International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol. 7, No. 6 (2014), pp. 231-242
http://dx.doi.org/10.14257/ijsip.2014.7.6.19

Multi Unit Iris Biometric Encrypted Template Formation and Authentication

Shoaib Amin Banday[1], Saba Mushtaq[1], A.H. Mir[1]

*[1]Department of Electronics and Communication Engineering,
NIT Srinagar J&K India-190006*

Shoaibee.a@gmail.com, sab.mushtaq@gmail.com, ahmir@nitsri.net

Abstract

Biometrics has been one the main security solutions in almost every type of infrastructure (whether critical or non-critical) ranging from the main doors at home, libraries to the critical infrastructures like banks and airports. Despite the forceful impetus on research on biometric security that has taken biometrics from one simple level to much higher levels of security, there are still some open challenges in this field of security that need to be filled. Among all those challenges and loopholes, the security of template is of the most important concern. The reason for this is that we don't want any identity compromises. If a biometric template in the database of the system of a person is compromised that consequently would mean identity theft of that person. This paper proposes a novel method that uses two different biometric data from the same person for making a biometric template against each person. The two biometric modalities that have been used in our work are left and right iris using best features. The features and verification of the proposed system has been done using MATLAB.

Keywords: *Biometrics, template security, cryptography, biometric security issues, Recognition rate*

1. Introduction

The security of the most important sectors (critical infrastructures) of a country is of essential concern. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to a country that their incapacitation, destruction or compromise would have a fatal effect on security, national economic security, national public health or safety, or any combination thereof. One way of securing these crucial places is to make authentic access systems that could filter out the legitimate and non-legitimate entrants. This key problem is solved using a variety of inherent human biometrics which were understood and studied over a span of large time. This decades old solution has been the use of human physiological and behavioral characteristics as data for authentication [1]. This individual data is very strong in a sense that varies significantly over the population. The biometric security system consists of mainly of five modules viz: a sensor module, pre-processing module, feature extraction module, matching module and a decision module. Traditional biometric identification/verification systems have shown a significant increase in terms of recognition accuracy and speed. Yet, every biometric system is vulnerable at all the stages. As the Figure 1 below shows, there can be attacks on every module and the result of it can be very fatal. In all these attacks however, the most challenging and of utmost importance is the attack on the template database. A biometric template (also called *template*) is a digital

ISSN: 2005-4254 IJSIP

representation of unique characteristics that have been extracted from a biometric sample of an individual. A template is the final gist of the overall human identity and its compromise can simply lead to an identity loss. Biometric templates now a days is known to be the identity of a person and these are used during the biometric authentication process.

The slow yet profound application of biometric identification system today has improved security and creates much convenience to identity authentication. However, there are still some inherent problems that need to be solved. For instance, masquerade attack, difficulties to republish when the template is lost and a series of other potential threats. The existences of these threats have created a bottleneck, constraining further development of the biometric identification technology.

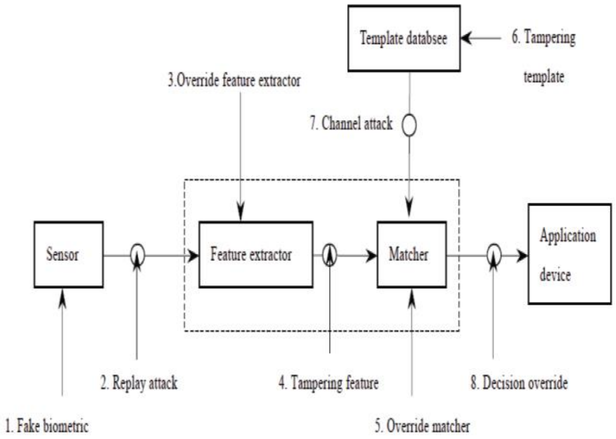

Figure 1. Sites of Biometric vulnerabilities [2]

The security and access control are major requirements that are essential in this highly sophisticated and technologically advanced society. Ranging from small gadgets at home to the most critical infrastructures, security and authentic access control are the need of the hour. Just like we have simple access control for laptops, mobiles phones, home entrances etc. there is a similar demand of the same at higher important levels like banks, airports hospitals etc. There has been an plethora of research that is inclined in the direction of security and access control. The initial systems used passwords, pin codes, swipe cards for access control and later they were replaced by use of human physiological and behavioral characteristics (biometrics) of a person for the same. The progress continued and the security systems went from good to better with each passing year. There however still remain plenty of open challenges that need an optimum solution. One such being issue is being addressed through this work.

Broadly speaking we have two types of security systems they are biometric authentication & biometric with cryptography [1]. Biometric authentication systems use human physiological and behavioral characteristics as data for authentication. This individual data is very strong in a sense that varies significantly over the population. However biometric authentication systems have the tendency of being vulnerable at all stages [2]. Biometric systems with encryption techniques have proven that they are potentially strong enough to withstand any attempt to be breached. However at the same time, with the use of the powerful computers, these encryption techniques can easily be broken. This demands the need for a more reliable system that has very little chances of being broken even with computationally more powerful computer.

Securing the biometrics templates is becoming a major task for the template security developers. The reason behind this is that literally a person's identity is finally stored as an template in the database. If this template is compromised or stolen, this would eventually mean that the person has lost its identity. Since the person cannot change or modify his biometric traits, that means he has lost it forever. So securing a template is big challenge in the field of security and considering the current trend of technology. The work in this paper proposes a novel approach for the template security. The paper is written in 6 sections. Section 2 discusses various security issues in template security. The literature survey in section 3 is followed by our proposed method in section 4. The results and discussions are put in section 5 and conclusion in section 6.

2. Security Issues

The security issues in biometric systems are increasing very rapidly. The security is the major task which should be taken care by the security system developers. The template data is the crux of the whole biometric autentication system. Once an imposter gets through the system, he can do damage of all kinds, so we need to take care of this very seriously and effectively. If ones templates are lost it is not easy to revoke them. For the security developers the template protection is critical task that needs to be addressed properly.

2.1 Liability of biometric systems

Based on the lack of proper secured infrastructure, the biometric system vulnerabilties occur. We have two kinds of biometric system failures:

1) Intrinsic failure

2) Adversary attack

1) **Intrinsic failure**: it generally happens because of improper decision made by the system.Two types of error decisions are made by the systems they are: false accept and false reject. The false acceptance generally is a result of lack of proper uniqueness and individuality of the templates. Due to this we will be having different people in the same cluster range. In false reject, the system rejects a legitimate user and the resaon for this is that, difference in the user stored template data.This happens mostly at the sensor level because of improper intraction with the sensor like change in position and expressions and also because of improper data acquisation of the individual. These all issues lead to Failure-to-enroll(FTE) Failure-to-acquire(FTA). Accepting a wrong person is more dangerous than rejecting a genuine person [3].

2) **Adversary attack**: In this adversary attacks on the biometric system his success is dependend on the loop holes of the system. Here we have three sub-classes of attacks.

a) *Administration attack* :-

This attack is also known as insider attack, this happens because of in secure administrationof system.This includes enrollment also.

b) *Non-secure infrastructure*:-

The system infrstructure means it includes all the software,hardware and communication channels of the biometric system.There many ways were an attacker can attack the infrastructure which laed to system attacks

c) *Biometric overtness*:-

There is possibilty that an adversary obtaining the fingerprint of genuine person and fake them by gummy finger method to avoid this the system should be capable of lively detection if so even the intruder provide spoofed finger prints the system wont allow him to get through.

Generally attacker attacks the system at one or more modules or interfaces. We divide these attacks into four categories.

1) Attacks at the user interface
2) Attacks at interfaces between modules
3) Attacks on the modules.
4) Attacks on the template database.

Attacks at user interface:-

In general the attacks on user interface occurs by producing the spoofed trait to the system. The system should be developed in away that it should be able to do lively detection so the intruders cant enter by spoofed traits [4-9].

Attacks at interfaces between modules:-

The inetrfaces are generally left unsecurely they also should be secured if so the intruder attacks at these places by keeping jammaers and many other methods.If the channel is not protected cryptographically and phsically the attacker can the change data and resend it.there chance of replay and hill-cli,bing attack.it is better use some keys and time stamps for better security [10-12].

Attacks on template database:-

The template data base attack is most dangerous attack on the biometric systems becauses the results of this are unable to expect.This attack leads to three vulnerabilities.

1) to gain access a spoof can be created from the orginal.

2) template can be replaced for gaining access.

3) the stolen template can be used any way to gain access to the system. By controlling all these drawbacks and loopholes we can decrease the chances of attacks on the system. We shuold improve techniques to revoke the stolen templates if not we cant expect threats (for example thr intruder can changes the template of any higher official by his template to gain access) [13-15].

3. Related Work

The field of biometric template security is a very important field that has got a continuous impetus because of challenges and loopholes that have emerged with time. Though we have a feeble work done in template security area and have less methods to eradicate these security issues but these are not sufficient to save template database from the attackers. Broadly a template security literature which comprises of techniques and algorithms for making templates secure can be divided into four groups:

Bio-hashing:

Bio-Hashing is an approach which is equal to the password approach.In this technique the biometric data only the pins or passwords are generated. The challenge of cancellable biometrics was addressed by [1] which used a technique known as Bio-hashing. [2] proposed a novel approach for authentication. It was based on inner products between tokenised pseudo-random number and the user specific fingerprint data. This produced a unique and compact code for every user and that was named as Bio-hashing. Hashing is completely based on password(p) generation which is connected with the pesudorandom(generation of random numbers by a definite computational process) string S for resulting H(P+S).

Non-invertible transformation:

The Non-invertible transformation [3] proposed this method of template data security. Here, a Non-invertible transformation is performed on the biometric template. Thus a transformed biometric template stores only the values of feature vector but not the original biometric data.This approch provides diversity of biometric template and also offers cancellable biometric features. It is very hard to obtain identical structures and Non-invertible features. The construction of the original image can be done by getting the triplet values as done by [4, 5] and [6].

Key-binding:

The method of key binding uses a user specific key that is known as the helper data. The helper data which is independent to every biometric data. The biometric data that is extracted from the user is binded with this helper data and together stored in the database. The tolerance can be determined by checking the error correcting capability. Leaking of key is big problem in this because matching is done by using the error correcting code for matching with the original template so we have chances of key leaking as in [7, 8, 9, 10, 11] and [12].

Key-generating:

In this key is generated by using the data of the biometric only. The cryptography technique plays a major role in this scheme. To obtain the key these are apllied on biometric template data. Generation of key can be done directly from the biometric data and no external mechanism is used . It invokes the cancellable biometrics. Generating a key with higher stability and entropy is very hard. So we a have chance of deriving same keys because of unclear features of template data which leads us to mismatch of template [13, 14, 15] and [16]. Different key generating techniques are as follows:

Fuzzy vault generation is one of the mostly used key generating technique and has been used quite a large in the security of the template. This is achieved by using feature level fusion for generating single multi-biometric template and they use fuzzy vault construction for the protection of templates [17]. Other key binding technique that is used makes use of multimodal biometrics. Here, bit-extraction from the multimodal biometric is done. In this type of template protection the use of secure and revocable biometric along with bit-string generation technique is used [18]. There has also been quite a significant work using higher order signal processing techniques which ensures a relaible security, privacy and canceability. These techniques are robust and uses hash functions [19]. Moreover, for securing the iris templates the water marking method is used. They make use of a smart shuffling algorithm to make difference between geniune and impostor [20]. Another technique that is capable of diversity, revocability, security and performance is by the use of simple orthonormal random project scheme. It is done based on block diagonal matrix of local rotations [21].

4. Proposed Method

The proposed template security approach is the extension of the previous biometric temlate security approaches as discussed in the literature survey in section.3. One of the main drawbacks in those approaches was that they used a key which was externally generated and had a good chance of being broken. In this work we have proposed a multimodal biometric (left and the right iris) authentication system with AES encrypted template generation. The left iris textural features are used as data for final template formation and right iris textural features are used as the key. The systematic diagram for this proposed approach is given in Figure 2. This approach works in two phases:

1) Enrolment phase

2) Verification phase

As can be seen from Figure 2, the users are first enrolled into the system. The process starts with the image acquisition of the user biometric which in this case are the left and the right iris. Once the images are captured from the user, these images are pre-processed in parallel. The pre-processing of images is done to reduce the noise which might have got incorporated at the time of acquisition. The other steps of pre-processing are done to qualitatively enhance the image so that more information can be extracted out of these. Since iris is such a biometric modality in human body that is very rich in textural information, we extracted the second order textural features from both left and right iris. The list of the textural features that were extracted are given. There were a total of eight textural features that were extracted from each left and right iris and later on only three features were found to vary considerably over population. The selection of proper features was done using Principle Component Analysis (PCA). The final feature set obtained from left and right iris is encrypted using Advanced Encryption Standard (AES) which is based on the principle of substation-permutation. The main issue here in these template encryption methods is that, the small change in the input feature vector is reflected quite largely at the output. This means that we won't be getting the template back with the input that has slightly changed. This issue was however addressed by assigning each user to a cluster. A cluster is group of points in space belonging to a single user. So a subject under consideration falls under two clusters for left and right iris respectively. For each cluster, a subject is assigned a unique data value and a key from left and right iris respectively.

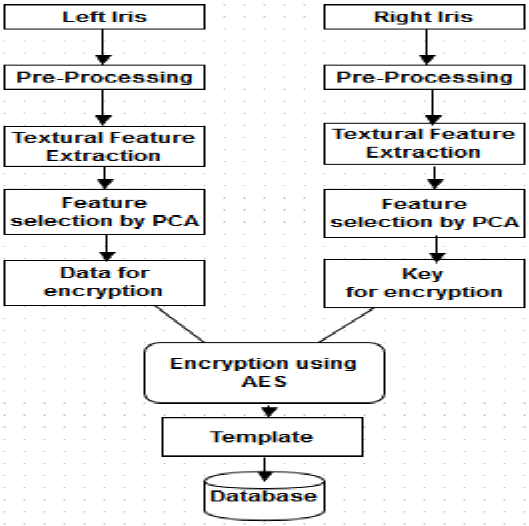

Figure 2. Enrollment Phase

The proposed method provides two-fold advantage, one being that it uses information from both irises of a person, thus making a strong authentication system. The other advantage is that one of the iris information is used to encrypt the information obtained from the other iris. The features of iris are the textural features (Gray Level Co-Occurence Matrix). These are the second order statistical features. There features are best suited to images that are having a rich texture as here in the case of the iris. Eight GLCM were computed from both the irises of a person and later only there were used since they features suffice the need and these are entropy, correlation, homogeneity. The features obtained left iris acts as a data and key for the same set of features from right iris respectively for our template security system. As shown in Figure 1 for enrolment phase, once the data and the key from left and right iris are obtained respectively, they are encrypted using Advanced Encryption Standard. This forms a final template for each person and this is stored in the database as shown in Figure 2. In a similar way, templates are developed for all legitimate persons and stored in database. In the verification phase the feature from both the irises similarly extracted as in the phase of enrolment. As shown in Figure 3, once the features have been calculated they are matched with the database. The extend of matching obtained through the matcher determines the legitimacy of the person. If either of the two matcher fails to match then the access is denied otherwise granted. If an person wants an access, firstly he should provide image acquisition of iris to the system then only he will be authenticated.

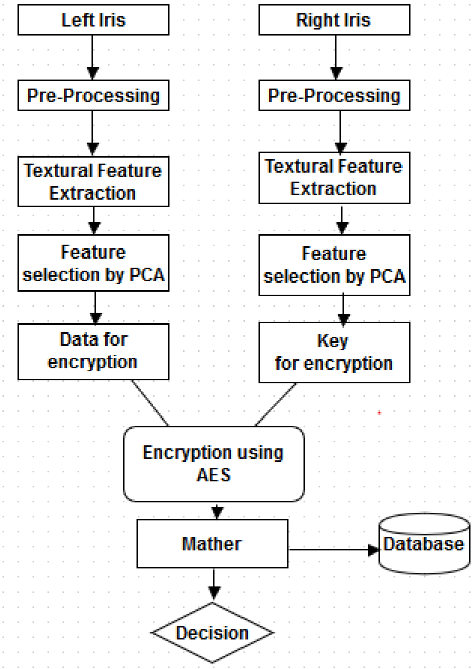

Figure 3. Verification Phase

5. Results and Discussion

Experiments were carried on CASIA eye image DB V1.0 and the each image is a Grey scale bit-map with resolution of 320 x 280. The parameters calculated for the evaluation of the results for this system are recognition rate (RR), false acceptance rate (FAR) and falsse rejection rate (FRR). The recognition rate is the extend to which a system correctly accepts the genuine user and correctly rejects the imposters. The FAR and FRR are other two parameters which actually shows the error comitted by the system. These parameters were saperately calculated for the fingerprint, iris and the encrypted system. For left iris these parameters obtained are:

FalseAcceptanceRate(FAR= $\frac{No\ of\ False\ Acceptance}{Total\ FA\ attempts}$ =0.57%

False Rejection Rate(FRR)= $\frac{No\ of\ False\ Rejection}{Total\ FR\ attempts}$ =7.7%

Recognition Rate(RR)= $\frac{GA+GR}{Total\ Attempts}$×100 = 95%

Where GA is genuine acceptance and GR is genuine rejection. Figure 4 is the plot between Threshold and False acceptance rate for the left iris. The minimum FAR was obtained for a threshold value of 30. Figure 5 shows the distribution plot for genuine and imposter using only left iris for authentication. As can be seen from the plot there is a significant overlap of the two plots. This indicates the extend to which some percentage of Genuine users are treated as imposter by the system.

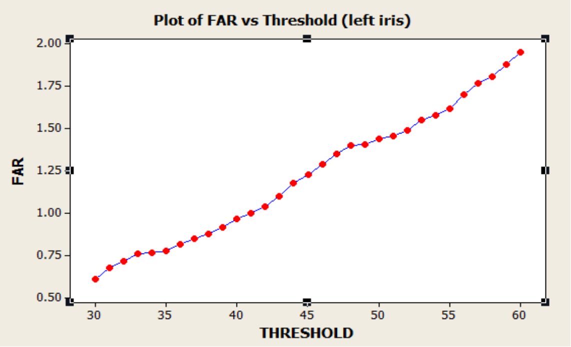

Figure 4. Plot between Threshold and FAR (Left Iris)

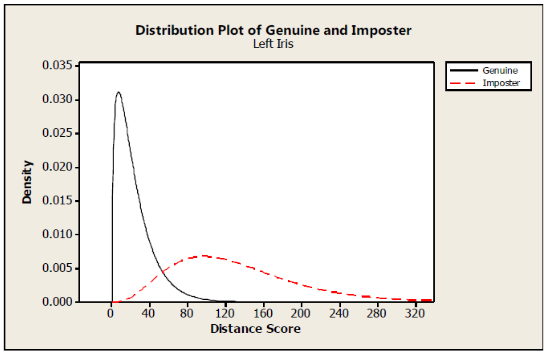

Figure 5. Plot of Overlap between Genuine and Imposters (Right Iris)

Similarly for right iris these parameters are:

$$\text{False Acceptance Rate(FAR)}= \frac{No\ of\ False\ Acceptance}{Total\ FA\ attempts} = 0.8\%$$

$$\text{False Rejection Rate(FRR)}= \frac{No\ of\ False\ Rejection}{Total\ FR\ attempts} = 8.3\%$$

$$\text{Recognition Rate(RR)}= \frac{GA+GR}{Total\ Attempts} \times 100 = 93.2\%$$

Similarly, the minimum FAR for right iris was found out to be 0.8% and FRR of 8.8%. Figure 6 shows a plot of various FAR's versus the threshold. Here also the amount of threshold between the two populations (Genuine and imposters) is large, which indicates a large error rate. However when both left and right iris are used together, we achieve a much better performance. Figure 8 shows a plot of the distributions of genuine and imposter populations when both left and right iris are used for authentication. As already mentioned, left iris features are encrypted using the features of the right iris.The overlap in this case is minimum as evident from the plot which means a small error rate.

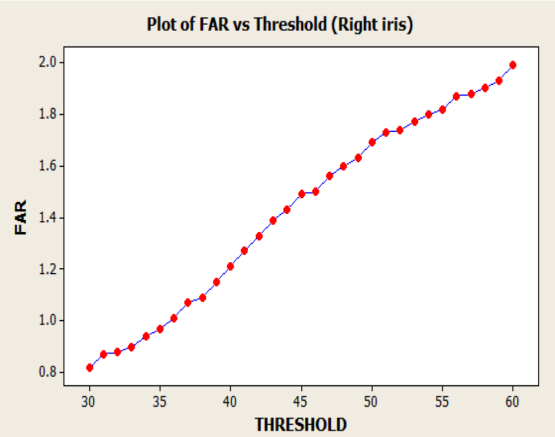

Figure 6. Plot between Threshold and FAR (Right Iris)

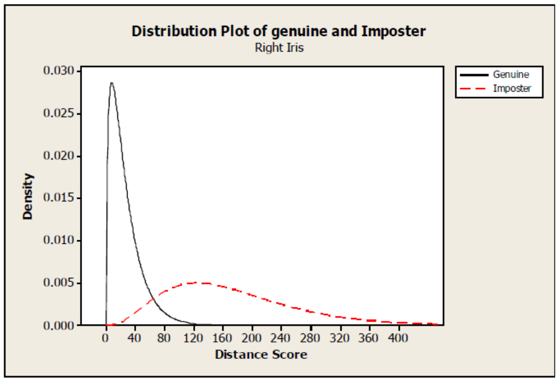

Figure 7. Plot Of Overlap between genuine and Imposters (Right Iris)

Performance Parameters final proposed system (of system):-

False Acceptance Rate(FAR) $= \frac{No\ of\ False\ Acceptance}{Total\ FA\ attempts}$ = 1.85%

False Rejection Rate(FRR)= $\frac{No\ of\ False\ Rejection}{Total\ FR\ attempts}$ =5.14%

Recognition Rate(RR)= $\frac{GA+GR}{Total\ Attempts}$×100 = 98.2%

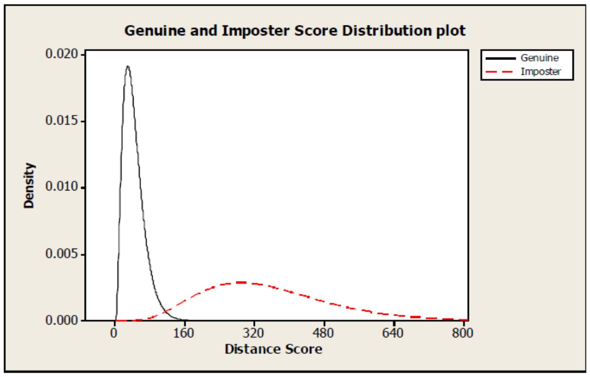

Figure 8. Plot Of Overlap between genuine and Imposters (using both irises)

6. Conclusion

The method discussed above depicts that this has a capability of eliminating most of the demerits which are put forward by the earlier techniques. This approach uses multi-unit iris biometric along encryption for securing the templates. The results show that this approach is better than the indivisual left or right iris systems. This technique can provide better security for the template database. The Recognition rate for left iris is obtained as 95% when used saperately. Similarly the recognition rate for right iris is 93.2%. Using the proposed system the recognition rate obtained was 98.2% which clearly depicts the success of this system.

References

[1] C. Roberts, “Biometric attack vectors and defences”, Computers and Security, vol. 26, no. 1, **(2007)**, pp. 14–25.

[2] N. Ratha, J. Connell and R. M. Bolle, “An analysis of minutiae matching strength”, Audio and Video-Based Biometric Person Authentication, Bigun, J. & Smeraldi, F, **(2001)**, pp. 223−228, Springer Berlin, ISBN 978-3-540-42216-7, Heidelberg, Germany.

[3] A. Ross, K. Nandakumar and A. K. Jain, “Handbook of Multibiometrics”, Springer, Berlin, Germany, **(2006)**.

[4] T. Connie, A. Jin, A. Goh and D. Ling, “PalmHashing: A novel approach for dual-factor authentication”, Pattern Analysis & Applications, vol. 7, no. 3, **(2004)** August, pp. 255−268, ISSN 1433-7541.

[5] A. Jin, D. Ling and A. Goh, “An integrated dual factor authenticator based on the face data and tokenised random number”, Biometric Authentication, Zhang, D. & Jain, A. **(2004)**, pp. 117−123, Springer Berlin, ISBN 978-3-540-22146-3, Heidelberg, Germany.

[6] N. K Ratha *et al.*, “Generating cancelable fingerprint templates”, IEEE Trans. PatternAnal. Machine Intell. vol. 29, no. 4, **(2007)**, pp. 561–572.

[7] 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, no. 4, **(2007)**, pp. 561-572.

[8] Y. Sutcu, H. T. Sencar and N. Memon, “A Secure biometric authentication scheme based on roust hashing”, Proceedings of the 7th Multimedia and Security workshop, **(2007)** August, pp. 111-116, New York, USA.

[9] A. B. J. Teoh, K. A. Toh and W. K. Yip, “2N Discretisation of Biophaser in cancelable biometrics”, proceedings of 2nd International conference on Biometrics, **(2007)** August, pp. 435-444, Seoul, South Korea.

[10] T. E. Boult, W. J. Scheirer and R. Woodwork, "Revocable fingerprint bio-tokens: Accuracy and security analysis", Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, **(2007)** June, pp. 1-8, USA.

