An Elaborated View on Biometric Template Protection

Anjana.P[1] Betty.P[2]
[1]P.G Scholar [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Kumaraguru College of Technology, Coimbatore, India

Abstract— Biometric is a biological traits and being a bodily elements used in various sectors and application because of its identity. Biometric is a biological element used to uniquely identify the individual. It is an alternative to a traditional approach because of its uniqueness. Biometric authentication has been used in various sectors like surveillance, authentication. One of the most important characteristics of biometric authentication is Irrevocability. It is one of the important characteristics of biometrics since unlike other data, biometric can't be faked. Biometrics are very sensitive data and it is more sensitive to vulnerability because biometric once compromised it is compromised forever. Because of its sensitivity many models adopted multi modal biometric rather than uni-modal biometric to provide better security. Thus biometric system needs higher security to preserve the biometric hacking. Biometrics has been adopted in much application now-a –days. To secure such a sensitive data many security models have been introduced like multilevel encryption, hybrid encryption etc., a detailed survey on these template protections has been discussed with the advantages and disadvantages.

Key words: Biometric template; Security; Encryption methodology; Irrevocability

I. INTRODUCTION

Identification is very much important because of finding the person under mass surveillance. Authentication is also needed in various sectors as internet evolves everywhere. Today all technology evolves with the touch of internet and almost everything we do online which requires online authentication, identification and e-transaction [32]. As internet grows consequently identification and authentication are also needed. To identity the people under surveillance identification is much needed. Traditional approach of identification and authentication involves user name and password. Password based system is such a messy as people always prefers easy password and uses the same password for many accounts is makes the job of hackers very easy.

Thus unlike an password system , biometrics which is an bodily element and uses the biometric traits as password .Biometric traits is an bodily element so users doesn't want to carry it anywhere nor to remember . Biometric traits provide the unique to a great certainty. Biometric system in which the biometric data used are very sensitivity and can't be false proof. Biometric database once compromised it is compromised forever.

A biometric template is a digital reference of distinct characteristics that have been extracted from biometric sample. Processed image like templates are used during the biometric authentication process .In biometrics, a fingerprint template is the name used to describe a stored file in a fingerprint scanning system .When a fingerprint is entered in to the system, only a "template" of the fingerprint [7]. Is stored, not an image of the fingerprint. A fingerprint template is smaller than the actual fingerprint image and using the template instead of an image makes for faster processing time.

Attacks on Biometric template are the following [19]:

- Template can be replaced by an imposter's template to gain unauthorized access
- Physical spoof can be created from template to gain unauthorized access to the system
- The stolen template can be replayed to matcher to gain unauthorized access.

An ideal template protection scheme should possess the following properties [19]

- Diversity: The secure template must not allow across matching across the databases, thereby ensuring users privacy.
- Revocability: It should be straightforward to revoke compromised template and reissue a new one based on the same biometric data.
- Security: It must be computationally hard to obtain original biometric template from secure template.
- Performance: The biometric system should not degrade the recognition performance of the biometric system.

Biometric security has few characteristics which should be preserved to have a secure processing using these biometric features. These characteristics are very unique especially for the sensitiveness of biometrics. The characteristics are broadly classified into physiological and behavioral characteristics. Any distinguishing characteristics of an individual that can be measured and extracted from a biometric sample for the purpose of biometric identification. Biometric is mainly used to follow a simple rule of "Defend yourself against identity theft.

Characteristics of successful biometric identification needs [22]

- The physical characteristics should not change over the course of the person's lifetime.
- The physical characteristics must identity the individual person uniquely
- The physical characteristics need to be easily scanned or read in the field, preferably with inexpensive equipment, with an immediate result.
- The data must be easily checked against the actual person in a simple, automated way

One of the most challenging characteristics of biometric is that these characteristics may be affected by changes in age, environment, disease, stress, occupational factors change in human interface etc. These characteristic of biometric template can be handled using the approximate security algorithms in which storage issues are also concerned. The user keys are replaced with biometric trait for flexible usage of the system.

Biometric systems meet the requirements of revocability, diversity, security and performance. These requirements greatly influence the security as well as storage of the biometric templates. Problem of ensuring securing of biometric data is crucial. Biometric system has four main modules. It has sensor module, feature extraction module, database containing biometric template and module of comparison.

