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/© 2016 Elsevier B.V. All rights reserved.

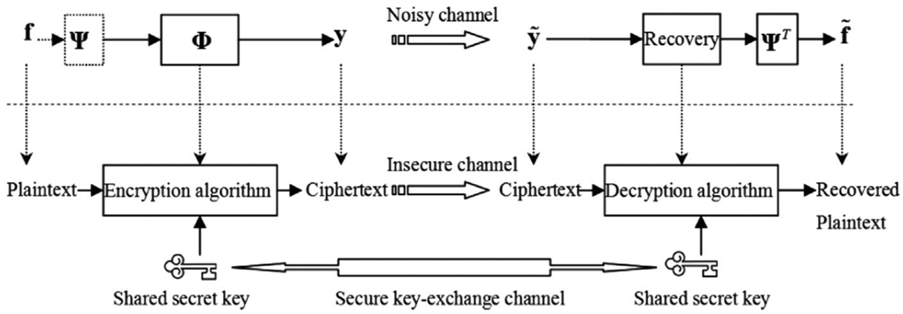

Fig. 1. The relationship between CS and symmetric-key cipher.

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

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

which means that $\mathbf{f}$ could be sparsely represented in a certain domain by the transform matrix $\mathbf{\Psi} := [\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots, \boldsymbol{\psi}_M]$ 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 $\mathbf{\Psi}$ domain. Instead of sampling $\mathbf{x}$ directly, we take a small number of CS measurements. Let $\mathbf{\Phi} := [\boldsymbol{\varphi}_1, \boldsymbol{\varphi}_2, \ldots, \boldsymbol{\varphi}_M]$ denote a $K \times M$ matrix with $K \ll M$. Then K non-adaptive linear samples $\mathbf{y}$ can be obtained by

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

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

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

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

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

Definition 1 (*Candès and Tao [7]*). Matrix $\mathbf{\Phi}$ 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 $\mathbf{\Phi}$ is created from this sequence column by column,