Cancelable Face Recognition System Based on Optical Scanning Holography

Mohamed Safan
Menoufia University
3 PUBLICATIONS **26** CITATIONS
SEE PROFILE

Walid El-Shafai
Menoufia University
353 PUBLICATIONS **4,196** CITATIONS
SEE PROFILE

Ahmed Nabih Zaki Rashed
faculty of electronic engineering menoufia university
562 PUBLICATIONS **15,588** CITATIONS
SEE PROFILE

M.I. Dessouky
Menoufia University
440 PUBLICATIONS **4,253** CITATIONS
SEE PROFILE

Cancelable Face Recognition System Based on Optical Scanning Holography

Mohamed Safan
Department of Electronics and Electrical Communications Engineering
Faculty of Electronic Engineering
Menoufia University:
Menouf, Egypt
muhamed.safan@gmail.com

Walid El-Shafai
Department of Electronics and Electrical Communications Engineering
Faculty of Electronic Engineering
Menoufia University:
Menouf, Egypt
eng.waled.elshafai@gmail.com

Abd Naser Mohamed
Department of Electronics and Electrical Communications Engineering
Faculty of Electronic Engineering
Menoufia University:
Menouf, Egypt
abdnasermohamed@yahoo.com

Ahmed Rashed
Department of Electronics and Electrical Communications Engineering
Faculty of Electronic Engineering
Menoufia University:
Menouf, Egypt
ahmedrashed@gmail.com

Moawad I. Desouky
Department of Electronics and Electrical Communications Engineering
Faculty of Electronic Engineering
Menoufia University:
Menouf, Egypt
moawaddesouky@hotmail.com

El-Sayed El-Rabaie
Department of Electronics and Electrical Communications Engineering
Faculty of Electronic Engineering
Menoufia University:
Menouf, Egypt
sayedrabaie@yahoo.com

Fathi E. Abd El-Samie
Department of Electronics and Electrical Communications Engineering
Faculty of Electronic Engineering
Menoufia University, Egypt
fathi_sayed@yahoo.com

***Abstract*—Recently, biometrics has emerged joined of the foremost necessary methods of template preservation and most modern security systems rely on biometrics. Unfortunately, these systems have experienced for quite a while hacking endeavors. If biometric databases are compromised and stolen, biometrics spared in these databases will be lost until the end of time. Consequently, there is an immediate need to grow new upgrade biometric systems. The concept behind cancelable biometrics is to convert biometric data or extracted feature to an alternative template, which can't be easily used by the impostor or intruder and can be eliminated if it is breached. In this paper, the optical scanning holography (OSH) algorithm is utilized as cancelable face recognition system. In the proposed cancelable face recognition technique, the encrypted images are generated by OSH technique. Simulation results using evaluation metrics False Positive Rate (FPR), False Negative Rate (FNR), Equal Error Rate (EER), Receiver Operating Characteristic (ROC) and Area under ROC (AROC) prove that the the proposed cancelable biometric technique is good.**

Keywords—Biometrics, Enrollment and presentation, Optical scanning holography, EER, AROC.

I. INTRODUCTION

Biometrics is defined as automatic recognition of persons dependent on their physical or conduct attributes. The most used biometrics is fingerprints, faces, iris, and speech signals. Since biometric properties are implicitly associated with the person, they provide strong evidence of their identity. The fundamental thought of operation of biometric systems is to collect the biometrics from some authorized persons, extract discriminating features from the biometrics as a tool for data reduction, and store these features in a database. This is known as the training phase. In the other phase of biometric systems, which is the testing phase, features are extracted from the incoming biometrics for new persons and matched to the features in the database. The testing phase can be performed with or without classifiers [1-5]. The external body part plays a crucial role in our social interaction, conveyance of title people's identity.

Utilizing the face as a key to security, biometric face acknowledgment innovation has gotten essential consideration inside the past numerous years due to its potential for a decent form of applications in each social control enforcement and non-law enforcement. As compared with alternative statistics systems mistreatment fingerprint/palmprint and iris, face recognition has distinct blessings thanks to its non-contact method. Face images may be captured remotely while not contacting the person being known, and therefore the identification doesn't need interacting with the person. Additionally, face recognition serves the crime deterrent purpose because of face images that are recorded and archived will later facilitate determine a person. Most biometric technology systems use equivalent fundamental standards of operation [6]. The operation of biometric systems can be summarized as follow:

Enrollment: The procedure by which a client's biometric information is at first obtained, got to, prepared, and put away as a layout for progressing use in a biometric system is called enrollment. Consequent confirmation and ID endeavors are led against the template(s) created amid enrollment.

Presentation: Presentation is a procedure by which client gives biometric information to a securing gadget the equipment used to gather biometric information. Contingent upon the biometric framework, Presentation may require looking toward a camera, putting a finger on a platen, or presenting pass phrase.

Biometric data: The biometric information clients give in a natural image or recording of a trademark. The natural information is likewise alluded to as crude biometric information or as a biometric test.

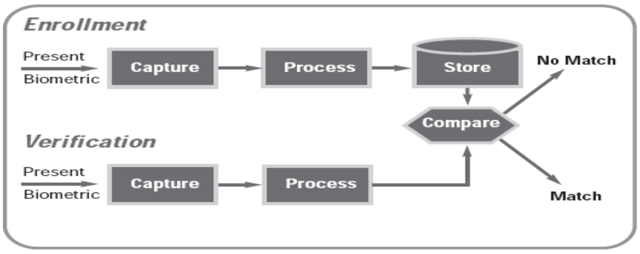

Fig. 1 General Biometric System.

Raw biometric information can't be utilized to perform biometric matches. Rather, biometric information given by the client during recording/verification and confirmation is utilized to create biometric formats, and in pretty much every framework is disposed of from that point. Along these lines Biometric frameworks don't store biometric information frameworks use information for the creation layout. Enrollment needs the generation of an identifier like ID or username. This identifier is normally generated by the user or administrator during entry of personal data. When the user goes to verify, she or he enters the identifier, and then gives biometric data. After acquisition of biometric data, the biometric templates can be generated using feature extraction process.

Feature extraction: feature extraction is the process which dedicates the encoding and location of the biometric data characteristics to produce the templates. Feature extraction can be given during the enrollment/verification process. The process of feature extraction comprises filtration and optimization operation of images. For instance, the scan of voice technologies usually filters specific frequencies and templates. The higher the goodness of features, the greater the performance of the biometric system.

All technologies systems possess their restrictions and biometrics is not an exclusion. Biometric authentication provides many advantages, however, the disadvantages of biometric authentication must be taken into our consideration. The characteristics of biometric are permanent, this reality is one of foundation stone of biometric authentication. Nevertheless, it also consider a disadvantage due to the loss of the biometric identifiers. Unlike, password or PIN which can be modified if stolen. Unluckily, biometric identifiers such as gait, heat map, face, ect.are risky and may be taken without the owner's knowledge. In biometric authentication, prevention is agood remedy. Development the technology of biometric systems can reduce these disadvantages.

According to these reasons, it is necessary to implement cancelable technologies in biometric systems. Many solutions are presented in letrature forcancelability in biometric systems. These systems provide some modification for the biometric data. Several of these modification techniques include functional and polar modifications of Ratha et al., Cartesian [2, 3], cancelable filters of Savvides et al. [5], BioHashing of Jin et al. [4], modifications proposed by Maiorana et al. [8], and Revocable biotokens of Boult et al. [7]. Due to the impairments of these cancelable biometric systems, the performance decreases in comparison with the base line biometric system. However, the performance can be improved by adding some parameter such as (key, token, PIN, password, etc). The verifcation performance of these systems must be analyzed in the stolen key scenario. The performance of BioHashing systems in stolen key scenario is degarded in comparison with the baseline biometric system. Biometric systems based oncryptographic key can give cancelable templates, but the goal of these sytems is to acquire a cryptographic key. Therefore, we will not discuss these methods here [9-12].

In the present paper, we will present a new approach of cancelable face recognition system using the OSH algorithm for cancelable face recognition systems. In this proposed scheme, the face biometric is encrypted with the OSH algorithm. So, the cancelable face recognition scheme is based on the generation of encrypted images using OSH technique. The next stage is based on estimating the correlation coefficient between the encrypted feature matrix of the original face template and the encrypted feature matrix of the user face template. Based on a threshold value, the matcher can decide and classify the output encrypted results as accepted or reject. The quantitative evaluations of the proposed cancelable face recognition scheme have been performed using EER based on the FAR and FRR, the AROC, and decidability.

The rest of the paper a brief introduction about the OSH and the proposed scheme is explained in detail in the third section. The experimental results and discussion are covered in section 4. Finally, the conclusion of the paper is presented in section 5.

The reminder of this paper is arranged as follows. In section 2, the double random phase encryption (DRPE) optical encryption system is presented. In section 3, the proposed cancelable face recognition scheme based on OSH algorithm is explained. Section 4 presents the used evaluation metrics. Section 5 presents the simulation results of the proposed system. Section 6 gives the conclusion of this paper.

II. Cancelable System Based On Optical DRPE Encryption

Optical techniques have exhibited fantastic potential in the information security field. One of the foremost popular methods is the double random phase encryption technique. The DRPE introduced by Refregier and Javidi is based on the modulation of the image spectral distribution. Without any previous knowledge about this spectral modulation or the target image at the receiver, the decoding of the image will not be done. The concept of this approach demonstrated in Fig. 2, which is called 4f optical encryption system. The setup is an optical system consisting of two cascaded lenses separated by two focal lengths as in Fig. 2. The system is implemented as 4 focal lengths with two lens and two random phase masks. In the classical DRPE encryption process, the input plane is put in front of the input image, which is one focal length far from the input lens, and then the Fourier transform is implemented at one focal length far from the lens on the other side [13]. The process of decryption uses the same Fourier Random Phase Mask (RPM) as in the process of encryption. The DRPE has a high quality to prevent attacks [14, 15].

We can implement the DRPE technique for the encryption process using the following equation [13, 16]:

$$\psi(x,y) = FT^{-1}\{FT\{f(x,y)\varphi_n(x,y)\}\times\varphi_m(u,v)\} \qquad (1)$$

where FT represents the Fourier transform, *Ψ (x,y)* is the encrypted image, (*x*, *y*) is the first Random Phase Mask (RPM1) in the spatial domain, and (*u, v*) is the second Random Phase Mask (RPM2) in the spatial domain. It is better to generate random phase masks to execute high quality image encryption by using different distributions like Gaussian, uniform, and impulse distributions.

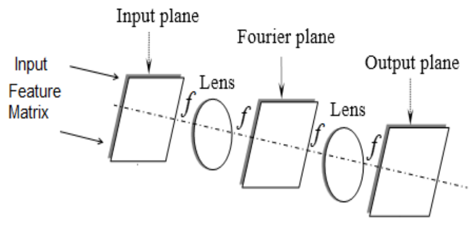

Fig. 2 The DRPE encryption setup.

Fourier transform analysis has witnessed great development in recent years. The FrFT function can be used into image encryption applications [17,18]. The FrFT can be defined as an alternation of time and frequency domain of the two dimensions Fourier transform with definite fractional orders. It can be represented as follows [17]:

$$F_{(\alpha,\beta)}(u,v) = \sum_{x=0}^{X-1}\sum_{y=0}^{Y-1} f(x,y)\Re_{(\alpha,\beta)}(x,y;u,v) \qquad (2)$$

The inverse of FrFT can be represented as follows [17]:

$$f_{(x,y)} = \sum_{x=0}^{X-1}\sum_{y=0}^{Y-1} F_{(\alpha,\beta)}(u,v)\Re_{(-\alpha,-\beta)}(x,y;u,v) \qquad (3)$$

where $\Re_{(\alpha,\beta)}(x,y;u,v)\infty$is the mainly function of the FrFT, α and β are represent the fractional orders. The FrFT can be utilized instead of FT into DRPE technique for the encryption of image [19].

III. THE PROPOSED SYSTEM BASED ON OSH ALGORITHM

Biometry in general and fingerprinting in particular are becoming increasingly important in diverse areas from electronic commerce to homeland security. There is heightened interest to develop new methods and devices for faster and more reliable acquisition of biometric information. In our purposed cancelable fingerprint recognition scheme, we are using the optical scanning holography technique. The OSH is a form of electronic (digital) holography [14]. Electronic holography refers to the fact that holographic recording is done electronically, thereby avoiding the nonreal-time darkroom processing of the film. Digital holography traditionally employs a CCD camera for recording. Optical scanning holography is a real-time technique in which holographic information of a 3D object can be acquired by using a single 2D optical scan where scattered light from the object is detected by a photodetector. Hence, optical scanning holography is a form of digital holography. Optical scanning holography was first proposed by Poon and Korpel [15] and the original idea was later formulated in [16]. The technique was eventually called optical scanning holography to emphasize that holographic recording can be achieved by active optical scanning [17]. Applications of optical scanning holography include scanning holographic microscopy, 3D image recognition, 3D and 3D cryptography [18]. Optical scanning holography involves the principle of optical heterodyne scanning.

In Fig. 3, we demonstrate a typical optical scanning imaging system such as a laser-scanning microscope. A collimated laser beam is projected through the x-y optical scanner to scan out the input object specified by transparency $\Gamma_o(\mathrm{x},\mathrm{y})$. The photodetector converts the light to an electrical signal that contains the processed information for the scanned object. If the scanned electrical signal is digitally stored (in a computer) in synchronization with the 2D scan signals of the scanning mechanism (such as the x-y scanning mirrors), the stored record is a processed 2D image of the scanned object.

Figure 4 shows the optical scanning holography setup. The thick specimen is scanned two-dimensionally by the combination of a spherical wave and a plane wave of different frequencies. The photodetector PD collects all the light and delivers a heterodyne signal at frequency Ω. The heterodyne signal is then electronically processed to give two processed outputs. BPF is a bandpass filter and LPF is a lowpass filter.

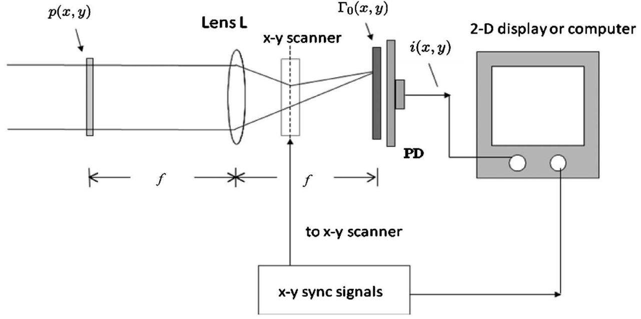

Fig. 3 Standard optical scanning system for imaging.

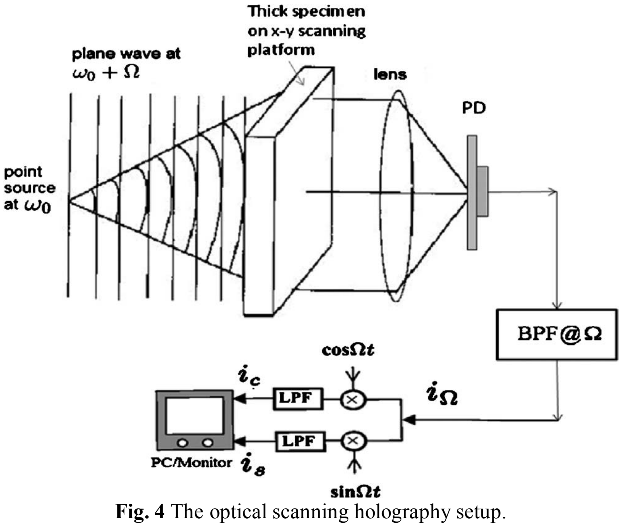

Fig. 4 The optical scanning holography setup.

The solution to this problem is optical scanning heterodyning. In the latter, the object is scanned by a time-dependent Fresnel zone plate, which is the superposition of a spherical wave and a plane wave of different temporal frequencies. The top part of Fig. 3 shows the configuration. The lens is utilized as a light collector that collects all of the transmitted light to the photodetector. In the actual experimental setup, the plane wave and the spherical wave are combined, though a beam splitter and the spherical wave can be derived from a focusing laser beam. The temporal frequency difference Ω between the two waves can be provided by using an acousto-optic modulator [19] or an electro-optic modulator [20] in the path of the plane wave. In the proposed cancelable face recognition system, we exploit the above-mentioned great features and advantages of the OSH technique to generate a new templeate of face image which act as encrypted face image.

IV. Valuation Metrics

A. *False Positive Rate (FPR)*

False positive rate measures the probability that the system gives invalid authentication for genuine subscriber. FPR = (*number of false reject / number of comparisons*) × 100 %.

B. *False Negative Rate (FNR)*

False negative rate measures the probability that the system gives valid authentication for impostor subscriber. FNR = (*number of false accept / number of comparisons*) × 100 %.

C. *Equal Error Rate (EER)*

Equal error rate is the point value which false positive rate and false negative rate are equal due to the intersection between the distributions of genuine and impostor subscribers. Therefore, the lower the value of EER, the greater the security rate of the system.

D. *Receiver Operating Characteristic (ROC) curve*

ROC curve is acquired by calculating the relationship between false positive rate FPR (T) and the True Positive Rate TPR (T) for every threshold value T.

E. *Area under ROC (AROC)*

Area under ROC is a discrimination parameter which demonstrates the capability of the system to distinguish the genuine and impostor subscribers. If the value of AROC near to one this means that the system is more secure.

V. Simulation Results

Performance valuation of cancelable face recognition biometric system relies on the evaluation metrics that measure the relation between subscribes template whose want to access the biometric device and the templates kept on database of biometric device. The correlation coefficient is one of the most commonly used to evaluate performance of cancelable face recognition system due to the reality value of the created template codes. The proposed system can be tested by using the evaluation metrics mentioned above and compared with optical DRPE encryption system. The test can be implemented using face images from the ORL database.
The cancelable templates which generated from face images using the proposed system illustrated in Fig. 5 are shown in Fig. 6. It is obvious that the image templates produced by the proposed system have hidden features which increase the security of the system. To illustrate the performance of the proposed system compared with optical DRPE encryption system based on performance evaluation metrics, the distributions of genuine and impostor for both systems are shown in Fig. 7 and Fig. 8, respictively. ROC curves are evaluated in Fig. 9 and Fig. 10, respictively. Table 1 illustrates a comparison between both systems using AROC and EER metrics. From the table values, it is obvious that the proposed system is better than the optical DRPE encryption system.

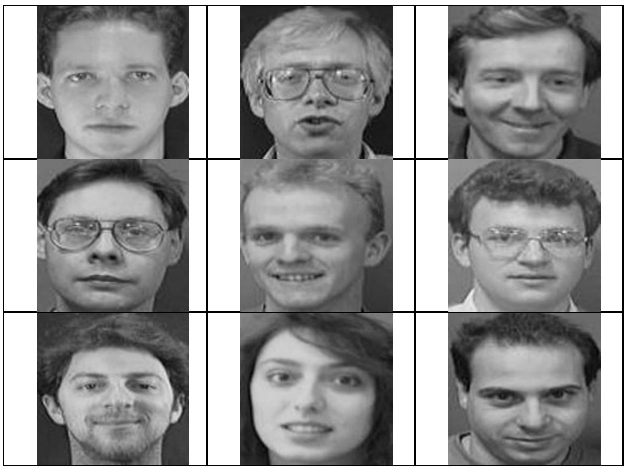

Fig. 5 The original samples of face biometrics.

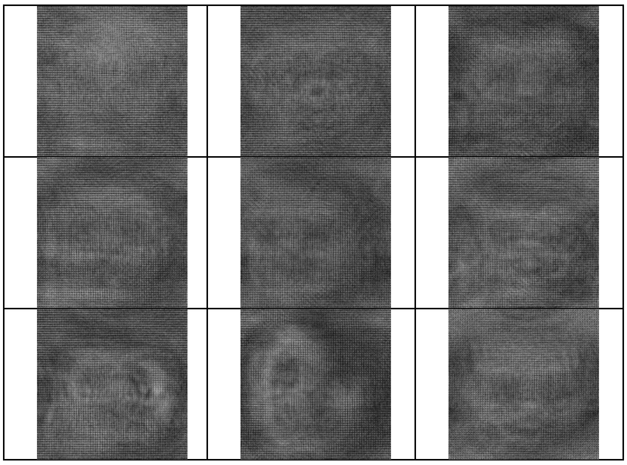

Fig. 6 Samples of cancelable face templates generated with the proposed system.

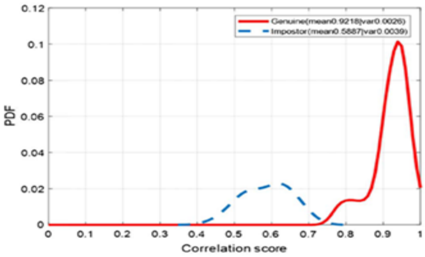

Fig. 7 Distributions of genuine and impostor for the optical DRPE encryption cancelable face recognition system.

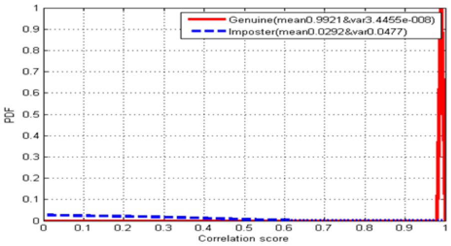

Fig. 8 Distributions of genuine and impostor for the proposed cancelable face recognition system.

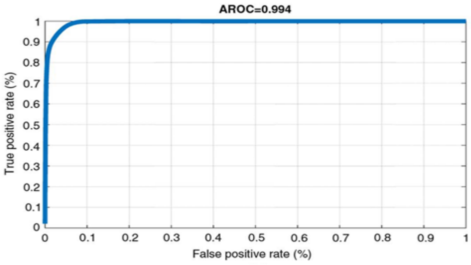

Fig. 9 Distributions of genuine and impostor for the optical DRPE encryption cancelable face recognition system.

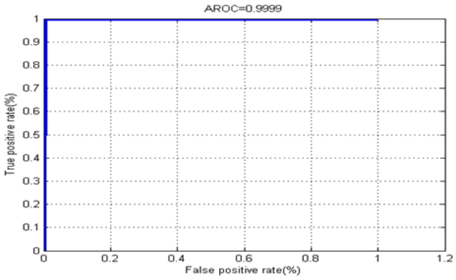

Fig. 10 Distributions of genuine and impostor for the optical encryption cancelable face recognition system.

Table 2 and table 3 are illustrating the effect of noise at difference variance for both DRPE and proposed systems. According to table values, it is clear to us that the proposed system is slightly affected by noise; this is because the idea of the system work is based on adding noise to the original image.

Table 1 Evaluation metrics for both cancelable face recognition systems.

Evaluation metric	Optical DRPE encryption system	Proposed system
AROC	0.993	1
EER	0.0017	0

Table 2 Evaluation metrics for the optical DRPE encryption face recognition system in the presence of noise.

Noise variance	ERR	AROC
0.01	0.00166	0.993
0.02	0.0019	0.994
0.03	0.0013	0.995
0.04	0.0008	0.995
0.05	0.0008	0.9995

Table 3 Evaluation metrics for proposed face recognition system in the presence of noise.

Noise variance	ERR	AROC
0.01	0	1
0.02	0	1
0.03	0	1
0.04	0	1
0.05	0	0.9999

VI. Conclusion

This paper proposed a new system for cancelable face recognition. The proposed system is based on OSH algorithm. The original face images are encrypted by the OSH encryption algorithm. The obtained results show that the proposed system gave high performance as cancelable face recognition biometric systems with comparing with the other related methods.

