Image-based Multimodal Biometric Authentication Using Double Random Phase Encoding

Eman Tarek, Osama Ouda, and Ahmed Atwan
(Corresponding author: Eman Tarek)

Department of Information Technology, Faculty of Computers and Information Sciences
El Gomhouria St, Mansoura, Dakahlia Governorate 35516, Egypt
(Email: eman_tarek@mans.edu.eg)

(Received Aug. 20, 2017; revised and accepted Nov. 21, 2017)

Abstract

This paper presents an image-based multimodal biometric authentication scheme that utilizes a popular image encryption technique, known as double random phase encoding (DRPE). The proposed scheme aims at protecting biometric templates against unauthorized disclosure without deteriorating the recognition accuracy. Unlike conventional feature-based biometric authentication methods, the proposed scheme uses phase-based image matching of images captured from the employed biometric modalities; namely, palmprint and fingerprint, in order to enhance both accuracy and security of the suggested recognition system. A palmprint image is used as a secret key to encrypt a fingerprint image, captured from the same user, using DRPE. The encrypted fingerprint image can be successfully decrypted only if the phase-only-correlation between enrollment and authentication palmprint images is sufficiently high (*i.e.* the two images belonging to the same user). Then, the decrypted image is matched against a fresh fingerprint image, also captured during verification, and the overall authentication process succeeds if the matching result exceeds a predefined threshold. The experimental results illustrate the efficacy of the proposed scheme and show that it can improve the security of biometric data without deteriorating the recognition accuracy.

Keywords: Double Random Phase Encoding; Image-Based Matching; Multimodal Biometric Authentication

1 Introduction

Traditional authentication systems that rely on user-specific passwords and/or tokens are susceptible to several usability issues. For instance, passwords can be forgotten or stolen and tokens can easily be lost, shared or misplaced [3, 5, 11]. Biometric authentication systems, on the other hand, identify individuals using their physiological or behavioral traits such as iris, face, fingerprint, palmprint, signature, and voice. These traits are unique across individuals and thereby cannot be duplicated, forgotten, or lost [10,14]. Despite these inherent advantages, the widespread deployment of biometric technology has been impeded due to several reasons; the most crucial are the issues of template security and the less than desirable recognition accuracy of biometric systems [4].

These issues need to be addressed in order to enhance public acceptance of biometric technology. Compromising biometric templates leads to serious security threats during every authentication attempt since such templates, unlike passwords and tokens, cannot be revoked or reissued. As a result, several template protection schemes have been proposed over the past few years [9, 15, 16] in order to address the issue of template security. Unfortunately, such schemes cannot preserve the recognition accuracy exhibited by original (unprotected) biometric systems [20].

On the other hand, many multimodal biometric authentication schemes have been proposed in the past decade [30, 34] in order to improve recognition accuracy as well as security of biometric-based authentication systems. Obviously, chances of compromising biometric templates derived from multiple biometric modalities are small compared to chances of compromising templates generated from a single biometric modality. However, these biometric templates are stored as unprotected templates in central databases.

In this paper, we present a new multi-modal biometric authentication scheme based on the well-known image encryption technique: Double Random Phase Encoding (DRPE) [17]. The DRPE scheme benefits from the high correlation existing between phase components of encryption and decryption keys (masks) to recover the encrypted image. In the case of biometric authentication, enrollment and verification samples, belonging to the same user, can be employed as encryption and decryption keys in DRPE [22–25, 28, 31] since the Phase-Only Correlation (POC) between these samples is expected to be high enough to restore the encrypted image [6, 7]. The goal of our proposed scheme is to protect the stored biometric templates (images) using DRPE without deteriorating the recognition accuracy through utilizing two different biometric modalities; namely, fingerprint and palmprint, for authenticating individuals. That is, images acquired from one biometric modality will be used to encrypt images captured from the other modality using DRPE.

The rest of this paper is organized as follows. Section 2 provides a brief overview of both POC-based image matching and DRPE. Section 3 introduces the proposed image-based multi-modal biometric authentication scheme. Section 4 presents the experimental results and discusses the efficacy of the proposed method. Finally, Section 5 concludes the paper.

2 Preliminaries

In this section, we first give a brief overview of phase-only correlation (POC), describe a band-limited variant of POC (BLPOC), and explains how both techniques can be employed for image matching. Then, a brief description of DRPE is provided.

2.1 Phase Only Correlation (POC)

The demand for highly accurate image matching techniques is rapidly increasing in many fields, such as computer vision, image sensing and analysis, biometrics and security [1, 2, 6, 7, 21, 33]. POC-based image matching techniques, which uses the phase components in Discrete Fourier Transforms (DFTs) of images, have demonstrated their effectiveness in implementing several biometric authentication schemes [6,7]. In this subsection, we describe the basic definition and mathematical formula of the POC function used for image matching.

Consider two $M \times N$ images $f_1(x, y)$ and $f_2(x, y)$ with index ranges $x = -M_0, \cdots, M_0(M_0 > 0)$ and $y = -N_0, \cdots, N_0(N_0 > 0)$, and $M = 2M_0 + 1$ and $N = 2N_0 + 1$ for mathematical simplicity. Let $F_1(u, v)$ and $F_2(u, v)$ denote the 2D discrete Fourier transforms of $f_1(x, y)$ and $f_2(x, y)$ in which $u = -M_0, \cdots, M_0$ and $v = -N_0, \cdots, N_0$, given by:

$$\begin{aligned} F_1(u,v) &= \mathrm{DFT}[f_1(x,y)] \\ &= \sum_{m=-M_0}^{M_0} \sum_{n=-N_0}^{N_0} f_1(x,y) e^{-j2\pi(\frac{mu}{M}+\frac{nv}{N})} \\ &= A_{F1}(u,v) e^{j\theta_{F_1}(u,v)}, \end{aligned} \quad (1)$$

$$\begin{aligned} F_2(u,v) &= \mathrm{DFT}[f_2(x,y)] \\ &= \sum_{m=-M_0}^{M_0} \sum_{n=-N_0}^{N_0} f_2(x,y) e^{-j2\pi(\frac{mu}{M}+\frac{nv}{N})} \\ &= A_{F2}(u,v) e^{j\theta_{F_2}(u,v)}, \end{aligned} \quad (2)$$

where DFT[·] denotes the 2D discrete Fourier transform, $A_{F1}(u, v)$ and $A_{F2}(u, v)$ are the amplitude components, and $e^{j\theta_{F_1}(u,v)}$ and $e^{j\theta_{F_2}(u,v)}$ are the phase components of the two images. The cross phase spectrum $R_{F_1F_2}(u, v)$ between $F_1(u, v)$ and $F_2(u, v)$ is given by:

$$\begin{aligned} R_{F_1F_2}(u,v) &= \frac{F_1(u,v)\overline{F_2(u,v)}}{|F_1(u,v)\overline{F_2(u,v)}|} \\ &= e^{j\{\theta_{F_1}(u,v)-\theta_{F_2}(u,v)\}} \\ &= e^{j\theta(u,v)}, \end{aligned} \quad (3)$$

where $\overline{F_2(u,v)}$ is the complex conjugate of $F_2(u, v)$ and $e^{j\theta(u,v)}$ is the phase difference of $F_1(u, v)$ and $F_2(u, v)$. Then POC function is the 2D inverse Fourier transform of $R_{F_1F_2}(u, v)$:

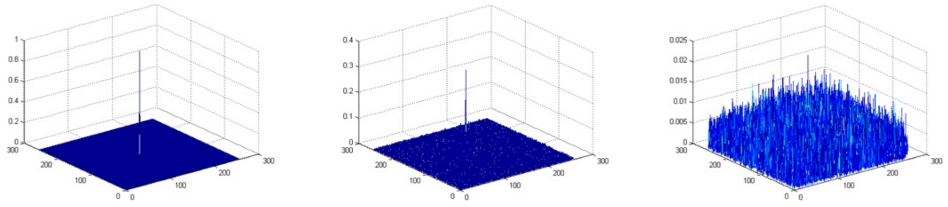
$$P_{f_1f_2}(x,y) = \frac{1}{MN} \sum_u \sum_v R_{F_1F_2}(u,v) e^{j2\pi(\frac{ux}{M}+\frac{vy}{N})}. \quad (4)$$

If there is a similarity between two matched images, their POC function gives a distinct sharp peak. If not, a random noise with lower peaks are observed. The height of the correlation peak is a good similarity measure for image matching and the location of the peak is also a good measure for translational displacement between two images. Figure 1 illustrates an example of fingerprint image matching using POC function and their corresponding POC similarity.

2.2 Band-Limited Phase Only Correlation (BLPOC)

In POC-based image matching, all the phase components of the 2D-DFT of given images are involved. However, some phase components in high frequency domain are not reliable and can be prone to error. It has been observed that the height of the correlation peak, resulting from matching similar images, is significantly reduced if the high frequency components are taken into account in the matching process [6, 7, 21, 33]. Ito *et al.* [6] proposed the Band-Limited Phase-Only Correlation (BLPOC) function that eliminates meaningless phase components in high frequency region and only uses the effective frequency band of matched images to improve the performance of image matching.

Figure 2 illustrates a fingerprint image and its corresponding amplitude components of the 2D-DFT. The frequency components that are higher than this dominant frequency band have very low power, and hence thier phase components are not reliable. Assuming that the ranges of an effective frequency band of given matched images are defined by $u = -U_0, \cdots, U_0(U_0 > 0)$, $v = -V_0, \cdots, V_0(V_0 > 0)$, $L_1 = 2U_0 + 1$, and $L_2 = 2V_0 + 1$, where L_1 and L_2 define the effective band size, the BLPOC function is defined as:



(a) POC of identical images (b) POC of similar images (c) POC of different images

Figure 1: Fingerprint image matching using POC function

$$P^{U_0V_0}_{f_1f_2}(x,y) = \frac{1}{L_1L_2}\sum_{u=-U_0}^{U_0}\sum_{v=-V_0}^{V_0} R_{F_1F_2}(u,v)e^{j2\pi(\frac{xu}{L_1}+\frac{yv}{L_2})}. \quad (5)$$

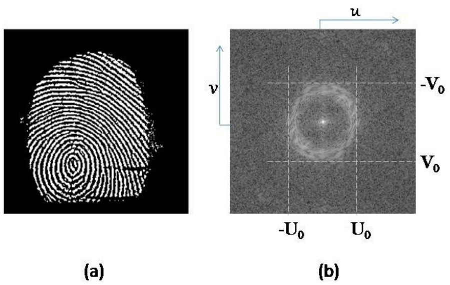


Figure 2: Fingerprint image with its corresponding amplitude components of the 2D-DFT

Figure 3 shows an example of palmprint image matching, where the figure compares the original POC and the BLPOC functions. The BLPOC provides a higher correlation peak than that of the original POC. Thus, the BLPOC function exhibits a much higher discrimination capability than the original POC function.

2.3 Double Random Phase Encoding (DRPE) Scheme

The DRPE scheme is an optical image encryption technique proposed by Refergier and Javidi [17]. The idea of this scheme is to encode the original image into a complex stationary white noise, employing two statistically independent random phase masks; namely, $RPM1$ and $RPM2$, in the spatial and Fourier domains respectively. The DRPE scheme can be implemented optically or digitally. An optical setup, also called $4f$ setup, which is commonly used to optically implement DRPE is illustrated in Figure 4. This setup consists of two cascaded optical Fourier transformation lenses separated by two focal lengths, with one focal length outside the lens with each of the input and output image planes, and hence the total is four focal lengths $4f$.

The overall process of the DRPE scheme can be described as follows. Let $f(x,y)$ denotes the input image to be encoded and $\psi(x,y)$ denotes the encrypted image. Let $n(x,y)$ and $m(u,v)$ are two independently random noisy functions uniformly distributed over the interval $[0,1]$ where(x,y) denotes the spatial domain coordinates and(u,v) denotes the Fourier domain coordinates.

As illustrated in Figure 4(a), two random phase masks are used in the encryption process; namely,
$RPM1 = exp[j2\pi n(x,y)]$ and $RPM2 = exp[j2\pi m(u,v)]$.

The encrypted image $\psi(x,y)$ is obtained by multiplying the input image $f(x,y)$ with $RPM1$ in the spatial domain and then convolving the resulting image with the function $h(x,y)$. That is, the encrypted image is given by:

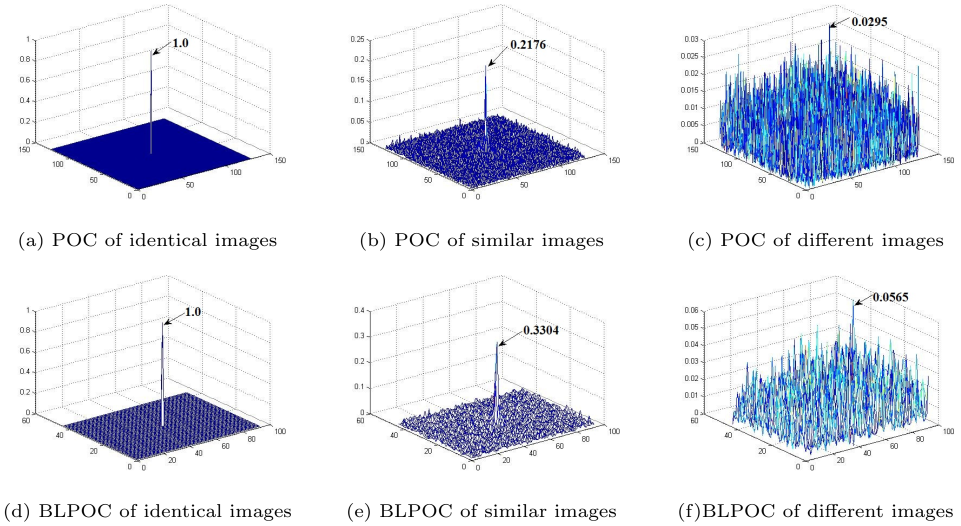
$$\psi(x,y) = \{f(x,y)exp[j2\pi n(x,y)]\} * h(x,y), \quad (6)$$

where $h(x,y)$ is the impulse response of $h(u,v) = exp[j2\pi m(u,v)]$ and $*$ denotes the convolution operation. To recover back (decrypt) the original image, as shown in Figure 4(b), the encrypted image $\psi(x,y)$ is Fourier transformed and multiplied with the complex conjugate of the $RPM2$ used in the frequency domain $exp[-j2\pi m(u,v)]$, and then inverse Fourier transformed to produce the output $f(x,y)exp[j2\pi n(x,y)]$ whose absolute value is the decrypted image $f(x,y)$ since $f(x,y)$ is a positive image. The decryption process can be expressed as:

$$\begin{aligned} & f(x,y)exp[j2\pi n(x,y)] \\ = \ & IFT\{FT\{\psi(x,y)\}exp[-j2\pi m(v,w)]\}, \quad (7) \end{aligned}$$

where $FT[\cdot]$ and $IFT[\cdot]$ donate the Fourier Transform and the Inverse Fourier Transform, respectively.

The statistical analysis of DRPE [18, 27] proved its efficiency as a secure image protection scheme because of its efficient reconstruction of the original image and its robustness against blind deconvolution. Moreover, it has been shown that it is difficult to recover the encoded image without knowing the employed random phase mask [18]. Due to these attractive advantages, several schemes based on the main idea of DRPE have been proposed [8, 12, 29]. In addition, many security systems are devised to merge DRPE with other methods such as holographic methods [26, 32], watermarking [19], information hiding [13] and Biometric authentication [22–25, 28, 31].



(a) POC of identical images (b) POC of similar images (c) POC of different images

(d) BLPOC of identical images (e) BLPOC of similar images (f)BLPOC of different images

Figure 3: Example of palmprint image matching using the original POC and the BLPOC

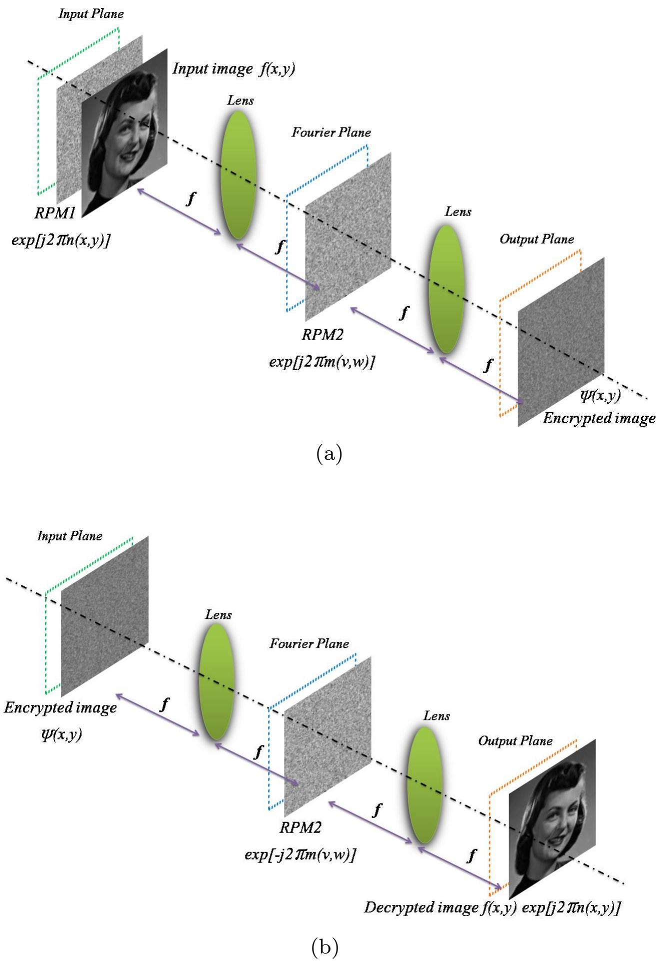
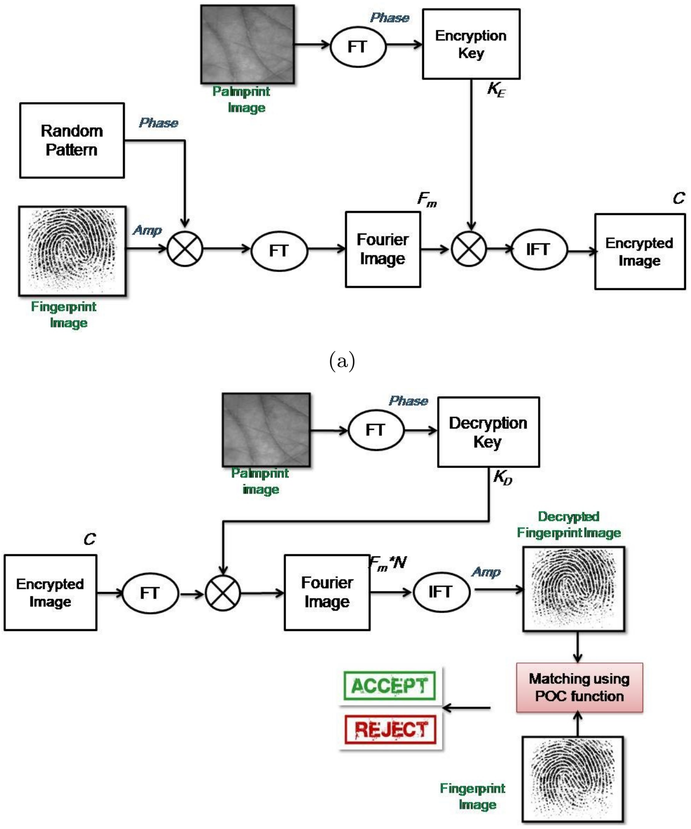


Figure 4: Optical implementation of the DRPE scheme (a) Encryption process and (b) Decryption process

3 Proposed Scheme

This paper presents a secure multimodal biometric authentication scheme that uses a palmprint image as a secret key to encrypt a fingerprint image, both belonging to the same individual, using DRPE. In DRPE, it is possible to recover the original image even if the two encryption and decryption keys are not identical. In other words, the restoration accuracy of decrypted image relies on the similarity between two keys. Therefore, the DRPE is appropriate as encryption method for fingerprint image when uses the palmprint image as a cipher key. Figure 5 illustrates the main idea behind the proposed multi-modal authentication scheme. During the enrollment stage, DRPE is employed to encrypt a fingerprint image, taken from the fingertip of the user being enrolled, using a key represented by the phase components of the 2D-DFT of a palmprint image captured from the palm of the same user. The encrypted random image (complex amplitude) is safely stored as a protected template in a central database.

At verification, the encrypted fingerprint image can be successfully decrypted only if the phase only correlation between enrollment and authentication palmprint images is sufficiently high *i.e.* the two images belonging to the same user). Then, the decrypted image is matched against a fresh fingerprint image, also captured during verification, using POC-based image matching and the overall authentication process succeeds if the matching result, of the fingerprint images, exceeds a predefined threshold. This improves the security of the overall authentication system since the user must present genuine fingerprint and palmprint images in order to successfully authenticate himself to the system. In other words, if some adversary managed to present a true image of one of the two modalities to the authentication system, he/she would not be able to pass the authentication test successfully unless he present a genuine sample of the other



(a)

(b)

Figure 5: Image-based multimodal biometric authentication using DRPE (a) Encryption process and (b) Decryption process

modality.

3.1 Encryption

Let $F_E(x,y)$ and $P_E(x,y)$ denote fingerprint and palmprint images, captured during enrollment (encryption). At enrollment, the amplitude of $F_E(x,y)$ is multiplied by the first phase mask extracted from a random pattern $R(x,y)$ to obtain a phase modulated image $F_{Em}(x,y)$ as follows:

$$F_{Em}(x,y) = F_E(x,y)exp[jR(x,y)]. \qquad (8)$$

The obtained phase modulated image, $F_{Em}(x,y)$, is then transformed into the frequency domain using the 2D-DFT and the resulting coefficients matrix, $F_{Em}(u,v)$, is multiplied by the second phase mask $exp[jK_E(u,v)]$, that represents the phase components of 2D-DFT of the user's palmprint image $P_E(x,y)$ (encryption key) and is given by:

$$\begin{aligned} P_E(u,v) &= FT[P_E(x,y)] \\ &= A_E(u,v)exp[jPh_E(u,v)], \end{aligned} \qquad (9)$$

where $A_E(u,v)$ is the amplitude components and $Ph_E(u,v)$ is the phase components of the 2D-DFT of the palmprint image. That is, using $K_E(u,v) = Ph_E(u,v)$, the encrypted image $C(x,y)$ is obtained as a complex amplitude random image expressed as follows:

$$C(x,y) = IFT[F_{Em}(u,v)exp[jK_E(u,v)]]. \qquad (10)$$

3.2 Decryption

Let $F_D(x,y)$ and $P_D(x,y)$ denote fingerprint and palmprint images, captured during verification (decryption). To decrypt, the complex conjugate of encrypted image, $C^*(u,v) = F^*_{Em}(u,v)exp[-jK_E(u,v)]$, is multiplied by the phase mask (Decryption Key), $exp[jK_D(u,v)]$, extracted from a fresh palmprint image $P_D(x,y)$, captured during verification as follows:

$$\begin{aligned} & C^*(u,v)exp[jK_D(u,v)] \\ = \; & F^*_{Em}(u,v)exp\{j[-K_E(u,v)+K_D(u,v)]\}, \end{aligned} \qquad (11)$$

where the image $K_D(u,v)$ represents the phase components, $Ph_D(u,v)$, of the palmprint decryption image $P_D(x,y)$. That is,

$$\begin{aligned} P_D(u,v) &= FT[P_D(x,y)] \\ &= A_D(u,v)exp[jPh_D(u,v)]. \end{aligned} \qquad (12)$$

Obviously, the inverse Fourier transform of the obtained result releases the decrypted image as follows:

$$\begin{aligned} & F_r(x_d,y_d) \\ & = IFT[F^*_{Em}(u,v)exp\{j[-K_E(u,v)+K_D(u,v)]\}] \\ & = F^*_{Em}(x,y) * n(x_d,y_d), \end{aligned} \qquad (13)$$

where $*$ denotes the convolution and $n(x_d,y_d) = FT[exp\{j[-K_E(u,v)+K_D(u,v)]\}]$ represents the phase only correlation(POC) between enrollment and authentication palmprint images.That is, $n(x_d, y_d)$ approximately satisfies the following relation

$$n(x_d, y_d) \cong \begin{cases} \delta(x_d - \alpha, y_d - \beta)(geniunepalmprint) \\ random\ sequence(imposterpalmprint), \end{cases}$$

where $\delta()$ denotes the Dirac delta function and α and β represent the shift between enrollment and authentication palmprint images. When a correct palmprint is used, the restored image $F_r(x_d, y_d)$ is expressed as $F^*_{Em}(x - \alpha, y - \beta)$ with the same intensity pattern as that of $F_E(x, y)$. When an incorrect palmprint is used, $F_r(x_d, y_d)$ produces a random image, which is the convolution of$F_{Em}(x, y)$ and a random sequence.

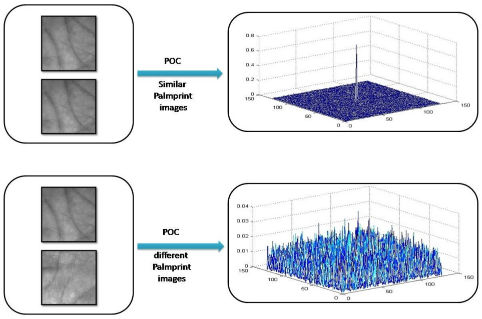


Figure 6: Palmprint image matching using POC

Apparently, the result of the decryption process in DRPE equal to the result of the convolution between enrollment fingerprint image and the phase only correlation (POC) between enrollment and authentication palmprint images. As illustrated in Figure 6, if the two palmprint images are belonging to the same user, the POC exhibits a distinct sharp peak. Otherwise, it exhibits a random noise. Then, the encrypted fingerprint image can be successfully decrypted only if the phase only correlation between the two palmprint images is sufficiently high.

3.3 POC-based Image Matching

After decryption, the decrypted image is matched against a fresh fingerprint image $F_D(x, y)$, captured during verification, using POC-based image matching method to decide the acceptance or the rejection of an individual based on a predefined threshold. The POC-based method uses the phase components of the Fourier transformed fingerprint images for effective image matching [6]. As discussed earlier, POC-based image matching has proven its efficiency even for low quality fingerprint images [6, 7] as illustrated eariler in Figure 1. An example of POC-based fingerprint image matching after geniune and imposter decryption is illustrated in Figure 7. Figure 7 (a) illustrates geniune fingerprint image, captured during verification, matched against (b) the correctly decrypted fingerprint image and (c) shows the POC similarity between matched image. Figure 7 (d) illustrates imposter fingerprint image, captured during verification, matched against (e) randomly decrypted image and (f) shows the POC similarity between matched image.

4 Experimental Results

In this section, we describe a set of experiments that have been carried out to evaluate the verification accuracy of our proposed encoding method and to confirm the randomness of images decrypted using an imposter key.

4.1 Experimental Setup

All experiments have been implemented using Matlab R2011a on a $core^{TM}$ 2 Duo 2 GHz processor with 2GB RAM. We used CASIA palmprint image dataset with three different fingerprint image datasets to check the robustness of the proposed method against shift and rotation variations in the fingerprint images and to compare its performance with the existing fingerprint verification method that is also based on the DRPE scheme [22–25, 28]:

1) *The 1st fingerprint dataset.* This dataset was employed to test the robustness of methods proposed in [22, 25, 28]. It contains 8 experimental subjects; each contributes with 6 fingerprint images captured using a capacitive fingerprint sensor developed by NTT Electronics Corporation [25]. This dataset has a good quality fingerprint images whose shift and rotation are aligned.

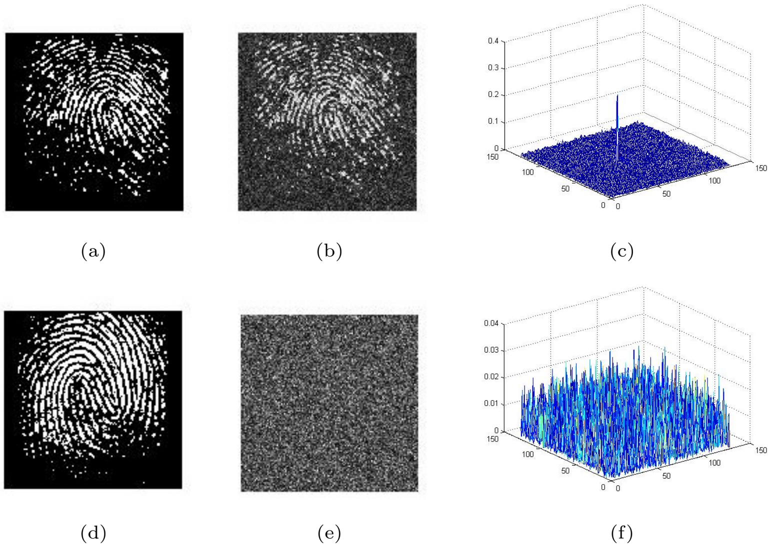
2) *The 2nd fingerprint image dataset.* This dataset contains 210 fingerprint images captured from 21 experimental subjects (10 fingerprint images per person) [24]. These fingerprint images are collected with some shift change.

3) *The 3rd fingerprint image dataset.* The popular CASIA fingerprint image database (ver. 5.0). Images in this dataset have various levels of shift and rotation changes.

For each individual, one fingerprint image and one palmprint image are used for enrollment (encryption) and the others are used for verification (decryption). Each fingerprint and palmprint images are originally 8 bit gray-level BMP files with palmprint image resolution 128*128 and with fingerprint image resolution 256*256 in the 1st and the 2nd datasets but 356 x 328 in the 3rd dataset, which is reduced to 128*128 in the spatial domain and encoded as binary images to be encrypted with the secret key generated from the palmprint image. The verification accuracy is then evaluated under genuine and imposter decryption.

4.2 Robustness of Decryption Process

In this section, we evaluate the robustness of the proposed scheme under geniune and imposter decryption.



(a) (b) (c)

(d) (e) (f)

Figure 7: Example of POC-based fingerprint image matching after decryption in the proposed scheme

Figure 8 shows an example of a fingerprint image for enrollment, a palmprint image used as a secret key for encryption, captured from the same user and the encrypted random image which is safely stored as a protected template in a central database for verification.

At verification (Decryption and POC-based image matching), the encrypted fingerprint image can be successfully decrypted only if the same user's palmprint image is used as a secret key for decryption. then, the decrypted image is matched against a fresh fingerprint image, also captured during verification, using POC. To test the effectiveness of the proposed method in improving the security of the overall authentication system since the user must present genuine fingerprint and palmprint images in order to successfully authenticate himself to the system. As illustrated in Figure 9, we implemented and tested all possible combinations of fingerprint and palmprint images,captured during verification:genuine palmprint for decryption with genuine fingerprint for poc-matching,genuine palmprint for decryption with imposter fingerprint for poc-matching,imposter palmprint for decryption with genuine fingerprint for poc-matching, and imposter palmprint for decryption with imposter fingerprint for poc-matching.

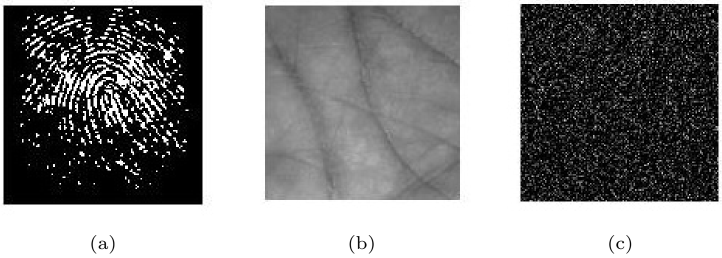
1) *Decryption with geniune palmprint image.* The encrypted fingerprint image can be successfully decrypted only if the same user's palmprint image is used as a secret key for decryption. Figure 9 (a) and (f) show the encrypted image, Figure 9 (b) and (g) show a palmprint image captured from the same user,used as a decryption key, and Figure 9 (c) and (h) the correctly decrypted fingerprint image.

2) *Decryption with imposter palmprint image.* Figure 9 (k) and (p) show the encrypted image, Figure 9 (l) and (q) show a palmprint image captured from different user,used as a decryption key, and (m) and (r) the randomly decrypted image.

As a result, the proposed scheme has proven its robustness against imposter decryption since the imposter-decrypted image has high degree of randomness. Whereas the encrypted fingerprint image can be successfully reconstructed only if the POC between enrollment and verification palmprint images is sufficiently high (*i.e.* the two images belonging to the same user), otherwise, the encrypted fingerprint image becomes a random image.

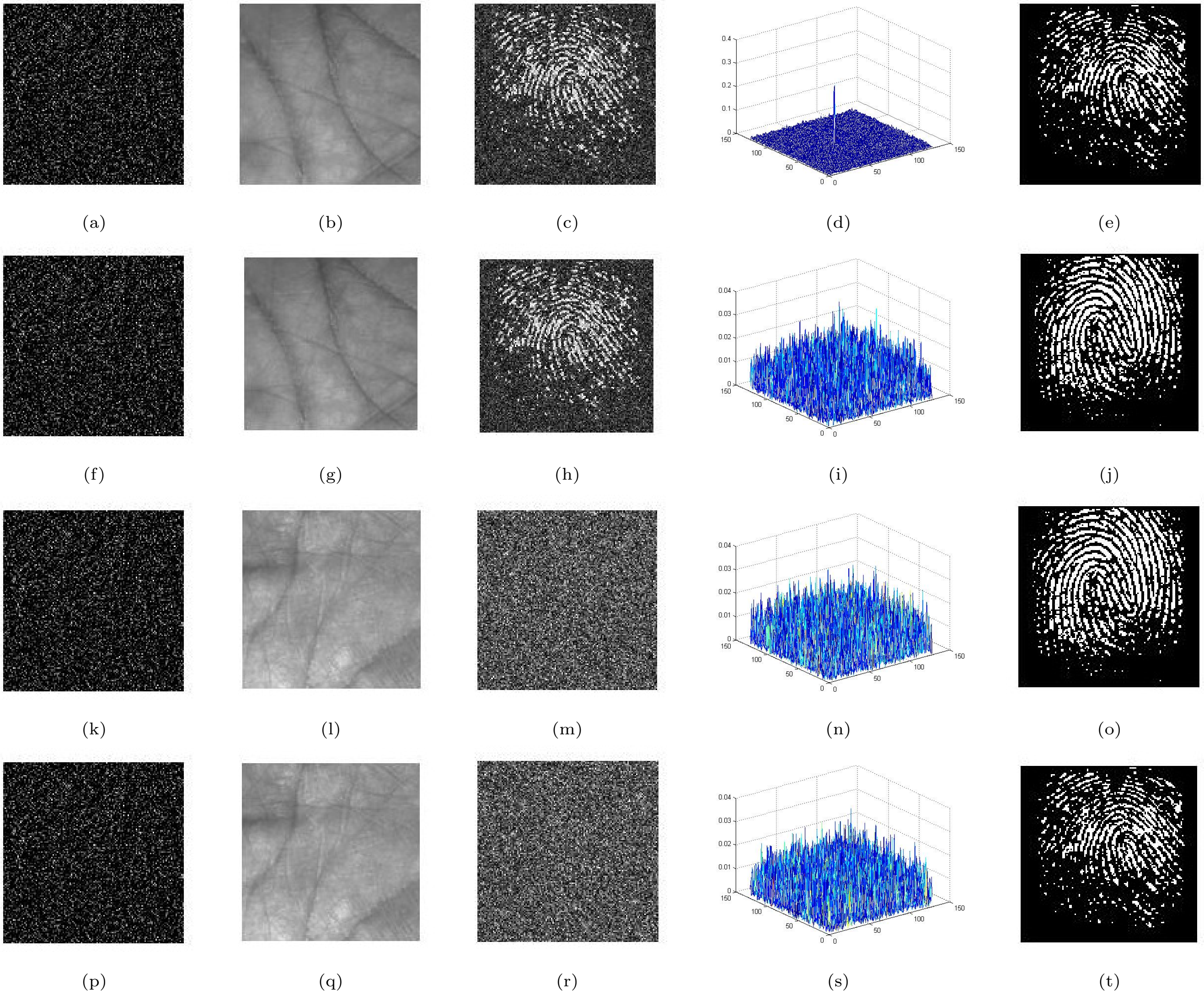
4.3 Matching Score Calculation

After decryption, the decrypted image is matched against a fresh fingerprint image, also captured during verification, using POC-based image matching function to calculate the matching score between matched images and the overall authentication process succeeds only if the matching result exceeds a predefined threshold. The height of correlation peak in POC function is a good similarity measure to calculate matching scores between matched images. Figure 9 also illustrates the matching scores of the four different decryption cases using POC function. Figure 9 (c) shows the correctly decrypted fingerprint image that matched against a geniune fingerprint image shown in Figure 9 (e) and Figure 9 (d) illustrates the poc similarity as a distinct sharp peak. Figure 9 (h) shows the correctly decrypted fingerprint image that matched against an imposter fingerprint image shown in Figure 9 (j) and Figurer 9 (i) illustrates the poc similarity as a random noise with lower peaks. Figure 9 (m) shows the randomly decrypted image that matched against an imposter fingerprint image shown in Figure 9 (o) and Figure 9 (n) illustratws the poc similarity as a random noise with lower peaks.Figure 9 (r) shows the randomly decrypted image that matched against a genuine fingerprint image shown in Figure 9 (t) and Figure 9 (s) illustrates the poc similarity as a random noise with lower peaks.



(a) (b) (c)

Figure 8: Examples of resultant images in Encryption process. (a) fingerprint image for enrollment, (b) palmprint image (encryption key) and (c) the encrypted image



(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

(k) (l) (m) (n) (o)

(p) (q) (r) (s) (t)

Figure 9: Examples of resultant images, It is confirmed that the fingerprint image is reconstructed correctly using same individual's palmprint image for decryption, and nothing appears using different individual's palmprint image for decryption, (a) the encrypted image, (b) the same individual's palmprint image for decryption, (c) the correctly decrypted fingerprint image using (b), (d) POC similarity between (c) and (e), (e) the same individual's fingerprint image for verification, (f) the encrypted omage, (g) the same individual's palmprint image for decryption, (h) the correctly decrypted fingerprint image using (g), (i) POC similarity between (h) and (j), (j) different individual's fingerprint image for verification, (k) the encrypted image, (l) different individual's palmprint image for decryption, (m) the randomly decrypted image using (l), (n) POC similarity between (m) and (o), (o) different individual's fingerprint image for verification, (p) the encrypted image, (q) different individual's palmprint image for decryption, (r) the randomly decrypted image using (q), (s) POC similarity between (r) and (t), (t) the same individual's fingerprint image for verification.

As a result, the proposed method increases the system security since the user must present geniune fingerprint and palmprint images in order to successfully authenticate himself to the system. In other words, if some adversary manages to present a true image of one of the two modalities, he would not be able to pass the authentication unless he present a true sample of the other modality.

Since the BLPOC proves its effeiciency than POC by providing much higher correlation peaks.We implemented the proposed method using either POC and BLPOC to calculate the matching scores and evaluate verification accuracy of the proposed method in either case (POC and BLPOC). Figure 10 illustrates the matching score calculations of the four different decryption cases found in Figure 9 using POC and BLPOC matching functions.

4.4 Verification Accuracy

The performance of our proposed method is measured by using the false reject rate (FRR) and the false accept rate (FAR) criteria that calculated by:

$$FAR = \frac{N_{FN}}{N_S}$$

$$FRR = \frac{N_{FP}}{N_S}$$

Where N_{FN} is the number of the false negative trails, N_{FP} is the number of the false positive trails and N_S is the total number of trails in the experiment.

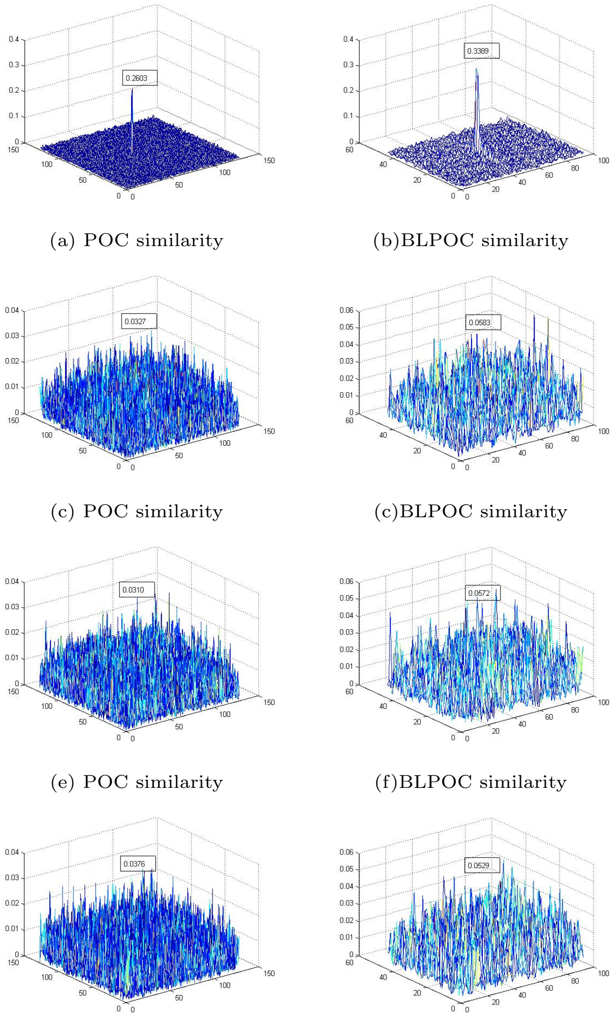
To test the efficacy of our proposed method, we implemented it using the same fingerprint image datasets of [22–25, 28] (1st and 2nd Databases) to make a comparison with the only existing fingerprint verification method that also based on DRPE scheme [22–25, 28]. The results in Table 1, shows that the verification accuracy of the proposed encoding method outperforms the existing fingerprint verification method also based on DRPE [22–25] by improving the little high FRR while keeping the FAR enough low, especially with the BLPOC matching function besides ensuring the security of biometric data without deteriorating the recognition accuracy by employing a multimodal system and also using POC image matching method that proved its effectiveness in low quality biometric images [1, 2, 6, 7, 21, 33] since it is highly robust against noise, image shift and brigthnes change. So it is very appropriate for matching decrypted fingerprint images that represent enrollment fingerprint images with some noise.

We also implemented the unimodal POC-based fingerprint matching [6], the unimodal POC-based palmprint matching [7] and POC-based multimodal fingerprint and palmprint score level fusion methods to make a comparison between them and our proposed multimodal encoding method. As illustrated in Table 1, we used the 1st and 2nd fingerprint image Datasets to check the effectiveness of using a mix of fingerprint and palmprint images for a secure template in our proposed method (POC and BLPOC) with POC-based fingerprint matching and POC-based palmprint matching. With the 1st dataset, we conduct 40 genuine trails and 280 imposter trails for all possible combinations and conduct 189 genuine trails and 3780 imposter trails for all possible combinations with the 2nd dataset. Table 1 shows the verification accuracy for each method using the two datasets.

From experimental results in Table 1, we can observe that the FRR of our proposed encoding method that secure a fingerprint image by a key extracted from a palmprint image is little high compared to the FRR of POC-based fingerprint matching because the restoration accuracy of the decrypted fingerprint image is related to the similarity between enrollment and authentication palmprint images, so that the encrypted fingerprint image can be successfully decrypted only if the phase-only-correlation between enrollment and authentication palmprint images is sufficiently high and hence the decrypted fingerprint image is similar, not exact to the enrolled fingerprint image. And hence this little high FRR can be acceptable specially with improving the security of biometric data by using DRPE and a multimodal system. Despite, the little FRR of POC-based multimodal score fusion that insecurely stores the enrollment fingerprint and palmprint images for verification, our proposed method can safely stores the enrollment fingerprint and palmprint images as a mix template for a secure verification.

We also tested our proposed method with three different fingerprint image datasets; using the same number of subjects for each dataset to check the robustness of the proposed method against shift and rotation variation in fingerprint images. We conduct 32 genuine trails and 224 imposter trails for all possible combinations in each dataset. Table 2 illustrated the verification accuracy of the proposed method for each dataset.

From experimental results in Table 2, the proposed method is based on POC image matching, which is shift invariant method. When authentication fingerprint image shifted from enrollment one, the correlation peak is shifted with the same translational displacement between two fingerprint images but the value of the correlation peak is not influenced by shift change. And thus the probability of accurate verification cannot influence with respect to image shift change. POC, on the other hand, is very sensitive to image rotation. So, image rotation cant be acceptable because the verification accuracy decreases remarkably and some improvements are required to achieve high tolerance for a variety of fingerprint images. Figure 11 shows the ROC curves for the experimental results from Tables 1 and 2.



(a) POC similarity

(b)BLPOC similarity

(c) POC similarity

(c)BLPOC similarity

(e) POC similarity

(f)BLPOC similarity

(g) POC similarity

(h)BLPOC similarity

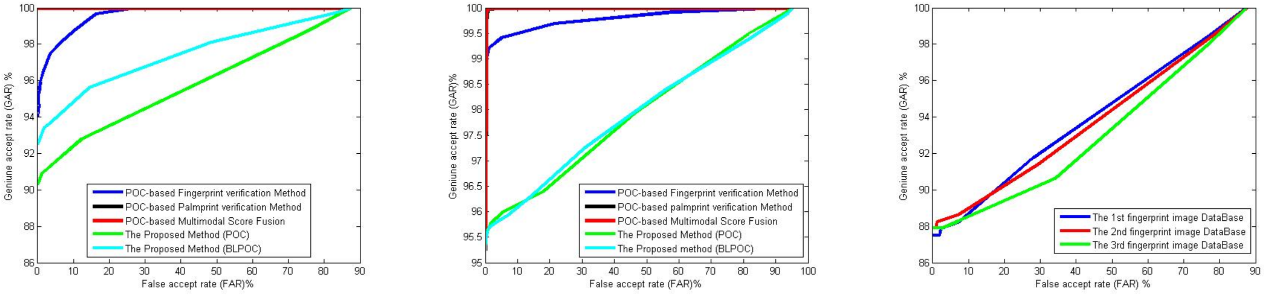
Figure 10: Matching score calculation between matched images using POC and BLPOC functions

Table 1: The verification accuracy of Experiment 1

Experiment.1	The 1st fingerprint image database FRR% at FAR%=0	The 2nd fingerprint image database FRR% at FAR%=0
POC-based Fingerprint image matching	5.63	3.25
POC-basedPalmprint image matching	0.0	0.63
POC-based multimodal score fusion	0.0	0.25
The proposed method (POC)	9.38	4.59
The proposed method (BLPOC)	7.50	4.43

Table 2: The verification accuracy of Experiment 2

Experiment.2	**The Proposed Method (POC)** FRR% at FAR%=0
The 1st fingerprint image database	9.77
The 2nd fingerprint image database	10.16
The 3rd fingerprint image database	11.33



(a) (b) (c)

Figure 11: ROC curves for: (a) the 1st dataset, (b) the 2nd dataset, (c) comparision between three different fingerprint datasets

5 Conclusions

This paper presented an optical template protection scheme, produces a secure biometric template as a mix of fingerprint image and palmprint image based on the principles of the optical (DRPE) scheme. Through the experimental results we confirmed that the verification accuracy of the proposed encoding method under genuine and imposter decryption was found to be effectively comparable with the existing fingerprint verification method that also based on the (DRPE) [22–25, 28] by effectively improving the FRR besides a higher level of security by using a multibiometrics and POC image matching.

References

[1] M. Abe, X. Zhang and M. Kawamata, "An efficient subpixel image registration based on the phase-only correlations of image projections," in *International Symposium on Communications and Information Technologies (ISCIT'10)*, pp. 997–1001, 2010.

[2] S. Almaadeed, I. Rida and A. Bouridane, "Gait recognition based on modified phase-only correlation," *Signal, Image and Video Processing*, vol. 10, no. 3, pp. 463–470, 2016.

[3] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

[4] S. C. Draper, S. Rane, Y. Wang and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 51–64, 2013.

[5] M. S. Hwang, C. C. Lee, Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack", *International Journal of Informatica*, vol. 12, no. 2, pp.297–302, Apr. 2001.

[6] K. Ito and *et al.*, "A fingerprint matching algorithm using phase-only correlation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 87, no. 3, pp. 682–691, 2004.

[7] K. Ito and *et al.*, "A palmprint recognition algorithm using phase-based image matching," in *IEEE International Conference on Image Processing*, pp. 2669–2672, 2006.

[8] R. Kumar and B. Bhaduri, "Double image encryption in fresnel domain using wavelet transform, gyrator transform and spiral phase masks," in *Fifth International Conference on Optical and Photonics Engineering*, pp. 104490O, June 2017.

[9] C. T. Li, M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181-2188, May 2010.

[10] C. T. Li, M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

[11] C. W. Lin, C. S. Tsai, M. S. Hwang, "A new strong-password authentication scheme using one-way hash functions", *International Journal of Computer and Systems Sciences*, vol. 45, no. 4, pp. 623–626, July 2006.

[12] Z. Liu and *et al.*, "Image encryption algorithm by using fractional fourier transform and pixel scrambling operation based on double random phase encoding," *Optics and Lasers in Engineering*, vol. 51, no. 1, pp. 8–14, 2013.

[13] X. Lu, P. Lu, Z. Xu and X. Liu, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 16, pp. 2514–2518, 2013.

[14] D. Maltoni, J. Wayman, A. Jain and D. Maio, "An introduction to biometric authentication systems," *Biometric Systems*, pp. 1–20, 2005.

[15] A. Nagar, *Biometric template security*, Michigan State University, Computer Science, 2012.

[16] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 3, 2011.

[17] P. Refregier and B. Javid, “Optical image encryption based on input plane and fourier plane random encoding,” *Optics Letters*, vol. 20, no. 7, pp. 767–769, 1995.

[18] P. Refregier and B. Javid, “Optical image encryption using input plane and fourier plane random encoding,” in *Proceeding of SPIE*, pp. 767–769, 1995.

[19] Z. Shao and *et al.*, “Combining double random phase encoding for color image watermarking in quaternion gyrator domain,” *Optics Communications*, vol. 343, pp. 56–65, 2015.

[20] K. Simoens and *et al.*, “Criteria towards metrics for benchmarking template protection algorithms,” in *5th IAPR International Conference on Biometrics (ICB’12)*, pp. 498–505, 2012.

[21] S. A. Suandi, M. S. M. Asaari and B. A. Rosdi, “Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics,” *Expert Systems with Applications*, vol. 41, no. 7, pp. 3367–3382, 2014.

[22] H. Suzuki and *et al.*, “Fingerprint verification for smart-card holders based on optical image encryption scheme,” in *Proceeding of SPIE Vol*, vol. 5202, pp. 89, 2003.

[23] H. Suzuki and *et al.*, “File encryption software using fingerprint keys based on double random encoding,” in *Frontiers in Optics*, pp. JWA50, 2005.

[24] H. Suzuki and *et al.*, “Experimental evaluation of fingerprint verification system based on double random phase encoding,” *Optics Express*, vol. 14, no. 5, pp. 1755–1766, 2006.

[25] H. Suzuki and *et al.*, “Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack,” *Optics Express*, vol. 18, no. 13, pp. 13772–13781, 2010.

[26] H. Suzuki, M. Takeda, K. Nakano and M. Yamaguchi, “Encrypted sensing based on digital holography for fingerprint images,” *Optics and Photonics Journal*, vol. 5, no. 01, pp. 6, 2015.

[27] M. Takeda, K. Nakano and H. Suzuki, “Key-length analysis of double random phase encoding,” *Applied Optics*, vol. 56, no. 15, pp. 4474–4479, 2017.

[28] M. Takeda and *et al.*, “Encoding plaintext by fourier transform hologram in double random phase encoding using fingerprint keys,” *Journal of Optics*, vol. 14, no. 9, pp. 094003, 2012.

[29] S. Vashisth, H. Singh, A. K. Yadav and K. Singh, “Fully phase image encryption using double random-structured phase masks in gyrator domain,” *Applied Optics*, vol. 53, no. 28, pp. 6472–6481, 2014.

[30] N. Wang and *et al.*, “A novel hybrid multibiometrics based on the fusion of dual iris, visible and thermal face images,” in *International Symposium on Biometrics and Security Technologies (ISBAST’13)*, pp. 217–223, 2013.

[31] S. Yuan and *et al.*, “An optical authentication system based on encryption technique and multimodal biometrics,” *Optics & Laser Technology*, vol. 54, pp. 120–127, 2013.

[32] G. Zhang, B. Javidi and J. Li, “Encrypted optical memory using double-random phase encoding,” *Applied Optics*, vol. 36, no. 5, pp. 1054–1058, 1997.

[33] L. Zhang, L. Zhang and D. Zhang, “Fingerknuckleprint verification based on band-limited phase-only correlation,” in *Computer Analysis of Images and Patterns*, pp. 141–148, 2009.

[34] W. Zhang, M. Zhang, B. Yang and T. Takagi, “Multibiometric based secure encryption, authentication scheme with fuzzy extractor,” *International Journal of Network Security*, vol. 12, no. 1, pp. 50–57, 2011.

Biography

Eman Tarek. received her B.S. degree in 2012 in Department of information technology, Mansoura University, Egypt. She is currently pursuing here M.S. degree in information technology. Here current research interests include Pattern Recognition, Information Security, Biometrics.

Osama Ouda. received his B.S. in Computer Science from Mansoura University, Egypt, in 2000, his M.S. in Computer Science from Ain-Shams University, Egypt, in 2007, and his Ph.D. in Computer and Information Sciences from Chiba University, Japan, in 2011. From November 2013 to May 2014, he was a research fellow at iPRoBe laboratory, Michigan State University, East Lansing, USA. Currently, he is an assistant professor in the Department of Information Technology, Mansoura University, Egypt. Dr. Ouda is a member of IEEE since 2011. His research interests include information security,biometrics, image processing and machine learning.

Ahmed Atwan. received his B.S degree in 1988, his M.S. degree in 1998 and Ph.D degree in 2004, all in Department of Communications and Electronics Engineering, Mansoura University, Egypt. His current research interests include Networking, Expert Systems, Biometrics, and Machine Learning.