Optics and Lasers in Engineering ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Hierarchical multilevel authentication system for multiple-image based on phase retrieval and basic vector operations

Xianye Li [a], Xiangfeng Meng [a,*], Yongkai Yin [a], Xiulun Yang [a], Yurong Wang [a], Xiang Peng [b], Wenqi He [b], Xuemei Pan [a], 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 Techology, University of Chinese Academy of Sciences, Beijing 100049, China
[d] College of Electronic Science and Technology, Shenzhen University, Shenzhen 518060, China

ARTICLE INFO

Article history:
Received 7 January 2016
Received in revised form
10 April 2016
Accepted 26 April 2016

Keywords:
Image authentication
Phase retrieval
Secret sharing
Vector decomposition and composition

ABSTRACT

A hierarchical multilevel authentication system for multiple-image based on phase retrieval and basic vector operations in the Fresnel domain is proposed, by which more certification images are iteratively encoded into multiple cascaded phase masks according to different hierarchical levels. Based on the secret sharing algorithm by basic vector decomposition and composition operations, the iterated phase distributions are split into n pairs of shadow images keys (SIKs), and then distributed to n different participants (the authenticators). During each level in the high authentication process, any 2 or more participants can be gathered to reconstruct the original meaningful certification images. While in the case of each level in the low authentication process, only one authenticator who possesses a correct pair of SIKs, will gain no significant information of certification image; however, it can result in a remarkable peak output in the nonlinear correlation coefficient of the recovered image and the standard certification image, which can successfully provide an additional authentication layer for the high-level authentication. Theoretical analysis and numerical simulations both verify the feasibility of the proposed method.

1. Introduction

In recent years, the optical information security (including optical image encryption, information hiding or watermarking, image or identity authentication, the cryptanalysis, etc.) has experienced a significant development, since Réfrégier and Javidi introduced the double random phase encoding (DRPE) technique in 1995 [1]. To build more versatile security systems, the DRPE technique has been combined with many optical information processing techniques or principles, such as fractional Fourier transform [2,3], digital holography [4,5], phase-shifting interferometry [6,7], gyrator transform [8], fractional Mellin transform [9], two beam interference [10,11], joint transform correlator [12], diffractive imaging [13], ghost imaging [14,15], aperture movement [16], sparse-phase multiplexing [17], etc.

In terms of information security, collision is a situation that occurs when two or more distinct inputs into a security system produce identical or undistinguishable outputs, which is undesirable in many security applications, especially concerning identity authentication, digital watermarking, and digital signature. Since Carnicer et al. revealed the weakness of DRPE to the chosen-ciphertext attack in 2005 [18], there have been several studies [19–21] pointing out that the DRPE-based encryption/authentication systems are not resistant to collision. In this sense, to eliminate the collision risk, recently, more encryption/authentication studies focused on phase retrieval algorithm. These methods were first proposed by Wang et al. [22] in 1996, in which a secret image was encoded into a random phase distribution at the Fourier plane relating to a fixed phase mask using a modified projection-onto-constraint-sets (POCS) algorithm. Li et al. demonstrated an optical security system based on iteratively retrieved phase encoding with POCS algorithm implemented in a joint transform correlator (JTC) [23]. Situ and Zhang reported two-phase-encoding-mask security methods with a 4-f setup where the phase distributions of both masks can be adjusted simultaneously in each iteration process [24,25], and this method is successfully extended to the Fresnel domain [26]. In 2012, Huang et al. proposed a lensless multiple-image optical encryption method based on the modified Gerchberg–Saxton algorithm (MGSA) by

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

http://dx.doi.org/10.1016/j.optlaseng.2016.04.021
0143-8166/

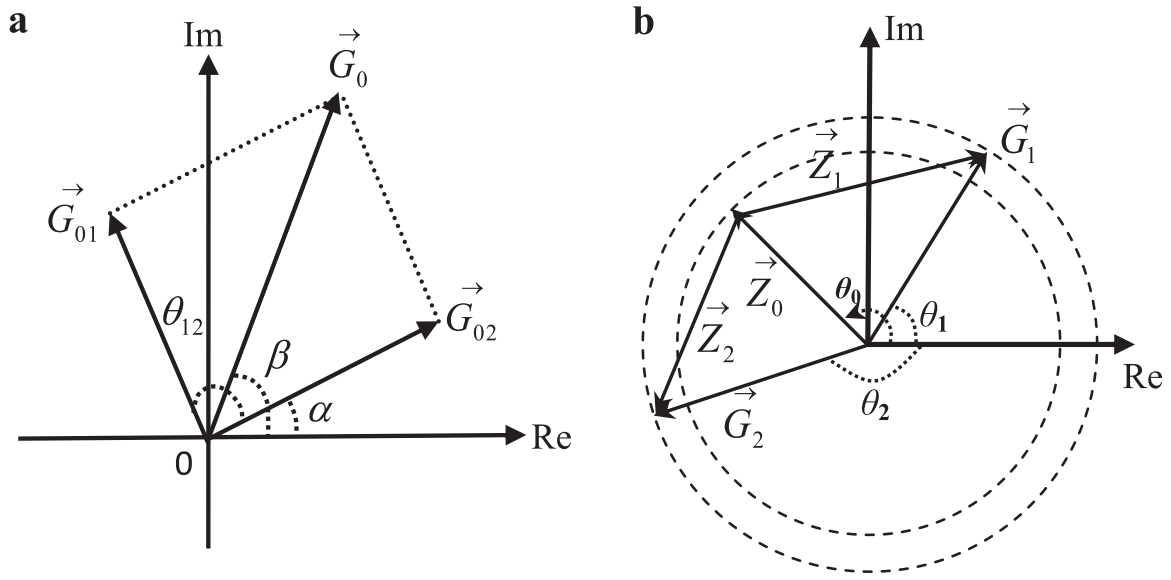

Fig. 1. Schematic diagram of basic vector operation.

using cascading phase-only functions in the Fresnel domain [27].

Besides the phase retrieval mentioned above, recently, some pioneer studies have focused on the method of basic vector operations. In 2011, Wang et al. proposed an image encoding scheme based on coherent superposition and basic vector operations [28], in which the original image can be directly separated into two phase masks, one is the a random phase mask (RPM), and the other is a modulation of the RPM. In 2015, Chen et al. proposed a pseudo color image encryption method based on three-beams interference principle and common vector composition [29], in which an original grayscale image can be divided into three parts of amplitude information and three parts of phase information by a common vector composition, and finally, with all the correct keys, the decrypted grayscale image can be obtained by the Fourier transform and three-beams interference. Soon after, this scheme was extended for a new image encryption method based on multi-beams interference and vector composition [30], in which the original image is encoded into $n-1$ phase only masks which are regarded as the keys of the encryption system and a ciphertext according to multi-beams interference principle and vector composition; when n beams of parallel incident light illuminate at the phase only masks and the ciphertext, the original image can be decrypted by Fourier transforms. Recently, we proposed a triple-image encryption scheme based on phase-truncated Fresnel transform (PTFT) and basic vector operation [31], in which two random phase masks are firstly generated by basic vector decomposition operations over the first and the second plaintext images; and then a ciphered image in the input plane is fabricated by XOR encoding for the third plaintext image. During decryption, possessing all the correct keys, the original three plaintext images can be successfully decrypted by inverse PTFT, basic vector composition, and XOR decoding.

To overcome the weakness of the traditional system based on one to one principle, recently, Deng et al. proposed a threshold secret sharing scheme based on basic vector operations and coherence superposition [32], in which a secret image to be shared can be divided into n shadow images by basic vector operations; while in the reconstruction stage, the secret image can be recovered by recording the intensity of the coherence superposition of any two shadow images, however, this method is suited for only binary images. Therefore, to build versatile authentication system and increase the authority levels, we present here a hierarchical multilevel authentication system for multiple-image based on phase retrieval and basic vector operations, which can accomplish not only the low-level authentication but also the high-level authentication for multiple certification images; furthermore, the authentication system are suitable for both binary images and grayscale images. We first give the theoretical analysis, description, and procedure of the method, then provide its simulation verification, and finally draw the conclusion.

2. Description of the authentication system design

2.1. Secret sharing algorithm based on basic vector operations

In cryptography, the keys are the core of whole cryptosystem, and the security of keys is showed in two aspects: firstly anyone using the cracked key could not get the whole secret. Secondly, once the keys were lost or deleted by accident, they can be recovered in some methods. Secret sharing scheme can solve this problem, by which, the secret data is encoded into N shares and then distributed to N participants, any T ($T \leq N$) or more of the shares can be collected to recover the secret, but any $T-1$ or fewer of them can not [32,33]. Here we introduce the secret sharing algorithm based on basic vector operations [28–32].

A two-dimensional Cartesian coordinate system is plotted in Fig. 1(a), in which the real part is acted as the horizontal component and the imaginary part as the vertical axis. In this Cartesian coordinate system, a vector $\vec{G}_0$ can be denoted in a more direct format which is $\sqrt{G_0}\exp(i\beta)$, where $\sqrt{G_0}$ is the modulus of the vector $\vec{G}_0$ and β stands for the argument, that is the angle between $\vec{G}_0$ and the horizontal axis. Based on the rules of basic vector decomposition and composition, the complex number $\vec{G}_0$ can also be taken as the sum of two vectors $\vec{G}_{01}$ and $\vec{G}_{02}$, which can be expressed as [28–32]:

$$\vec{G}_0 = \vec{G}_{01} + \vec{G}_{02} = \sqrt{G_0}\exp(i\beta), \tag{1}$$

Based on the cosine-law, the angle θ_{12} between two vectors $\vec{G}_{01}$ and $\vec{G}_{02}$ can be computed mathematically as

Please cite this article as: Li X, et al. Hierarchical multilevel authentication system for multiple-image based on phase retrieval and basic vector operations. Opt Laser Eng (2016), http://dx.doi.org/10.1016/j.optlaseng.2016.04.021