Optics and Photonics Journal, 2015, 5, 6-14
Published Online January 2015 in SciRes. http://www.scirp.org/journal/opj
http://dx.doi.org/10.4236/opj.2015.51002

Encrypted Sensing Based on Digital Holography for Fingerprint Images

Masafumi Takeda[1*], Kazuya Nakano[2], Hiroyuki Suzuki[3], Masahiro Yamaguchi[4]

[1]Graduate School of Science & Engineering, Tokyo Institute of Technology, 4259 Nagatsuta-cho, Midori-ku, Yokohama, Japan
[2]Nippon Sport Science University, 1221-1 Kamoshida-cho, Aoba-ku, Yokohama, Japan
[3]Imaging Science & Engineering Laboratory, Tokyo Institute of Technology, 4259 Nagatsuta-cho, Midori-ku, Yokohama, Japan
[4]Global Scientific Information and Computing Center, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo, Japan
Email: [*]takeda.m.ad@hotmail.com

Received 23 November 2014; accepted 5 December 2014; published 13 January 2015

Abstract

We propose a novel biometric sensing technique for personal authentication in which fingerprint images are captured using an optical encryption method. This method can reduce the risk of data theft or leakage of personal information captured by biometric sensing. This method, termed encrypted sensing, is implemented using digital holography with double random phase encoding. We demonstrate experimentally that a fingerprint image can be captured as an optically encrypted image and can be restored correctly only when the correct cipher key is used. Moreover, we investigate experimentally the verification accuracy of the decrypted images.

Keywords

Biometric Authentication, Digital Holography, Double Random Phase Encoding, Fingerprinting

1. Introduction

Recently, there has been a rise in the use of biometric authentication systems in a wide variety of secure interfaces, including computer logins, banking systems, automated teller machines, and building entrance management. Because biometric information represents important personal data, and because enrolled biometric information, unlike most personal authentication information such as passwords, cannot be altered, it is necessary to take great care to prevent leakage of these data. Correspondingly, template protection techniques

[*]Corresponding author.

How to cite this paper: Takeda, M., Nakano, K., Suzuki, H. and Yamaguchi, M. (2015) Encrypted Sensing Based on Digital Holography for Fingerprint Images. *Optics and Photonics Journal*, **5**, 6-14. http://dx.doi.org/10.4236/opj.2015.51002

for biometric authentication have been actively pursued through the development of cryptographic algorithms that protect raw biometric information obtained using a sensor while preserving high verification accuracy [1]-[4]. However, particular threats, such as side-channel attacks [5] occurring while raw biometric information is being transformed into a protected template, are becoming increasingly realistic. It is believed that threats such as these can be avoided by encrypting biometric images prior to image sensing, *i.e.*, optical encryption.

Optical encryption techniques apply optical calculation methods such as optical wave propagation oroptical phase modulation for image encryption and decryption. These techniques are advantageous not only for rapid calculations using parallel processing, but also security enhancement due to non-electronic computation methods, because there is less risk of optical information being read, as opposed to digital data in electronic devices, which are inevitably exposed to a number of security risks. Double random phase encoding (DRPE) [6] is a well-known optical encryption method that has been studied extensively for two decades. DRPE is an optical symmetric-key encryption technique in which an optical image is encrypted by multiplying two random phase masks in the spatial and Fourier or Fresnel planes. To obtain an optically-encrypted image, digital holography (DH) [7]-[10] is commonly employed. DH makes it possible to not only capture an optical wavefront as holographic data, but also to reconstruct various styles of optical wavefront computationally from the holographic data. DRPE has been implemented using DH [7] [11], whereby the random phase masks are typically inserted into the object beam path. Suchan optical system requires precise alignment; however, it is challenging to reconstruct the object image with high quality from the DH. Tajahuerce and Javidi proposed an optical encryption system for three-dimensional (3D) objects [12], whereby an encrypted image was obtained with simple alignment because only the reference beam was modulated using a random phase mask, and a non-modulated wave was used as the object beam. This optical arrangement could be implemented easily and can restore a clear object image from a DH. However, the encrypted image was not equivalent to DRPE because the object beam was not modulated by a random phase mask, which might decrease the security level of encryption. To obtain a fingerprint image for biometric authentication, both sufficient security to prevent data leakage and sufficient image quality for highly accurate recognition are required. Therefore, we propose an optical security system that is suitable for obtaining fingerprint images as optically encrypted holographic data. We term this system "encrypted sensing". In addition, we also propose an image reconstruction method through which we can obtain a clear fingerprint image from the encrypted hologram. To obtain the reconstructed image with high quality, we apply speckle reduction using multiple holograms, as well as reconstruction using a phase only mask, rather than a complex amplitude mask. We demonstrate that improved recognition accuracy is obtained by applying only a phase-only mask and speckle reduction.

