Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack

Hideaki Tashima,1,* Masafumi Takeda,2 Hiroyuki Suzuki,1 Takashi Obi,2 Masahiro Yamaguchi,1 and Nagaaki Ohyama1

1Imaging Science and Engineering Laboratory, Tokyo Institute of Technology, 4259, Nagatsutacho, Midoriku, Yokohama, Kanagawa, Japan
2Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology, 4259, Nagatsutacho, Midoriku, Yokohama, Kanagawa, Japan
*tashima@isl.titech.ac.jp

Abstract: We have shown that the application of double random phase encoding (DRPE) to biometrics enables the use of biometrics as cipher keys for binary data encryption. However, DRPE is reported to be vulnerable to known-plaintext attacks (KPAs) using a phase recovery algorithm. In this study, we investigated the vulnerability of DRPE using fingerprints as cipher keys to the KPAs. By means of computational experiments, we estimated the encryption key and restored the fingerprint image using the estimated key. Further, we propose a method for avoiding the KPA on the DRPE that employs the phase retrieval algorithm. The proposed method makes the amplitude component of the encrypted image constant in order to prevent the amplitude component of the encrypted image from being used as a clue for phase retrieval. Computational experiments showed that the proposed method not only avoids revealing the cipher key and the fingerprint but also serves as a sufficiently accurate verification system.

©2010 Optical Society of America

OCIS codes: (070.0070) Fourier optics and signal processing; (070.4560) Data processing by optical means; (200.4740) Optical processing; (060.4785) Optical security and encryption.

References and links

1. P. Refregier, and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. 20(7), 767–769 (1995).
2. B. Javidi, A. Sergent, and E. Ahouzi, “Performance of double phase encoding encryption technique using binarized encrypted images,” Opt. Eng. 37(2), 565–569 (1998).
3. B. Wang, C.-C. Sun, W.-C. Su, and A. E. T. Chiu, “Shift-tolerance property of an optical double-random phase-encoding encryption system,” Appl. Opt. 39(26), 4788–4793 (2000).
4. H. Suzuki, T. Yamaya, T. Obi, M. Yamaguchi, and N. Ohyama, “Fingerprint verification for smart card holders identification based on optical image encryption,” Jpn. J. Opt. 33, 37–44 (2004) in Japanese.
5. H. Suzuki, M. Yamaguchi, M. Yachida, N. Ohyama, H. Tashima, and T. Obi, “Experimental evaluation of fingerprint verification system based on double random phase encoding,” Opt. Express 14(5), 1755–1766 (2006).
6. H. Suzuki, H. Tashima, M. Yamaguchi, T. Obi, M. Yachida, and N. Ohyama, “File encryption software using fingerprint keys based on double random encoding,” in Frontiers in Optics, OSA Technical Digest Series (Optical Society of America, 2005), paper JW50. http://www.opticsinfobase.org/abstract.cfm?URI=FiO-2005-JW50
7. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, “Vulnerability to chosen-plaintext attacks of optical encryption schemes based on double random phase keys,” Opt. Lett. 30(13), 1644–1646 (2005).
8. X. Peng, H. Wei, and P. Zhang, “Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain,” Opt. Lett. 31(22), 3261–3263 (2006).
9. X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” Opt. Lett. 31(8), 1044–1046 (2006).
10. U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, “A known-plaintext heuristic attack on the Fourier plane encryption algorithm,” Opt. Express 14(8), 3181–3186 (2006).
11. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” Opt. Express 15(16), 10253–10265 (2007).
12. R. W. Gerchberg, and W. O. Saxton, “A practical algorithm for the determination of the phase from image and diffraction plane pictures,” Optik (Stuttg.) 35, 237–246 (1972).
1. Introduction