In all these modules there are possibility of attack .These are roughly eight levels of attack in biometric systems. Some of the attacks are,

Two most important concern of biometric system are security and storage of biometric templates. Storing such a template means that it requires more storage space and also it should be stored securely. These two concerns must be addressed in all biometric systems. If the biometric data is recorded in central database, privacy concerns may be higher. To satisfy the privacy concerns many encryption algorithms are used and for storage space reduction many cropping and size reduction algorithms are used.

Problems With large database make biometric identification process does not scale well with size and also search space will be high. Biometric templates are high dimensional and has no linear ordering or sorting exists for biometric data. Biometric templates with no privacy means other person to easily theft the person's individuality and it will severe issue since biometrics once compromised it is compromised forever.

Biometric traits follow very important characteristics irrevocability. Thus to maintain its characteristics biometric must be reversed. Unlike password system in which once password are compromised we can demand for another password .But in biometric system in which once the biometric traits are compromised then we can't change or demand for another biometric as it is bodily element of an individual .Thus biometric can't be replaced. Thus securing these biometric traits are growing now and many technology and methodology have been followed. The biometric traits are secured in database, communication channel, etc.

Various techniques have been discussed along with advantages and disadvantages in the following sections with the explanation of the algorithm being discussed.

II. Review on Various Biometric Template Protection Techniques

Biometric has been used in various applications for its uniqueness and authentication .While using biometric systems, only the feature which are extracted from the biometric are used. These feature of the biometric trait are called as biometric template and these template are stored in the database and used during enrollment and verification process .During the process the biometric traits are taken as input using the sensors and they are converted into digital information and these digital information of a biometric traits are called as template and used for the authentication purpose.

These biometric template has to be protected because biometric once compromised then it is compromised forever. Thus to maintain its irrevocability characteristics template protection is needed. Thus if a user A wants to create a mail account with another user B using his biometric , the user A may think that B is an imposter and he is interested in his account or the communication channel is vulnerable similarly the user B may be imposter and later deny his service and also communication channel is vulnerable. Thus to avoid these vulnerabilities template protection is needed. Compromising the biometric traits makes an individual to lose his identity and it cannot be replaced. Two most important concern of biometric system are security and storage of biometric templates. Storing such a template means that it requires more storage space and also it should be stored securely. These two concerns must be addressed in all biometric systems. If the biometric data is recorded in central database, privacy concerns may be higher. To satisfy the privacy concerns many encryption algorithms are used and for storage space reduction many cropping and size reduction algorithms are used.

Problems With large database make biometric identification process does not scale well with size and also search space will be high. Biometric templates are high dimensional and has no linear ordering or sorting exists for biometric data. Biometric templates with no privacy means other person to easily theft the person's individuality and it will severe issue since biometrics once compromised it is compromised forever.

Biometric traits follow very important characteristics irrevocability. Thus to maintain its characteristics biometric must be reversed. Unlike password system in which once passwords are compromised we can demand for another password. But in biometric system in which once the biometric traits are compromised then we can't change or demand for another biometric as it is bodily element of an individual. Thus biometric cannot be replaced. Thus securing these biometric traits are growing now and many technology and methodology have been followed. The biometric traits are secured in database, communication channel, etc.

Various techniques have been discussed along with advantages and disadvantages in the following sections with the explanation of the algorithm being discussed.

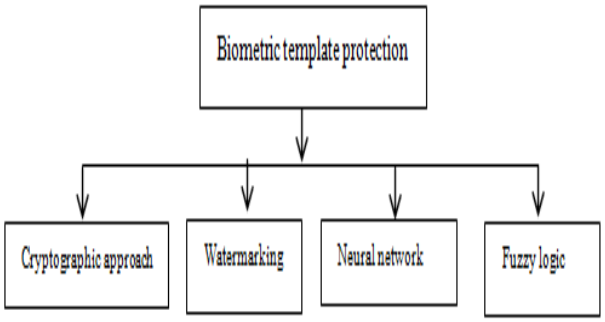

Fig. 1: Various methods of biometric template protection

A. *Cryptographic based Methods:*

In this approach an encrypted version are used to secure the biometric model. Due to information exchange through the internet, and the storage of important data on open networks, cryptography is becoming increasingly important feature of computer security [1]. A brief overview of techniques under this category is exemplified below.

