Optics and Lasers in Engineering 110 (2018) 72–79

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging

Nanrun Zhou[a,*], Hao Jiang[a], Lihua Gong[a], Xinwen Xie[b]

[a] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
[b] University of Poitiers, XLIM, (UMR CNRS 7252), France

ARTICLE INFO

Keywords:
Image encryption
Co-sparse representation
Compressive sensing
Pixel scrambling

ABSTRACT

To enhance the confidentiality and the robustness of double image encryption algorithms, a novel double-image compression-encryption algorithm is proposed by combining co-sparse representation with random pixel exchanging. Firstly, two scrambled plaintext images are expressed by the co-sparse analysis model with different row-scrambled basis matrices while the co-sparse representations could be regarded as the intermediate ciphertext. Subsequently, the co-sparse representations are compressed and encrypted concurrently by compressive sensing. Furthermore, the corresponding measurements obtained are processed by the random pixel exchanging operator and the Arnold transform. Finally, the corresponding results are combined into an enlarged image and then the resulting image is re-encrypted by the discrete fractional angular transform to improve the security of the whole algorithm. A series of numerical simulations are carried out to show the security performance of the proposed double-image compression and encryption algorithm.

1. Introduction

Image encryption is one of the hot topics in the field of image processing. In order to prevent the divulgation of the private original image information, a number of image encryption algorithms have been presented with different technologies, such as chaotic system [1–4], optical system [5,6], Gray code [7,8], circular random grids (CRG) [9], wave transmission [10], Brownian motion [11], and so on. Although the image encryption algorithms mentioned above are apparently different, but almost all of them transform the plaintext images into noise-like ciphertext images. For an unauthorized user, it is impossible to capture any useful information about the original image through analyzing the ciphertext image. If the size of the ciphertext image exceeds that of the plaintext image, then it will require more transmission bandwidth and more storage space, which is extremely inconvenient for practical applications. Thus, it is necessary to develop a scheme to achieve image compression and encryption simultaneously.

Compressed sensing (CS) has attracted widespread attention because of its achievements in image compression [12]. Over the years, many image encryption schemes combining CS with other efficient encryption techniques have been introduced. For instance, a CS-based digital image encryption scheme based on block Arnold scrambling and bit wise XOR operation was presented to resist a variety of common attacks [13]. P Lu et al. suggested an image encryption algorithm, where the original image is firstly compressed and encrypted by CS, and then the compressed and encrypted result is re-encrypted by the double random-phase encoding (DPRE) operation [14]. To improve the security of the scheme, a chaotic diffusion followed by DPRE was employed after CS, which achieved an excellent encryption effect [15]. An image encryption process based on compressive fractional Fourier transform with the kernel steering regression in DRPE was designed for de-noising and sampling [16]. All of the image encryption systems mentioned above have good security performance against attacks, however, most of them share a common drawback that the consumption of key is too large since the entire measurement matrix in CS is regarded as the key. To overcome this deficiency, S N George et al. suggested constructing the measurement matrix in CS with multiple chaotic maps, where each value in the measurement matrix can be obtained by two different one dimensional chaotic maps [17]. In 2014, N R Zhou et al. came up with a novel image compression-encryption algorithm, in which the first row vector of the measurement matrix was controlled by Logistic map [18]. Subsequently, they proposed a hybrid image compression-encryption algorithm by utilizing partial Hadamard matrix as the secure measurement matrix manipulated by chaos [19]. A special approach to constructing the measurement matrix based on linear feedback shift register (LFSR) was proposed, where the initial state of the LFSR system was considered as the secret key [20]. N R Zhou et al. devised a novel image compression-encryption algorithm by connecting nonlinear fractional Mellin transform with 2D CS, where the original image was firstly measured by the measurement matrices in two directions, and then the intermediate result was re-encrypted by the nonlinear fractional Mellin transform [21]. Moreover, an image compression and encryption scheme based on 2D

