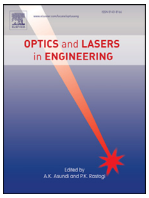
Optics and Lasers in Engineering 107 (2018) 258–264

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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



Hierarchical multiple-image encryption based on the cascaded interference structure and vector stochastic decomposition algorithm

Xue Zhang[a], Xiangfeng Meng[a,*], Yurong Wang[a], Xiulun Yang[a], Yongkai Yin[a], Xianye Li[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, 27 Shanda Nanlu, 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:
Image encryption
Digital image processing
Interference

ABSTRACT

A new kind of hierarchical multiple-image encryption method based on the cascaded interference structure and vector stochastic decomposition algorithm is proposed. In this method, by using the nonequal modulus decomposition and vector stochastic decomposition algorithm, the Kth-level secret image modulated by a random phase distribution is analytically encoded into a Kth-level phase-only mask (POM) key and the (K−1)th-level complex amplitude field whose real amplitude is the (K−1)th-level secret image. Then, served as the input condition, the generated complex amplitude field is further encoded into a (K−1)th-level POM key and the (K−2)th-level complex amplitude, and so on, until the 1st-level complex amplitude field is decomposed into two POMs: one is the 1st-level key, and the other is the ciphertext. When decryption occurs, only when the high-level users simultaneously obtain all the phase keys, the correct sequential orders of phase keys, and the correct geometrical parameters, all the secret images are retrieved successfully. Both theoretical analysis and numerical simulations verify the feasibility of this method.

1. Introduction

Since Réfrégier and Javidi proposed the double random phase encoding (DRPE) technique in 1995 [1], optical information security has received extensive attention due to the characteristics of high-speed parallel computing, multiple encoding dimensions, etc. Subsequently, the DRPE techniques in the fractional Fourier and Fresnel domains were put forward successively [2–6] and the techniques in other domains were also studied [7–13], in which the system parameters could serve as auxiliary keys to make the cryptosystem safer. Other various optical methods such as joint transform correlator [14], diffractive imaging [15], polarization encoding [16], jigsaw transform [17], aperture movement [18], phase reservation and compression [19], ghost imaging [20], photon-counting [21] etc., have also been employed for both encryption and watermarking, which ramped up the development of optical encoding in recent years.

Since Zhang and Wang proposed interference-based encryption [22], it has received tremendous attention, because the hidden image can be encrypted into two phase-only masks (POMs) without any time-wasting iterative algorithm, and the decryption could be carried out optically or digitally. Later, the optical experiment based on this technique was successfully carried out by Weng et al. [23]. However, the silhouette problem impeded the application of this technique. In 2009, Zhang et al. proposed a security-enhanced method [24] to remove the silhouette of the original image by randomly exchanging the subpart of two POMs, but the algorithm was complex and time-consuming. Recently, more and more researchers have devoted themselves to removing the silhouette, and many papers have been published. However, these modified methods either adopted the time-consuming iterative algorithm [25,26], or generated extra POM [27,28]. Recently, Kong et al. proposed a new vector stochastic decomposition algorithm [29], and from the decrypted results, we can see that the inherent silhouette problem has been well solved, which means that either POM fails to decrypt the silhouette of original image, but only when all the correct keys are gathered, the secret image could be recovered exactly and clearly.

To improve the encryption capacity, the multiple-image encryption schemes have also been studied for many years, which mainly utilize the methods such as wavelength multiplexing [30–33], position multiplexing [34,35], and phase multiplexing [36], etc. In 2010, by using a combination of interference principle and wavelength multiplexing, Niu et al. proposed a two-image encryption and verification method

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

https://doi.org/10.1016/j.optlaseng.2018.04.002
Received 1 February 2018; Received in revised form 2 April 2018; Accepted 2 April 2018
0143-8166/

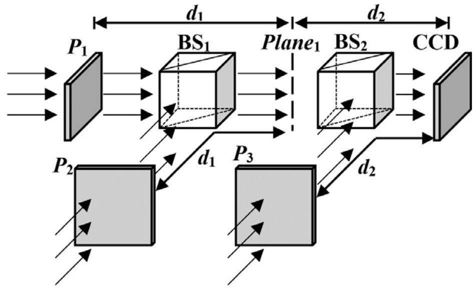


Fig. 1. Schematic of the two-level cascaded interference setup.

[37], in which two different images can be encoded into three diffractive phase elements by using two different incident wavelengths. Subsequently, Niu et al. proposed a two-image hiding method based on the interference principle and DRPE method [38], in which two encrypted images can be recovered by using the frequency spectrum center shift technique. In 2011, Chen and Chen realized multiple-image encryption based on the interference principle and multiplane phase retrieval [39], in which all plaintext images can be simultaneously encrypted into a single phase-only mask by multiplane phase retrieval and can be further noniteratively encrypted into two phase-only masks using interference principle. In 2013, Wang et al. proposed a multiple-image encryption based on interference principle and phase-only mask multiplexing in the Fresnel transform domain [40], in which each secret image is encoded into two analytically obtained POMs and one computer-generated random POM. Combined with the techniques of grating modulation and position multiplexing, He et al. completed a series of explorations in multiple-image encryption or authentication methods based on interference principle [41–43]. In the present paper, to encrypt images to POMs without time-consuming iteration, the interference-based method is considered. To achieve K images encryption, cascaded interference structure and nonequal modules decomposition are proposed and repeated K−1 times, and vector stochastic decomposition is then adopted one time. We first give the theoretical analysis, description, and procedure of the method, then provide its simulation verification, and finally draw the conclusion.

2. Theoretical analysis and description

2.1. Two-level image encryption and decryption

In Zhang's encryption scheme [22], two POMs are defined as

$$\mathrm{POM}_1 = \arg(D) - \arccos[\mathrm{abs}(D)/2], \tag{1}$$

$$\mathrm{POM}_2 = \arg[D - \exp(i\mathrm{POM}_1)] = \arg(D) + \arccos[\mathrm{abs}(D)/2], \tag{2}$$

where the operators arg( ), abs( ), and arccos( ) represent taking phase, modulus, and arccosine operation, respectively.

Vector stochastic decomposition algorithm [29] emphasizes that the angle assignment of POM_1 and POM_2 can be random, which can be written as

$$\mathrm{POM}_1 = \arg(D) - G \bullet \arccos[\mathrm{abs}(D)/2], \tag{3}$$

$$\mathrm{POM}_2 = \arg(D) + G \bullet \arccos[\mathrm{abs}(D)/2], \tag{4}$$

where, '$A \bullet B$' returns the Hadamard product of A and B, and

$$G(x, y) = \begin{cases} 1, rand(x, y) > t \\ -1, rand(x, y) \le t \end{cases}, \tag{5}$$

where *rand* is a random function distributed in the interval [0, 1].

To ensure readers understand our work, here, two-level cascaded interference structure is first introduced. As shown in Fig. 1, two coherent plane waves modulated by two POMs P_1 and P_2 are combined by beam split (BS_1), they are superposed coherently on each other resulting in a complex amplitude output at $Plane_1$. The complex amplitude continues to propagate forward. It encounters a coherent plane wave modulated by POM P_3, and the two diffractive fields are combined by BS_2. Thus, these two beams interfere with each other at the CCD plane, and a 2nd-level secret image is obtained. If a mask or a CCD is located at the $Plane_1$, 1st-level secret image can be obtained prior to the 2nd-level secret image. The distance between P_1 and $Plane_1$is d_1, which is the same as the distance between P_2 and $Plane_1$. The distance between $Plane_1$and CCD is d_2, which is also the same as the distance between P_3 and CCD.

In the two-level cascaded encryption frame, the key issue is to obtain three POMs P_1, P_2, and P_3. To achieve it, nonequal module decomposition proposed by us is first used: 2nd-level object function $\sqrt{f_2}\,\exp(iR)$ with random phase R can be expressed as the interference of P_3 and complex amplitude at $Plane_1$:

$$\mathrm{FrT}_{d_2}[\sqrt{f_1}\exp(iM_1)] + \mathrm{FrT}_{d_2}[\exp(iP_3)] = \sqrt{f_2}\exp(iR), \tag{6}$$

or

$$\sqrt{f_1}\exp(iM_1) + \exp(iP_3) = \mathrm{iFrT}_{d_2}[\sqrt{f_2}\exp(iR)] = D_2, \tag{7}$$

where f_1 and f_2 represent 1st-level and 2nd-level secret real-amplitude image, respectively. M_1, R, and P_3 uniformly distributed in the interval [0, 2π]. FrT_d and iFrT_d represent the Fresnel transform and inverse Fresnel transform of distance d, respectively. To make data effective, we first change the pixel values of f_1 into the interval (max $\{[1 - \mathrm{abs}(D_2)]^2\}$, min $\{[1 + \mathrm{abs}(D_2)]^2\}$), where 'max' and 'min' represent taking the maximal value and minimum value, respectively. As P_3 is a pure phase element, we have:

$$\begin{aligned} &\left|D_2 - \sqrt{f_1}\exp(iM_1)\right|^2 \\ &= [D_2 - \sqrt{f_1}\exp(iM_1)][D_2 - \sqrt{f_1}\exp(iM_1)]^* \\ &= 1, \end{aligned} \tag{8}$$

where, '*' and | • | express the complex conjugate and modulus extraction operation, respectively. Through mathematical deduction, and taking randomness into account, we get the M_1:

$$M_1 = \arg(D_2) + G \bullet \arccos(Q), \tag{9}$$

where, $Q = [\mathrm{abs}^2(D_2) + f_1 - 1]/[2\sqrt{f_1}\mathrm{abs}(D_2)]$ should be greater than or equal to −1, and less than or equal to 1, which is why the pixel values change operation needs to be done on f_1, so that P_3 will be obtained:

$$P_3 = \arg\left[D_2 - \sqrt{f_1}\exp(iM_1)\right] \tag{10}$$

Next, the vector stochastic decomposition algorithm is followed to generate P_1 and P_2. Because the complex amplitude at $Plane_1$ is the interferential result of P_1 and P_2, served as input condition, it can be expressed as

$$\exp(iP_1) + \exp(iP_2) = \mathrm{iFrT}_{d_1}[\sqrt{f_1}\exp(iM_1)] = D_1, \tag{11}$$

and P_2 can be written as

$$P_2 = \arg(D_1) + G \bullet \arccos[\mathrm{abs}(D_1)/2], \tag{12}$$

finally P_1 can be calculated out:

$$P_1 = \arg[D_1 - \exp(iP_2)]. \tag{13}$$

Eventually, two secret images are encrypted into three POMs. Like above, more secret images can be encoded, and the keys increase with the hidden images, but without the visibility of recovered images decreasing.

2.2. K-level image encryption and decryption

The above-mentioned method can easily extend to K-level encryption system, and nonequal decomposition is repeated K−1 times and followed once by vector stochastic decomposition. As shown in Fig. 2, a flow chart of the K-level image encryption scheme is clearly given.