Double random phase encoding (DRPE), which is used to encrypt a plain image by means of random phase modulations on spatial domain and Fourier domains respectively, is a typical technique for applying optical information processing methods to information security [1–3]. DRPE is a combination of data ciphering and pattern matching; that is, the degree of restoration of the plain image reproduced in the decrypted image depends on the degree of similarity between two key images used in the encryption and decryption process. Therefore, the key image used in DRPE is allowed to include some redundancy between encryption and decryption. Biometrics information, which is difficult to be used as a cipher key on conventional cryptographic technology because of variety of acquired data, can be used as a cipher key by employing DRPE. As an application of this method, we proposed a smart card authentication system [4,5], which is a combination of fingerprint verification and conventional personal identification number (PIN) verification systems. In this system, a PIN is encoded to a bit pattern image, encrypted by a fingerprint image, and recorded as a hologram on a smart card. In addition, we proposed a file encryption system in which fingerprints are used as a key [6]; in this system, a file is encrypted using a common-key cryptosystem and the common key is encrypted by DRPE using a fingerprint as a cipher key. However, it has recently been reported that DRPE is vulnerable to certain types of attacks such as the chosen ciphertext attack, chosen plaintext attack [7,8], and known plaintext attack (KPA) [9–11]. Two types of KPAs on DRPE have been proposed: (1) estimation of the random phase key using the Gerchberg-Saxton (GS) algorithm [12,13] and (2) use of simulated annealing [10,11]. In this study, we investigate the vulnerability of DRPE to the KPA by using the GS algorithm on the DRPE process in which a fingerprint is used as a key; further, we propose a method for avoiding this attack. The effectiveness of this method is proven using computational experiments.

2. Binary data encryption using fingerprint as cipher key

2.1. Basic principle

In conventional cipher techniques, the cipher keys used in the encryption and decryption process are required to be identical. In contrast, the keys used in DRPE are not required to be identical. However, if the cipher keys are similar to some extent, then the decryption process can be successful.

In order to encrypt binary data using a fingerprint as a cipher key, we first encode the binary data into the plain image—called the bit pattern image—which represents the information of the binary data [5] (see Fig. 1 for an example of a bit pattern image). The bit pattern image used in Ref. [5], is controlled in order to ensure that the energy of the plain image remains constant for any bit patterns. The plain image is then encrypted by DRPE which uses the cipher key generated from the fingerprint. Binary data can thus be encrypted and decrypted using a fingerprint as a cipher key.

2.2. Image encryption and pattern matching

Figure 1 and Fig. 2 show the procedures of encryption and decryption by DRPE respectively. Let \( f(x, y) \) and \( r(x, y) \) denote the amplitude of the bit pattern image and the random pattern phase, respectively. The phase modulated image \( f_m(x, y) \) is expressed as follows:

\[
 f_m(x, y) = f(x, y) \exp \{jr(x, y)\}. \tag{1}
\]
Further, the Fourier transform \( F_m(u,v) \) of this image is multiplied by another random phase mask that corresponds to an encryption key image \( \exp\{jK_e(u,v)\} \). This image is generated using a fingerprint image. Subsequently, the encrypted image \( \Phi(u,v) \) is obtained as follows:

\[
\Phi(u,v) = F_m(u,v)\exp\{jK_e(u,v)\}.
\]

During decryption, the complex conjugate \( \Phi^\ast(u,v) \) of the encrypted image is multiplied by a phase mask that corresponds to a decryption key image \( \exp\{jK_d(u,v)\} \). The complex amplitude image \( F_m^\ast(u,v)\exp\{j[-K_e(u,v)+K_d(u,v)]\} \) is Fourier transformed in the following manner to produce the decrypted image \( \hat{f}_m(x_d,y_d) \):

\[
\hat{f}_m(x_d,y_d) = \Im\left[F_m^\ast(u,v)N(u,v)\right]
= f_m^\ast(x_d,y_d)*n(x_d,y_d),
\]

where \( N(u,v) = \exp\{j[-K_e(u,v)+K_d(u,v)]\} \), \( n(x_d,y_d) = \Im\left[N(u,v)\right] \), and \( \Im\left[\right] \) denotes the Fourier transform operator. When the phase component of the Fourier-transformed fingerprint image is used as the encryption and decryption key, \( n(x_d,y_d) \) approximately satisfies the following relation [4,5]:

\[
n(x_d,y_d) \approx \begin{cases} 
\delta(x_d - \alpha, y_d - \beta) & \text{(correct fingerprint)} \\
\text{random sequence} & \text{(incorrect fingerprint)}
\end{cases},
\]

where \( \delta(\ ) \) denotes the Dirac delta function and \( \alpha \) and \( \beta \) represent the shift in the fingerprint. It should be noted that \( n(x_d,y_d) \) is equivalent to a phase-only correlation (POC) between two fingerprint images. It is well known that the POC between two fingerprint images acquired from the same fingerprint exhibits a sharp peak whereas that between two different fingerprints exhibits a random pattern. When a correct fingerprint is used, the restored image \( \hat{f}_m(x_d,y_d) \) is expressed as \( f_m^\ast(x_d - \alpha, y_d - \beta) \) with the same intensity pattern as that of \( f(x,y) \). When an incorrect fingerprint is used, \( \hat{f}(x_d,y_d) \) produces a random sequence.

There are certain practical difficulties in cryptographic systems in that the fingerprint images are used as cipher keys. The fingerprint images in the encryption and decryption procedure are not completely identical because of shift, rotation, effect of the sensor noise, etc. In the case that the positions of the two fingerprints are different, the correct bit pattern image can be restored because the POC is a shift-invariant operation. However, the rotation of fingerprints is unacceptable since the POC is very sensitive to rotation. In order to solve this problem, we generate some slightly rotated fingerprint images and use all of them for decrypting the encrypted image. The image that is best decrypted is selected according to the quality of the restored binary bit pattern.
3. KPA on DRPE and method for avoiding it

3.1. KPA on DRPE

In KPA, cryptanalysts are supposed to know the encrypted image $\Phi(u,v)$ and the plain image $f(x,y)$ that is to be encrypted by DRPE. Further, with reference to Eq. (2), $\Phi(u,v)$ and $F_m(u,v)$ have the same amplitude components, expressed as follows:

$$|\Phi(u,v)| = |F_m(u,v)|.$$  \hfill (5)

Therefore, we can retrieve the phase component $r(x,y)$ of $f_m(x,y)$, which is the random phase, from $f(x,y)$ and $|\Phi(u,v)|$ by applying the GS algorithm. This algorithm involves iteration of backward and forward Fourier operations between the spatial domain and the Fourier domain. The iteration continues until the cost function that represents the level of

Fig. 1. Encryption by double random phase encoding

Fig. 2. Decryption by double random phase encoding
restoration of the plain image reaches convergence. Once the estimated random phase \( \hat{r}(x, y) \) is achieved, we can obtain the estimated encryption key \( \hat{\mathcal{K}}_E(u, v) \) as follows:

\[
\exp\left\{ j\hat{\mathcal{K}}_E(u, v) \right\} = \frac{\Phi(u, v)}{\hat{F}_m(u, v)} = \frac{\Phi(u, v)}{\Re\left[f(x, y) \exp\left\{ j\hat{r}(x, y) \right\} \right]}. \quad (6)
\]

If the estimated encryption key \( \exp\left\{ j\hat{\mathcal{K}}_E(u, v) \right\} \) is correct, the fingerprint image can be obtained by Fourier transforming \( \exp\left\{ j\hat{\mathcal{K}}_E(u, v) \right\} \).

### 3.2. Method for avoiding KPA

In this section, we propose a method for avoiding the KPA. We focused on the fact that the KPA algorithm uses the amplitude components of the plain image and encrypted image. If the amplitude component of the encrypted image could be made constant, then it would be difficult for the attackers to retrieve the encryption key and obtain the fingerprint of the user.

The phase-only encrypted image \( \Phi_p(u, v) \) can be expressed as follows:

\[
\Phi_p(u, v) = \frac{\Phi(u, v)}{\Phi(u, v)}. \quad (7)
\]

In this case, the decrypted image is described as follows:

\[
\hat{f}_p(x_d, y_d) = \Re\left[ \frac{F_m^*(u, v)}{F_m(u, v)} N(u, v) \right] = f_p(x_d, y_d) * n(x_d, y_d), \quad (8)
\]

where \( f_p(x_d, y_d) = \Re\left[ \frac{F_m^*(u, v)}{F_m(u, v)} \right] \). If \( n(x_d, y_d) \) is the Dirac delta function, then the decrypted image is the approximate plain image that is filtered with the amplitude component of the encrypted image. It is shown in Ref. [2] that when the key images are identical, then the images decrypted from the phase-only encrypted images have a low mean squared error. In the computational experiment described in the next section, we investigate whether the images decrypted from the phase-only encrypted images using fingerprint images as cipher keys have an allowable level of noise.

### 4. Experiments

#### 4.1. Vulnerability of DRPE to KPA

We conducted a computational experiment to confirm that the DRPE in which a fingerprint is used as a cipher key is vulnerable to the KPA described in section 3 and to demonstrate that the proposed phase-only method can be used to avoid the attack. We also evaluated whether it is possible to restore the fingerprint image from the estimated key and to decrypt another image that has been encrypted with the same key as the one used in KPA.

In this experiment, the fingerprint images are captured using the optical fingerprint sensor U.are.U 4000B manufactured by DigitalPersona, Inc. Each image produced by the sensor has a size of 256 \( \times \) 256 pixels in grayscale with a color depth of 8 bits per pixel.

Figure 3 shows the images used in the experiment. We generated a 256 \( \times \) 256 pixel plain image, as shown in Fig. 3(a). It was generated from the ASCII character sequence “1234ABCDEFGH” using the bit pattern encoding method described in Ref. [5]. Figure 3(d) shows a 256 \( \times \) 256 pixel image as the phase component of the Fourier transform of the
fingerprint image shown in Fig. 3(c). Here, for the purpose of improving the restoration accuracy of the plain image, we applied certain types of image processing techniques to the fingerprint image; that is, we compressed the image to a 128 × 128 pixel size, enlarged the compressed fingerprint image to a 512 × 512 pixel size by filling the area around the fingerprint pattern with zero-value pixels, and cropped the central 256 × 256 pixel area of the Fourier phase component. Figure 3(e) is the key image obtained using the above image processing techniques. Figure 3(f) shows the inverse Fourier transform of the key image; in this figure, we can observe that the shrunken fingerprint image is restored because of the effect of the image processing. Figures 3(g) and 3(h) show the amplitude and phase components of the encrypted image, respectively. These images are obtained by encrypting the plain image (Fig. 3(a)) with the key image (Fig. 3(e)). The proposed phase-only method for avoiding KPA makes the amplitude image (Fig. 3(g)) constant.

In a KPA to the conventional DRPE that uses both amplitude and phase components of the encrypted image for the GS algorithm, the attackers can access the plain image and the amplitude and phase components of the encrypted image. The random phase mask, which is multiplied with the plain image, can be estimated from the plain image and the amplitude component of the encrypted image using a phase retrieval algorithm. However, the attackers cannot use the amplitude component in the phase-only method because this component is made constant. Figure 4 shows the convergences of the cost functions to the iteration number of the phase retrieval algorithm. We employed the sum-squared error (SSE) and the POC peak value between the plain image and the decrypted image as a cost function. The SSE is defined as follows:

$$SSE = 10 \log \frac{\sum |f - f^{(m)}_m|^2}{\sum f^2}, \quad (9)$$

where $|f^{(m)}_m|$ represents the computed amplitude distribution after $n$ iterations. In the case of the conventional method that uses both amplitude and phase components, the SSE and POC peak value rapidly converge, whereas the corresponding values of the phase-only method do not converge. Figure 5 shows the POC peak value between the restored fingerprint image and the original fingerprint image in the iteration. The POC peak value was calculated by adjusting the size of the original fingerprint image to that of the restored fingerprint image. Figure 5 also shows the POC peak value between the decrypted image of another encrypted image and its corresponding plain image. In this case, the plane image multiplied with another random phase mask was encrypted with the original key and the encrypted image was subsequently decrypted with the estimated key. Figure 6 (Media 1) shows the images obtained in the KPA during the GS algorithm. In the case of the conventional DRPE, the key image and user’s fingerprint are revealed within minutes. In contrast, in the case of the proposed method that uses only the phase component of the encrypted image, the fingerprint image is not revealed although the cost functions converge and the key image is obtained using the GS algorithm. This result indicates that the estimated key in the proposed method is completely different from that in the conventional DRPE. Further, Figs. 6(c) and 6(g) show that the estimated key by the KPA in the conventional DRPE can decrypt another encrypted image successfully, whereas the one in the proposed method cannot.
Fig. 3. Images in the encryption scheme: (a) plaintext image to be encrypted; (b) random phase image to be multiplied with (a); (c) fingerprint image; (d) phase image of Fourier transform of (c); (e) key image for encryption, which is the center part of (d); (f) restored fingerprint image, which is the inverse Fourier transform of (c); (g) amplitude component of the encrypted image; and (h) phase component of the encrypted image.

Fig. 4. SSEs of the phase retrieval algorithm versus iteration (left) and POC peak between plaintext image and decrypted image of the encrypted image used in the KPA versus iteration (right).
4.2. Verification accuracy

In this section, we discuss the decryption accuracy of the phase-only method, in which the loss of amplitude information can lead to the increase in the noise level of the decrypted images. As an evaluation index of decryption accuracy, we compared the average bit error rate (BER) of the restored bit pattern from the decrypted image of the proposed phase-only method with that of the conventional method. BER is defined as follows:

\[
BER = \frac{N_{\text{err}}}{N_{\text{total}}},
\]  

Fig. 5. Recovery accuracy versus iterations in the case of the restored fingerprint image (left) and in the case of the restored plain image that is obtained by decrypting another encrypted image with the estimated key (right).

Fig. 6. (Media 1) Single frame excerpt from animation showing convergence of the KPA during the GS algorithm; images obtained after 215 iterations: (a)–(d) are for the conventional method and (e)–(h) are for the phase-only method. (a) and (e) show amplitude images obtained by the GS algorithm; (b) and (f) show revealed key images; (c) and (g) show images decrypted from another encrypted image; and (d) and (h) show fingerprint images, which are inverse Fourier transforms of (b) and (f), respectively.
where $N_{\text{error}}$ denotes the number of error bits contained in the decrypted data and $N_{\text{total}}$ denotes the total number of bits contained in the corresponding plaintext data. In order to calculate the average BER, we captured 420 fingerprint images from 42 fingers (ten images per finger and two fingers per person). An average of four images captured from the same finger is used for encryption and the others are used for decryption. In the encryption process, the rotation and shift of the fingerprint images are adjusted in order to obtain the average image. The results are shown in Table 1. The BER of the phase-only method is slightly increased but still remains comparable to that of the conventional method.

Table 1. Comparison of Bit Error Rate

| BER (%)       | Genuine | Impostor |
|---------------|---------|----------|
| Conventional Method | 5.6     | 58       |
| Phase-only Method      | 6.4     | 58       |

Examples of the decrypted images are shown in Fig. 7. This figure shows that the bit patterns of the decrypted images using the same individual’s fingerprint image are readable and those using a different individual’s fingerprint image become random patterns. It also shows that there is no significant difference between the decrypted images in the case of the conventional method and those in the case of the phase-only method.

![Fig. 7. Examples of decrypted images: (a) and (b) conventional method; (c) and (d) phase-only method; (a) and (c) using same individual’s fingerprint image; and (b) and (d) using different individual’s fingerprint image.](image)

4.3. Discussion

The experimental results in section 4.1 indicate that the conventional method for binary data encryption using fingerprints based on DRPE is vulnerable to the KPA, which uses the phase retrieval algorithm. An encryption method that is vulnerable to KPA is at a critical
disadvantage when it is applied to an authentication system through an open network like the Internet; for instance, in the case of challenge-response authentication, attackers can easily find an opportunity to access the plaintext and the corresponding encryption data. Therefore, an encryption algorithm that is vulnerable to KPA should not be employed in a biometric authentication system through the Internet even if the verification accuracy of the algorithm is sufficient. The proposed method, which not only avoids KPAs using the phase retrieval algorithm but also provides sufficient verification accuracy, can be used to realize a secure biometric authentication system through the Internet.

In our experiment, we noticed differences between the key that was estimated using the conventional DRPE and the one that was estimated using the phase-only DRPE. The former is similar to the encryption key used in the encryption procedure, whereas the latter is not so similar. Therefore, it is impossible to decrypt another encrypted image with the key estimated using the phase-only DRPE even if this image is encrypted with the same encryption key as the one used in the KPA.

Although we have only discussed the KPA using the phase retrieval algorithm in this paper, it is also important to discuss the KPA using simulated annealing. We believe that it would be difficult to estimate the correct key image by employing the proposed method because the KPA using simulated annealing also uses the amplitude of the encrypted image. We will attempt to experimentally evaluate this method in the future.

5. Conclusion

We investigated the vulnerability of DRPE using fingerprints as cipher keys to the KPA using a phase retrieval algorithm. By means of computational experiments, the encryption phase key was estimated and the fingerprint image was revealed using the estimated key. This feature of the encryption method could cause a problem if the method is used in an authentication system through the Internet. On the other hand, we showed that the phase-only DRPE, for which the amplitude component of the encrypted image is made constant, can be used to avoid the KPA using the phase retrieval algorithm. We also showed that the phase-only DRPE as well as the conventional DRPE can be used to perform decryption with an acceptable level of noise.