The remainder of the paper is organized as follows. In the following section, a theoretical description of the proposed sensing system is given. In Section 3, experiments for obtaining encrypted fingerprint images are described, together with an investigation of the quality of the decrypted fingerprint images. Conclusions are drawn in Section 4.

2. Method

2.1. User Authentication Scheme

Figure 1 shows a schematic diagram that illustrates the concept of biometric encrypted sensing proposed here. During enrollment, biometric information (*i.e.*, a fingerprint pattern) is encrypted using the optical system within the biometric sensor, and the encrypted information is transmitted to the verification system for user authentication. This encrypted biometric information is then decrypted using a corresponding decryption key and the biometric information is stored in the biometric template database. During verification, encrypted biometric information is also captured, and it is then sent to the verification system. Subsequently, it is also decrypted in the verification system, and the biometric information and the enrolled data are verified by calculating their similarity. If both the biometric image and the encryption key are provided correctly, the user is authorized. This system makes it possible to perform two-factor authentication that will authorize users only when both biometric and the secret data are verified. The verification system, which is assumed to be a securely protected using, for example, a tamper-resistant device can be located in either a centralized server or a user device. Throughout this overall process, raw biometric information in digital form exists only in the protected verification system, and the risk of theft or leakage of biometric data is thus significantly reduced.

2.2. Encrypted Sensing Based on DRPE

In our system, optical encryption is performed via a combination of DH and DRPE. With DH, a wavefront encoding the optical information from an object wave is typically captured via interference with a reference plane wave, as shown in **Figure 2**. In ref. [12], random phase-modulated light was used as the reference wave, which is used as an encryption key. In our system, both the object wave and the reference wave are modulated using diffusers, as shown in **Figure 3**. To capture fingerprints stably, we place a total reflection prism in the middle of the object wavepath. The resulting DH is captured using a charged coupled device (CCD) image sensor, and can be expressed as follows:

$$\begin{aligned} I_O(x_1,y_1) = &\left|FsT\left[O(x_0,y_0)\exp\left\{j\varphi_1(x_0,y_0)\right\},z\right]\right|^2 + \left|R_{K_E}(x_1,y_1)\right|^2 \\ &+ FsT\left[O(x_0,y_0)\exp\left\{j\varphi_1(x_0,y_0)\right\},z\right]^* R_{K_E}(x_1,y_1) \\ &+ FsT\left[O(x_0,y_0)\exp\left\{j\varphi_1(x_0,y_0)\right\},z\right] R^*_{K_E}(x_1,y_1), \end{aligned} \tag{1}$$

where $O(x_0,y_0)$ represents the fingerprint image, $\varphi_1(x_0,y_0)$ is the phase modulation by the diffuser in the object wavepath, $R_{K_E}(x_1,y_1)$ is the complex amplitude distribution of the phase-modulated reference wave on the CCD plane, (x_0,y_0) and (x_1,y_1) are coordinates of the object and the CCD planes, and * denotes the complex conjugate. The operator $FsT[f,z]$ denotes a Fresnel transform in which f and z are the original wavefront and the propagation distance, respectively. $R_{K_E}(x_1,y_1)$ is derived as the Fresnel transform of the phase object assigned by the diffuser D2 (see **Figure 3**).

Figure 4 shows a flow chart of the Fresnel-type DRPE process. An encrypted image is obtained via two phase modulations—one in the space domain, and the other in the Fresnel domain. With the approaches described in Refs. [7] and [11], two phase masks were inserted in the object wave path for DRPE; however, with our system,

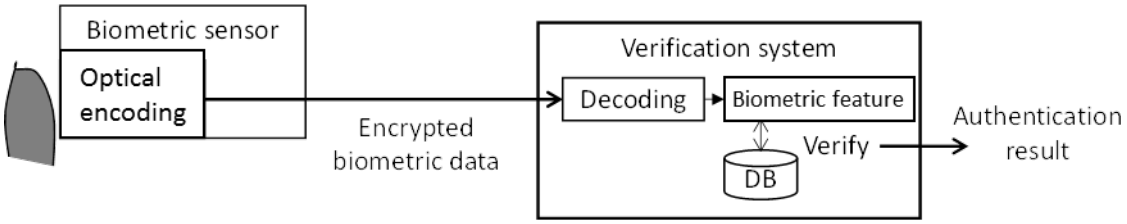


Figure 1. Concept of the encrypted biometric sensing system. The database (DB) in the verification system represents the template database for user biometric information.

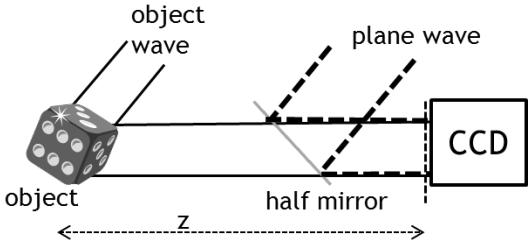


Figure 2. Typical optical system used in digital holography.

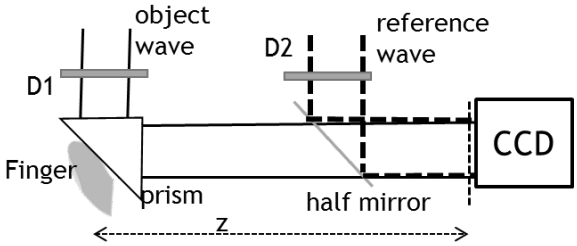


Figure 3. The optical system used with our encrypted sensing scheme. Here D1 and D2 are diffusers.

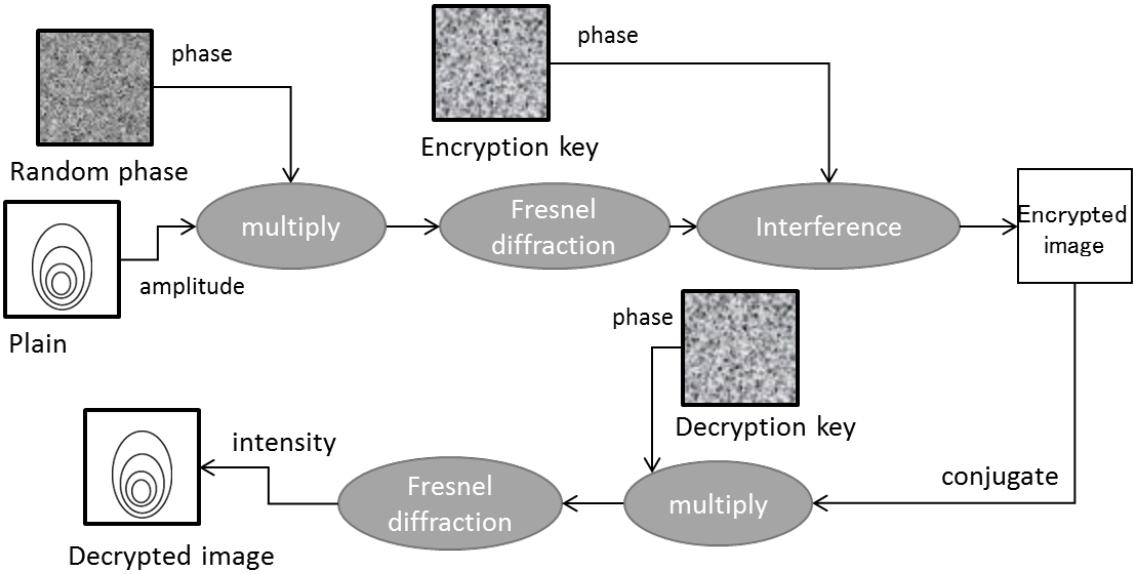


Figure 4. Schematic diagram illustrating the Fresnel-type DRPE scheme.

they are applied to the object and reference waves. The Fresnel-type DRPE uses three cipher keys: the phase distribution on the Fresnel domain, the distance of Fresnel diffraction, and the wavelength of laser; all of which that must be provided correctly to restore the plaintext image from the encrypted image. In this paper, the laser wavelength is assumed to be unique, whereas the other two components are employed as cipher keys.

Let us consider the third term of Equation (1), which is similar to DRPE. If the amplitude of $R_{K_E}(x_1, y_1)$ can be approximated to be constant, the third term of Equation (1) corresponds to the encrypted image of Fresnel-type DRPE. In this case, $R_{K_E}(x_1, y_1)$ can be expressed as

$$R_{K_E}(x_1, y_1) = A_E \exp\{jK_E(x_1, y_1)\} \tag{2}$$

where A_E is a constant amplitude and $K_E(x_1, y_1)$ is the phase distribution of the encryption key. The encrypted image $C(x_1, y_1)$ is then given by

$$\begin{aligned} C(x_1, y_1) &= FsT\left[O^*(x_0, y_0)\exp\{-j\varphi_1(x_0, y_0)\}, z\right] \cdot R_{K_E}(x_1, y_1) \\ &\cong FsT\left[O^*(x_0, y_0)\exp\{-j\varphi_1(x_0, y_0)\}, z\right] \cdot \exp\{jK_E(x_1, y_1)\} \end{aligned} \tag{3}$$

where the constant A_E has been omitted for clarity. The encrypted image $C(x_1, y_1)$ can be derived by reconstructing the first-order diffracted wave from the digital hologram captured by the CCD sensor.