* Corresponding author.
E-mail address: nrzhou@ncu.edu.cn (N. Zhou).

https://doi.org/10.1016/j.optlaseng.2018.05.014
Received 14 March 2018; Received in revised form 8 April 2018; Accepted 15 May 2018

CS and discrete fractional random transform was introduced, in which 2D discrete cosine transformation dictionary was employed to express the original image, and then the resulting image was processed by the key-related measurement matrices and the discrete fractional random transform [22]. In addition, Y S Zhang et al. invented a secure parallel CS scheme based on random permutation, which can relax the restricted isometry property (RIP) of the measurement matrix and achieve the asymptotic spherical secrecy [23]. Started with the appropriate reference image construction of significant blocks chosen from the grayscale host image, L S Sui et al. presented an optical color image watermarking scheme based on CS and human visual characteristics in gyrator domain, which achieves embedding the color watermark into the grayscale host image [24].

However, these image encryption systems are intended for single image, which is far from the real-life demand. For this reason, a double image encryption algorithm based on Arnold transform and discrete fractional angular transform was proposed, where two original images denoted by the amplitude and the phase of a complex function, respectively, are encrypted by the Arnold transform and the discrete fractional angular transform [25]. Furthermore, L S Sui et al. presented a multiple-image encryption scheme with the nonlinear iterative phase retrieval algorithm in the gyrator transform domain and designed a chaotic structured phase mask based on the logistic map, Fresnel zone plate and radial Hilbert mask [26]. Besides, X F Meng et al. presented a secret multiple-image encryption method combining row scanning compressive ghost imaging with phase retrieval in the Fresnel domain, which achieves phase keys sharing and management by a group of participators [27].

It is worth noting that all of the CS-based image encryption algorithms mentioned above are built on the sparse representation synthesis model. Nevertheless, it is not given enough attention for the similar sparse representation model, named co-sparse analysis model [28]. It has been revealed that the co-sparse analysis model demanding lower complexity and lower memory shows better effect in image denoising compared with other classical methods [29]. R Gao et al. investigated how to achieve the reconstruction and fusion of multi-focus images with the co-sparse analysis model simultaneously and introduced a particular fusion function based on this model [30]. A novel image compression-encryption algorithm based on the analysis sparse model was proposed, in which the analysis sparse representation of the plaintext image was compressed and encrypted by CS, and then the measurement was re-encrypted by a pixel-scrambling process controlled by chaos [31].

So far, multi-image encryption based on the co-sparse analysis model has not been studied. Motivated by this, a novel double-image compression and encryption scheme based on the co-sparse representation, random pixel exchanging and discrete fractional angular transform will be designed in this paper. Two rearranged original images are represented by the co-sparse analysis model with a couple of row-scrambled dictionaries. Then the two co-sparse representations are compressed and encrypted by CS, respectively. The random pixel exchanging process and the Arnold transform are utilized to re-encrypt the two compressed images. Besides, the two encryption images are combined into an enlarged image in the horizontal direction. The discrete fractional angular transform is employed to re-encrypt the resulting image to strengthen the confidentiality of the scheme. In the compression and encryption process, the two reshaped dictionaries are constructed by scrambling the rows of a fixed DCT dictionary with a pair of different random sequences controlled by the 2D-Logistic map. The measurement matrices in CS and the decision matrix in random pixel exchanging operator are regarded as the circular matrices, where the initial rows of the circular matrices are generated by chaotic system.

The rest of this paper is organized as follows. The next section introduces some necessary fundamental knowledge in brief. The proposed double-image compression and encryption scheme is described in Section 3. Simulation results and security analyses are demonstrated in Section 4. Our work is concluded in the last section.

