Optics & Laser Technology 91 (2017) 212–225

Contents lists available at ScienceDirect

Optics & Laser Technology

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

Full length article

# Multi-focus image fusion and robust encryption algorithm based on compressive sensing

Di Xiao[a,*], Lan Wang[a], Tao Xiang[a], Yong Wang[b]

[a] Key Laboratory of Dependable Service Computing in Cyber Physical Society of Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, China
[b] Key Laboratory of Electronic Commerce and Logistics of Chongqing, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

ARTICLE INFO

*Keywords:*
Image encryption
Image fusion
Compressive sensing
Robust

ABSTRACT

Multi-focus image fusion schemes have been studied in recent years. However, little work has been done in multi-focus image transmission security. This paper proposes a scheme that can reduce data transmission volume and resist various attacks. First, multi-focus image fusion based on wavelet decomposition can generate complete scene images and optimize the perception of the human eye. The fused images are sparsely represented with DCT and sampled with structurally random matrix (SRM), which reduces the data volume and realizes the initial encryption. Then the obtained measurements are further encrypted to resist noise and crop attack through combining permutation and diffusion stages. At the receiver, the cipher images can be jointly decrypted and reconstructed. Simulation results demonstrate the security and robustness of the proposed scheme.

## 1. Introduction

Nowadays, multimedia sensor networks have wide application prospects in the fields such as military affairs and environment monitor. The sensors are actually cameras that record still image or video. Due to the fact that the commonly used optical lenses suffer from a problem of limited field depth, it is often impossible to get an image that contains all relevant objects in focus and we call these images multi-focus image. Image fusion can merge the different information taken from the same scene with different focuses to obtain a new and improved image [1]. Multi-focus image fusion has been widely used in various fields, such as computer vision and remote sensing.

Currently, the existing multi-focus image fusion methods are mainly based on spatial domain [2], transform domain [3] and compressive sensing (CS) [4–7]. However, these image fusion methods focus on how to integrate multi-focus images into a single visual enhanced image, and do not care about secure transmission and robustness. During image transmission over unreliable wireless channels, packets loss or malicious attack is inevitable [8]. Generally, the confidentiality is protected with encryption methods. However, conventional encryption algorithms are not suitable for image when considering their costs and traffic load [9]. Since images are often sparse or compressible while CS can enable sub-Nyquist sampling and low-energy data reduction, it is promising to utilize CS to fill in the gap.

In the related field of image encryption based on CS, several works have been proposed. Liu et al. [8] proposed the image encryption scheme based on CS theory with robustness to packet loss. Huang et al. [10] proposed a compression-combined digital image encryption method which is robust against consecutive packet loss and malicious crop attack. Subsequently, a robust still-image transmission coding scheme based on CS is presented in [11]. A robust coder, based on CS with structurally random matrix (SRM), for encrypted images over packet transmission networks is proposed in [12]. A simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos can be found in [13]. But in the experiment result of the method, the correlation and histograms distributions of the encrypted images are not uniform which implies the scheme is not very secure and valid in some extent. Since good fusion performance, transmission security and robustness are not always considered or valid, the aforementioned approaches are not suitable for fusion and robust encryption of multi-focus images.

In this paper, a multi-focus image fusion and robust encryption scheme based on CS is presented to ensure the efficiency and security of image transmission. In this scheme, the source images are firstly fused based on wavelet decomposition and then the fused image is sparsely represented with discrete cosine transform (DCT). The obtained coefficients are measured with a structurally random measurement matrix (SRM) [14] and finally ciphertext can be obtained by

* Corresponding author.
*E-mail address:* dixiao@cqu.edu.cn (D. Xiao).

http://dx.doi.org/10.1016/j.optlastec.2016.12.024
Received 26 August 2016; Received in revised form 11 November 2016; Accepted 20 December 2016

