Optics & Laser Technology 62 (2014) 152–160

Contents lists available at ScienceDirect

Optics & Laser Technology

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

Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing

Nanrun Zhou [a,b,*], Aidi Zhang [a], Fen Zheng [a], Lihua Gong [a,c]

[a] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
[b] Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
[c] Jiangxi Province Key Laboratory of Image Processing and Pattern Recognition, Nanchang Hangkong University, Nanchang 330063, China

ARTICLE INFO

Article history:
Received 16 January 2014
Received in revised form
21 February 2014
Accepted 25 February 2014
Available online 31 March 2014

Keywords:
Image encryption
Image compression
Compressive sensing

ABSTRACT

The existing ways to encrypt images based on compressive sensing usually treat the whole measurement matrix as the key, which renders the key too large to distribute and memorize or store. To solve this problem, a new image compression–encryption hybrid algorithm is proposed to realize compression and encryption simultaneously, where the key is easily distributed, stored or memorized. The input image is divided into 4 blocks to compress and encrypt, then the pixels of the two adjacent blocks are exchanged randomly by random matrices. The measurement matrices in compressive sensing are constructed by utilizing the circulant matrices and controlling the original row vectors of the circulant matrices with logistic map. And the random matrices used in random pixel exchanging are bound with the measurement matrices. Simulation results verify the effectiveness, security of the proposed algorithm and the acceptable compression performance.

1. Introduction

With the development of multimedia technology, more and more information comes from images. The security of images becomes a serious issue and hence a number of image encryption algorithms were proposed [1–10]. For example, Chen et al. proposed a new phase retrieval algorithm for optical image encryption in three-dimensional space [1], where the two-dimensional plaintext was considered as a series of particles distributed in 3D space, and an iterative phase retrieval algorithm was developed to encrypt the series of particles into phase-only masks. Later, they proposed a new optical image encryption method based on multiple-region plaintext and phase retrieval in 3D space [2], where the plaintext was divided into multiple regions and each region was encrypted into one phase-only mask based on phase retrieval in 3D space. An optical image encryption based on coherent diffractive imaging using multiple wavelengths was proposed [3], where the coherent diffractive imaging with multiple wavelengths was applied into optical image encryption. He et al. analyzed the collision property of the optical image encryption technique based on interference [4] and found that various distinct pairs of phase-only masks yielded almost the same outputs by use of a modified phase retrieval algorithm. A multiple-image encryption scheme was proposed based on the phase retrieval process and phase mask multiplexing in the fractional Fourier transform domain by Sui [5], where each original image was encoded into a phase-only function by using the proposed phase retrieval process and all the obtained phase functions were modulated into an interim, which was encrypted into the final ciphertext by using the fractional Fourier transform. Lu presented a novel method for optical image encryption based on a modified radial shearing interferometer [6], where the plaintext image was first encoded into a phase-only mask and then modulated by a random phase mask; the result was regarded as the input of the radial shearing interferometer and was divided into two coherent lights, which interfered with each other, leading to an interferogram. An optical authentication technique based on interference image hiding system and phase-only correlation was proposed by Yuan [7], where some predefined complex images with different amplitudes and the same phase were respectively encoded into two phase-only masks according to the interference principle. Their proposed technique can easily generate different verification keys for different users, so it brought convenience for multi-user application. A flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique was proposed [8], where images were transformed by log-polar transform and compounded, and then encrypted by double random phase encoding. A color image encryption algorithm was designed with the affine transform in the gyrator transform domains [9], where the RGB components of the color image were converted into the real part and the imaginary part of a complex function by employing the affine transform and

* Corresponding author at: Department of Electronic Information Engineering, Nanchang University, No. 999, Xuefu Avenue, Honggutan Xinqu, Nanchang 330031, China. Tel.: +86 791 83969670.
E-mail address: nrzhou@ncu.edu.cn (N. Zhou).

http://dx.doi.org/10.1016/j.optlastec.2014.02.015
0030-3992/

subsequently the complex function was encoded and transformed in the gyrator domain. And Liu et al. proposed a double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains, where the random pixel exchanging (RPE) was introduced [10].

Compressive sensing (CS) [11,12] is a newly sampling–reconstruction technique which can complete the sampling and compressing simultaneously. Some researchers investigated the security of image encryption algorithms with CS. Rachlin and Baron investigated the security when eavesdroppers had no idea of the measurement matrix and demonstrated a computational notion of secrecy [13]. Orsdemir and Altun examined the security and robustness of a compressive sensing based encryption algorithm and indicated that the CS based encryption is computationally secure [14]. Abdulghani and Rodriguze-Villegas showed the additional benefits of compressive sensing in preserving data privacy and indicated that the inherent multidimensional projection perturbation feature made it hard to breach the privacy [15]. And several image encryption algorithms based on CS have been proposed. For example, compressive sensing was introduced in an image encryption method based on double random-phase encoding [16] to lower the encryption data volume due to the dimensional decrease properties of CS [17]. Based on the method in [17], the Arnold transforming was introduced later to enhance the security [18]. Huang and Sakurai divided the original image to blocks and vectorized each block to one-dimensional vectors, and then encrypted and compressed these vectors with CS and block Arnold scrambling [19]. Zhang and Ren proposed a scheme of compressing and decompressing encrypted image based on CS where the original image was encrypted by a secret orthogonal transform and then compressed by CS with a pseudo-random measurement matrix, and stated that the smoother the original image, the better the quality of the reconstructed image [20]. To overcome the problem that the measurement data from linear dimension reduction projection directly serving as the encrypted image failed to resist against the chosen-plaintext attack [21], Huang et al. proposed a parallel image encryption method based on CS, where block cipher structure consisting of scrambling, mixing, S-box and chaotic lattice XOR is designed to further encrypt the quantized measurement data [22]. Sreedhanya and Soman employed both compressive sensing and Arnold scrambling to encrypt color image [23]. Athira et al. proposed a novel image encryption algorithm based on CS, which generates the key by linear feedback shift register [24].

While all the above CS-based encryption algorithms adopted the whole measurement matrix as key, which renders the key too large to distribute and memorize. The compression and the encryption in some schemes cannot perform simultaneously. To overcome these shortcomings, we explore a new hybrid compression–encryption algorithm where the measurement matrix is controlled by keys and constructed as a circulant matrix. The plain image is divided into 4 blocks to compress and encrypt, and then the 4 compressed and encrypted blocks are scrambled by random pixel exchanging with the random matrices.

The outline of this paper is as follows: some fundamental knowledge is introduced in Section 2, the proposed algorithm is described in Section 3, experimental results and discussion are given in Section 4, and a brief conclusion is arrived at in Section 5.

2. Fundamental knowledge

2.1. Compressive sensing

The CS theory takes the space structure of signal in consideration and samples signal in the space domain. In this way, CS does not sample so many redundancy data. CS theory shows that a signal x with length N has the representation in the Ψ domain:

$$\alpha = \Psi^T x \tag{1}$$

Projecting α onto a measurement matrix Φ of size $M \times N$, one can obtain an $M \times 1$ vector y, where M is the number of measurements, and $M \ll N$, i.e.,

$$y = \Phi x = \Phi\Psi\alpha = \Theta\alpha, \tag{2}$$

where the sensor matrix Θ is the product of Φ and Ψ, which satisfies restricted isometry property (RIP) [11].

Definition of RIP: for each integer $k = 1, 2, \ldots$, define the isometry constant δ_k of a matrix Φ as the smallest number such that

$$(1-\delta_k)\|f\|_2^2 \le \|\Phi f\|_2^2 \le (1+\delta_k)\|f\|_2^2 \tag{3}$$

holds for all vectors $f \in R^n$.

It is clear that the substance of RIP is that matrix Θ satisfied RIP can keep the approximate Euclidean distance of k-sparse signal, which ensures the k-sparse signal is not in the null space of Θ so that it is possible to reconstruct the signal.

It is required to estimate the sparest solution to $y = \Theta\alpha$ to recover the signal x. The problem of estimating the sparse solution can be expressed as

$$\min \|\alpha\|_0 \ \text{ subject to } \ y = \Theta\alpha. \tag{4}$$

The above problem may be solved by exhaustive combinatorial search. But it will become an NP-hard problem [25] for large N. To overcome this problem, some reconstruction algorithms such as matching pursuit (MP) [26], orthogonal matching pursuit (OMP) [27] and smooth l^0 algorithm (SL_0) [28] and so on, have been developed. SL_0 is adopted in our proposed algorithm.

2.2. Random pixel exchanging

The random pixel exchanging process is shown in Fig. 1 [10]. I_1 and I_2 are two matrices. The variables m and n are the indices of the matrices. R is a random matrix whose elements are all limited in the interval [0, 1]. The symbol $\rightleftharpoons$ is defined to swap the pixels at the left side and the right one. I_1' and I_2' are the outputs of the pixel exchanging operation. The new position (m', n') is computed as [10]

$$\begin{cases} m' = f_1(m,n) = 1 + \text{round}\,\{(M-1)\sin\,[\pi R(m,n)]\} \\ n' = f_2(m,n) = 1 + \text{round}\,[(N-1)R(m,n)] \end{cases}, \quad 1 \le m \le M, \quad 1 \le n \le N \tag{5}$$

where M and N are the sizes of the random matrix R. The matrices I_1 and I_2 have $M \times N$ pixels. The round function is toward nearest integer for input number. The mean value $\bar{R}$ of random matrix R

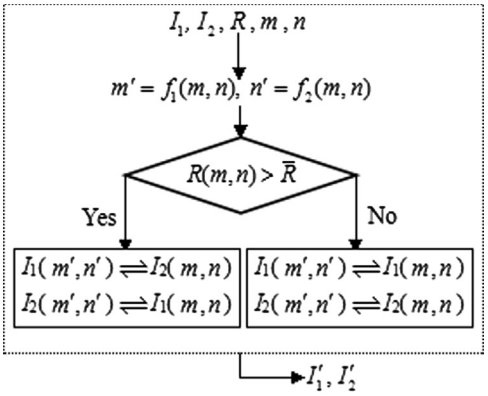

Fig. 1. The random pixel exchanging.