There are two types of cryptographic methods like key generating and key binding methods.

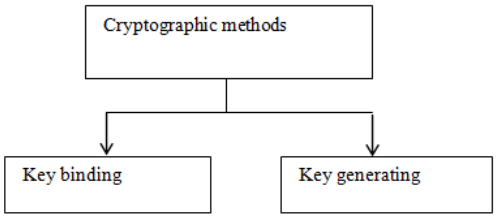

Fig. 2: Types of cryptographic methods

Swetha et al. [2] the biometric cryptosystem require the storage of biometrics data with some key to provide protection. The biometrics data are combined with some other data as key to generate helper data. In key binding biometric cryptosystem, helper data is obtained by binding a chosen key to a biometric template. As a result of the binding process a fusion of the secret key and the biometric template is stored as helper data. Applying an appropriate algorithm, keys are obtained from the helper data during authentication. Since cryptographic keys are independent of biometric features these are revocable while an update of the key usually requires re-enrollment in order to generate new helper data.

So, basically the aim of the paper is to combine one physiological trait with one behavioral trait. The approach has combined one physical and one behavioral approach for identification or verification to uniquely identify a person. The approach takes two different biometric traits. One finger print as physiological and other online signature as behavioral biometric trait. It uses modules of decision module and fusion module .Decision module have been used for both physiological and behavioral approach .The feature is extracted from both data and fused together which in turn is used to secure the system. The working of the module for the proposed approach is described in figure 4. During enrollment, the biometric features are extracted and key are used to make it more secure. During authentication, biometric trait is matched with the stored template using a matcher [26] [27]. If retrieved key matches with the key bounded at the time of enrollment the individual is same person otherwise not.

In another paper, Mohammed et al [3] presents hybrid combination of cryptographic algorithm for biometric security systems. Hybrid systems serve various advantages. The hybrid system can capture unique characteristics of biometrics and it makes a system to difficult to spoof. This technique adopted the concepts of combining the simple symmetric key algorithm and RSA asymmetric key algorithm techniques. Symmetric key algorithm operates on synthetic data which is based on user ID. Then the key generation involves the natural procedure of symmetric algorithm. RSA algorithm is based on integer factorization which is assumed to be difficult since it's not easy to found out the prime factors of a number .Experiments were performed with selected different algorithm and performance speed were analysed .The results shows that it increases the performance of the security, key generation and rapidity and concluded that proposed method has least performance time and key generation time others has taken maximum time in encryption for same amount of data.

Kavin and Ramamoorthy [4] use the double encryption methodology to secure the biometric authentication system. The reason behind this double encryption methodology is to provide trust between client and server. This is because the trust between client and server depends on trusted third party and there may be chances to TTP be hacked. In this approach uses the RSA algorithm at client side and 3DES algorithm at server side. It is to secure the biometric data both in network and database. During enrollment the user give his biometric data to client machine which extract the features and request the key from server in order to provide public key encryption .The encrypted minutiae has been forwarded to the server and decrypted by the server and encrypted it using the triple DES algorithm. After this the client has been notified with the success of enrollment. During authentication system the same methodologies are followed between client and server and comparison take place between the generated minutiae with already stored minutiae. The user will be notified with accepted and rejected comment.

In [5] a robust security model for biometric template protection using chaos phenomenon is considered. This phenomenon uses a feature transform approach and it generates a transformation function which is applied to the biometric template and only the transformed template is stored in the database. Unlike key binding approach the keys are generated directly from the biometric feature. Choas variables are usually generated by logistic map .Logistic map is a one-dimensional quadratic map .Logistic map are used to generate the chaotic evolutions and the chaotic system are deterministic and sensitive to the initial values. It has a complex active action which can be used to protect data content. The session keys are used to protect the encrypted biometric template. These session keys are generated using chaos phenomenon. This session keys are randomly generated to ensure the security of a communication sessions.

