Contents lists available at ScienceDirect

Optics Communications

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

Optical threshold secret sharing scheme based on basic vector operations and coherence superposition

Xiaopeng Deng*, Wei Wen, Xianwu Mi, Xuewen Long

Department of Physics and Information Engineering, Huaihua University, Huaihua 418008, China

ARTICLE INFO

Article history:
Received 8 August 2014
Received in revised form
10 November 2014
Accepted 28 November 2014
Available online 4 December 2014

Keywords:
Optical information processing
Optical threshold secret sharing
Vector operations
Coherence superposition

ABSTRACT

We propose, to our knowledge for the first time, a simple optical algorithm for secret image sharing with the $(2,n)$ threshold scheme based on basic vector operations and coherence superposition. The secret image to be shared is firstly divided into n shadow images by use of basic vector operations. In the reconstruction stage, the secret image can be retrieved by recording the intensity of the coherence superposition of any two shadow images. Compared with the published encryption techniques which focus narrowly on information encryption, the proposed method can realize information encryption as well as secret sharing, which further ensures the safety and integrality of the secret information and prevents power from being kept centralized and abused. The feasibility and effectiveness of the proposed method are demonstrated by numerical results.

1. Introduction

In recent decades, owning to the characteristics of high-speed and parallel processing ability, optical information security techniques, especially optical image encryption techniques, have been receiving more and more attention since Refregier and Javidi proposed the double random phase encoding [1]. Many optical encryption methods have been proposed [2–9]. Although these encryption methods possess many advantages, they also have some insurmountable defects, i.e. these encryption methods focus narrowly on information encryption and lack effective secret management, which will cause secrets to become too concentrated and overlook secret sharing. As we all known, optical encryption system belongs to symmetric encryption system and its safety is based on an assumption that decryption keys are absolutely safe. However, decryption keys will be inevitably divulged and lost in the processes of storage and transmission. Although we can use the public-key cryptography to manage and distribute keys for avoiding leak, [10] we have seldom attached importance to the security problem resulting from the loss and damage of keys. Since in most of optical encryption systems random phase masks are often chosen as keys and difficult to be duplicated, original image cannot be recovered when the crucial information is destroyed by human factors or natural disasters in the processes of storage and transmission. In addition, we know that ciphertext is as important as keys for original image restoration. Although there is no problem of ciphertext leak, ciphertext as well as keys might be lost or destroyed in the processes of storage and transmission. So how to ensure the safety of the crucial information for original image restoration and manage it effectively has become an important problem to be solved urgently in the optical information security fields.

Practices in the digital information security fields indicate that the secret sharing technique provides an available method for solving the above problem. Of all the secret sharing schemes, the threshold secret sharing scheme is the most typical and significant one because it is very useful in some places, such as bank, company and so on [11–15]. In the threshold secret sharing scheme, [11–15] the shared secret is firstly encoded into n parts (called shadows) and then these shadows are distributed to n participants, respectively. In the secret recovering stage, the sharing algorithm guarantees that any t $(t \le n)$ or more of the participants can join together to recover the shared secret, while any $t-1$ or fewer of them cannot obtain any information about the shared secret. By the above method, we can solve the security problem resulting from leak of individual keys and prevent power from being kept centralized and abused because only when adequate keys must be obtained by attacker or licensor can the shared secret be recovered. On the other hand, when some keys are destroyed by human factors or natural disasters, the holders of other keys still can join together to recover the shared secret, which ensures the safety and integrality of the shared secret. However, the existing threshold secret sharing schemes are constructed by using

* Corresponding author.
E-mail address: dxpzqh@163.com (X. Deng).

http://dx.doi.org/10.1016/j.optcom.2014.11.098
0030-4018/© 2014 Elsevier B.V. All rights reserved.

complicated mathematical operations based on digital encryption [11–15]. To our knowledge, Optical threshold secret sharing scheme has not been reported.

In order to take full advantages of the high-speed, parallel processing ability and multidimensional encoding in optical information processing and overcome some common defects of the existing optical encryption techniques, we propose a simple optical algorithm in this paper for secret image sharing with the (2, n) threshold scheme based on basic vector operations and coherence superposition. In the formation stage of shadow images, the secret image to be shared is firstly divided into n shadow images by use of basic vector operations. In the reconstruction stage, the secret image can be retrieved by recording the intensity of the coherence superposition of any two shadow images. Compared with the published encryption techniques which focus narrowly on information encryption, the proposed method can realize information encryption as well as secret sharing, which further ensures the safety and integrality of the secret information and prevents power from being kept centralized and abused. In the following sections, we will show how the algorithm realizes threshold secret sharing.

