Optics and Lasers in Engineering 102 (2018) 106–111

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

# Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme

Xianye Li [a], Xiangfeng Meng [a,*], Xiulun Yang [a], Yurong Wang [a], Yongkai Yin [a], Xiang Peng [b], Wenqi He [b], Guoyan Dong [c], Hongyi Chen [d]

[a] Department of Optics, School of Information Science and Engineering, and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Jinan 250100, China
[b] College of Optoelectronics Engineering, Shenzhen University, Shenzhen 518060, China
[c] College of Materials Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, China
[d] College of Electronic Science and Technology, Shenzhen University, Shenzhen 518060, China

ARTICLE INFO

*Keywords:*
Compressive ghost imaging
Lifting wavelet transform
XOR operation

ABSTRACT

A multiple-image encryption method via lifting wavelet transform (LWT) and XOR operation is proposed, which is based on a row scanning compressive ghost imaging scheme. In the encryption process, the scrambling operation is implemented for the sparse images transformed by LWT, then the XOR operation is performed on the scrambled images, and the resulting XOR images are compressed in the row scanning compressive ghost imaging, through which the ciphertext images can be detected by bucket detector arrays. During decryption, the participant who possesses his/her correct key-group, can successfully reconstruct the corresponding plaintext image by measurement key regeneration, compression algorithm reconstruction, XOR operation, sparse images recovery, and inverse LWT (iLWT). Theoretical analysis and numerical simulations validate the feasibility of the proposed method.



## 1. Introduction

In recent years, the development of cloud services and the Internet of things (IoT) has added convenience to much of our work and daily life, but these technologies have also exposed many data security problems. As a result, data protection such as encryption and signatures represent a significant portion of the research undertaken nowadays. As a branch of data security, optical information security has also been developing rapidly since double random phase encoding (DRPE) was proposed by Réfrégier and Javidi in 1995 [1]. Subsequently, the DRPE technique has been successfully combined with many classical optical transformations such as the fractional Fourier transformation [2,3], Fresnel transformation [4,5], gyrator transformation [6], fractional Mellin transformation [7], phase-shifting interferometry [8], joint transform correlator (JTC) [9], phase retrieval [10,11], diffractive imaging [12], and two beam interference [13], etc.

Ghost imaging, first proposed by Klyshko in 1988 [14], is imaging through total light intensity behind the object plane and light intensity distribution before the object plane, in which the total light intensity is detected by a single-photon detector (SPD), and the light intensity distribution before the object plane is gathered by a charge coupled device (CCD) in another reference arm. In 2009, Bromberg et al. proposed the concept of computational ghost imaging (CGI) with only a single pixel detector [15], where the light intensity distribution before the object plane could be calculated by the Fresnel transformation. However, the traditional ghost imaging algorithm, which uses a correlation operation always needs many detection times, even millions, to achieve a satisfactory result. To decrease the measurement times and promote the quality of the output images, Katz subsequently proposed a compressive ghost imaging (CSGI) scheme [16], which combines CGI with a compressive sensing (CS) algorithm [17,18]. In 2011, Duran proposed an optical encryption scheme using compressive ghost imaging [19]. In 2015, Zhao et al. proposed a high-performance optical encryption method based on computational ghost imaging with the QR code and a compressive sensing technique [20].

To improve encryption capacity, some researchers have focused on multiple-image encryption methods based on wavelength multiplexing [21], position multiplexing [22], space multiplexing [23], phase-only mask (POM) multiplexing [24,25], lateral shifting [26], etc. In 2016, Sui et al. proposed a multiple-image encryption method based on chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain [27], where the vortex beam could integrate more system parameters as additional keys into one phase mask. Qin et al.

* Corresponding author.
*E-mail address:* xfmeng@sdu.edu.cn (X. Meng).

https://doi.org/10.1016/j.optlaseng.2017.10.023
Received 3 August 2017; Received in revised form 26 October 2017; Accepted 27 October 2017
0143-8166/

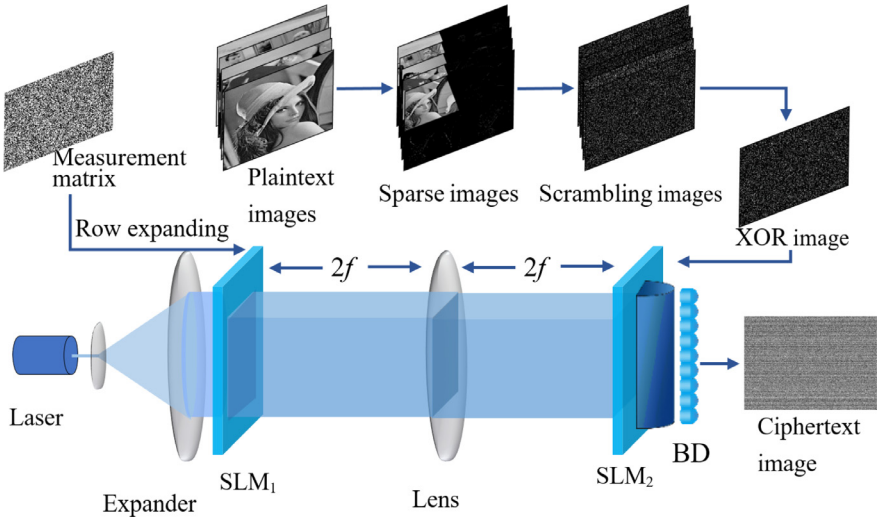


**Fig. 1.** A schematic diagram of the proposed multiple-image encryption and encoding scheme.

proposed a multiple-image encryption method in a diffractive-imaging-based scheme using spectral fusion and a nonlinear operation [28], in which the discrete cosine transformation (DCT) spectra of the primary images were extracted, compacted, nonlinear-transformed and then encoded into a single intensity pattern. In addition, multiple-image encryption methods based on ghost imaging have also been proposed by researchers [29–32]: In 2014, Chen et al. demonstrated that an object and multiple hidden marks can be simultaneously recovered using only one rebuilt reference intensity sequence in ghost imaging [29], and that multiple marks can be hidden using sparse reference intensity patterns. Subsequently, Chen et al. proposed a multiple-image authentication method via photon-synthesized ghost imaging using optical nonlinear correlation [30], in which multiple series of photons recorded at the object beam arm could be arbitrarily controlled for the generation of synthesized objects. In 2015, Liu et al. proposed a multiple-image encryption method based on computational ghost imaging and position multiplexing [31], where each plain image was encrypted into an intensity vector using computational ghost imaging with different diffraction distances. In 2016, we proposed a multiple-image encryption method based on a modified logistic map algorithm, compressive ghost imaging and coordinate sampling [32]. To realize the transform from integer to integer and allow the possibility of lossless coding, here we propose a multiple-image encryption method using the lifting wavelet transform (LWT) and XOR operation based on a compressive ghost imaging scheme, which can realize multiple-image encryption with lossless encoding and decoding. The principle and procedure will be described first, and then a set of simulations will be given to verify the feasibility and robustness of the scheme, and finally the conclusions are presented.

## 2. Theoretical analysis and description

### 2.1. Compressive sensing theory

Computational ghost imaging using compressive sensing algorithm can obviously decrease measurement times and improve the reconstruction result. In compressive sensing theory [33–35], any image, which is sparse or can be sparse in some transform domain such as the discrete cosine transformation (DCT) and discrete wavelet transform (DWT), can be compressed by a measurement matrix Φ, such as a Gaussian distribution matrix or Hadamard matrix, etc., which is selected randomly. This compression procedure can be denoted as:

$$B = \Phi \times T, \tag{1}$$

where $T$ is the sparse image whose size is $N \times N$, and Φ is the measurement matrix with the size $M \times N$. Only $M$ satisfies the condition in Eq. (2), and it can achieve a high-quality reconstruction result,

$$M \geq c \times K \log\left(\frac{N}{K}\right), \tag{2}$$

where $c$ is a constant, $N$ is the number of total pixels in a row and $K$ expresses the maximum row sparsity of the scrambled certification image. Thus, an additional scrambling operation is necessary to create a uniform distribution. As for the reconstruction procedure, recovering the sparse image $T$ from the measurement matrix Φ and compressive result $B$ is a process for solving an ill-conditioned equation, and this is a convex optimization problem, which can be solved by:

$$\hat{T} = \arg\min \|T\|_{L1} \qquad s.t.\ B = \Phi \times T, \tag{3}$$

where $\|\bullet\|_{L1}$ means the $L_1$-norm. Many researchers have done considerable work on compressive sensing reconstruction algorithms, such as the orthogonal matching pursuit (OMP) [36], basic pursuit (BP) [37], and subspace pursuit (SP) [38], etc. In this work, we adopted a sparsity adaptive matching pursuit algorithm (SAMP) modified from the orthogonal matching pursuit algorithm to get a more accurate result [39].

### 2.2. Description of the proposed scheme

To an increasing extent, researchers have been applying compressive sensing in optical information encryption because of the virtue of its data compression and optical implementation. Yet, thousands of measurements are demanded in the encryption process using compressive sensing, and the reconstruction for plaintext also takes a long time. Thus, some researchers have proposed different kinds of schemes for encryption capacity enhancement [23,29,30,32]. In this work, based on a ghost imaging scheme, we propose a multiple-image encryption method for compressive sensing using LWT and XOR operations as shown in Fig. 1. The encryption process is shown in the following steps.

(a) **Sparsity operation with lifting wavelet transform**

Multiple plaintext images of size $N \times N$ are sparse throughout the LWT operation, which transforms the images into the wavelet domain with an integer distribution, where small coefficients in the wavelet domain will be set as zero to achieve a better reconstruction result. Compared to the first-generation discrete wavelet transform, LWT has much lower data loss when applied in image encoding. In addition, the integer data is the basis for bit manipulation such as XOR.