References

[1] A. K. Jain, A. A. Ross, and K. Nandakumar," Introduction to Biometrics", Springer, 2017.

[2] N. K.Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, Vol. 40, pp. 614–634, 2001.

[3] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29,pp. 561–572, 2007.

[4] A. B. J. Teoh, D. Ngo, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number", Pattern Recognition, Vol. 37, pp. 2245–2255, 2004.

[5] M. Savvides, B.V. Kumar and P. K. Khosla, "Cancelable biometric filters for face recognition", Proceedings of the 17th International Conference on Pattern Recognition (ICPR04), Vol. 3, pp. 922–925, 2004.

[6] L. C. Jain, "Intelligent Biometric Techniques in Fingerprint and Face recognition", 1999.

[7] T. E. Boult, W. J. Scheirer and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis", IEEE Conference on Computer Vision and Pattern Recognition, pp. 1–8, 2007.

[8] E. Maiorana, P. Campisi, J. Ortega-Garcia, and A. Neri, "Cancelable Biometrics for HMM-based Signature Recognition", IEEE Conference on Biometrics: Theory, Applications and Systems (BTAS), 2008.

[9] A. Juels, and M. Wattenberg, "A fuzzy commitment scheme", Proceedings of the Sixth ACM Conference on Computer and communication Security (CCCS), pp. 28–36, 1999.

[10] S. Kanade, D. camara, E. Krichen, D. Petrovska-Delacretaz, and B. Dorizzi, "Three Factor Scheme for Biometric-Based Cryptographic Key Regeneration Using Iris", The 6th Biometrics Symposium (BSYM)**,** 2008.

[11] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi, "Generating and Sharing Biometrics Based Session Keys for Secure Cryptographic Applications", IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)**,** 2010.

[12] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi, "Obtaining Cryptographic Keys Using Feature Level Fusion of Iris and Face Biometrics for Secure User Authentication", IEEE CVPR Workshop on Biometrics**,** 2010.

[13] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", Optics Letters, Vol. 20, pp. 767-769, 1995.

[14] T.-C. Poon, "Optical Scanning Holography with MATLAB", Springer, New York, 2007.

[15] B. D. Duncan and T.-C. Poon, "Gaussian beam analysis of optical scanning holography," J. Opt. Soc. Am. 9, 229–236 (1992).

[16] A. M. Elshamy, A. N. Z. Rashed, A. A. Mohamed, O. S. Faragallah, Y. Mu, S. A. Alshebeili, and F. E. Abd El-Samie, "Optical image

encryption based on chaotic Baker map and double random phase encoding", IEEE Journal of Lightwave Technology, Vol. 31, No.15, pp. 2533-2539, 2013.

[17] SC. Pei, and MH. Yeh, "Two dimensional discrete fractional Fourier transform", Signal Processing, Vol. 67, pp 99-108, 1998.

[18] H. M. Ozaktas, "Fractional Fourier Domains", Signal Processing, Vol. 46, pp. 119–124, 1995.

[19] S. K. Rajputa, and N. K. Nishchal, "Optical double image security using random phase fractional Fourier domain encoding and phase-retrieval algorithm", Optics Communications, Vol. 388, pp. 38–46, 2017.

[20] R. Soliman, G. El-Banby, A. D. Algarni, M. Elsheikh,"Double Random Phase Encoding for Cancelable Face and Iris Recognition", Applied optics, Vol. 57, pp. 10305–10316, 2018.

[21] D. Giveki, M. A. Soltanshahi, and G. A. Montazer, " A new image feature descriptor for content based image retrieval using scale invariant feature transform and local derivative pattern", Optik - International Journal for Light and Electron Optics,Vol.131, pp 242-254, 2017.

[22] R. Rajkumar and K. M. Singh, " Digital image forgery detection using SIFT feature", International symposium on Advanced Computing and Communication, Silchar India, pp.1-6, 2015.