section 5. The last section concludes this paper.

2. Related work

There are a number of studies exploring the scheme that uses CS as a cryptosystem. In [18], Huang et al. proposed a remote image sensing scheme by scrambling the CS measurement. In contrast, Zhang et al. suggested scrambling the frequency coefficients of image before the CS sampling [19]. The approach in [19] has the advantage of reconstruction performance promotion, since the restricted isometry property (RIP) of CS can be relaxed by scrambling the frequency coefficients of image. Another noticeable approach is to use optical encryption technique to enhance the secrecy of CS framework, such as the works proposed in [20–22]. It is worth pointing out that all the CS-based ciphers proposed in [18–22] must work in a "one-time-sampling" manner, i.e., the sensing matrix is never re-used. Otherwise, the secrecy of these cryptosystems is vulnerable under CPA scenario. Subsequently, many efforts were made to ensure the CPA-security of CS-based cryptosystem. For example, Huang et al. proposed a CS-based image encryption scheme by adding some conventional block cipher components followed by the CS sampling process [23]. In [23], the CPA-security is contributed by the block cipher components. Apart from that, Fay proposed a general model for altering the secret CS sensing matrix on every new signal by introducing the counter mode to the CS-based cryptosystem [24]. This approach offers a good solution to ensure CPA-security in the CS sampling process, which is inspired to our work. However, in [24], the energy information of the plaintext is still leaked, what is not expected in some special scenarios (see Section 4.2). Moreover, in [25], Zhang et al. proposed a bi-level CS protection scheme, in which CPA-security is guaranteed by taking a distinct key-related sparsifying basis to construct a non-RIP sensing matrix. This approach provides an alternative way to achieve CPA-security in the CS sampling process.

3. Preliminaries

3.1. Parallel CS for image

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 $\mathbf{\Phi} \in R^{M\times N}$, $(M < N)$, be the sensing matrix. Then, the sampling process of parallel CS can be formalized as:

$$\mathbf{y}_i = \mathbf{\Phi}\mathbf{x}_i, \quad \text{where } i = 1,\ldots,N;\ \mathbf{y}_i \in R^M. \tag{1}$$

In this way, the whole measurement is represented as $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N]$. Note that real image date is rarely sparse, while it can be transformed into sparse signal by a sparse representation basis. i.e., $\mathbf{x}_i = \mathbf{\Psi}\mathbf{s}_i$, where $\mathbf{\Psi}$ is a $N \times N$ sparse representation basis that is incoherent with $\mathbf{\Phi}$. Thus, if $\mathbf{\Phi}$ satisfies the restricted isometry property (RIP) of a certain order, the sparse signal $\mathbf{S} = [\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_N]$ could be recovered via the following l_1-minimization problem:

$$\hat{\mathbf{s}}_i = \arg\min_{\mathbf{s}_i \in R^N} \|\mathbf{s}_i\|_1 \quad s.t. \quad \mathbf{y}_i = \mathbf{\Phi}\mathbf{x}_i = \mathbf{\Phi}\mathbf{\Psi}\mathbf{s}_i, \quad \text{where } i = 1,\ldots,N. \tag{2}$$

After obtaining the sparse signal, image date can be reconstructed via $\hat{\mathbf{x}}_i = \mathbf{\Psi}\hat{\mathbf{s}}_i$, where $i = 1,\ldots,N$. Thus, the entire reconstructed image can be formed as $\widehat{\mathbf{X}} = [\hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2, \ldots, \hat{\mathbf{x}}_N]$.

Since both the sampling process and the reconstruction process of parallel CS are performed individually column by column, the required storage and computational complexity are much lower than that of the conventional scheme. This makes the parallel CS very suitable for processing image with bulk date size.

Besides, it is worth mentioning that the storage and transmission of a random CS sensing matrix as a key may be very costly for practical applications. Because of that, the seed of a pseudo-random function used for generating the entries of the random sensing matrix is usually defined as the secret key of a CS-based cryptosystem. In our scheme, the pseudo-random entries of sensing matrix are generated by a chaotic system. Naturally, the initial state and control parameter of the chaotic system are defined as the secret key.

3.2. Security issue analysis and potential attack model

In this section, the security issue of exploiting parallel CS in image cryptosystem will be discussed. Recalling the classical attack CPA in cryptanalysis [26], adversary has access to an encryption oracle that encrypts arbitrary plaintext to obtain the corresponding ciphertext. Considering the encryption process of parallel CS-based cryptosystem $\mathbf{y}_i = \mathbf{\Phi}\mathbf{x}_i$, where $i = 1,\ldots,N$. If the adversary asks the encryption oracle to encrypt an artificial chosen plaintext $\mathbf{x}'_i = [0,\ldots,0,1_i,0,\ldots,0]^T$, (i.e., $\mathbf{y}'_i = \mathbf{\Phi}\mathbf{x}'_i$), then the i-th column of $\mathbf{\Phi} \in R^{M\times N}$ could be revealed, which 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 matrix can be exposed. Therefore, we can conclude that the parallel CS-based cryptosystem with re-using of the same sensing matrix cannot resist CPA. The leading reason why this cryptosystem is vulnerable to CPA is for the fact that the encryption is deterministic for a fixed sensing matrix. A solution to achieve CPA-security is to adopt a probabilistic encryption scheme.

Another security issue is about the energy information leakage from measurement vectors. As in some scenarios, the adversary is