Optik 125 (2014) 5075–5080

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Novel hybrid image compression–encryption algorithm based on compressive sensing

Nanrun Zhou[a,b,c,*], Aidi Zhang[a,b], Jianhua Wu[a], Dongju Pei[d], Yixian Yang[c]

[a] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
[b] Jiangxi Province Key Laboratory of Image Processing and Pattern Recognition, Nanchang Hangkong University, Nanchang 330063, China
[c] Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
[d] School of Computer and Information Engineering, Jiangxi Agricultural University, Nanchang 330045, China

ARTICLE INFO

Article history:
Received 30 September 2013
Accepted 10 April 2014

Keywords:
Compressive sensing
Image encryption
Image compression

ABSTRACT

A new hybrid image compression–encryption algorithm based on compressive sensing is proposed, which can accomplish image encryption and compression simultaneously. The partial Hadamard matrix is adopted as measurement matrix, which is controlled by chaos map. The measurement is scrambled. Compared with the methods adopting the Gaussian random matrix as measurement matrix, and those using the whole measurement matrix as key, the proposed algorithm reduces the burden of transferring key and is more practical. The proposed algorithm with sensitive keys and nice image compression ability can resist various attacks. Simulation results verify the validity and reliability of the proposed algorithm.

1. Introduction

Recently, a new theory, compressive sensing (CS) [1,2] was proposed. Compressive sensing jumps out of the framework of the traditional approach to sampling signals since it samples signals in space domain. Compared with the traditional way, CS can complete the sampling and compressing simultaneously. Since the advantage of CS, it is considered that whether CS can be introduced into the image encryption algorithm. Abdulghani and Rodriguze-Villegas [3] covered the secrecy properties of compressive sensing for noisy data and indicated that the inherent multidimensional projection perturbation feature made it hard to breach the privacy. Orsdemir et al. [4] examined the security and robustness of a compressive sensing based encryption algorithm and indicated that the CS based encryption is computationally secure. Rachlin and Baron [5] investigated the security when eavesdroppers had no idea of the measurement matrix and demonstrated a computational notion of secrecy. Drori [6] stated that the encryption matrix in compressive sensing based algorithms can be viewed as a one-time pad which is completely secure.

Since the potential capability of measurement matrix in CS to provide a certain level of security in the compressed data, some image encryption algorithms have been proposed. For example, compressive sensing was introduced in an image encryption method based on double random-phase encoding [7] to lower the encryption data volume due to the dimensional decrease properties of CS [8]. Huang and Sakurai [9] divided the original image to blocks and vectorized each block to a one-dimensional vector, and then encrypted and compressed these vectors with CS and block Arnold scrambling. Zhang et al. [10] proposed a scheme of compressing and decompressing encrypted image based on CS and stated that the smoother the original image, the better quality of reconstructed image, where the original image was encrypted by a secret orthogonal transform and then compressed by CS with a pseudo-random measurement matrix. To overcome the problem that the measurement data from linear dimension reduction projection directly serve as the encrypted image failed to resist against the chosen-plaintext attack [11], Huang et al. [12] 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. Sreedhanya and Soman [13] proposed a scheme where both compressive sensing and Arnold scrambling are employed to encrypt color image.

While all the above algorithms are not so practical since the Gaussian random matrix itself was adopted as measurement matrix. And the whole measurement matrix was treated as key in some encryption algorithms, which renders the key too large to distribute, store and memorize. The compression and the encryption

* Corresponding author at: Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China.
E-mail addresses: znr21@163.com, nrzhou@ncu.edu.cn (N. Zhou).

http://dx.doi.org/10.1016/j.ijleo.2014.06.054
0030-4026/

in some schemes cannot be performed simultaneously. Even some of them cannot resist the chosen-plaintext attack. To overcome these shortcomings, we firstly have devised a novel image compression–encryption hybrid algorithm with key-controlled measurement matrix in compressive sensing to realize compression and encryption simultaneously in a compact manner [14] and in this paper we will explore a new hybrid compression–encryption algorithm where the measurement matrix is controlled by keys and constructed as partial Hadamard matrix and the measurement is scrambled by chaos index sequence.

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

2. Fundamental knowledge

2.1. Compressive sensing (CS)

CS is a novel sample theory, which can reconstruct original signal by directly sampling a sparse or compressible signal at a rate much lower than the Nyquist rate. For a 1-D signal x with length N, its transform coefficient α is:

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

where ψ is an orthogonal basis or an over-complete dictionary. In a general case, most coefficients of α are close to zero and just a few large coefficients capture the principal information of the signal. Projecting x onto a measurement matrix Φ with size $M \times N$, one can get an $M \times 1$ vector y, 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) [15], Φ is incoherent with basis matrix Ψ, M is the number of measurements, and $M \ll N$. The measurement process is not adaptive, since Φ is fixed and does not depend on the signal x.

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

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

holds for all vectors $f \in R^n$. One can see that the substance of RIP is that matrix Θ satisfied RIP can keep the approximate Euclidean distance of sparse signal, which ensures the sparse signal is not in the null space of Θ so it is possible to reconstruct the signal.

To recover the signal x from y, it is required to estimate the sparest solution to $y = \Theta\alpha$, i.e.,

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

Solving the above problem by exhaustive combinatorial search is an NP-hard problem [16] for large N. To overcome this problem, some reconstruction algorithms have been developed, such as smoothed l^0 (SL_0) [17], matching pursuit (MP) [18], orthogonal matching pursuit (OMP) [19] and so on. SL_0 algorithm is adopted in our proposed algorithm.

2.2. Logistic map

Since chaos system is sensitive to the initial condition and has pseudo-randomness property, it is often used in cryptography. The definition of logistic map is:

$$x_{n+1} = \mu x_n(1-x_n), \quad x_n \in (0,1). \tag{5}$$

When $\mu \in [3.57, 4]$, it becomes chaotic.

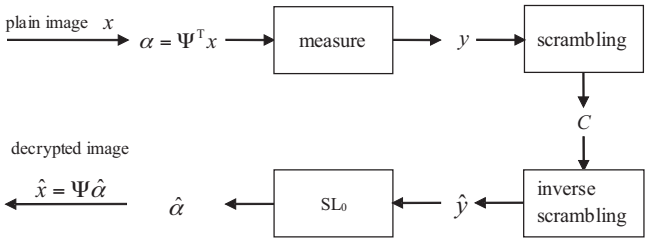

Fig. 1. The proposed image encryption algorithm.

3. The image encryption–compression algorithm based on CS

The proposed image encryption–compression algorithm is illustrated in Fig. 1, and the image encryption–compression steps are as follows:

Step 1: Extend x in Ψ domain to obtain α;

Step 2: Construct the measurement matrix Φ and measure α to obtain y. To enhance the security, α but not x is measured by Φ, i.e.,

$$\begin{aligned} y &= \Phi\alpha \\ &= \Phi\Psi^{\mathrm{T}} x \end{aligned} \tag{6}$$

It is equivalent to presume that $\Phi\Psi^{\mathrm{T}}$ is the measurement matrix, and the sensor matrix $\Theta = \Phi$. Thus the attacker not only needs Φ, but also needs Ψ, or else he cannot reconstruct x even if α is available;

Step 3: Scramble the measurement y: generate an index sequence t with length $M \times N$ by logistic map with initial condition r_1, sort y with the index sequence t to obtain the encrypted image C. It is easy to find that the attacker can obtain the measurement matrix without keys by setting $\alpha = \mathbf{I}_{N\times N}$, where $\mathbf{I}_{N\times N}$ is the $N \times N$ unit matrix. That is to say, the method which treats the measurement as the encrypted image cannot resist the chosen plaintext attack. And since the image is encrypted as

$$\begin{aligned} y &= \Phi\alpha \\ &= \Phi[\alpha_1, \alpha_2, \ldots, \alpha_N] \\ &= [y_1, y_2, \ldots, y_N] \end{aligned} \tag{7}$$

when the encrypted image suffers the occlusion attack, the more data losing on the vertical direction, the more distortion. To resist the chosen plaintext attack and improve the performance of resisting occlusion attack, the chaos sequence is introduced to scramble y.

Perform the inverse scrambling operation on the encrypted image to obtain $\hat{y}$, and then one can obtain the decrypted image with the SL_0 algorithm.

For practice, the measurement matrix Φ is constructed as partial Hadamard matrix. The steps are as follows:

Step 1: Generate a sequence with length $2N$ by logistic map with initial condition r_2, abandon the preceding N elements to obtain the index sequence $s = [s_1, s_2, \ldots, s_N]$;

Step 2: Sort the nature sequence $n = [1, 2, \ldots, N]$ with the index sequence s, note the sorted sequence as $p = [p_1, p_2, \ldots, p_N]$, where $p_i \in [1, N]$ and $i \in [1, N]$;

Step 3: Generate the Hadamard matrix H of order N, and choose the row vectors, $H(p_1, :)$, $H(p_2, :)$, …, $H(p_M, :)$, to group into the measurement matrix Φ, i.e.,

$$\Phi = \begin{bmatrix} H(p_1,:) \\ H(p_2,:) \\ \vdots \\ H(p_M,:) \end{bmatrix}, \tag{8}$$