2. Secret distribution algorithm

Generally, a secret sharing scheme is composed of a secret distribution algorithm and a secret reconstruction algorithm. The main aim of secret distribution algorithm is to divide a secret image into a number of shade images and distribute these shade images to a group of participants. First, let us show you how to design the shade images by using basic vector operations [16]. As shown in Fig. 1, a complex number $\vec{g}_0$, which is denoted by $\sqrt{I}\exp i\beta_0$, can be viewed as a position vector in a two-dimensional Cartesian coordinate system, in which the real part is used as the horizontal component and imaginary part as vertical. Based on the summation rule of vectors, the complex number $\vec{g}_0$ can also be taken as the sum of two vectors and expressed as

$$\vec{g}_0 = \vec{z}_1 + \vec{z}_2 = \sqrt{I}\exp i\beta_0. \tag{1}$$

The angle θ_{12} between $\vec{z}_1$ and $\vec{z}_2$ can be computed by

$$\theta_{12} = \arccos\frac{I - \left|\vec{z}_1\right|^2 - \left|\vec{z}_2\right|^2}{2\left|\vec{z}_1\right|\left|\vec{z}_2\right|}, \tag{2}$$

where $|\cdot|$ denotes the modulus operation.

According to the triangle inequality, the modulus of $\vec{g}_0$ is within the range from $\left|\left|\vec{z}_1\right| - \left|\vec{z}_2\right|\right|$ to $\left|\vec{z}_1\right| + \left|\vec{z}_2\right|$. Suppose that $\vec{z}_1$ and $\vec{z}_2$ are two unit vectors, the modulus of $\vec{g}_0$ should be within the range of 0–2. Conversely, any vector of which modulus is smaller than 2 can be always divided into two unit vectors. Under these circumstances, Eq. (2) can be rewritten as

$$\theta_{12} = \arccos\left(\frac{I}{2} - 1\right) \tag{3}$$

It can be seen from Eq. (3) that the angle θ_{12} between $\vec{z}_1$ and $\vec{z}_2$ can be determined as long as we know the modulus of $\vec{g}_0$. So it does not matter where the vector $\vec{z}_1$ or $\vec{z}_2$ is placed. Assume that the phase of the unit vector $\vec{z}_1$ is $\exp i\alpha$, the other unit vector $\vec{z}_2$ can be expressed as

$$\vec{z}_2 = \exp[i(\alpha + \theta_{12})] \tag{4}$$

Since a pixel value of an image can be represented by a complex number, it is possible for us to divide an image into two phase-only masks, which could also mean that a positive image can be retrieved by recording the intensity of the coherence superposition of two phase-only masks.

However, although the above algorithm can readily divide a secret image into two phase-only shadow images, it still cannot realize threshold secret sharing scheme because in a threshold secret sharing scheme the minimum number of shadow images or participants must be larger than 2. So in order to realize threshold secret sharing scheme, more shadows images must be obtained. If we notice that Eq. (3) is a nonlinear function and linear change of I will result in nonlinear change of θ_{12}, the problem will be readily solved.

As we all know, linear change of intensity cannot result in change of image itself. So different angles, between which the interrelationships are nonlinear, can be obtained by changing I of Eq. (3), which can be expressed by

$$\theta_{1n} = \arccos\left[\frac{k_{1n}I}{2} - 1\right] \quad n = 2, 3, \ldots \tag{5}$$

where k_{1n} is a constant and used to change linearly I. It must be noted that in order to meet the triangle inequality, the constant k_{1n} should be within the range of 0–4 when I is normalized to the range of 0–1. Thus, based on Eqs. (4) and (5) we can obtain a series of different unit vectors

$$\vec{z}_n = \exp[i(\alpha + \theta_{1n})] \quad n = 2, 3, \ldots \tag{6}$$

Based on the summation rule of vectors, the sum of $\vec{z}_1$ and $\vec{z}_n$ can be expressed as

$$\vec{g}_{n-2} = \vec{z}_1 + \vec{z}_n = \sqrt{k_{1n}I}\exp i\beta_{n-2} \quad n = 2, 3, \ldots \tag{7}$$

Obviously, when $n = 2$ and $k_{1n} = 1$, Eqs. (1), (3) and (4) are special cases of Eqs. (7), (5) and (6), respectively. Since $\vec{z}_1$ and $\vec{z}_n$ are unit vectors, the angle β_{n-2} between $\vec{g}_{n-2}$ and the horizontal

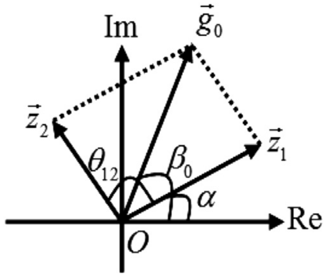

Fig. 1. Basic vector addition operation; Im: imaginary part; Re: real part.

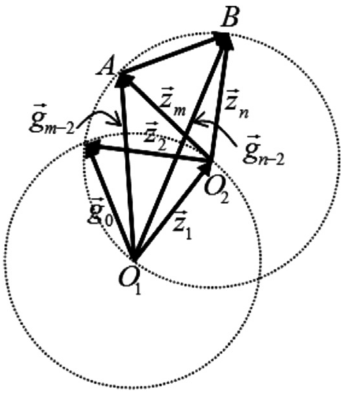

Fig. 2. Schematic diagram of the proposed algorithm.