Similarly in [6] the chaotic behavior of logistic maps to build the projection matrix based on biometric template and identity. It constructs the spiral cube which is a 4d matrix of a biometric vector. Map cube are generated .It is non-invertible transformation with no need of user's key .Logistic map generate the multiple random vectors .These vectors are stored in 4D matrix called spiral cube. This cube is used to construct the projection matrix. Then the map cube and spiral cube are mapped to get the transformed function and these functions are used to secure the biometric feature.

B. Watermarking Based Template Protection:

A stenographic approach is to transmit biometric data (i.e. template data) hidden into some arbitrary carrier / host data or biometric samples of different biometric modalities.[9] The idea is to conceal the fact that biometric data transfer takes place.

Reinhard et al. [10] presents Two-Factor Biometric Recognition with Integrated Tamper-protection Watermarking. It uses the application of semi –fragile watermarking and uses a two way authentication schemes using iris recognition and smart cards. One of the ideas is to combine biometric technologies and watermarking is "biometric watermarking" [18]. The aim of watermarking is to employ biometric templates as "message" to be embedded in classical robust watermarking applications like

copyright protection in order to enable biometric recognition after the extraction of the watermark (WM). Semi-fragile WM is used to embed the template data stored on the smart-card into the sample data acquired at the authentication site. In this approach included the experimental results in the case of an iris recognition system, that indeed semi-fragile integrity verification is achieved [10].

In [11] uses a two watermarking algorithms .It uses discrete wavelet transforms and LSB based watermarking algorithm. It embeds a face template in a finger print image. In this technique they have used fingerprint as a cover image and facial feature as watermarking. The features from the face are extracted using the 2D Gabor filter. It works by watermarking embedded algorithm and extraction algorithm.

In [12] presentedan application scenario of security system. Security of fingerprint data introduced strong semi-blind watermarking algorithm of hiding fingerprint vectors into host image. Thus fingerprint data is protected while transmitted through channel/client to server. It uses a discrete cosine transforms. Feature points (minutia points) of fingerprint with explained minutia extraction algorithm are extracted. Minutia extraction algorithm gives strong feature points by removing false minutia and finally we have 25 to 30 minutia points per finger. These minutia points are embedded into host image by proposed semi-blind watermarking algorithm which is decided by neighborhood based estimation criteria.

C. Neural Network Based Template Protection:

Hao et al., [1] presented a technique for combining crypto with biometrics effectively. The author proposed a practical and secure way to incorporate the iris biometric into cryptographic applications. The [1]author proposed a two-layer error correction approach that merges Hadamard and Reed-Solomon codes for deliberating on the error patterns within iris codes. The key was obtained from the iris image of the user through the supplementary error correction data that do not disclose the key and can be saved in a tamper resistant token like a smart card. The performance evaluation of the methodology[1] was performed with the samples from 70 different eyes, 10 samples being obtained from every eye. It was observed that an error free key can be reproduced consistently from genuine iris codes with a success rate of 99.5 percent.

Kwanghyuk Bae et al., [14] proposed an Iris feature extraction using Independent Component Analysis (ICA). A traditional approach based on Gabor wavelets selects the parameters (e.g., orientation, spatial location and frequency) for fixed bases. ICA is applied to generate optimal basis vectors for the difficulty of extracting effective feature vectors which represent iris signals. The base vectors learned by ICA are localized in both frequency and space like Gabor wavelets. The feature vectors are obtained from the coefficients of the ICA expansion. Then, each of the iris feature vector is encoded into an iris code. From the experimental observational, it is observed that the proposed approach has a similar Equal Error Rate (EER) to a conventional technique based on Gabor wavelets. The advantages of the proposed technique are

- The size of an iris code and the processing time of the feature extraction are significantly very less;
- The linear transform can be calculated for feature extraction from the iris signals themselves.

Urias et al. [15] proposed a new method for response integration in modular neural networks using type-2 fuzzy logic .In this logic they used biometric authentication for person recognition. Biometric characteristics like face, fingerprint, and voice are used in this recognition[15]. A modular neural network of three modules is used. Each module is a local expert on person recognition based on each of the biometric features. The response integration approach of the modular neural network has the objective of integrating the responses of the modules to enhance the recognition rate of the individual modules. The results of a type-2 fuzzy logic approach for response integration has shown higher performance over type-1 fuzzy logic approaches

D. Fuzzy Logic Based Biometric Template Protection:

A fuzzy set is an object which is characterized by its membership function. That function is assigned to every object in the set and it is ranging between zero and one. The membership (characteristic) function is the grade of membership of that object in the mentioned set [16].