2. Fundamental knowledge

2.1. Co-sparse analysis model

The co-sparse analysis model for an $N\times 1$ dimension signal $\mathbf{x}\in R^{N\times 1}$ with respect to $\mathbf{\Omega}\in R^{P\times N}$ $(P\geq N)$ is defined as:

$$l = P - ||\mathbf{\Omega x}||_0 \tag{1}$$

where $\mathbf{\Omega}$ denotes an analysis dictionary [32] or an analysis operator [33], and each row of $\mathbf{\Omega}$ is considered as an atom. The so-called co-sparsity l represents the number of zeros in $\mathbf{\Omega x}$. There is a co-sparse representation of the signal $\mathbf{x}$, i.e., $\mathbf{s}=\mathbf{\Omega x}$ $(\mathbf{s}\in R^{P\times 1})$, if the co-sparsity of singal $\mathbf{x}$ is large enough. For an image $\mathbf{x}$ with co-sparsity, the co-sparse analysis model for $\mathbf{x}$ can be formulated as:

$$\arg\min_{\mathbf{s}} ||\mathbf{s}||_0 \quad \text{s.t.} \quad \mathbf{s}=\mathbf{\Omega x} \tag{2}$$

where the vector $\mathbf{s}$ denotes the co-sparse representation of image $\mathbf{x}$.

2.2. Compressive sensing

In the co-sparse analysis model, the sampling process of $\mathbf{s}$ can be expressed as:

$$\mathbf{y}=\mathbf{\Phi s}=\mathbf{\Phi\Omega x} \tag{3}$$

where $\mathbf{\Phi}$ denotes an $M\times P$ $(M\ll P)$ measurement matrix, and $\mathbf{y}$ is the measurement vector of dimension $M\times 1$ with respect to $M\ll N$. The reconstruction of signal $\mathbf{x}$ is an optimization problem, i.e.,

$$\hat{\mathbf{x}}=\arg\min_{\mathbf{x}} \|\mathbf{\Omega x}\|_0 \quad \text{s.t.} \quad \mathbf{y}=\mathbf{\Theta x} \tag{4}$$

where $\|\mathbf{\Omega x}\|_0$ represents the l_0 norm of vector $\mathbf{\Omega x}$, and $\mathbf{\Theta}=\mathbf{\Phi\Omega}$ is an $M\times N$ sensing matrix. The optimization problem in Eq. (4) is an analysis pursuit problem [32]. Some feasible algorithms such as Greedy Analysis Pursuit (GAP) algorithm [28], Optimized Backward Greedy (OBG) algorithm [32], Analysis SimCO algorithm [34], and Split Bergman Iteration (SBI) algorithm [35] have been developed to recover the original signal $\mathbf{x}$ from the measurement $\mathbf{y}$. In this paper, the Split Bergman Iteration algorithm is adopted.

2.3. Chaotic system

The Logistic map is able to generate a chaotic sequence with a stable chaotic property, which can be defined as:

$$z_{n+1}=\mu z_n(1-z_n) \tag{5}$$

where the initial state z_0 belongs to (0, 1) and the control parameter μ is in [3.57, 4]. The 2D-Logistic map composed of two Logistic maps is given as:

$$\begin{cases} x_{n+1}=\lambda_1 x_n(1-x_n)+\gamma_1 {y_n}^2 \\ y_{n+1}=\lambda_2 y_n(1-y_n)+\gamma_2(x_n+x_n y_n) \end{cases} \tag{6}$$

If the initial values x_0, y_0 and the control parameters λ_1, λ_2, γ_1, γ_2 satisfy the conditions such as: $0<x_0<1$, $0<y_0<1$, $2.75<\lambda_1<3.4$, $2.7<\lambda_2<3.45$, $0.15<\gamma_1<0.21$, $0.13<\gamma_2<0.15$, then the system will become chaotic. After all components are calculated step by step, two chaotic sequences can be generated.

3. Double-image compression and encryption algorithm

3.1. Compression and encryption process

For the sake of clarity, we firstly give the block diagram of the image compression and encryption process as shown in Fig. 1. The details of the image compression and encryption process are as follows: