Optics Communications 405 (2017) 53–59

Contents lists available at ScienceDirect

Optics Communications

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

Shift, rotation and scale invariant optical information authentication with binary digital holography

Shuming Jiao, Changyuan Zhou, Wenbin Zou *, Xia Li

Shenzhen Key Lab of Advanced Telecommunication and Information Processing, College of Information Engineering, Shenzhen University, Shenzhen, Guangdong, China

ARTICLE INFO

Keywords:
Optical authentication
Digital holography
Shift rotation and scale
Invariant
Fourier transform
Log polar transform

ABSTRACT

An optical information authentication system using binary holography is proposed recently, with high security, flexibility and reduced cipher-text size. Despite the success, we point out one limitation of this system that it cannot well verify scaled and rotated versions of correct images and simply regard them as wrong images. In fact, this limitation generally exists in many other optical authentication systems. In this paper, a preprocessing method based Fourier transform and log polar transform is employed to allow the optical authentication systems shift, rotation and scale invariant. Numerical simulation results demonstrate that our proposed scheme significantly outperforms the existing method.

1. Introduction

Optical technologies have been extensively investigated for information security applications such as information encryption [1–4], information authentication [5–11] and information watermarking [12–17]. Compared to commonly used digital information security technologies, optical technologies have significant advantages of multiple dimensions, high information capacity and high processing speed.

Secure information authentication (or verification) allows an authentication authority to identify the truth of certain information entity (e.g. fingerprint, photo, ID card number) and in the meanwhile the correct entity is maintained secret to the authority. In optical authentication, the correct reference information (usually in the form of images) is first processed through a one-directional optical imaging system and the system output image serves as a secret identifier of input image. The original image is difficult to recover from the corresponding secret identifier. But the correlation between secret identifier and one arbitrary image can verify the similarity between original image and the arbitrary image. The secret identifier of correct reference image is pre-stored in the authentication authority side and any given image can be verified based on the secret identifier.

Both the one-directional optical imaging system and the secret identifier verification system can be implemented optically. In previous works, the former can be implemented in various ways such as digital holography [5], diffractive imaging and phase retrieval [6,7], 3D random phase object [8], binary amplitude masks [9], ghost imaging [10] and photo counting imaging [11]. The latter is most commonly implemented by nonlinear joint power spectrum based optical correlator [18] or joint fractional Fourier transform based optical correlator [19,20]. If the image to be authenticated is very similar to the correct reference image, a peak signal can be observed in the output of optical correlator indicating "succeed in authentication" and otherwise noise-like signals will appear in the output indicating "fail in authentication".

Recently, an optical information authentication scheme based on binary digital holography is proposed with an advantage of high security, flexibility and reduced cipher-text size [5]. However, we notice that there is one limitation in this system that it is not scale and rotation invariant. For example, if an input image to be identified is exactly the same as the correct reference image except that it is enlarged or shrinked by 10% or rotated by 5 degrees, the abovementioned verification systems will usually identify such an image as "fail in authentication". However, in many applications, users expect the system to give a "succeed in authentication" result even though the input image is a slightly scaled or rotated version of the correct one. In other words, the authenticate system shall distinguish a scaled or rotated version of correct image from a completely wrong image. In fact, this limitation is rather common in many other existing optical authentication systems [6–11].

The abovementioned problem can be partially solved by using a log-polar transform-based wavelet-modified maximum average correlation height filter [21,22] in the authentication system. However, such a filter

* Corresponding author.
E-mail address: wzouszu@sina.com (W. Zou).

http://dx.doi.org/10.1016/j.optcom.2017.07.069
Received 6 June 2017; Received in revised form 23 July 2017; Accepted 26 July 2017
0030-4018/

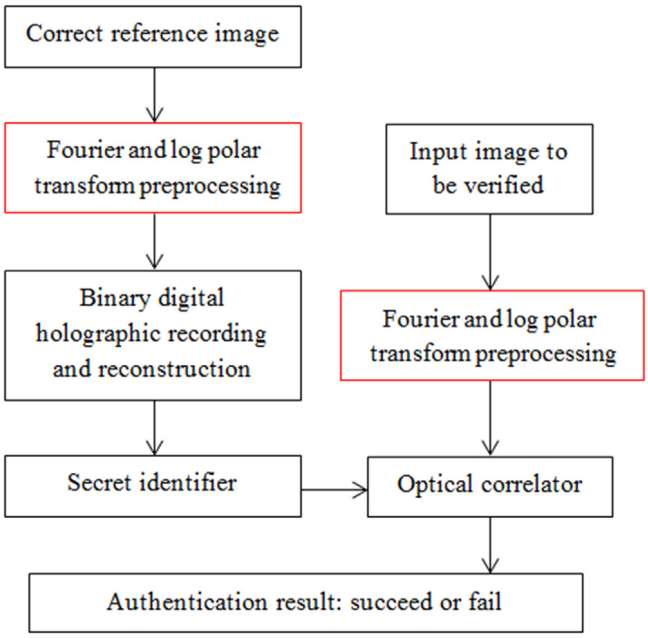

Fig. 1. Overall structure of the optical information authentication scheme based on binary digital holography [5] (black boxes) and our proposed additional preprocessing steps in this paper (red boxes).

will yield a rotation and scale invariant but shift variant correlator result (the center of scaled/rotated image shall be the same as original image), which is still not favorable in many applications. The objective of this paper is to propose an optical authentication scheme that is both shift and rotation & scale invariant, shown in Table 1.

