Mansoura Journal of Computers and Information Sciences

A secure Multimodal Biometric Authentication with Cryptographic key Management Using Double Random Phase Encoding

Eman Tarek
Faculty of computers and information systems , I.T dep.
Mansoura University, Egypt
eman_tarek@mans.edu.eg

Osama Ouda
Faculty of computers and information systems , I.T dep.
Mansoura University, Egypt
oouda@mans.edu.eg

Ahmed Atwan
Faculty of computers and information systems , I.T dep.
Mansoura University, Egypt
atwan@mans.edu.eg

ABSTRACT

Multibiometric systems are more efficient and reliable than unibiometric systems as they can provide lower error rates as well as robustness against frauds and subsystem failures. However, the deployment of multibiometric systems in large-scale biometric applications increases the risk of users' privacy violation because once a multibiometric system is compromised; multiple biometric traits are disclosed to adversaries. As a result, protecting biometric templates stored in centralized databases of multibiometric systems has become a necessary prerequisite to allow wide-spread deployment of these systems. In this paper, we propose a biometric template protection method for securing image templates in multibiometric systems using the double random phase encoding (DRPE) scheme. DRPE is a well-known image encryption scheme and therefore it is more suited to secure image-based biometric templates. First, the proposed method encodes a randomly generated key as a binary image. Second, the phase components of two images captured from two different biometric modalities; namely, palmprint and fingerprint are convolved to produce a multi-biometric image of the same size as the binary image-encoded key. Finally, image-encoded key is encrypted using DRPE employing the multi-biometric image as a cipher key. During authentication, the encoded key is correctly recovered only if genuine biometric images are presented to the system; otherwise, the authentication process fails. Therefore, the proposed method can not only protect image-based biometric templates but also can provide a reliable means for securing cryptographic keys. Experimental results illustrate that the proposed method can secure both biometric templates and cryptographic keys without sacrificing the recognition accuracy of the underlying unprotected biometric recognition system.

Keywords

Multimodal biometric authentication, Biometric template protection, Cryptographic key security, Double random phase encoding.

1. INTRODUCTION

The popularization of internet services and modern communication technologies has led to much research effortin the field of data security and privacy protection. Against such a problem, a number ofauthentication and data encryptiontechniques have got much attention to guarantee safeguards for data and the validity of the person.

Identity-based authentication techniques are extensively used in several applications and services to truly validate the identity of a person. Traditionally, user specific passwords and/or tokens which for years have been the most widely used tools to secure systems are susceptible to many user inconvenience and unreliability issues. For instance, tokens and cards may be lost or stolen; Passwords and PINs may be forgotten, easily guessed or even broken by fraudulent attacks and long passwords are difficult to remember as well as non-certainty of who is the actual user. Biometric technologies, on the other hand, identify individuals based on linking a person with his normally unique, permanent and hard to reproduce body parts such as fingerprint, iris, voice, palmprint, face and signature. These physical and behavioral traits are unique across individuals and thereby can't be lost, stolen, guessed, borrowed or forgotten [1-2].

Traditional biometric systems are unimodal as they rely on a single biometric modality for authentication. By using unibiometric system so as to have poor accurateness with unacceptable error rates and may not be sufficient to guarantee security against spoof attacks.Multibiometric systems, on the other hand, integrate different types of biometric traits [10-16]. There are a number of benefits inherent to multimodal biometrics, the most prominent being heightened levels of security and accuracy either by reducing the false reject rate (FRR) or false accept rate (FAR) and greater levels of reliability/flexibility. However, if a multibiometric system is compromised; multiple biometric traits are disclosed to adversaries. As a result, protecting biometric templates stored in centralized databases of multibiometric systems has become a necessary prerequisite to allow wide-spread deployment of these systems, since such templates can't be revoked or reissued, like passwords and tokens[3-9]. As a solution to these issues, we proposed a biometric template protection method for securingimage templates in multibiometric systems by applying double random phase encoding (DRPE) [20].

DRPE is a well-known optical image encryption technique that based on pattern matching and the phase only correlation (POC) between encryption and decryption keys [17-18]. In short, the cipher key used in DRPE is allowed to includesome redundancy between encryption and decryption.Owing to this property, biometrics information whichis difficult to be used as a key on conventional cipher cryptographies [35] because of variety of acquiredbiometric data, can be used as a cipher key for data encryption by applying DRPE.

DRPE encrypts an input image as a stationary white noise by the means of multiplying the image with two statistically independent random phase masks as 2D images both in the spatial and Fourier domains. The second mask located at the Fourier domain serves as a cipher key of encryption process. DRPE has potential applications infingerprint verification systems [38-45], information hiding [22], watermarking [21], color image encryption [24], and multipleimage encryption [23, 29].

In this paper, the proposed method first encodes a randomly generated key as a binary image. Second, the phase components of two images captured from two different biometric modalities; namely, palmprint and fingerprint are convolved to produce a multi-biometric image of the same size as the binary image-encoded key. Finally, image-encoded key is encrypted using DRPE employing the multi-biometric image as a cipher key. During authentication, the encoded key is correctly recovered only if genuine biometric images are presented to the system; otherwise, the authentication process fails. Therefore, the proposed method can not only protect image-based biometric templates but also can provide a reliable means for securing cryptographic keys. Computer simulations have been carried out to support the objectives of the proposed method to secure both biometric templates and cryptographic keys without sacrificing the recognition accuracy of the underlying unprotected biometric recognition systemthat today's system environment demands.

The paper is organized as follows. Section (2) Related works, Section (3) Overview of DRPE, Section (4) Implementation details of the proposed method, Section (5) Results and Discussion, Section (6) Conclusion.

2. Related Works

From the literature researches have been reported for applying DRPE to biometrics, brief reviews of such research work are consulted here. Hiroyuki Suzuki et. al.[38] proposed a hybrid PIN and fingerprint verification system for smart card holder authentication based on DRPE. The probability of accurate verification decreases remarkably due to the influence of fingerprints that are shifted significantly or with different rotation angles. In ref. [39], they review the proposed system and present a preprocessing todetect the shift amount and eliminate significantly shifted fingerprint images to improve the FRR. However, the verification accuracy is lower than that of conventional system and its security level is insufficient. In ref. [45], they proposed shift and rotation invariant method for the purpose ofeliminating tags from the plain image and correct rotation angles of fingerprint images. The proposed method provided sufficient FRR as well as the conventional method. Ref. [40], presented the development of file encryption software using a key created from fingerprint by applying DRPE. In ref. [42], they proposed a novel bit coding methodthat makes imposterdecrypted images more random compared with the conventionalmethod.The main feature of thisproposed methodis that the restored bit pattern image is not shifted even if thefingerprint image used for decryption is shifted with respect to that used for encryption. In ref. [44], they proposedan encrypted sensing system for personal authentication in which fingerprintimages are captured using digital holography with DRPE. The principal advantage of thissystem is that it can enhance the security of biometric authenticationby capturing optically encrypted images rather than raw fingerprints to reduce the risk of datatheft or leakage of personal information captured by biometric sensing.

3. OVERVIEW OF DOUBLE RANDOM PHASE ENCODING

The double random phase encryption (DRPE) [20] is the most studied among all optical encryptiontechniques [17-18] because of its easy implementation using 4f optical set up shown in Fig.1.In a DRPE system, the original image can be converted into a complex stationary white noiseusing two statistically independent random phasemasksplaced in the spatial and Fourier domains respectively.It is critically important to discuss the numerical simulation of encryption and decryption processes in the classic DRPE architecture.

3.1 Encryption process

To obtain the encrypted image $\psi(x,y)$in DRPE [33], the input image $f(x,y)$is first multiplied by the first random phase mask in the spatial domain $PRM1 = \exp\{jn(x,y)\}$.Where (x,y) denotes the spatial coordinates.

$$\mathbf{f_m(x,y) = f(x,y).\exp\{jn(x,y)\}} \qquad (\mathbf{1})$$

Afterwards, the phase modulated image $f_m(x,y)$ is Fourier transformed$F_m(u,v) = FT[f_m(x,y)]$ and then multiplied by the second phase mask in the frequency domain $PRM2 = \exp\{jE(u,v)\}$ used as an encryption key.Finally, this complex amplitude image$F_m(u,v).\exp\{jE(u,v)\}$ is inverse Fourier transformed and the encrypted image is obtained at the spatial domain.

$$\psi(x,y) = IFT[F_m(u,v).\exp\{jE(u,v)\}] \qquad (2)$$

(u,v)denotesthe frequency coordinates. $FT[\ \ ]$ and $IFT[\ ]$denote the Fourier transform and the inverse Fourier transform operators.

3.2 Decryption process

Fora decryption, the encrypted image $\psi(x,y)$ is Fourier transformed and then multiplied by the decryption key $PRM2 = \exp\{jD(u,v)\}$

$$\begin{aligned} &F_d(u,v) \\ &= FT[\psi(x,y)]\,.\exp\{jD(u,v)\} \qquad (3) \\ &= F_m(u,v)\,.\exp[j\{E(u,v) + D(u,v)\}] \end{aligned}$$

Finally, the complex amplitude image $F_d(u,v)$ is inverse Fourier transformed to produce the decrypted complex image $f_d(x,y)$.

$$f_d(x,y) = \mathrm{IFT}[F_m(u,v)\,.\exp[j\{E(u,v) + D(u,v)\}]] \qquad (4)$$

$$= \mathrm{IFT}[F_m(u,v)\,.\,N(u,v)]$$

$$= |f(x,y) \ * n(x,y)|$$

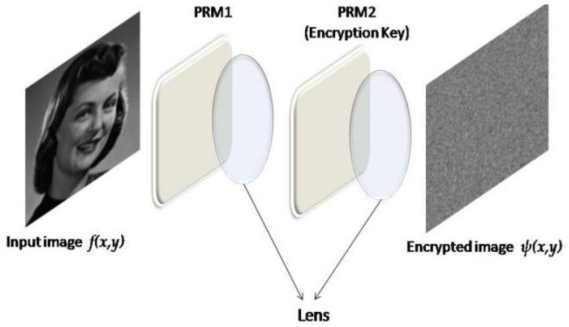


Fig.1: The optical system of DRPE.

Where

$$N(u,v) = \exp[j\{E(u,v) + D(u,v)\}] \qquad (5)$$

$$n(x,y) \ = \mathrm{IFT}[\ N(u,v)]$$

Where $n(x,y)$denotes the phase onlycorrelation (POC) between encryption and decryption keys. It is well known that the POCbetween similar keys, becomes a Dirac delta function $\delta(x,y)$, and the decryptedimage $f_d(x,y)$ can be expressed as the correctcomplex image $f_m(x,y)$, which has the same intensitypattern as the input image$f(x,y)$. But when the decryptionkey is significantly different from the encryptionkey, $n(x,y)$ exhibits a random noise distribution, andthe decrypted image becomes a random noise image.

DRPE can be implementedoptically or numerically and has a number of differentarchitectures, includingseveral based on Fourier transform [28], Fresnel transform[30,32],fractional Fourier transform[25],as well as several architectures [34,43].

4. PROPOSED SCHEME

We proposed method, employing DRPEto securely authenticate individualswithout exposing their sensitive biometric data to potential adversaries. It can not only protect image-based biometric templates but also can provide a reliable means for securing cryptographic keys.

As illustrated in Fig.2, the proposed method first encodes a randomly generated key as a 2D binary image. Second, the phase components of two images captured from two different biometric modalities; namely, palmprint and fingerprint are convolved to produce a multi-biometric image of the same size as the binary image-encoded key. Finally, image-encoded key is encrypted using DRPE employing the multi-biometric image as a cipher key. During authentication, the encoded key is correctly recovered only if genuine biometric images are presented to the system; otherwise, the authentication process fails. Figs.3 and 4 shows the procedures of encryption and decryption in the proposed method.

4.1 Image-encoded cryptographic key

To securea multi-biometric image employed as a cipher key in DRPE, a randomly generated key must be encoded as 2D binary image and used as a plain image for encryption. Black and white squares are used to represent binary data sequence, in which black squares represent ‘0’ bits and white squares represent ‘1’ bits. Finally the squares are laid out as a quadrate to obtain 2D binary image as shown in Fig.5.

4.2 Encryption process

Let $C(x,y)$ denotes the image-encoded cryptographic key where(x,y)denotes the spatial domain coordinates. $F_E(x,y)$and$P_E(x,y)$denote the fingerprint and palmprint images, captured during enrollment.

The amplitude of $C(x,y)$ is first multiplied by the first random phase mask generated from a random pattern $R(x,y)$to obtain a complex amplitude image$C_a(x,y)$.

$$C_a(x,y) = C(x,y)\exp[jR(x,y)] \qquad (6)$$

Afterwards,$C_a(x,y)$, is transformed into the frequency domain using the 2D-DFT and the resulting coefficients matrix, $C_a(u,v)$, is multiplied by the second phase mask $\exp[jK_E(u,v)]$ that represents the phase components of 2D DFT of the multi-biometric image $P_E(x,y)$ and $F_E(x,y)$.

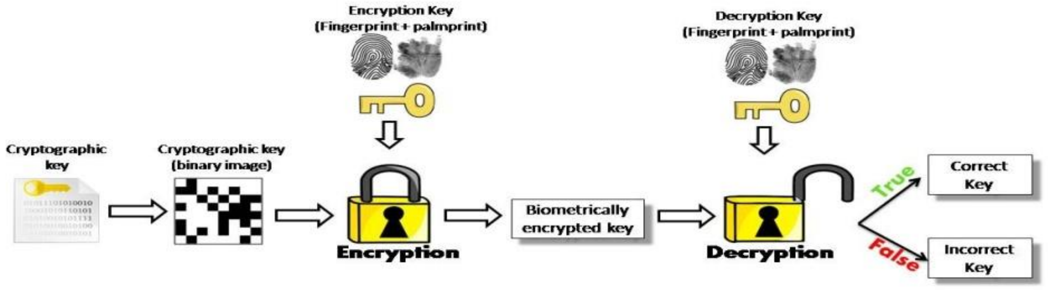


Fig.2: The Proposed Scheme.

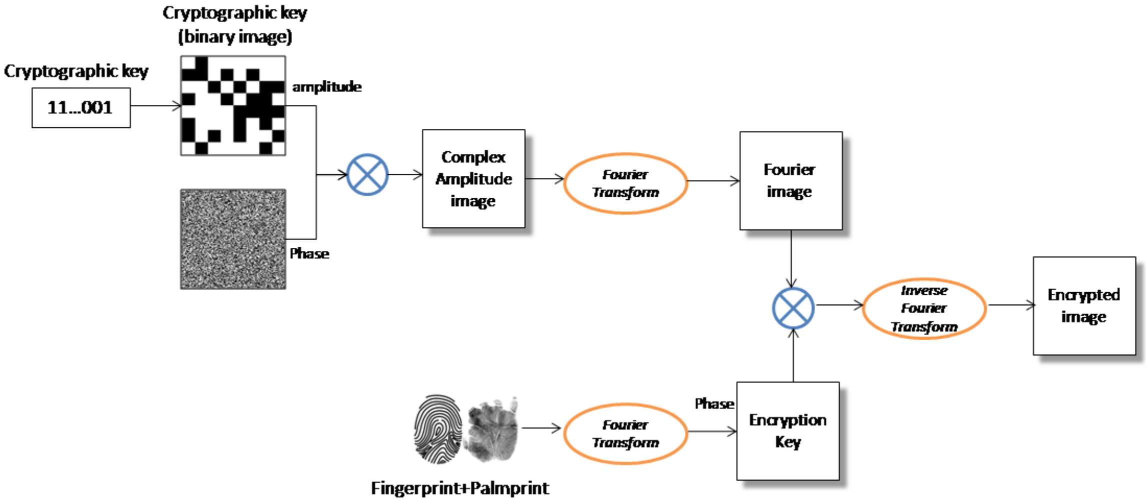


Fig.3: Encryption Process of the proposed encryption scheme using DRPE.

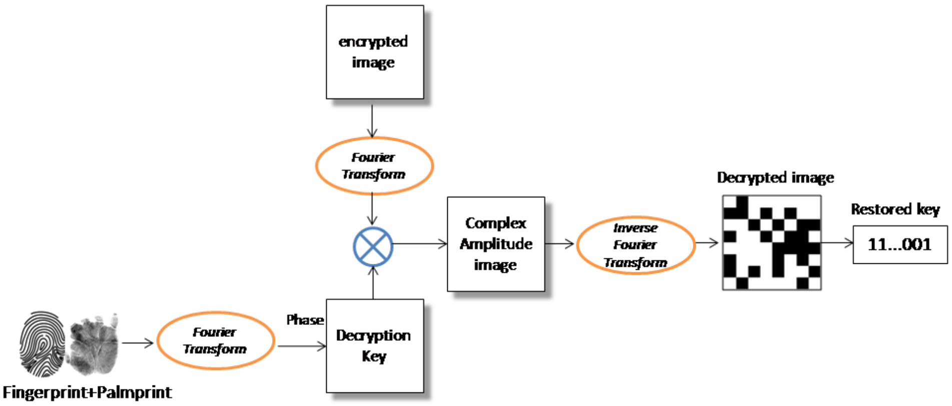


Fig.4: Decryption Process of the proposed encryption scheme using DRPE.

$$\mathrm{P_E(u,v) = FT[P_E(x,y)] = A_{PE}(u,v)\ exp[jPh_{PE}(u,v)]} \quad (7)$$

$$\mathrm{K_E(u,v) = Ph_{PE}(u,v) + Ph_{FE}(u,v)} \quad (9)$$

Where $\mathrm{A_{PE}(u,v)}$ and $\mathrm{A_{FE}(u,v)}$ are the amplitude components, $\mathrm{Ph_{PE}(u,v)}$ and $\mathrm{Ph_{FE}(u,v)}$are the phase components of the 2D-DFT of palmprint and fingerprintimages, and$\mathrm{(u,v)}$ denotes the frequency domain coordinates.

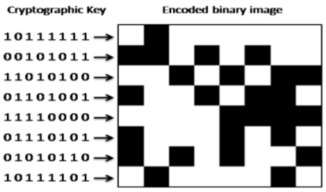


Fig.5: binary image encoded-key.

$$\mathrm{F_E(u,v) = FT[F_E(x,y)] = A_{FE}(u,v)\ exp[jPh_{FE}(u,v)]} \quad (8)$$

Finally the encrypted image $\mathrm{E(u,v)}$ is obtained as a complex random image expressed as follows:

$$\mathrm{E(u,v) = C_a(u,v)exp[jK_E(u,v)]} \quad (10)$$

4.3 Decryption process

Let $\mathrm{F_D(x,y)}$ and $\mathrm{P_D(x,y)}$denote the fingerprint and palmprint images, captured during authentication.For a decryption, the complex conjugate of encrypted image is carried out,

$$\mathrm{E^*(u,v) = C_a^*(u,v)exp[-jK_E(u,v)]} \quad (11)$$

Followed by multiplication with decryption Key,$\mathrm{exp[jK_D(u,v)]}$,that represents the phase components of 2D DFT of fresh multi-biometric image $\mathrm{P_D(x,y)}$ and $\mathrm{F_D(x,y)}$.

$$\mathrm{K_D(u,v) = Ph_{PD}(u,v) + Ph_{FD}(u,v)} \quad (12)$$

$$\mathrm{E}^*(\mathrm{u},\mathrm{v})\exp[\mathrm{j}\mathrm{K}_\mathrm{D}(\mathrm{u},\mathrm{v})] = \qquad (13)$$

$$\mathrm{C}_\mathrm{a}^*(\mathrm{u},\mathrm{v})\exp[\,\mathrm{j}(-\mathrm{K}_\mathrm{E}(\mathrm{u},\mathrm{v})\ +\mathrm{K}_\mathrm{D}(\mathrm{u},\mathrm{v}))\,]$$

Lastly, Fourier transform operation releases the decryption image.

$$\mathrm{C}_\mathrm{r}(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d}) = \mathrm{FT}\{\mathrm{C}_\mathrm{a}^*(\mathrm{u},\mathrm{v})\exp[\,\mathrm{j}(-\mathrm{K}_\mathrm{E}(\mathrm{u},\mathrm{v}) + \mathrm{K}_\mathrm{D}(\mathrm{u},\mathrm{v}))\,]\}$$

$$= \mathrm{C}_\mathrm{a}^*(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d}) * \mathrm{n}(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d}) \qquad (14)$$

Where $*$ represents the convolution and $\mathrm{n}(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d}) = \mathrm{FT}\{\exp[\,\mathrm{j}(-\mathrm{K}_\mathrm{E}(\mathrm{u},\mathrm{v})+\mathrm{K}_\mathrm{D}(\mathrm{u},\mathrm{v}))\,]\}$ represents the phase only correlation (POC) between enrollment and authentication fingerprint and palmprint images [36-37]. $\mathrm{n}(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d})$satisfies the following relation

$$\mathrm{n}(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d}) \cong \begin{cases} \delta(\mathrm{x}_\mathrm{d}-\alpha,\mathrm{y}_\mathrm{d}-\beta) & \text{geniune individual} \\ \text{random sequence} & \text{imposter individ} \end{cases} \qquad (15)$$

$\delta()$denotes the Dirac delta function and α and β represent the shift between encryption and decryption keys. As illustrated in Fig.6, when enrollment and authenticationmulti-biometric imagesare belonging to the same user, POC is sufficiently high for correct decryption. And therefore the restored image $\mathrm{C}_\mathrm{r}(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d})$ is expressed as $\mathrm{C}_\mathrm{a}^*(\mathrm{x}-\alpha,\mathrm{y}-\beta)$ with the same intensity pattern as of $\mathrm{C}(\mathrm{x},\mathrm{y})$. On the other hand, when multi-biometric imagesare from different individuals, POC represents random noise distribution and $\mathrm{C}_\mathrm{r}(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d})$ produces a random noise image, which is the convolution of $\mathrm{C}_\mathrm{r}(\mathrm{x}_\mathrm{d},\mathrm{y}_\mathrm{d})$and a random sequence.

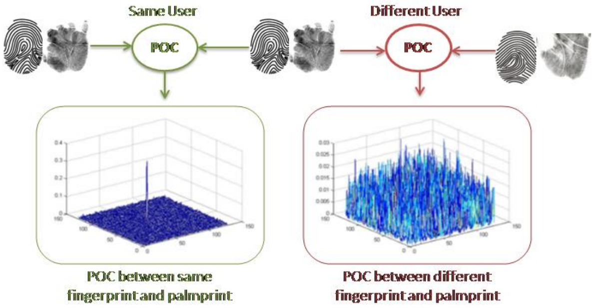


Fig.6: POC between enrollment and authentication multi-biometric images from same and different users.

5. EXPERIMENTAL RESULTS

In this section, we describe a set of experiments that have been implemented using Matlab platform in order to simulate and evaluate the verification accuracy of our proposed encoding method and to confirm the randomness in case of an impostor decryption.

5.1 Template generation

In order to generate multi-biometric templates used as cipher keysin DRPE; two types of a training datasets are used. *Dataset 1* contains 8 experimental subjects; each subject contributes with 6 images of each fingerprints and palmprints. Fingerprint images are from [38,40,42] to compare the performance with the only existing fingerprint verification systems based on DRPE andCASIA palmprint images [46].Each fingerprint image with a size of 256x256 pixels in 8 bit grayscale bmp files while palmprint image resolution is 128x128.

Dataset 2 contains 21 experimental subjects;each subject contributes with 10 images of each fingerprints and palmprints. Fingerprint images [39] collected in this dataset are with some shift changes but in the encryption process the shift of the fingerprint images are adjusted.

For each experimental subject, one fingerprint and palmprint images are used in enrollment(encryption) and others inauthentication (decryption).

5.2 Robustness of encryption and decryption

Examples of resultant images in encryption are shown in Fig.7.Fig.7 (a) shows the binary image encoded-key to be encrypted.Figs.7 (b) and (c) show palmprint and fingerprint images used to generate a multi-biometric image.Fig.7 (d) shows the encrypted random image using multi-biometric image as a cipher key.

As shown in Fig.8, when same individual'spalmprint and fingerprint images used for decryption Figs.8 (a) and (b), the encrypted image is successfully decrypted Fig.8 (c), and the encoded-key image is correctly restored Fig.8 (d) to reconstruct the cryptographic key. But whendifferent individual's palmprint and fingerprint images used Figs.8 (e) and (f), the encryptedimage randomly restored Fig.8 (g), and thereforethe encoded-key image is randomly reconstructedFig.8 (h).

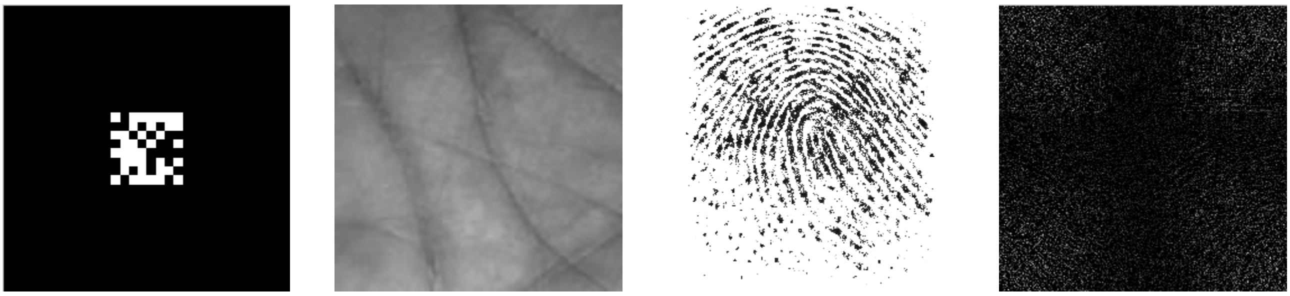
As a result, the encoded-key image is correctly recovered only if genuine biometric images are presented to the system; otherwise, the encoded-keyimage becomes a random image.

5.3 Verification accuracy

In order to evaluate the performance of the proposed schemeas biometric template protection method for securing image templates in multibiometric systems besidessecuring cryptographic keys, we calculated false reject rate (FRR), false accept rate (FAR) and Bit error rate (BER) as follows.

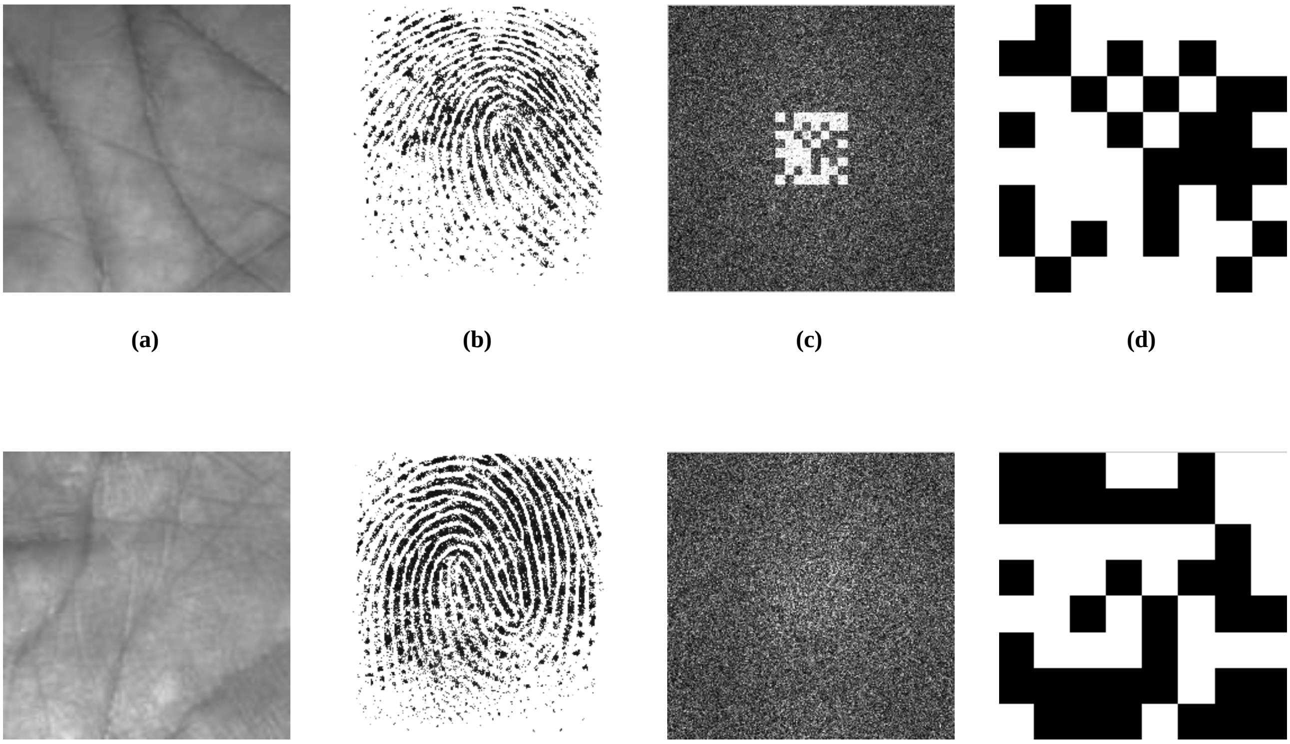
$$\mathrm{EER} = \frac{\mathrm{N}_\mathrm{error}}{\mathrm{N}_\mathrm{S}},$$

$$\mathrm{FAR} = \frac{\mathrm{N}_\mathrm{FA}}{\mathrm{N}_\mathrm{T}}, \qquad \mathrm{FRR} = \frac{\mathrm{N}_\mathrm{FR}}{\mathrm{N}_\mathrm{T}}$$



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

Fig.7: resultant images of encryption process. (a) Binary encoded-key image of cryptographic key, (b and c) palmprint and fingerprint images used for encryption, (d) the encrypted random image.



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

(e) (f) (g) (h)

Fig.8: resultant images of decryption process in case of genuine and impostor individuals. (a and b) same individual's palmprint and fingerprint images, (c) the successfully decrypted image, (d) the subtracted binary image from decrypted image to decode cryptographic key . (e and f) different individual's palmprint and fingerprint images, (g) the randomly decrypted image, (d) the subtracted binary image.

Where N_S is the bit number of cryptographic key (in case, 64 bits); N_{error} is the average number of error bits of decoded key. $N_{FA}$is the number of falsely accepted trails; N_{FR} is the number of falsely rejected trails and N_T is the total number of trails in experiments.

5.3.1 Securing multi-biometric images

As illustrated in Table 1 and 2, we have calculated FRR and FAR to investigate the proposed scheme's performance to secure a multi-biometric image, compared to performance when securing only fingerprint or palmprint images.We can observe that FRR of securing multi-biometric images is slightly increased but still comparable with the good FRR when only securing palmprints. Despite, it canbe acceptable as it increases reliability and heightens levels of security by using multi-biometric systems. Also, comparisons with the only existing fingerprint verification systems are conducted [38, 42]as shown in Table 1 and 2. And therefore the proposed method proved its efficiency in improving FRR by employing multi-biometric images as a cipher key. Fig.9 shows the ROC curves of the proposed method when employing multi-biometric and uni-biometric images as a cipher keys.

5.3.2 Securing cryptographic keys

When employing proposed system to secure cryptographic keys, we have investigated the performance calculating BER in case of genuine and imposter individuals. BER of the proposed method is significantly improved in case of a genuine decryption but slightly decreased for an impostor decryptionas compared to employinguni-biometric keys and the existing fingerprint verification systems [].Though this imposter BER is not so good accuracy compared by other methods, we think that the accuracy may be better byimprovements of the method. Despite, it can be acceptable as the system correctly releases the key in case of a genuine decryption as illustrated in Table 3 and 4 andmaintain security as strong as possible.

6. CONCLUSION

This paper introduces a biometric template protection methodto secure biometric images in multimodal systems using DRPE.The proposed method can not only protect biometric templates but also can provide a reliable means for securing cryptographic keys. Through theexperimental results we confirmed that the verificationaccuracy of the proposed encoding method under genuineand imposter decryption was found to be effectively comparable with using uni-biometric images and with the existing fingerprint verification methodthat also based on principles of DRPEby effectively improving the FRR and heightened levels of security by using multi-biometric images.On the other hand, BER for imposter decryption might not be sufficient and need to be improved further but it can be acceptable as it maintains security more stronger than using uni-biometric images as in [38-45].

Table.1: results of verification accuracy of experimental dataset 1.

Dataset.1	FRR% at FAR=0	BER Genuine%	BER Impostor %
Proposed system(multi-biometric image)	1.88	0.39	43.16
Proposed system(Fingerprint only image)	5.31	6.25	62.50
Proposed system(Palmprint only image)	0.63	1.56	61.33
PIN verification using fingerprint keys[38]	11.9	0.357	49.0
Modified PIN verification using fingerprint keys[42]	5.71	0.584	49.2

Table.2: results of verification accuracy of experimental dataset 2.

Dataset.2	FRR% at FAR=0	BER Genuine%	BER Impostor %
Proposed system(multi-biometric image)	2.29	2.08	45.83
Proposed system(Fingerprint only image)	3.65	13.45	66.15
Proposed system(Palmprint only image)	1.44	4.17	64.36
Shift invariant PIN verification using fingerprint keys [39]	29	3.2	51.0
Shift and rotation invariant PIN verification using fingerprint keys [45]	8.57		40.8

Table.3: Bit error rate for experimental subjects in dataset 1, in case of genuine individuals for decryption.

BER $_{Genuine}$%	P1	P2	P3	P4	P5	P6	P7	P8
Proposed system	0	0	1.56	1.56	0	0	0	0
Fingerprint only	1.56	0	9.38	7.81	1.56	3.13	23.44	1.56
Palmprint only	0	0	3.13	0	4.69	0	1.56	0
PIN verification using fingerprint [38]	0	0.781	1.17	0	0	0	1.04	0

Table.4: Bit error rate for experimental subjects in dataset 1, in case of impostor individuals for decryption.

BER $_{Impostor}$%	P1	P2	P3	P4	P5	P6	P7	P8
Proposed system	45.31	45.31	46.88	50.00	37.50	40.63	43.75	39.16
Fingerprint only	59.38	60.94	59.38	64.06	67.19	62.50	65.63	62.50
Palmprint only	59.38	64.06	57.81	62.50	60.94	65.63	60.94	61.33
PIN verification using fingerprint[38]	49.0	49.6	47.4	49.2	49.6	48.8	49.4	49.2

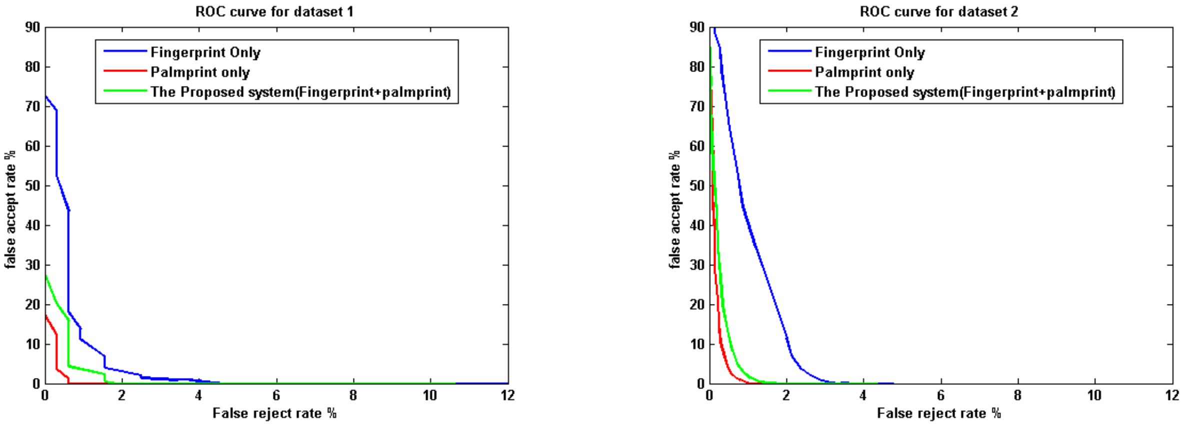


Fig.9: ROC curves for verification accuracy of dataset 1 and 2.

\

7. REFERENCES

[1] Jain, Anil K., Arun Ross, and SalilPrabhakar., “An introduction to biometric recognition”, IEEE Transactions on circuits and systems for video technology , vol. 14, no. 1,pp. 4-20, 2004.

[2] Saini, Rupinder, and NarinderRana., “Comparison of various biometric methods”, International Journal of Advances in Science and Technology (IJAST), vol. 2 , 2014.

[3] Subramaniam, Bharathi, and SudhakarRadhakrishnan., “ A novel technique to improve template security for biometric recognition”, Int. Arab J. Inf. Technol, vol. 13, no. 6A ,pp. 923-929, 2016.

[4] Prabhakar, Salil, SharathPankanti, and Anil K. Jain., “Biometric recognition: Security and privacy concerns”, IEEE security & privacy, vol. 99, no. 2, pp. 33-42, 2003.

[5] Memon, Nasir., “How Biometric Authentication Poses New Challenges to Our Security and Privacy [In the Spotlight]”, IEEE Signal Processing Magazine , vol. 34, no. 4 ,pp. 196-194 2017.

[6] Rane, Shantanu, et al., “Secure biometrics: concepts, authentication architectures, and challenges”, IEEE Signal Processing Magazine , vol. 30, no. 5, pp. 51-64, 2013.

[7] Jain, Anil K., KarthikNandakumar, and Abhishek Nagar., “Biometric template security”, EURASIP Journal on Advances in Signal Processing, pp. 113, 2008.

[8] Rathgeb, Christian, and Andreas Uhl., “A survey on biometric cryptosystems and cancelable biometrics”, EURASIP Journal on Information Security ,vol. 1,pp. 3, 2011.

[9] Ashish, M. M., and G. R. Sinha., “Biometric Template Protection”, J Biostat Biometric App, vol. 1, no. 2, pp. 202, 2016.

[10]Nadheen, M. Fathima, and S. Poornima., “Feature level fusion in multimodal biometric authentication system”, International Journal of Computer Applications, vol. 69,no. 18, 2013.

[11]Sheena, S., and Sheena Mathew., “Multimodal biometric authentication: secured encryption of iris using fingerprint id, International Journal on Cryptography and Information Security (IJCIS), vol. 6, no. 3/4, 2016.

[12]Wang, Ning, et al., “A novel hybrid multibiometrics based on the fusion of dual iris, visible and thermal face images”, Biometrics and Security Technologies (ISBAST), 2013 International Symposium on. IEEE, 2013.

[13]Jiwnani, Gunjan, and MTech Student., “Multi-modal Biometric Authentication using Fingerprint and Iris: a Review”, International Journal of Computer Science & Communication Networks, vol. 5, no. 2, pp. 115-119.

[14]Eshwarappa, M. N., and Mrityunjaya V. Latte., “Multimodal Biometric Person Authentication using Speech, Signature and Handwriting Features”, International Journal of Advanced Computer Sciences and Applications Special+ Issue, Artificial+ Intelligent, pp. 77-86,2011.

[15]Gad, Ramadan, et al., “Multi-biometric systems: A state of the art survey and research directions”, Int.

J. Adv. Comput. Sci. Appl, vol. 6,no. 6 ,pp. 128-138, 2015.

[16]Nagar, Abhishek, KarthikNandakumar, and Anil K. Jain., “Multibiometric cryptosystems based on feature-level fusion”, IEEE transactions on information forensics and security,vol. 7, no. 1, pp. 255-268 , 2012.

[17] Chen, Wen, BahramJavidi, and Xudong Chen, “Advances in optical security systems”, Advances in Optics and Photonics,vol. 6, no. 2,pp. 120-155,2014.

[18]Liu, Shi, ChangliangGuo, and John T. Sheridan., “A review of optical image encryption techniques”, Optics & Laser Technology, vol. 57, pp. 327-342, 2014.

[19]R.Chandramouli, M. Iorga, S. Chokhani., “Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing”, Springer, New York, pp. 1–30, 2014.

[20]Refregier, Philippe, and BahramJavidi., “Optical image encryption based on input plane and Fourier plane random encoding”, Optics Letters,vol. 20, no. 7, pp. 767-769,1995.

[21]Kishk, Sherif, and BahramJavidi., “3D object watermarking by a 3D hidden object”, Optics express , vol. 11, no. 8, pp. 874-888, 2003.

[22]Sheng, Yuan, et al., “Information hiding based on double random-phase encoding and public-key cryptography”, Optics express , vol. 17, no. 5, pp. 3270-3284, 2009.

[23]Liu, Zhengjun, et al., “Triple image encryption scheme in fractional Fourier transform domains”, Optics Communications,vol. 282, no. 4, pp. 518-522, 2009.

[24]Zhang, Shuqun, and Mohammad A. Karim., “Color image encryption using double random phase encoding”, Microwave and optical technology letters, vol. 21, no. 5 , pp. 318-323, 1999.

[25]Liu, Zhengjun, 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.

[26]Singh, Hukum, et al., “Fully phase image encryption using double random-structured phase masks in gyrator domain”, Applied optics, vol. 53, no. 28, pp. 6472-6481 ,2014.

[27]Zhou, Nan Run, et al., “Quantum image encryption based on generalized Arnold transform and double random-phase encoding”, Quantum Information Processing, vol. 14, no. 4, pp. 1193-1213, 2015.

[28]Yang, Yu-Guang, et al., “Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding”, Information Sciences, vol. 277, pp. 445-457,2014.

[29]Deepan, B., et al., “Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique”, Applied optics, vol. 53, no. 20, pp. 4539-4547,2014.

[30]Kumar, Ravi, and BasantaBhaduri, “Double image encryption in Fresnel domain using wavelet transform, gyrator transform and spiral phase masks”, Fifth International Conference on Optical and Photonics Engineering. International Society for Optics and Photonics, 2017.

[31]Markman, Adam, and BahramJavidi., “Full-phase photon-counting double-random-phase encryption”, JOSA A, vol. 31, no. 2 , pp. 394-403. 2014.

[32]Kumar, Ravi, and BasantaBhaduri., “Double image encryption in Fresnel domain using wavelet transform, gyrator transform and spiral phase masks”, Fifth International Conference on Optical and Photonics Engineering. International Society for Optics and Photonics, 2017.

[33]Nakano, Kazuya, Masafumi Takeda, and Hiroyuki Suzuki., “Key-length analysis of double random phase encoding”, Applied Optics, vol. 56, no. 15 , pp. 4474-4479, 2017.

[34]Nakano, Kazuya, et al., “Encrypted imaging based on algebraic implementation of double random phase encoding”, Applied optics , vol. 53, no. 14 , pp. 2956-2963,2014.

[35]Singh, Gurpreet., “A study of encryption algorithms (RSA, DES, 3DES and AES) for information security”, International Journal of Computer Applications, vol. 67, no. 19, 2013.

[36]Ito, Koichi, 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.

[37]Ito, Koichi, et al., “A palmprint recognition algorithm using phase-based image matching”, Image Processing, 2006 IEEE International Conference on. IEEE, 2006.

[38]Suzuki, Hiroyuki, et al., “Fingerprint verification for smart-card holders based on optical image encryption scheme”, Proc. of SPIE ,vol. 5202, 2003.

[39]Suzuki, Hiroyuki, et al., “Experimental evaluation of fingerprint verification system based on double random phase encoding”,Optics express, vol. 14, no. 5 , pp. 1755-1766, 2006.

[40]Suzuki, Hiroyuki, et al., “File encryption software using fingerprint keys based on double random encoding”, Frontiers in Optics. Optical Society of America, 2005.

[41]Tashima, Hideaki, 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.

[42]Takeda, Masafumi, 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.

[43]Nakano, Kazuya, et al., “Evaluations of phase-only double random phase encoding based on key-space analysis”, Applied optics,vol. 52, no. 6,pp. 1276-1283,2013

[44]Takeda, Masafumi, et al., “Encrypted sensing based on digital holography for fingerprint images”, Optics and Photonics Journal, vol. 5, no. 01, pp. 6, 2015.

[45]Takeda, Masafumi, et al., “Shift and Rotation Invariant Double Random Phase Encoding Using Fingerprint Keys”, Frontiers in Optics. Optical Society of America, 2010.

[46]CASIA Palmprint Image Database: http://biometrics.idealtest.org