In [17] paper presents the basis of theoretical foundations of fuzzy logic. In first step for a given value of false acceptance rate we determine the value of the membership functions for given level of security. In second step through appropriate application of fuzzy rules we receive a result of fuzzy request of the threshold value.

Those rules are developed in order to obtain an answer to a question about the relationship between threshold (T) and the specified level of security (S).In third step we apply defuzzification during which the fuzzy values are transformed based on specified values of the membership functions and point a fuzzy centroid of given values. The development of this concept in the use of fuzzy logic to determine the threshold value associated with a given level of security provides an interesting alternative to the traditional concept to define threshold values in biometric authentication systems.

Mukhwinder et al. [18] presents Iris and Fingerprint images are taken as input images. Iris template is extracted from iris image using Daugman's Integro differential operator and then the unique patterns of 1‟s are extracted from iris code. Fingerprint minutia points (ridge endings and bifurcations) are extracted from fingerprint image using CN number technique. Feature sets extracted from iris and fingerprint are then fused and made compatible as input to fuzzy vault to generate the vault, fuzzy vault is created after fusing the features extracted from iris and fingerprint. Here the genuine features are represented by crosses and chaff points by squares in Galois field. The feature set generated from iris is normalized by extracting specific patterns of 1‟s from it using Crossing Number technique so that the two sets of features can be fused to form a multimodal feature set as input to the fuzzy vault. During authentication process the query fingerprint and iris are passed to the system and feature sets from both are extracted following the same procedure and the fused set is used to select the polynomial projections of the fuzzy vault. Feature set and its projections are computed using Lagrange‟s Interpolation in Galois field to extract the

correct polynomial. So, if the set of query images are of the genuine person then the correct secret key would be generated confirming the authenticity of the user.

III. DISCUSSION

After reviewing different methods proposed by various authors, it can be concluded that most of the work is done under the method of cryptography. A brief analysis of the biometric template protection is structured in a tabular format in Table 1.

Various algorithms were employed and are experiments with various biometrics.

S.NO	Methods	Algorithm used	Test data	Publication year
1	[2]	Fusion and decision	fingerprint	2013
2	[4]	RSA and 3DES	fingerprint	2012
3	[11]	DWT and LSB	fingerprint	2006
4	[14]	ICA ,Gabor filter	Iris	2003
5	[15]	Type 2 fuzzy logic	Face, voice fingerprint	2007
6	[6]	Chaos and logistic map	fingerprint	2012
7	[18]	Integro differential operator	iris and fingerprint	2014

Table 1: Comparison of different methodologies of template protection

IV. CONCLUSION

This survey deals with various methods that have tried to overcome the security problem in biometric template protection. In this paper various methodologies have been adopted like cryptographic methods, watermarking technique, fuzzy logic and neural network methods. Among them most of the work is done on cryptographic methods and key generating and key binding methodologies and few paper on other methodologies. Summarizing the overall methods, every technique has its pros and cons and each is effective in its own field of usage.

REFERENCES

[1] Collin soutar, Danny roberge, Alex Stoianov, Rene Gilroy, and B.V.K Vijaya Kumar, "Biometric encryption" Bioscrypt Inc (formely mytec Technologies Inc.), 5450 Explorer Drive, Suite 500 Mississauga, ONT L4W 5M1.

[2] Shweta Malhotra, Chander Kant Verma, "A Hybrid Approach for Securing Biometric Template", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

[3] Mohammed shahnawaz Nasir, Prakash Kuppuswamy, "implementation of biometric security using hybrid combination of RSA and simple symmetric key algorithm ", International Journal Of Innovative Research In computer and communication enginnering (AN ISO:3297:2007 CERTIFIED ORGANIZATION) VOL 1,ISSUE 8, OCTOBER 2013.

[4] S.Kavin hari hara sudhan,S.Ramamoorthy , " Double Encryption Based Secure Biometric Authentication System" ,ISSN:2231-5381 (2012).