[11] K. Nandakumar, A. Nagar and A. K. Jain, "Hardening Fingerprint Fuzzy Vault Using Password", Proceedings of 2nd International Conference on Biometrics, **(2007)** August, pp. 927-937, South Korea.

[12] X. Boyen, "Reusable cryptographic fuzzy extractors", proceedings of ACM conference on Computer and Communication security, **(2004)** October , pp. 82- 91, Washington, USA.

[13] S. Yang and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme", Proceedings of the IEEE International Conference on acoustic and Signal Processing, vol. 5, **(2005)** March, pp. 602-612, Philadelphia, USA.

[14] Y. Chang, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, "Automatic Alignment of fingerprint features for fuzzy fingerprint vault", Proceedings of the 1st Conference on Information security and cryptology, vol. 3822 of Lecture Notes in Computer Science, **(2005)** December pp. 358-369, Beijing, China.

[15] U. Uludag and A. K. Jain, "Securing fingerprint template: Fuzzy vault with helper data", Proceedings of the Conference on Computer Vision and Pattern Recognition Workshops, **(2006)** June, pp.163, Bewyork, USA.

[16] Y. J. Chang, W. Zhang and T. Chen, "Biometric based cryptographic key generation", proceedings of the IEEE International Conference on Multimedia and Expo, vol. 2, **(2004)** June, pp. 2203-2206, Taipei, Taiwan.

[17] C. Viellhauer, R. Steinmetz and A. Mayyerhofer, "Biometric hash based on statistical features of online signatures", Proceedings of the International conference on Pattern Recognition, vol. 1, **(2002)** August, pp. 10123- 10126, Canada.

[18] Y. Dodis, R. Ostrovsky, L. Reuzin and A. Smith, "Fuzzy extractor: how to generate strong keys from biometrics and other noisy data", Tech. Rep. 235, **(2006)** February.

[19] Y. Dodis, L. Reuzin and A. Smith, "Fuzzy extractor: how to generate strong keys from biometrics and other noisy data", Proceedings of International Conference of the Theory and Applications of cryptographic Techniques: Advances in Cryptology, vol. 3027 of Lecture Notes in Computer Science, **(2004)** May, pp. 523-540, Switzerland.

[20] K. Nandakumar and A. K. Jain, "Multibiometric Template Security Using Fuzzy Vault".

[21] Y. J. Chin, T. S. Ong, A. B. J. Teoh and M. K. O. Goh, "Multimodal Biometrics based Bit Extraction Method for Template Security".

[22] B. Chen and V. Chandran, "BIOMETRIC TEMPLATE SECURITY USING HIGHER ORDER SPECTRA.

[23] M. Fouad, A. EI Saddik and E. Petriu, "COMBINING DW T AND LSB WATERMARKING TO SECURE REVOCABLE IRIS TEMPLATES", 10th International Conference on Information Science, Signal Processing and their Applications, **(2010)**.

Authors

Shoaib Amin Banday received his B.TECH degree in Electronics and Communications Engineering from Islamic University of Science and Technology, J&K, India in year 2011. He has done his M. Tech. degree in Communication and Information Technology from National Institute of Technology, Srinagar, India in 2013. Presently he is a research scholar at NIT Srinagar in Department Of Electronics and Communication. His research interests are Image Processing, Pattern Recognition and Biometric Security.

Saba Mushtaq received her B.E. degree in Electronics and Communications Engineering from Kashmir University, India in 2008. She has done her M. Tech. degree in Communication and Information Technology from National Institute of Technology, Srinagar, India in 2012. She joined NIT Srinagar in September 2012, as a faculty member. Presently she is a research scholar at NIT Srinagar in Department Of Electronics and Communication. Her research interests are Image Processing and Biometrics.

Ajaz Hussain Mir has done his B.E in Electrical Engineering with specialization in Electronics & Communication Engineering (ECE) .He did his M.Tech in Computer Technology and Ph.D both from IIT Delhi in the year 1989 and 1996 respectively. He is Chief Investigator of Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA). He has been guiding PhD and M.Tech thesis in Security and other related areas and has a number of International publications to his credit Presently he is working as Professor in the Department of Electronics & Communication Engineering at NIT Srinagar, India. His areas of interest are Biometrics, Image processing, Security, Wireless Communication and Networks.