Optics Communications 392 (2017) 223–233

Contents lists available at ScienceDirect

Optics Communications

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

A novel image compression–encryption hybrid algorithm based on the analysis sparse representation

Ye Zhang, Biao Xu, Nanrun Zhou*

Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

ARTICLE INFO

MSC:
00-01
99-00

Keywords:
Analysis sparse representation
Image encryption
Image compression
Compressive sensing

ABSTRACT

Recent advances on the compressive sensing theory were invoked for image compression–encryption based on the synthesis sparse model. In this paper we concentrate on an alternative sparse representation model, i.e., the analysis sparse model, to propose a novel image compression–encryption hybrid algorithm. The analysis sparse representation of the original image is obtained with an overcomplete fixed dictionary that the order of the dictionary atoms is scrambled, and the sparse representation can be considered as an encrypted version of the image. Moreover, the sparse representation is compressed to reduce its dimension and re-encrypted by the compressive sensing simultaneously. To enhance the security of the algorithm, a pixel-scrambling method is employed to re-encrypt the measurements of the compressive sensing. Various simulation results verify that the proposed image compression–encryption hybrid algorithm could provide a considerable compression performance with a good security.

1. Introduction

Image encryption is a subject of considerable research since it attempts to ensure the image security during transmission or storage. Generally, the image encryption algorithms are based on the permutation and diffusion of the image pixels [1–6]. A fast image encryption and authentication scheme was proposed by introducing a keyed Hash function [1], where the Hash value was the key for the encryption/decryption and also used to authenticate the decrypted image. Wang et al. proposed an image encryption algorithm by performing the permutation and diffusion of the image pixels simultaneously [2], where the original image was partitioned into some small blocks, and then a spatiotemporal chaos system was employed to shuffle and diffuse the blocks. An image encryption algorithm based on the chaos theory was introduced [3], where a pseudorandom sequence generated from a group of one dimensional chaotic maps was used to shuffle the positions and change the values of the image pixels simultaneously. A single round permutation-diffusion chaotic cipher for gray image encryption scheme was presented [4], in which some temp-value feedback mechanisms are introduced to resist the known attacks. A double image encryption scheme using discrete Chirikov standard map and chaos-based discrete fractional random transform was proposed [5], where two images scrambled by the discrete version of Chirikov standard map were regarded as the amplitude and phase of a synthesized signal, and then the double random phase encoding technology was utilized to encrypt the signal. In [6], the author presented some properties of Fridrich's chaotic image encryption scheme and provided some bases for further optimizing attack on Fridrich's scheme and its variants.

Recently, compressive sensing (CS) theory has been introduced into the image encryption scheme to realize the image compression and encryption simultaneously [7]. And most of the CS-based encryption methods combine the CS with other encryption techniques to enhance the security of the methods. Endra et al. proposed an image compression–encryption method based on the CS [8], in which they employed the modified closed-ETF (Equiangular Tight Frame) to optimize the measurement matrix of the CS and utilized the CS to compress and encrypt the original image simultaneously. Huang et al. proposed a compression-combined digital image encryption method based on the CS and block Arnold scrambling [9], which is robust against consecutive packet loss and malicious shear attack. Athira et al. proposed an image encryption scheme [10], where the original image was first divided into some small blocks and then the measurement matrix corresponding to each block was shuffled based on the different keys generated by the linear feedback shift register (LFSR), and the scheme has a high resistance to the known plaintext attack. An image encryption method was proposed combining the CS with the Arnold transform and double random phase encoding [11], where the Arnold transform was used to scramble the pixel's positions of the image encrypted with the CS, and then the scrambled image was re-encrypted

* Corresponding author.
E-mail addresses: zhangye@ncu.edu.cn (Y. Zhang), biaoxu1992@163.com (B. Xu), nrzhou@ncu.edu.cn (N. Zhou).

http://dx.doi.org/10.1016/j.optcom.2017.01.061
Received 19 December 2016; Received in revised form 30 January 2017; Accepted 31 January 2017

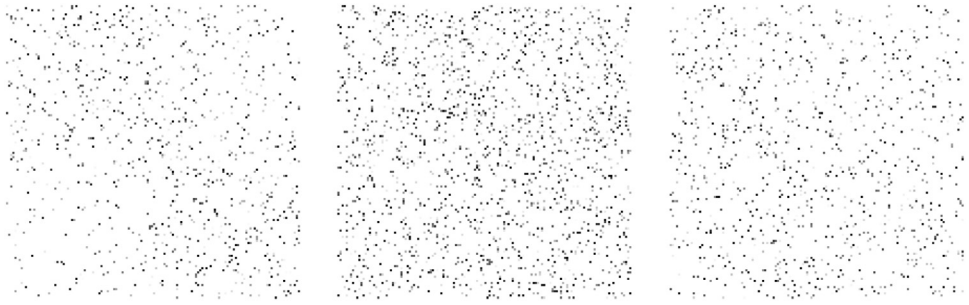

Fig. 1. The magnitude spectrums: (a) “Lena”; (b) “House”; and (c) “Peppers”.

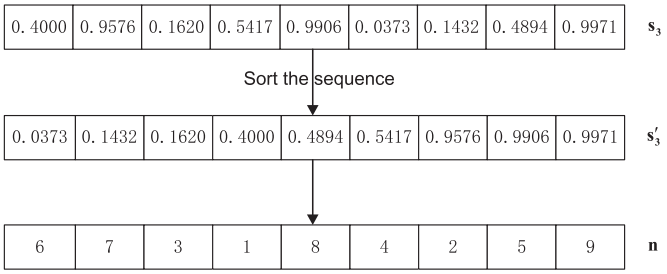

Fig. 2. An example for the generation of index sequence **n**.

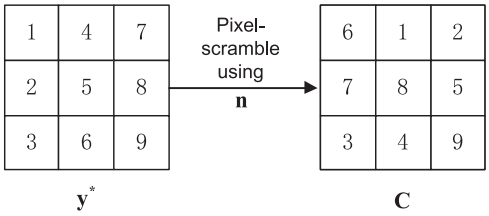

Fig. 3. An example for the pixel-scrambling method.

with the double random phase encoding technology. Rawat et al. presented a robust FrFT-based double random phase encryption scheme [12], where the CS was employed to simultaneously encrypt two multispectral images scrambled by the Arnold transform. A scheme of compressing and decompressing encrypted image based on the CS was presented [13], where the original image was encrypted with a secret orthogonal transform and then compressed by the CS with a pseudo-random measurement matrix. In the CS-based image encryption algorithms mentioned above, the measurement matrix was the key, generally, it was too large to transmit and store. To resolve the problem, some researchers proposed that the measurement matrix could be generated by a chaotic system since it is sensitive to its initial values, then the initial values of the chaotic system can be treated as the keys [14–18]. An image compression–encryption algorithm based on the CS and multichaotic system was proposed [14], where the measurement matrix of the CS was generated by the multichaotic system. Liu et al. proposed an image encryption algorithm based on the CS and the chaos system in the fractional Fourier transform (FrFT) domain [15], where the original image was first measured with a pseudo-random measurement matrix generated by a chaotic map and then the measurement data were re-encrypted with a chaotic-based double-random-phase encoding technology. An image compression–encryption scheme based on the 2D CS and discrete fractional random transform was presented [16], where the original image was represented in a 2D discrete cosine domain and measured by the measurement matrices which were constructed with the logistic map, and then the measurement data were re-encrypted by taking discrete fractional random transform. An image compression–encryption scheme based on the elementary cellular automata (ECA) and the Kronecker CS was proposed by Chen et al. [17], in which the ECA was utilized to scramble the sparsely transformed image and then the Kronecker CS was adopted to compress and encrypt the scrambled image, and the measurement matrix of the Kronecker CS was constructed with a piece-wise linear chaotic map. Zhou et al. proposed a hybrid image compression–encryption algorithm based on the CS, where the measurement matrix of the CS was constructed with a partial Hadamard matrix that was controlled by the chaotic map [18]. Subsequently, they proposed an image compression–encryption scheme by combining the 2D CS with nonlinear fractional Mellin transform, where the measurement matrix was constructed with logistic map [19]. Different from using the chaotic system to generate the measurement matrix, George et al. presented an approach to generate a random measurement matrix for the CS based on the LFSR [20], where the initial value of the LFSR system was the key. Sreedhanya et al. proposed a color image encryption scheme based on the CS and Arnold transform [21], in which the original image was first converted into three components, i.e., red, green and blue, and each of these components was encrypted and compressed with a random measurement matrix which was generated using a secret key, and then the measurement data of each component were scrambled by the Arnold transform. Recently, Zhang et al. discussed the theoretical security and the application security of the CS in the field of the information security [22].

However, these CS-based image encryption methods are based on the synthesis sparse model. In the synthesis model, a signal $\mathbf{x} \in R^{M\times 1}$ is represented as a linear combination of a few atoms (i.e., columns) from an overcomplete dictionary $\mathbf{D} \in R^{M\times N}(N \geq M)$, i.e., $\mathbf{x} = \mathbf{Da}$, where $\mathbf{a} \in R^{N\times 1}$ is the sparse coefficient, i.e., $\| \mathbf{a} \|_0 = L \ll N$, the l_0 quasi-norm $\|\cdot\|_0$ counts the number of nonzero components in its argument. In general, the dictionary could be obtained by using some dictionary learning algorithms, such as the greedy adaptive dictionary (GAD) algorithm, the K-SVD algorithm, or by a fixed dictionary, such as the DCT dictionary and the wavelet dictionary. In the past decade, the synthesis model has been extensively studied. However, as an alternative model of the sparse representation for signals, the analysis sparse model began to gain attention in recent years, and it was applied to image denoising [23] and blind source separation [24].

On the base of the analysis sparse model, we present a novel image compression–encryption hybrid algorithm. In the algorithm, the analysis sparse representation of an image could be obtained with an overcomplete fixed dictionary, such as the DCT dictionary, the wavelet dictionary, and the order of the atoms in the fixed dictionary is scrambled by the logistic map. Then the sparse representation can be considered as an encrypted representation of the image, and it is impossible to recover the image if the fixed dictionary is unknown. Moreover, we introduce the CS to re-encrypt the sparse representation and reduce its dimension simultaneously, where the measurement matrix of the CS is adopted as a circulant matrix and its first row is generated by the logistic map. To enhance the security, a pixel-scrambling method controlled by the logistic map is employed. Numerical experiments show that the proposed image compression–