For decryption, $C(x_1, y_1)$ is multiplied by the phase term of the decryption key image $K_D(x_1, y_1)$ as follows:

$$\begin{aligned} C_r(x_1, y_1) &= C(x_1, y_1)\exp\{-jK_D(x_1, y_1)\} \\ &= FsT\left[O^*(x_0, y_0)\exp\{-j\phi_1(x_0, y_0)\}, z\right]\exp\{j(K_E(x_1, y_1) - K_D(x_1, y_1))\} \end{aligned} \tag{4}$$

After this calculation, the complex amplitude image $C_r(x_1, y_1)$ is Fresnel-diffracted at a distance $\hat{z}$, and a decrypted image $\hat{O}(x_2, y_2)$ is obtained by calculating its amplitude components as follows:

$$\hat{O}(x_2, y_2) = \left|FsT\left[C_r(x_1, y_1), \hat{z}\right]\right|, \tag{5}$$

where (x_2, y_2) are coordinates on the new Fresnel transform domain. If the encryption key $K_E(x_1, y_1)$ and the decryption key $K_D(x_1, y_1)$ are identical or very similar, $C_r(x_1, y_1)$ becomes as follows:

$$C_r(x_1, y_1) \cong FsT\left[O^*(x_0, y_0)\exp\{-j\varphi_1(x_0, y_0)\}, z\right]. \tag{6}$$

If $z = -\hat{z}$, this yields the following:

$$\hat{O}(x_2, y_2) = \left| FsT\left[C_r(x_1, y_1), \hat{z} \right] \right| = \left| O(x_0, y_0) \exp\left\{ -j\varphi_1(x_0, y_0) \right\} \right| = \left| O(x_0, y_0) \right|. \quad (7)$$

From this equation, it follows that the original fingerprint image is obtained.

If the amplitude of $R_{K_E}(x_1, y_1)$ cannot be approximated to be constant, the complex amplitude of $R_{K_E}(x_1, y_1)$ must be obtained, which entails division process by its amplitude component in the decryption process, as described in Ref. [12]. This process can lead to amplification of the error of a restored fingerprint image, because some pixels of the amplitude component of $R_{K_E}(x_1, y_1)$ may be very small. In our experimental analysis below, we investigate both cases in which R_{K_E} has either a constant amplitude (our method) or a complex amplitude distribution (similar to Tajahuerce's method).

If the encryption and decryption keys differ significantly, the decrypted image becomes a random pattern. The diffraction distance *z* can be also used as a parameter to restore the correct plaintext image.

2.3. Obtaining the Decoding Key

To implement a recording system for encrypted DH, we employ off-axis holography, in contrast to the work described in Ref. [12], where they used in-line holography. To reconstruct a fingerprint image from an encrypted hologram, $R_{K_E}(x_1, y_1)$ must be obtained in advance. To implement this with off-axis holography, a Fourier transform-based method [13] was employed.

In the optical system shown in **Figure 5**, a hologram $I_{K_E}(x_1, y_1)$ is obtained via interference between $R_{K_E}(x_1, y_1)$ and a plane wave, *i.e.*,

$$I_{K_E}(x_1, y_1) = \left| A_p(x_1, y_1) \right|^2 + \left| R_{K_E}(x_1, y_1) \right|^2 + A_p(x_1, y_1)^* R_{K_E}(x_1, y_1) + A_p(x_1, y_1) R_{K_E}(x_1, y_1)^*, \quad (8)$$

Where $A_p(x_1, y_1) = \exp\left\{ -j2\pi(ax_1 + by_1) \right\}$ is a unit-amplitude plane wave, where *a* and *b* represent the angles between $R_{K_E}(x_1, y_1)$ and the plane wave. To eliminate the first and second terms of Equation (8), the intensity distribution of $\left| R_{K_E}(x_1, y_1) \right|^2$ is recorded by shielding the plane wave, and $\left| A_p(x_1, y_1) \right|^2$ (which is constant) and $\left| R_{K_E}(x_1, y_1) \right|^2$ are numerically subtracted from $I_{K_E}(x_1, y_1)$. Subsequently, the remaining terms are Fourier-transformed and we have

$$i'_E(u_1, v_1) = \delta(u_1 + a, v_1 + b) \otimes r^*_{K_E}(-u_1, -v_1) + \delta(u_1 - a, v_1 - b) \otimes r_{K_E}(u_1, v_1), \quad (9)$$

where (u_1, v_1) are coordinates on the Fourier domain, $r_{K_E}(u_1, v_1)$ is the Fourier transform of $R_{K_E}(x_1, y_1)$, and ⊗ denotes a convolution operator. If *a* and *b* are large enough to separate the two terms in Equation (9) in the spectral domain, the first and second terms do not overlap, and the first term can be extracted by shielding the second term. By calculating the inverse Fourier-transform, the complex amplitude distribution of $R_{K_E}(x_1, y_1)$ can be determined.

3. Experiments

3.1. Optical System

We carried out several experiments in which holograms of encrypted fingerprint images were captured and the original fingerprint images were then numerically restored. To do this, we constructed an optical system for acquiring holograms, as shown in **Figure 6**, which used a He-Ne laser with a wavelength of 633 nm as a light source and a CCD image sensor with 1024 × 768 pixels that was 4.65 μm × 4.65 μm. A fingerprint was placed on a total reflection prism and the reflected light was focused using two lenses (L3 and L4) to form an image on the CCD image sensor.

3.2. Image Reconstruction

As discussed in Section 2.2, the decrypted images were obtained so that $R_{K_E}(x_1, y_1)$ was either treated as a complex amplitude wave (as with Tajahuerce's method) or with the amplitude component replaced with a constant value (our method). Examples of an encrypted hologram $I_O(x_1, y_1)$ and the corresponding decrypted images are shown in **Figure 7**. **Figure 7(a)** shows that the fingerprint image is not visible in the encrypted hologram $I_O(x, y)$. **Figure 7(b)** shows adecrypted image using the correct $R_{K_E}(x_1, y_1)$ with a complex amplitude

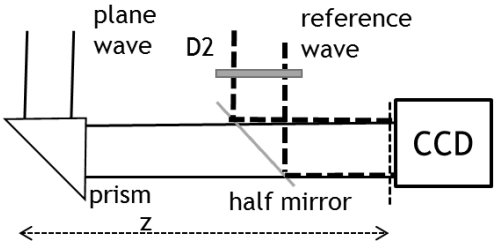


Figure 5. Optical system for obtaining decoding key.

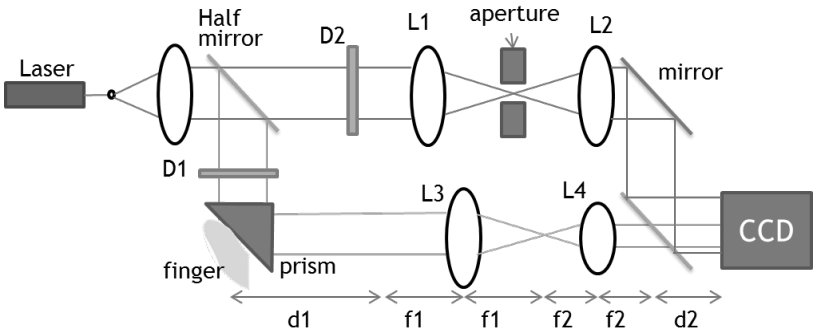
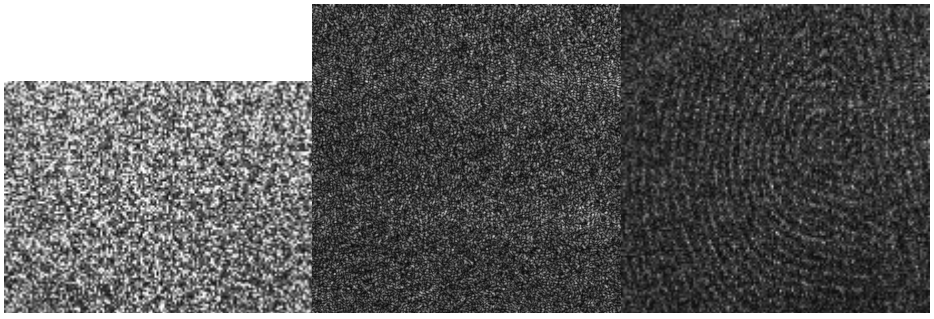
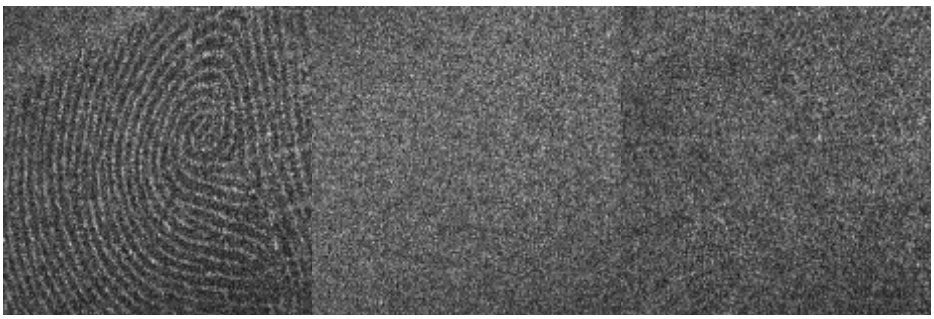


Figure 6. Schematic diagram showing the experimental optical system. Here f_1 = 0.2 m, f_2 = 0.1 m, d_1 = 0.056 m, and d_2 = 0.2 m.