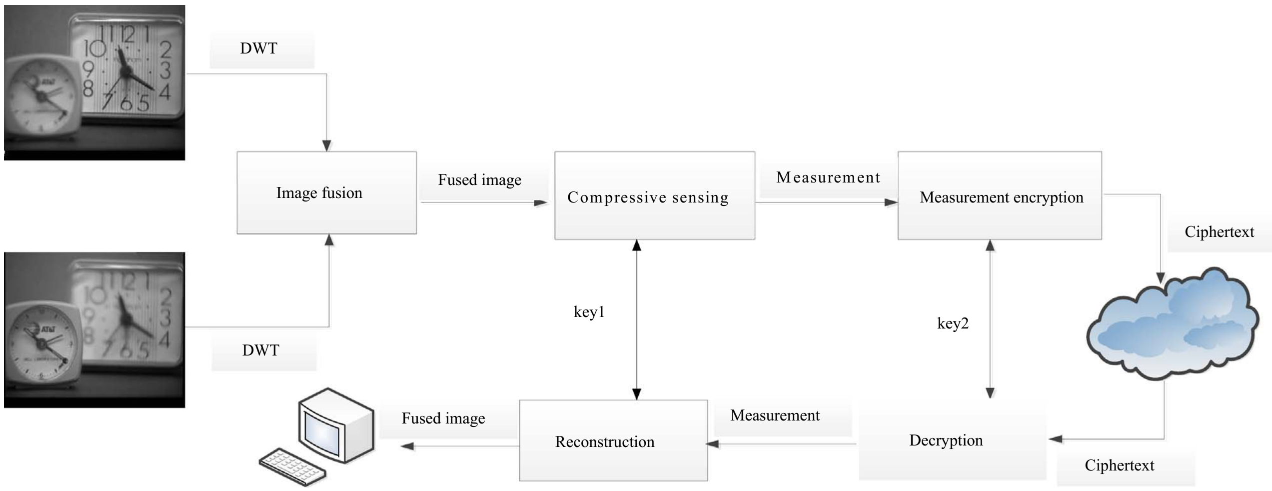


**Fig. 1.** The flowchart of the proposed main steps.

encrypting the integer of measurement with the combined scrambling and diffusion stages. At the receiver, the fused image can be reconstructed by decrypting the cipher image and using a recovery algorithm. The analyses and the numerical experiments are given to illustrate its fusion performance, security and robustness.

The rest of this paper is organized as follows. Section 2 is a brief review of the theory of CS and Logistic map. Section 3 proposes the image fusion based on wavelet decomposition and the robust encryption based on CS with SRM. In Section 4, the numerical experiments and analyses can be found. Finally, we conclude the paper in Section 5.

## 2. Preliminaries

In this section, we show the basic background, primarily on the theory of CS and Logistic map.

### 2.1. Compressive sensing

The fundamental Shannon/Nyquist sampling theory is widely accepted as the keystone in signal acquisition and reconstruction. Nevertheless, the number of required measurements can be so large that the storage becomes unbearable and the acquisition time can be very long sometimes. Compressive sensing (CS) in [15], as an emerging and fascinating field, shows that K-sparse signals or images can be recovered exactly from M measurements far fewer than N samples what are considered being necessary in Nyquist theorem, i.e., $M \ll N$. CS combines the traditional sampling and compressing process into a single non-adaptive linear measurement process by exploiting the data sparsity.

Many signals acquired from the physical world are sparse or compressible in the sense that when expressed in the proper orthonormal basis (such as a standard or wavelet basis), their coefficient entries decay rapidly. A signal $x \in R^N$ of length N is said to be K-sparse or compressible if it can be well approximated using only $K \ll N$ coefficients over some sparse basis φ as follows:

$$x = \varphi s \tag{1}$$

where s is the transform coefficient vector that contains at most K significant nonzero entries. For images, typical choices of φ can consider the widely used discrete Fourier transform (DFT), discrete cosine transform (DCT), or discrete wavelet transform (DWT) matrix, etc. If φ satisfies RIP (Restricted Isometry Property), we can reconstruct signal by solving the optimization problem below [16].

$$\min \|s\|_1 \; s.\,t.\; x = \varphi s \tag{2}$$

This is equivalent to find the sparsest solutions to $x = \varphi s$, provided $M \geq CK \log N/K$, where C is a small constant. Compressive sensing theory indicates that x can be acquired by the following random measurement matrix $\varnothing \in R^{M\times N}(M \ll N)$, i.e.,

$$y = \Phi x = \Phi\varphi s \tag{3}$$

where y is a sampled vector, and Φ is a $M \times N$ measurement matrix that is incoherent with the sparse basis φ, i.e., the maximum magnitude of the element in Φφ is small. Then x can be faithfully recovered from only $M=O(K \log N)$ measurements through $l_1$-minimization:

$$\min \|s\|_1 \; s.\,t.\; y = \Phi\varphi s \tag{4}$$

Eq. (4) presents an $l_1$ -minimization problem which can be solved by orthogonal matching pursuit algorithm [17].

### 2.2. Logistic map

Logistic map is usually used to generate pseudo-random sequences. Logistic map is defined as:

$$x_{n+1}=\mu x_n(1 - x_n) \tag{5}$$

The output sequence is chaotic if one chooses $\mu \in [3.57, \; 4]$, and μ is the control parameter. This chaos system is sensitive to the seed value $x_0$ and the generated sequence $x_n$ is distributed in the range of (0, 1). The initial value $x_0$ and control parameterμ can be combined as the secret key.

## 3. Proposed scheme

With the background knowledge presented in the previous section, the proposed image fusion and robust encryption algorithm based on CS is now described. All images considered in this paper are gray-scale images. The proposed algorithm is realized in the following main steps: (1) image fusion based on wavelet decomposition; (2) sparse representation of the fused images; (3) SRM measure; (4) measurement encryption; (5)the receiver decrypts the ciphertext; (6)reconstruct the fused image. The flowchart of the proposed main steps is illustrated in Fig. 1.

### 3.1. Image fusion based on wavelet decomposition

The key point in multi-focus image fusion is to decide which portions of each image are in better focus than their respective counterparts in the associated images and then combine these regions