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.

© 2017 Elsevier B.V. All rights reserved.

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/© 2017 Elsevier B.V. All rights reserved.

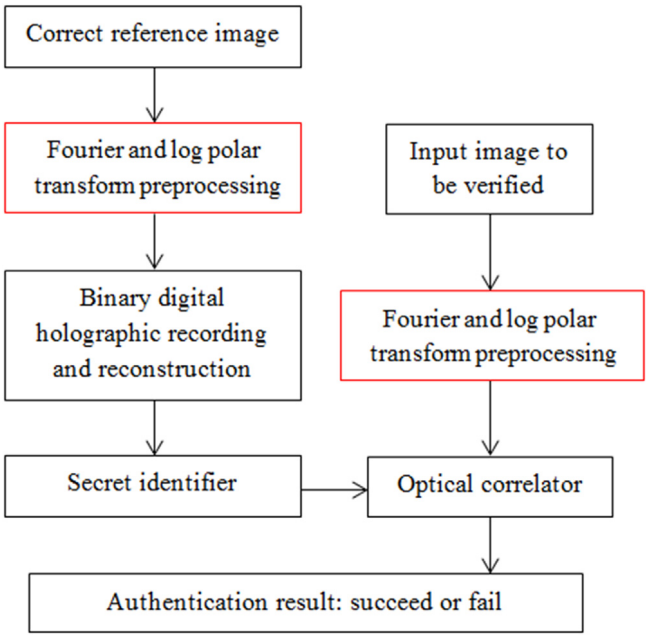

Fig. 1. Overall structure of the optical information authentication scheme based on binary digital holography [5] (black boxes) and our proposed additional preprocessing steps in this paper (red boxes).

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.

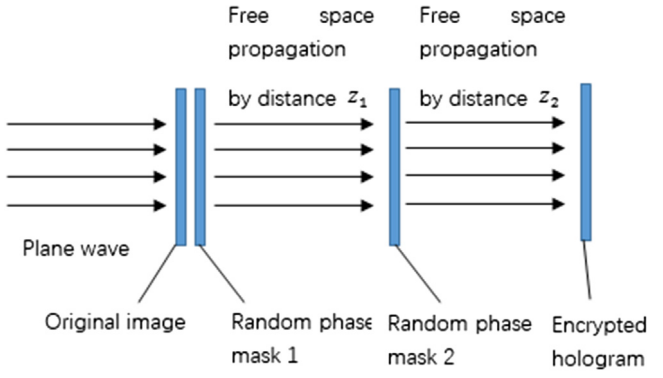

Fig. 2. Fresnel domain Double Random Phase Encoding (DRPE) optical encryption architecture.

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

Table 1
Comparison of our proposed scheme with existing schemes.

Methods	Shift invariant	Rotation and scale invariant
Conventional optical authentication	Yes	No
Previous scheme [21,22]	No	Yes
Proposed scheme in this paper	Yes	Yes