In pattern recognition research field, the problem of shift, rotation and scale invariance has been investigated from different perspectives [23–29]. Some representative methods such as Fourier transform and log polar transform [23,24], self-mapping transform [25], SIFT feature extraction [26,27], Zernike moments [28] and Gabor feature space [29] are proposed in the past. These methods can be possibly combined with conventional optical authentication systems to achieve shift, rotation and scale invariant optical authentication. Among them, the Fourier transform and log polar transform [23,24] method is easy to implement with low complexity and will only impose minor modification on the existing optical authentication systems. Therefore in this paper, we propose a rotation, scale plus shift invariant scheme for the binary digital holography authentication system based on Fourier transform and log polar transform preprocessing.

2. Optical information authentication scheme based on binary digital holography

We shall first briefly describe the working principles of the optical information authentication scheme based on binary digital holography proposed in previous work [5]. The overall structure of the optical information authentication scheme based on binary digital holography is illustrated in Fig. 1. The correct reference image is first encrypted by a Fresnel domain Double Random Phase Encoding (DRPE) optical encryption system, shown in Fig. 2. The encrypted hologram is binarized and the reconstructed image from the binary hologram is employed as a secret identifier. Whenever an arbitrary image to be verified and this secret identifier are jointly input to a nonlinear joint power spectrum optical correlator, the correlator output will indicate whether the authentication is successful or failed. In Sections 2.1 and 2.2, the working mechanism of secret identifier generation and optical correlator verification will be discussed respectively.

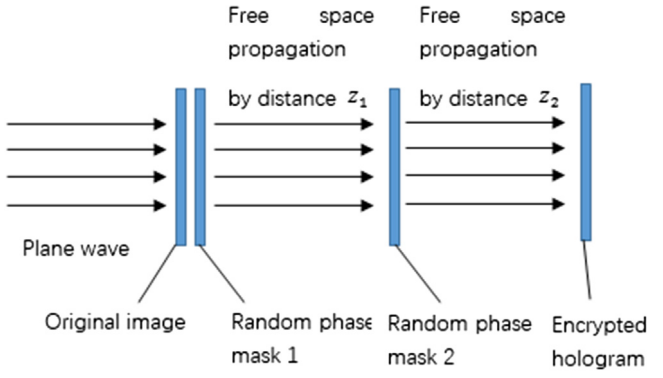

Fig. 2. Fresnel domain Double Random Phase Encoding (DRPE) optical encryption architecture.

2.1. Secret identifier generation

In previous work [5], the secret identifier of a reference image is acquired by a Fresnel domain Double Random Phase Encoding (DRPE) optical encryption architecture, shown in Fig. 2.

In this architecture, the Fresnel diffraction field of original reference image $f(x,y)$ (object image) is encrypted by two random phase masks $\varphi_1(x,y)$ and $\varphi_2(x,y)$ placed at two different distances z_1 and z_2, shown in Eq. (1).

$$h(x,y) = \mathrm{FrT}\left\{\mathrm{FrT}\left[f(x,y)\exp\left(j\varphi_1(x,y)\right), z_1\right]\exp\left(j\varphi_2(x,y)\right), z_2\right\} \quad (1)$$

where FrT denotes Fresnel transform.

An encrypted complex Fresnel hologram $h(x,y)$ is generated as the output and can be captured by a CCD sensor. Then the captured digital hologram is quantized to be a binary phase hologram $b(x,y)$, shown in Eq. (2).

$$b(x,y) = \begin{cases} 1 & 0 \le Phase[h(x,y)] < \pi \\ 0 & -\pi \le Phase[h(x,y)] < 0 \end{cases} \quad (2)$$

where Phase [] denotes the phase part of a complex signal.

When the conjugate of the binary phase hologram is input to the same system of hologram recording (Fig. 2), a holographically reconstructed image $u(x,y)$ can be obtained, shown in Eq. (3).

$$u(x,y) = \left|\mathrm{FrT}\left[\mathrm{FrT}\left(b^*(x,y), z_2\right)\exp\left(j\varphi_2(x,y)\right), z_1\right]\right| \quad (3)$$

where * denotes complex conjugate operation.

The magnitude of the reconstructed image $|u(x,y)|$ from the binary phase hologram is used as the secret identifier. The secret identifier is a noise-like image and no original image information can be visually observed from it. However, the secret identifier contains a small amount of original image information, which can be used for correlation verification.

2.2. Optical correlator verification

The mathematical model of nonlinear joint power spectrum optical correlator [18] is illustrated in Eq. (4), where $u(x,y)$ and $g_0(x,y)$ denote secret identifier and one arbitrary image to be verified correspondingly, FT and IFT denote Fourier transform and inverse Fourier transform, $|\mathrm{FT}[u(x,y)]|$ and $|\mathrm{FT}[g_0(x,y)]|$ are the magnitude components of Fourier transform spectrum, $\Phi_{FT(u)}$ and $\Phi_{FT(g_0)}$ are the phase components of Fourier transform spectrum and m is a nonlinear correlation coefficient (it is set to be 0.3 in this paper).

$$C = \mathrm{IFT}\left\{\left(|\mathrm{FT}[u(x,y)]|\cdot\left|FT[g_0(x,y)]\right|\right)^m \exp\left[j\left(\Phi_{FT(u)} - \Phi_{FT(g_0)}\right)\right]\right\}. \quad (4)$$

In case one input image to be verified, $g_0(x,y)$, is highly correlated with the secret identifier $u(x,y)$, the correlator can yield a correlation peak in the output