[5] Maithili Arjunwadkar ,DR.R.V.Kulkarni , " Robust Security Model for Biometric Template Protection using Chaos Phenomenon" , computer applications (0975-8887) volume 3 –no 6 (2010)

[6] Moujahdi, Ghouzali, Mikram, Rziza,Bebis, "Spiral cube for Biometric Template protection", Springer-Verlag Berlin Heidelberg (2012)

[7] A. K. Jain and U. Uludag "Hiding fingerprint minutiae in images. In Proceedings of AutoID ", 3rd Workshop on Automatic Identification Advanced Technologies, pages 97–102, Tarrytown, New York, USA, March 2002.

[8] A. K. Jain, U. Uludag, and R. L. Hsu, "Hiding a face in a fingerprint image", In Proceedings of the International Conference on Pattern Recognition (ICPR'02), pages 756–759, Quebec City, Canada, August 2002.

[9] A.K. Jain and U. Uludag.," Hiding biometric data", IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(11):1494–1498, November 2003.

[10] Reinhard Huber1 , Herbert St¨ogner1 , and Andreas Uhl1,2 1 School of CEIT, "Two-Factor Biometric Recognition with Integrated Tamper-protection Watermarking ",Carinthia University of Applied Sciences, Austria 2 Department of Computer Sciences, University of Salzburg, 2007

[11] Mayank Vatsa ,Richa Singh,Afzeel Noore,Max H.Hoack and Keith Morris, " Robust Biometric Image Watermarking for fingerprint And face template Protection", IEICE Electronics Express,vol 3,no-2 ,23-28,2006.

[12] Mita Paunwala & Suprava Patnaik, "Biometric Template Protection With Robust Semi – Blind Watermarking Using Image Intrinsic Local Property", International Journal of Biometrics and Bioinformatics (IJBB), Volume (5) : Issue (2) : 2011 28 ,2006

[13] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.

[14] K. Bae, S. Noh, and J. Kim, "Iris feature extraction using independent component analysis," in Proceedings of the 4th International Conference on Audio- and Video Based Biometric Person Authentication (AVBPA '03), vol. 2688, pp. 1059–1060,Guildford, UK, June 2003.

[15] J. Urias, D. Hidalgo, P. Melin, O. Castillo, "A New Method for Response Integration in Modular Neural Networks using Type-2 Fuzzy Logic for Biometric Systems", IJCNN 2007, International Joint Conference on Neural Networks, pp. 311 – 315, 2007.

[16] Zadeh, L.A.: Fuzzy sets. Information and Control 8 (1965)
[17] Sachenko, Arkadiusz Banasik, and Adrian Kapczyński , "The Concept of Application of Fuzzy Logic in Biometric Authentication Systems Anatoly "Silesian University of Technology, Department of Computer Science and Econometrics, F. D. Roosevelt 26-28, 41-800 Zabrze.
[18] Mukhwinder Singh* Tripatjot Singh Panag "Heterogeneous Multimodal Biometric System with Fuzzy Vault Template Security", International Journal of Advanced Research in Computer Science and Software Engineering Research PaperVolume 4, Issue 7, July 2014 ISSN: 2277 128X
[19] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," Proc. of the IEEE, vol. 92, no. 6, pp. 948–960, 2004.
[20] Christian Rathgeb and Andreas Uhl, "A Survey on Biometric Cryptosystems and Cancelable Biometrics" , 2007
[21] Beng.A, Jin Teoh and Kar-Ann Toh, "Securebiometrickey generation with biometric helper", in proceedings of 3rd IEEE Conference on Industrial Electronics and Applications,pp.2145-2150, Singapore, June 2008.
[22] N. K. Ratha, J. H. Connell, R. M. Bolle,"Enhancing security and privacy in biometrics based authentication systems", IBM Systems Journal, 40(3), pp. 614-634, 2001.
[23] R. M. Bolle, S. Pankanti, N. K. Ratha,"Evaluation techniques for biometrics based authentication systems (FRR)", Proceedings15th International Conference on Pattern Recognition, vol.2, pp. 831 - 837, 2000.
[24] Ari Juels, Madhu Sudan, "A Fuzzy Vault Scheme", IEEE International Symposium Information Theory, Lausanne, