Optics and Lasers in Engineering 108 (2018) 28–35

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Multilevel image authentication using row scanning compressive ghost imaging and hyperplane secret sharing algorithm

Xianye Li [a], Xiangfeng Meng [a,*], Yongkai Yin [a], Yurong Wang [a], Xiulun Yang [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
Optical authentication
Hyperplane secret sharing
Digital holography

ABSTRACT

A multilevel image authentication method is proposed which is based on row scanning compressive ghost imaging and a hyperplane secret sharing algorithm. In the image encoding process, after the wavelet transform and Arnold transform for the certification image, through row scanning compressive ghost imaging, the ciphertext matrix can be first detected by a bucket detector (BD). Based on a hyperplane secret sharing algorithm, the measurement key using in the row scanning compressive ghost imaging, can be decomposed and shared into n subkeys, which are then distributed to n different participants. In the high-level authentication process, based on a hyperplane secret sharing algorithm and a compressive reconstruction algorithm, any t or more participants with the corresponding correct subkeys can be gathered to reconstruct the original meaningful certification image with high correlation coefficient (CC); While in the case of low-level authentication process, only one authenticator who possesses a correct subkey will gain no significant information of certification image, however, it can result in a remarkable peak output in the nonlinear correlation coefficient distribution. Theoretical analysis and numerical simulations both verify the feasibility of the proposed method.

1. Introduction

Recently, information security has received increasing attention with the acceleration of informatization. Optical information security, a branch of information security including encryption, authentication, information hiding, and so on, has become more challenging and attracted more and more researchers because of its advantages, such as high degrees of freedom, high speed, parallel computing, etc. Réfrégier and Javidi first realized optical encryption in the Fourier domain with a double random phase encoding (DRPE) scheme in 1995 [1]. The optical encryption scheme was further extended in the Fresnel transform [2,3], fractional Fourier transform [4–6], joint transform correlator (JTC) [7], phase-shifting interferometry [8], phase retrieval [9,10], gyrator transform [11], fractional Mellin transform [12], two beam interference [13], diffractive imaging [14], polarization encoding [15], etc. In addition, many researchers proposed different attack schemes and discussions for DRPE in different transform domains [16,17].

Recently, ghost imaging applied in optical image encryption has attracted increasing attention. In this case the wave scattered at the object beam arm is collected by a bucket or pinhole detector, and after scanning the detector at the reference beam arm in which the object is not located, the object can be reconstructed by intensity correlation computation [18,19]. In 2010, Clemente et al. proposed an optical encryption scheme using computational ghost imaging [20], in which the image decoding process is digitally realized through a correlation algorithm between two intensity data from a single pixel detector and a computational optical filed distribution [21]. To reduce the measurement times, the compressive ghost imaging was recently applied in optical encryption, which realized the computational ghost imaging based on a compressive sensing algorithm instead of the intensity correlation operation [22–24].

Besides image encryption, image authentication and digital signature based on optical transforms have been reported. In 2004, Kishk and Javidi first proposed the optical authentication method based on DRPE and phase-shift digital holography [25], in which the recovered hidden image is authenticated using nonlinear correlation. Situ and Zhang proposed an optical watermarking authentication scheme based on a fragile image hiding scheme in 2005 [26]. In 2012, He et al. proposed an optical hierarchical authentication based on interference, a modified phase retrieval algorithm, and a hash function, which not only checks the legality of the users but also verifies their identity levels [27]. To eliminate the collision risk, we proposed an optical identity authentica-

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

https://doi.org/10.1016/j.optlaseng.2018.04.014
Received 29 November 2017; Received in revised form 19 April 2018; Accepted 20 April 2018

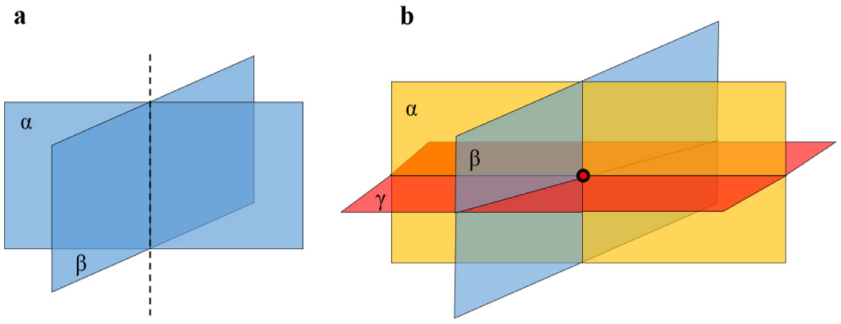

Fig. 1. The hyperplane concept in a 3-dimensional space.

tion scheme based on an elliptic curve digital signature algorithm and a phase retrieval algorithm in 2013 [28]; Subsequently, a multiple-image authentication method with a cascaded multilevel architecture was reported, which is implemented by amplitude field random sampling and phase information multiplexing [29].

To overcome the weakness of the traditional system based on a one-to-one principle, threshold secret sharing using a Lagrange interpolating polynomial [30] can be applied in optical information security, by which the secret data are encoded into n shares and then distributed to n participants, where any t ($t \le n$) or more of the shares can be collected to recover the secret, but any $t-1$ or fewer of them cannot. In 2014, we proposed a multilevel image authentication method using threshold secret sharing and a phase retrieval algorithm [31]. Subsequently, Deng et al. reported a (2, n) threshold secret sharing scheme based on vector operation and coherence superposition for binary images [32]. However, the existing secret sharing methods based on the Lagrange interpolating polynomial mentioned in [30,31] need at least two shadow images for a shareholder to decode the secret information, which increases key space redundancy and is hard to be implemented. Accordingly, the vector decomposition scheme has certain threshold number restrictions—only 2 threshold keys can be employed as in [32]—which is inflexible for multi-participant management.

To decrease the key data and build a flexible multilevel authentication system, we present here a multilevel image authentication scheme based on row scanning compressive ghost imaging and a hyperplane secret sharing algorithm, in which any subkey is seen as a hyperplane in a t-dimension space and the secret is the unique point of intersection of the n ($t < n$) hyperplanes; any t or more hyperplanes can uniquely intersect in this point, and then pass the high-level authentication with high correlation coefficient (CC), but fewer than t hyperplanes cannot. Any participant who has only one subkey can attempt to pass the low-level authentication with a peak in the nonlinear correlation coefficient (NCC) distribution. Obviously, the proposed scheme makes up for the disadvantages of existing schemes efficiently, since only one shadow is demanded for a participant and the threshold values can be selected as required. The details are described in the following sections and a set of simulations are made to verify the feasibility of the scheme.

2. Theoretical analysis and scheme description

2.1. Hyperplane secret sharing algorithm

The concept of hyperplane secret sharing was first proposed by Blakley [33]. Here, we implement its mathematical implementation for row scanning compressive ghost imaging in the multilevel authentication system. As shown in Fig. 1(a), in a 3-dimensional space, any two unparallel planes (planes α and β) have a line intersection. Furthermore, any three planes (planes α, β and γ) in 3-dimensional space have several possible intersections, but if the normal vectors $\vec{n}_\alpha, \vec{n}_\beta, \vec{n}_\alpha$ of three planes are not coplanar as $\vec{n}_\alpha \cdot |\vec{n}_\beta \times \vec{n}_\gamma| \neq 0$, three planes will have a unique intersection into a point as given in Fig. 1(b). That is, considering three

a

x_1	y_1	z_1	t_1	x_2
y_2	z_2	t_2	x_3	y_3
z_3	t_3	x_4	y_4	z_4
t_4	x_5	y_5	z_5	t_5
x_6	y_6	z_6	t_6	x_7

b

A_1	B_1	C_1	D_1	A_2
B_2	C_2	D_2	A_3	B_3
C_3	D_3	A_4	B_4	C_4
D_4	A_5	B_5	C_5	D_5
A_6	B_6	C_6	D_6	A_7

Fig. 2. The 5×5 example matrix for (a) initial key and (b) initial subkey.

planes given by the following Cartesian equations:

$$\begin{cases} A_1x + B_1y + C_1z = D_1 \\ A_2x + B_2y + C_2z = D_2 \\ A_3x + B_3y + C_3z = D_3 \end{cases}, \tag{1}$$

the condition for the three planes with only a point intersection is that both the rank of its coefficient matrix r and the rank of the augmented matrix r' are 3. The description in the matrix form can be written as

$$\begin{vmatrix} A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \\ A_3 & B_3 & C_3 \end{vmatrix} \neq 0 \,\&\&\, \begin{vmatrix} A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \end{vmatrix} \neq 0, \tag{2}$$

and, therefore, three equations of planes can calculate the position, but two or less cannot. Regarding the pixel values as the coordinates of the point of intersection, here we propose a (t, n) threshold multilevel image authentication scheme in a t-dimensional space. Only t or more hyperplanes can determine a point, but fewer than t will get a low-dimensional space.

Here, a (4, n) threshold scheme is taken as an example. In a 4-dimensional space, any hyperplane can be expressed in Cartesian equations as

$$Ax + By + Cz + Dw = E, \tag{3}$$

so any point can be described as

$$\begin{cases} A_1x + B_1y + C_1z + D_1w = E_1 \\ A_2x + B_2y + C_2z + D_2w = E_2 \\ A_3x + B_3y + C_3z + D_3w = E_3 \\ A_4x + B_4y + C_4z + D_4w = E_4 \end{cases}, \tag{4}$$

where both the ranks of the equations' coefficient matrix r and the augmented matrix r' are 4. So, the pixel values of the initial measurement key are regarded as the unknowns in the hyperplane expressions. The coefficients of the equations (Fig. 2(a)) are selected randomly and then form the subkeys' pixels (Fig. 2(b)); here, the 5×5 matrices are taken