(a) (b) (c)



(d) (e) (f)

Figure 7. Experimentally obtained images (a) An encrypted hologram; (b) A decrypted fingerprint image reconstructed using a complex amplitude wave; (c) A decrypted fingerprint reconstructed using a constant-amplitude wave (*i.e.*, our method); (d) A decrypted fingerprint using constant amplitude wave with speckle noise reduction; (e) A decrypted image with an incorrect decryption key, and (f) a decrypted image with an incorrect distance (244 mm).

component and the correct propagation distance. In this case, the fingerprint image is difficult to discern. **Figure 7 (c)** shows a decrypted image using the correct $R_{K_E}(x_1, y_1)$ with a constant amplitude and the correct propagation distance; the fingerprint pattern can be clearly seen in the decrypted image. These results indicate that better quality

fingerprints can be obtained by using a constant amplitude for $R_{K_E}(x_1, y_1)$ than by using a complex amplitude. However, the fingerprint pattern in **Figure 7(c)** contains significant speckle noise [14] [15], although it is sufficiently clear to recognize using the human eye. To reduce the amount of noise, we captured multiple holograms with differing speckle noise by changing the position of diffuser D1on the object beam path and summing the intensities of the decrypted images obtained from the holograms. **Figure 7(d)** shows a decrypted image obtained by summing four decrypted images, in which the restored fingerprint is more clearly visible than in **Figure 7(c)**.

Figures 7(e) shows a decrypted image using an incorrect $R_{K_E}(x_1, y_1)$, and **Figure 7(f)** shows a decrypted image using an incorrect propagation distance. In both cases, random patterns similar to stationary white noise were obtained.

3.3. Verification Accuracy

We evaluated the verification accuracy of the experimental setup described above in terms of the ability to match restored fingerprint images. Using the optical system shown in **Figure 6**, we captured 100 encrypted holograms of fingerprint images from 10 subjects (10 encrypted DHs per fingerprint). In these trials, five of the fingerprint images for each subject were used for enrollment and the others were used for testing; 250 genuine fingerprint trials (25 trials per subject) and 450 imposter trials (45 trials per subject) were carried out. Nonlinear correlation [16] was employed in these trials for pattern matching. The nonlinear correlation $n(x,y)$ between two images can be expressed as follows:

$$n(x,y) = IFT\left[\left|F_1(u,v)F_2(u,v)\right|^k \exp\left[j\left\{\varphi_{F_1}(u,v) - \varphi_{F_2}(u,v)\right\}\right]\right] \tag{10}$$

Where $F_m(u,v)$ (m = 1, 2) denotes the Fourier transform of each image, IFT denotes inverse Fourier transform operator, $\varphi_{F_m}(u,v)$ is the phase distribution of $F_m(u,v)$ and k is the degree of the applied nonlinearity. We choose k = 0.3, which was found to provide optimal discrimination between genuine and imposter cases. **Figure 8** shows the nonlinear correlation output; the correlation waveforms exhibited a sharp peak when verifying the correct fingerprint (a genuine case) with a constant amplitude $R_{K_E}(x_1, y_1)$, and with speckle noise reduction, the correlation peak became sharper. **Figure 8(d)** shows nonlinear correlation in case of verification between a correct and an incorrect decryption keys. Although both decrypted images were obtained from the same encrypted hologram, the nonlinear correlation did not exhibit a peak. **Figure 8(e)** shows the correlation waveform for imposter verification; here we also see a random pattern.

As a quantitative criterion for verification, the peak-to-side-lobe ratio (PSR) [17] was calculated as follows:

$$PSR = \frac{\text{peak} - \text{mean}}{\sigma}, \tag{11}$$

where σ denotes the standard deviation of $n(x,y)$ and *peak* and *mean* denote the peak value and spatial average of $n(x,y)$, respectively.

Using PSR as a verification score, the false rejection rate (FRR) of the genuine verification attempts and the false acceptance rate (FAR) of the imposter verification attempts were calculated. In addition, we determined a receiver operating characteristic (ROC) curve, in which each point is plotted according to the FRR (x-axis) and FAR (y-axis) for a given threshold value, as shown in **Figure 9**. The equal error rate (EER) of our method with speckle noise reduction was 12.4%, and that without speckle noise reduction was 35.0%. The EER obtained using a complex amplitude $R_{K_E}(x_1, y_1)$ was 45.0%. These results indicate that the phase-only method proposed here provides better image verification, and that the speckle noise reduction contributes significantly to the improvement in the verification accuracy.

The accuracy of our system was not better than that of image verification using a conventional sensor (i.e., unencrypted sensing). However, there are a number of possible causes of image degradation: first, we did not use a guide to fix the fingerprints; and second, we did not ask the subjects to restrain the pressure that they applied. The latter issue might cause a variation in the degree of fingerprint distortion among the images. In such cases, speckle reduction via summation may not be effective. By reducing the influence of such factors, our method has potential for further improvements in verification accuracy.

4. Conclusions

We have described an encrypted sensing system for capturing fingerprint images using digital holography and

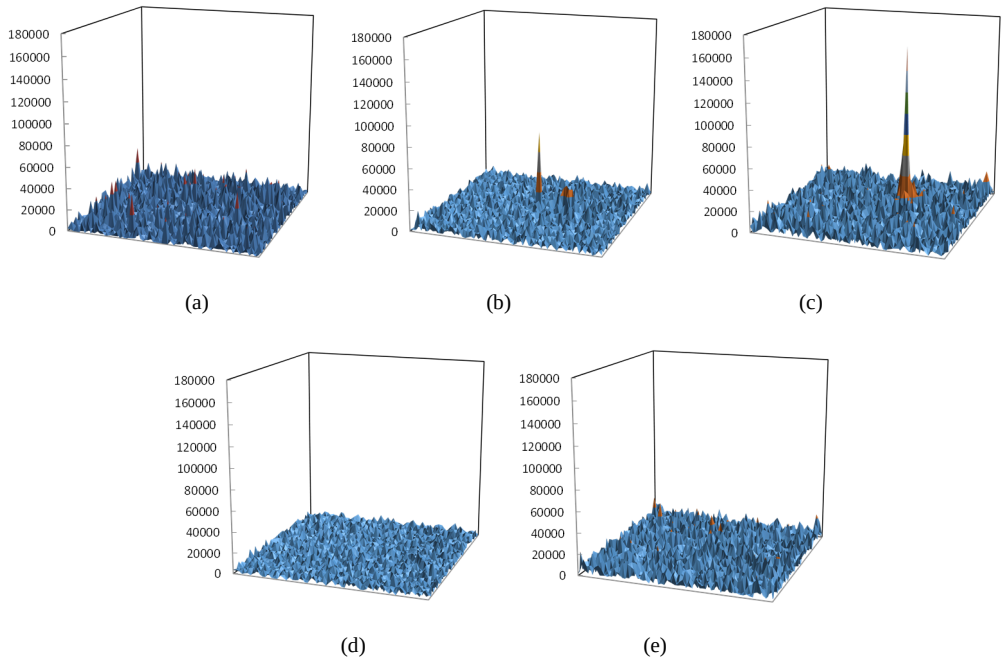


Figure 8. Nonlinear correlations. (a) Genuine (complex); (b) Genuine with speckle reduction (phase only); (c) Genuine without speckle reduction (phase only); (d) Genuine with incorrect decryption keys (phase only) and (e) Imposter (phase only).

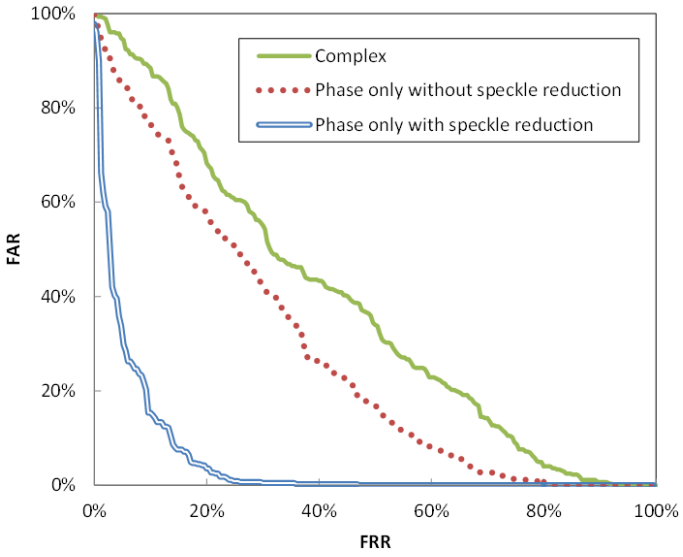


Figure 9. ROC curves.

optical encryption. We showed experimentally that a fingerprint image could be restored correctly by decrypting an encrypted hologram with the correct key and propagation distance. The quality of the restored fingerprint image could be more clearly visible than that when using a conventional method by improving the calculation method for restoring a fingerprint image from an encrypted digital hologram. The verification performance of the restored fingerprint images was investigated, and we demonstrated that our method has favorable verification accuracy.