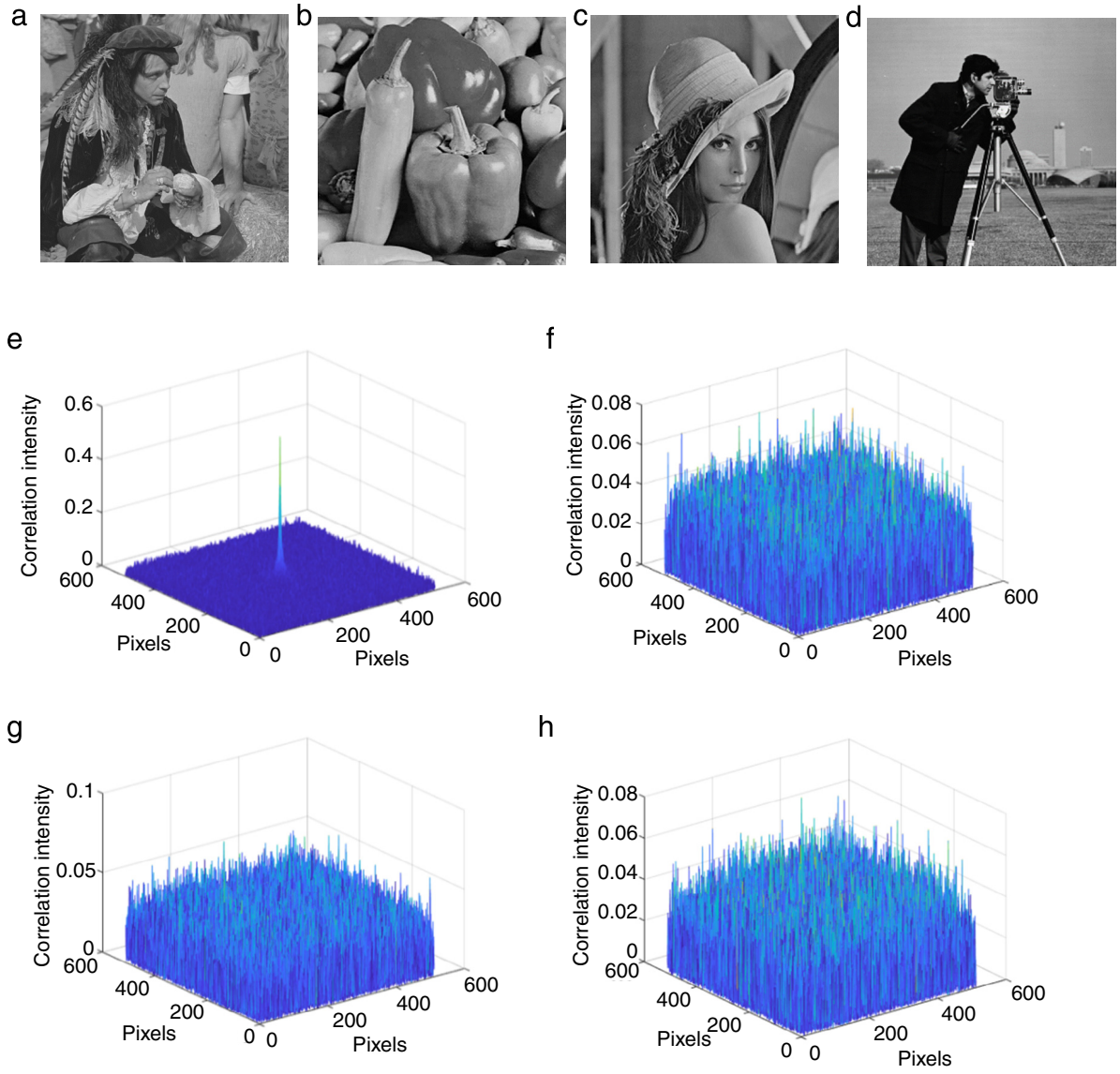

Fig. 3. (a) Correct reference image "Pirate"; (b) Test image "Pepper"; (c) Test image "Lena"; (d) Test image "Cameraman"; (e)–(h) The corresponding optical correlator output results of previous method [5] when (a)–(d) are employed as the input images to be verified and Fig. 3(a) is employed as the correct reference image.

(shown in Fig. 3(e)) and $g_0(x, y)$ is successfully authenticated. Otherwise, the correlator will yield a noise like output when $g_0(x, y)$ has very low correlation with $u(x, y)$ (shown in Figs. 3(f)–(h)).

2.3. Resistance to shift, scale and rotation distortion

It is assumed that an input image $g(x, y)$ is highly correlated with $u(x, y)$. A translational shifted version of $g(x, y)$ can be authenticated as well and the correlation peak position is shifted, shown in Fig. 4(d). This is due to the fact that the Fourier transform magnitude of a translational shifted image is the same as that of original image and only the phase part has a difference, shown in Eqs. (5) and (6), where (ε, η) denotes the Fourier transform space.

$$\left|\mathrm{FT}\left[g\left(x - x_0, y - y_0\right)\right]\right| = |FT\left[g\left(x, y\right)\right]| = M\left(\varepsilon, \eta\right) \tag{5}$$

$$\phi_{\mathrm{FT}[g(x-x_0,y-y_0)]} = \phi_{\mathrm{FT}[g(x,y)]} \exp\left[-j2\pi\left(x_0\epsilon + y_0\eta\right)\right]. \tag{6}$$

However, the scaled or rotated version of $g(x, y)$ will have substantially mismatched Fourier transform magnitudes with $g(x, y)$ and the authentication will fail, shown in Figs. 4(e) and (f), Eqs. (7) and (8), where θ denotes the rotation angle; a and b denote the scaling factors.

$$\begin{aligned}&|\mathrm{FT}\left[g\left(x\cdot\cos\theta + y\cdot\sin\theta, -x\cdot\sin\theta + y\cdot\cos\theta\right)\right]| \\ &\quad = M\left(\epsilon\cdot\cos\theta + \eta\cdot\sin\theta, -\epsilon\cdot\sin\theta + \eta\cdot\cos\theta\right) \neq |FT\left[g\left(x, y\right)\right]|\end{aligned} \tag{7}$$

$$|FT\left[g\left(ax, by\right)\right]| = \frac{1}{|ab|} M\left(\frac{\epsilon}{a}, \frac{\eta}{b}\right) \neq |FT\left[g\left(x, y\right)\right]|. \tag{8}$$

As a consequence, the optical information authentication scheme based on binary digital holography proposed in previous work [5], can distinguish a shifted version of correct image from a completely wrong image but cannot distinguish a scaled or rotated one from a wrong one.

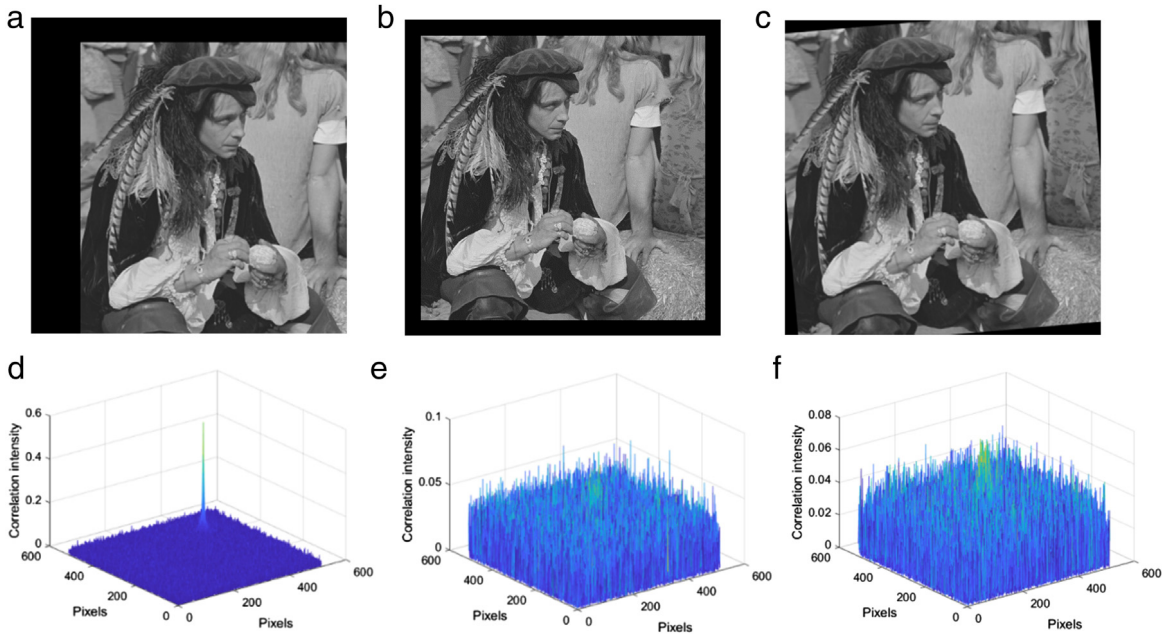

Fig. 4. (a) A shifted version of the correct reference image in Fig. 3(a); (b) A slightly scaled version of the correct reference image in Fig. 3(a) (image size is reduced to 90% of original); (c) A slightly rotated version of the correct reference image in Fig. 3(a) (rotated by 5 degrees); (d)–(f) The corresponding optical correlator output results of previous method [5] when (a)–(c) are employed as the input images to be verified and Fig. 3(a) is employed as the correct reference image.

3. Proposed shift, scale and rotation invariant optical authentication scheme

In this paper, we propose to employ a simple method to achieve shift, scale and rotation invariant authentication based on Fourier transform and log polar transform preprocessing of reference image and input image [23,24], illustrated in Fig. 1. We employ the preprocessed reference image instead of original reference image as the input to the binary holographic recording and reconstruction imaging system for secret identifier generation. We also employ the preprocessed image as the optical correlator input for verification.

The preprocessing (illustrated in Fig. 5) consists of three steps: (1) The original image (either correct reference image or an arbitrary image to be verified) $f(x, y)$ is Fourier transformed and the Fourier transform magnitude $|F(u, v)|$ is preserved; (2) The high frequency part in $|f(u, v)|$ is enhanced and the low frequency part in $|F(u, v)|$ is suppressed by a high pass filter [24]; (3) A log-polar coordinate transform is performed on filtered $|F(u, v)|$ and the two new coordinate axes are $\log_k(r)$ axis (k is the base of logarithmic operation and r is the radial distance of each pixel in filtered $|F(u, v)|$ to the spectrum origin) and θ axis (θ is the angle between the connected line of each pixel to origin and horizontal direction).

The rationale of such preprocessing can be explained as follows. As mentioned above, optical correlators [18,19] can tolerate translational shift of input images but not rotation and scaling. The preprocessing shall transform all translation, rotation and scaling distortions in original images into a translational shift in pre-processed results (after log polar transform in Step (3)). In the Fourier spectrum magnitude result $|F(u, v)|$ after Step (1), the translational shift variance in $f(x, y)$ will be eliminated since they will yield the same $|F(u, v)|$, the rotation variance in $f(x, y)$ will tend to yield a rotated $|F(u, v)|$ spectrum magnitude and the scaling variance in $f(x, y)$ will tend to yield an inversely scaled $|F(u, v)|$ spectrum magnitude. In other words, the Fourier spectrum magnitude of a shifted, rotated and scaled image becomes a rotated and scaled Fourier spectrum magnitude of original undistorted image. Then the log-polar transform in Step (3) can transform a rotated and scaled Fourier spectrum magnitude into a shifted Fourier spectrum magnitude. The detailed explanation of log-polar transform operation can be found in Ref. [24]. In this way, the shift, rotation and scaling variance in the original image $f(x, y)$ is finally transformed to a shift variance in the Fourier spectrum magnitude.

As a consequence, a correlation peak instead of noise can still appear in the optical correlator output when the preprocessed image (with translation, rotation and scaling) is compared with the secret identifier (without translation, rotation and scaling). It shall be noticed that our proposed preprocessing method

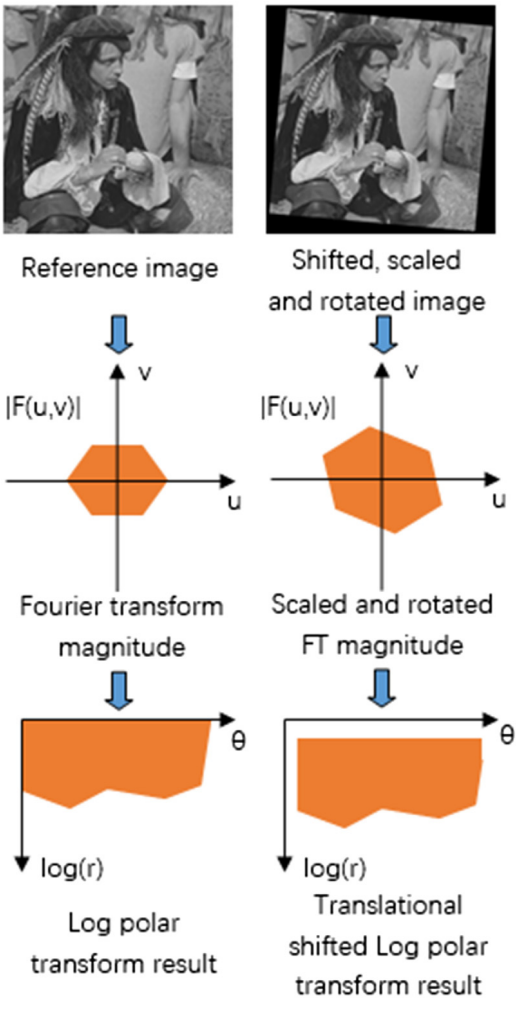

Fig. 5. Fourier transform and log polar transform based preprocessing.

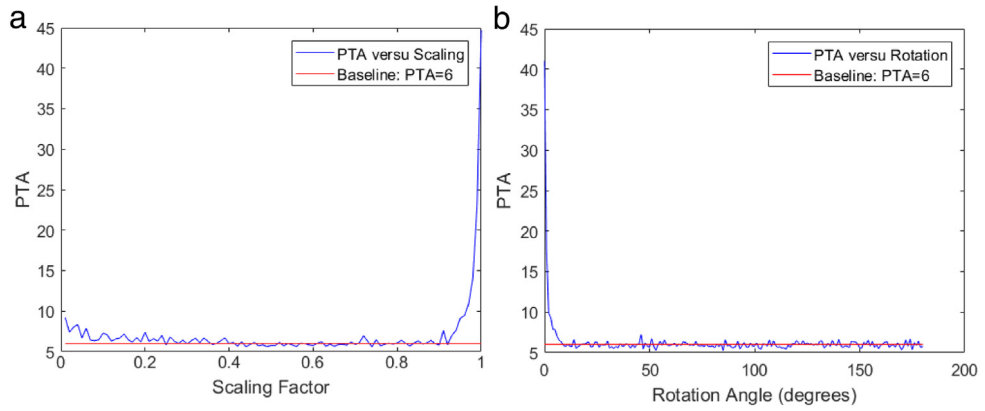

Fig. 6. (a) PTA value versus scaling factor curve (without rotation or shift) for original optical authentication system [5]; (b) PTA value versus rotation angle curve (without scaling or shift) for original optical authentication system [5].

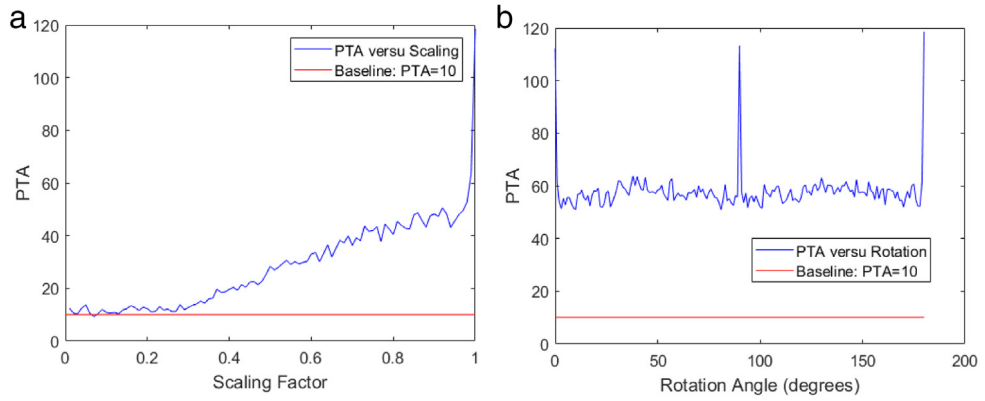

Fig. 7. (a) PTA value versus scaling factor curve (without rotation or shift) for our proposed optical authentication system; (b) PTA value versus rotation angle curve (without scaling or shift) for our proposed optical authentication system.

can also be combined with many other optical authentication systems (such as [6–11]) other than the binary holography one [5].

4. Numerical simulation results

Numerical simulation is conducted to evaluate the performance of our proposed scheme, in comparison with previous method [5]. In the simulation, the size of images and phase masks in the Fresnel domain DRPE system is 512×512 pixels. The wavelength of illuminating light is 630 nm and the pixel size is 4.65 μm.

In order to quantitatively measure the strength of correlation in the optical correlator output, a Peak to Average (PTA) indicator is calculated. PTA refers to the ratio of maximum peak intensity to the average of all pixel intensities in the output of optical correlator. A high PTA value corresponds to a single peak like correlator output and a low PTA value corresponds to a noise like correlator output. For example, in Figs. 3(e)–(h), the PTA values are 45.38, 5.94, 5.6 and 5.42 respectively. The PAE value in Fig. 3(e) is significantly higher than the other three cases. Since the PAE value is around 6 when different arbitrary images are employed as the input images to be verified, we take PAE = 6 as a baseline. When the PAE value is close to the baseline, the input image will be categorized as incorrect image.

It is assumed that Fig. 3(a) is employed as the correct reference image in the following simulation. We first evaluate the PAE value in the output of the original optical authentication system [5], when the input image to be verified is a shrinked version of Fig. 3(a) by reducing the scaling factor from 1 to 0 (e.g. the size is reduce to 25% when the scaling factor is 0.5), shown in Fig. 6(a) and when the input image to be verified is a rotated version of Fig. 3(a) with a rotation angle from 0 to 180 degrees, shown in Fig. 6(b).

It can be observed that the PTA value of a scaled reference image is almost undistinguishable from an arbitrary image (the baseline) in the authentication result, except when the scaling factor is very high (e.g. higher than 0.95), shown in Fig. 6(b). This indicates that the original authentication system [5] can only tolerate a very small level of scaling. Similarly, the original authentication system can only tolerate a very small angle of rotation, shown in Fig. 6(b).

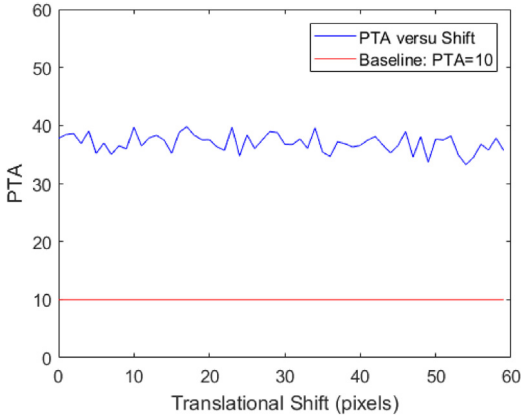

Fig. 8. PTA value versus horizontal and vertical translational shift curve (when the correct reference image is scaled to 0.7 times of original and rotated by 45 degrees) for our proposed optical authentication system.

In our proposed new optical authentication scheme, when Fig. 3(a) is employed as the correct reference image and Figs. 3(a)–(d) are employed as the input images to be verified, the PTA results are 118.68, 8.13, 9.99 and 10 respectively. The baseline can be set as PTA = 10.

Similar to Fig. 6, a scaling test and rotation test are conducted and the results are illustrated in Fig. 7.

It can be observed from Fig. 7(a) that the PTA value of a scaled reference image is significantly higher than the baseline provided that the image is not

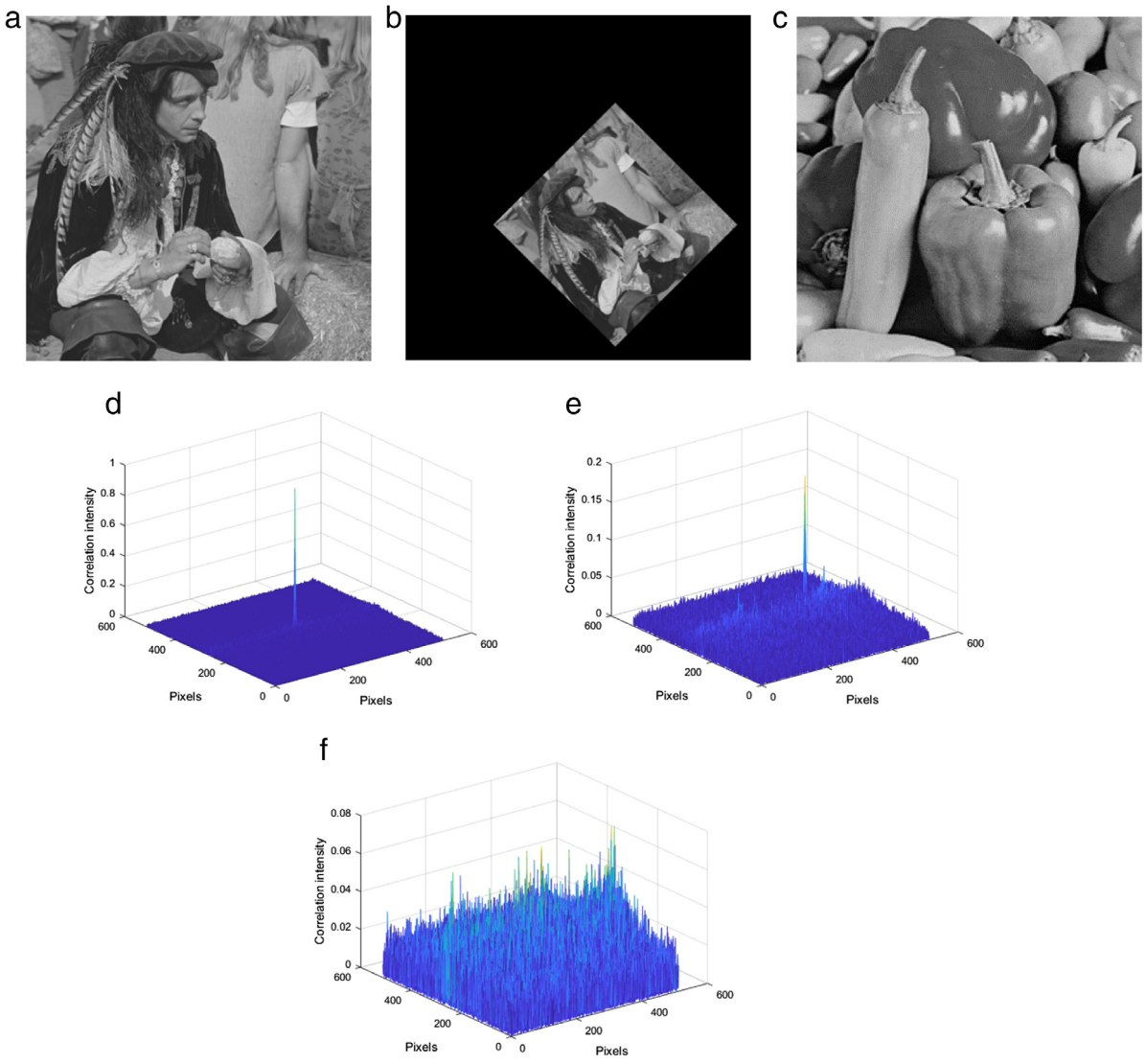

Fig. 9. (a) An input image to be verified that is identical to the correct reference image; (b) An input image to be verified that is a scaled, rotated plus shifted version of the correct reference image; (c) An arbitrary input image to be verified; (d)–(f) Output result from our proposed authentication scheme for (a)–(c) when Fig. 3(a) is employed as the correct reference image.

shrinked to a very small size. In addition, our proposed scheme demonstrates very strong tolerance to rotation variance, illustrated in Fig. 7(b). The PTA value at any rotation angle is constantly higher than four times of the baseline. These results reveal that our proposed scheme can distinguish a severely scaled or rotated correct image from a completely incorrect image.

Next, the robustness of our proposed scheme is demonstrated through an arbitrary example when scaling, rotation and shift are simultaneously applied to a correct input image to be verified. The correct reference image (Fig. 3(a)) is first scaled to 0.7 times of original size and then rotated by 45 degrees. Then it is shifted in both horizontal and vertical directions at a distance of various numbers of pixels, shown in Fig. 8.

The results indicate that our proposed scheme is robust to shift variance when the original image is already scaled and shifted. An example of scaled, rotated plus shifted reference image (scaled to 0.7 times of original size, rotated by 45 degrees plus horizontally and vertically shifted by 50 pixels) is shown in Fig. 9(b). The output of our proposed scheme for Fig. 9(b) is shown in Fig. 9(e) and it is evident that there is a peak signal in the authentication output indicating successful authentication. As a comparison, the output results of our proposed scheme for an input image exactly identical to the correct reference image (Fig. 9(a)) and an arbitrary incorrect image (Fig. 9(c)) are shown in Figs. 9(d) and (f) respectively. This example visually demonstrates that our proposed scheme can effectively distinguish a scaled, rotated and shifted correct reference image from an arbitrary incorrect image.

5. Conclusion

A binary digital holography system with Double Random Phase Encoding can be employed for optical information authentication application with high security, flexibility and reduced cipher-text size [5]. However, the rotation and scale invariant issue was not sufficiently considered in this scheme as well as in many other optical authentication systems. In this paper, we employ an image preprocessing method based on Fourier transform and Log polar transform to overcome this limitation. With our proposed scheme, the authentication system can allow substantially shifted, scaled and rotated versions of correct reference images to be successfully authenticated and distinguish the distorted correct image from an arbitrary incorrect image. Numerical simulation results demonstrate that our proposed scheme has good robustness compared to existing scheme.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (NSFC) project under Grant 61401287, and in part by the Natural Science Foundation of Shenzhen under Grant JCYJ20160307154003475 and Grant JCYJ20160506172651 25.

References

[1] P. Refregier, B. Javidi, Optical image encryption based on input plane and fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.
[2] B. Javidi, et al., Roadmap on optical security, J. Opt. 18 (8) (2016) 083001.
[3] S. Liu, C. Guo, J.T. Sheridan, A review of optical image encryption techniques, Opt. Laser Technol. 57 (2014) 327–342.
[4] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, H. Li, Optical image encryption via ptychography, Opt. Lett. 38 (9) (2013) 1425–1427.
[5] W. Chen, X. Chen, Digital holography-secured scheme using only binary phase or amplitude as ciphertext, Appl. Opt. 55 (24) (2016) 6740–6746.
[6] X. Wang, W. Chen, X. Chen, Optical information authentication using compressed double-random-phase-encoded images and quick-response codes, Opt. Express 23 (5) (2015) 6239–6253.
[7] W. Chen, Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation, IEEE Photon. J. 81 (2016) 1–9.
[8] O. Matoba, T. Sawasaki, K. Nitta, Optical authentication method using a three-dimensional phase object with various wavelength readouts, Appl. Opt. 47 (24) (2008) 4400–4404.
[9] X. Wang, G. Zhou, C. Dai, Optical double binary amplitude mask structure for security authentication, IEEE Photon. J. 8 (6) (2016) 1–7.
[10] W. Chen, X. Chen, Grayscale object authentication based on ghost imaging using binary signals, Europhys. Lett. 110 (4) (2015) 44002.
[11] E. Pérez-Cabré, M. Cho, B. Javidi, Information authentication using photon-counting double-random-phase encrypted images, Opt. Lett. 36 (1) (2011) 22–24.
[12] S. Kishk, B. Javidi, Information hiding technique with double phase encoding, Appl. Opt. 41 (26) (2002) 5462–5470.
[13] S. Kishk, B. Javidi, Watermarking of three-dimensional objects by digital holography, Opt. Lett. 28 (3) (2003) 167–169.
[14] H. Hamam, Digital holography-based steganography, Opt. Lett. 35 (24) (2010) 4175–4177.
[15] S. Jiao, P. Tsang, A hologram watermarking scheme based on scrambling embedding and image inpainting, Digital Holography and Three-Dimensional Imaging 2015, Optical Society of America, DT2A 4 (2015).
[16] J. Zhang, Z. Wang, T. Li, A. Pan, Y. Wang, Y. Shi, 3D object hiding using three-dimensional ptychography, J. Opt. 18 (9) (2016) 095701.
[17] W. Xu, H. Xu, Y. Luo, T. Li, Y. Shi, Optical watermarking based on single-shot-ptychography encoding, Opt. Express 24 (24) (2016) 27922–27936.
[18] B. Javidi, Nonlinear joint power spectrum based optical correlation, Appl. Opt. 28 (12) (1989) 2358–2367.
[19] S. Jin, S.Y. Lee, Joint transform correlator with fractional fourier transform, Opt. Commun. 207 (1) (2002) 161–168.
[20] S.K. Rajput, N.K. Nishchal, Image encryption and authentication verification using fractional nonconventional joint transform correlator, Optics and Lasers in Engineering 50 (10) (2012) 1474–1483.
[21] A. Aran, N.K. Nishchal, V.K. Beri, A.K. Gupta, Log-polar transform-based wavelet-modified maximum average correlation height filter for distortion invariance in a hybrid digital-optical correlator, Appl. Opt. 46 (33) (2007) 7970–7977.
[22] A. Aran, N.K. Nishchal, V.K. Beri, A.K. Gupta, Log-polar transform-based wavelet-modified maximum average correlation height filter for distortion-invariant target recognition, Optics and Lasers in Engineering 46 (1) (2008) 34–41.
[23] D. Asselin, H.H. Arsenault, Rotation and scale invariance with polar and log-polar coordinate transformations, Opt. Commun. 104 (4) (1994) 391–404.
[24] B.S. Reddy, B.N. Chatterji, An FFT-based technique for translation, rotation, and scale-invariant image registration, IEEE Trans. Image Process. 5 (8) (1996) 1266–1271.
[25] M. Fang, G. Hausler, Class of transforms invariant under shift, rotation, and scaling, Appl. Opt. 29 (5) (1990) 704–708.
[26] D.G. Lowe, Object recognition from local scale-invariant features, Proceedings of the Seventh IEEE International Conference on Computer Vision 2 (1999) 1150–1157.
[27] D.G. Lowe, Distinctive image features from scale-invariant keypoints, International Journal of Computer Vision 60 (2) (2004) 91–110.
[28] H.S. Kim, H. Lee, Invariant image watermark using Zernike moments, IEEE Transactions on Circuits and Systems for Video Technology 13 (8) (2003) 766–775.
[29] V. Kyrki, J. Kamarainen, H. Kälviäinen, Simple gabor feature space for invariant object recognition, Pattern Recognit. Lett. 25 (3) (2004) 311–318.