The principal advantage of the system described here is that it can enhance the security of biometric authentication by capturing optically encrypted images rather than raw fingerprints. Combining physically unclonable functions (PUFs) [18] with our system might enable the development of very secure user authentication methods.

For example, the use of an encoding key provided by a diffuser as a PUF may provide a secure key based on the physical features of an individual object.

References

[1] Ratha, N.K., Connell, J.H. and Jain, A.K. (2001) Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Systems Journal*, **40**, 614-634. http://dx.doi.org/10.1147/sj.403.0614

[2] Uludag, U., Pankanti, S. and Jain, A.K. (2005) Fuzzy Vault for Fingerprints. *Audio- and Video-Based Biometric Person Authentication Lecture Notes in Computer Science*, **3546**, 310-319. http://dx.doi.org/10.1007/11527923_32

[3] Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. and Kumar, B.V.K.V. (1999) Biometric Encryption™. http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf

[4] Hirata, S. and Takahashi, K. (2009) Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching. *Advances in Biometrics Lecture Notes in Computer Science*, **5558**, 868-878. http://link.springer.com/chapter/10.1007%2F978-3-642-01793-3_88

[5] Clancy, T.C., Kiyavash, N. and Lin, D.J. (2003) Secure Smartcard Based Fingerprint Authentication. *Proceedings of the* 2003 *ACM SIGMM Workshop on Biometrics Methods and Applications—WBMA*, 45. https://www.cs.umd.edu/~clancy/docs/bio-wbma2003.pdf

[6] Refregier, P. and Javidi, B. (1995) Optical Image Encryption Based on Input Plane. *Optics Letters*, **20**, 767-769. http://dx.doi.org/10.1364/OL.20.000767

[7] Javidi, B. and Nomura, T. (2000) Securing Information by Use of Digital Holography. *Optics Letters*, **25**, 28-30. http://dx.doi.org/10.1364/OL.25.000028

[8] Yamaguchi, I., Yamamoto, K., Mills, G.A. and Yokota, M. (2006) Image Reconstruction Only by Phase Data in Phase-Shifting Digital Holography. *Applied Optics*, **45**, 975-983. http://dx.doi.org/10.1364/AO.45.000975

[9] Javidi, B. and Nomura, T. (2000) Three-Dimensional Object Recognition by Use of Digital Holography. *Optics Letters*, **25**, 28-30. http://dx.doi.org/10.1364/OL.25.000028

[10] Matoba, O., Nomura, T., Perez-Cabre, E., Millan, M.S. and Javidi, B. (2009) Optical Techniques for Information Security. *Proceedings of IEEE*, **97**, 1128-1148. http://dx.doi.org/10.1109/JPROC.2009.2018367

[11] Liu, S., Guo, C.L. and Sheridan, J.T. (2014) A Review of Optical Image Encryption Techniques. *Optics & Laser Technology*, **57**, 327-342. http://dx.doi.org/10.1016/j.optlastec.2013.05.023

[12] Tajahuerce, E. and Javidi, B. (2000) Encrypting Three-Dimensional Information with Digital Holography. *Applied Optics*, **39**, 6595-6601. http://dx.doi.org/10.1364/AO.39.006595

[13] Takeda, M., Ina, H. and Kobayashi, S. (1982) Fourier-Transform Method of Fringe-Pattern Analysis for Computer-Based Topography and Interferometry. *Journal of the Optical Society of America*, **72**, 156-160. http://dx.doi.org/10.1364/JOSA.72.000156

[14] Spagnolo, G.S. and Cozzella, L. (2012) Laser Speckle Decorrelation for Fingerprint Acquisition. *Journal of Optics*, **14**, 094006. http://dx.doi.org/10.1088/2040-8978/14/9/094006

[15] Utsugi, T. and Yamaguchi, M. (2013) Reduction of the Recorded Speckle Noise in Holographic 3D Printer. *Optics Express*, **21**, 662-674. http://dx.doi.org/10.1364/OE.21.000662

[16] Javidi, B. (1989) Nonlinear Joint Power Spectrum Based Optical Correlation. *Applied Optics*, **28**, 2358-2367. http://dx.doi.org/10.1364/AO.28.002358

[17] Kumar, B.V.K.V., Savvides, M., Xie, C., Venkataramani, K., Thornton, J. and Mahalanobis, A. (2004) Biometric Verification with Correlation Filters. *Applied Optics*, **43**, 391-402. http://dx.doi.org/10.1364/AO.43.000391

[18] Helinski, R., Acharyya, D. and Plusquellic, J. (2009) A Physical Unclonable Function Defined Using Power Distribution System Equivalent Resistance Variations. *Proceedings of the* 46*th Annual Design Automation Conference on ZZZ-DAC*'09, 676. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5227103&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5227103

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.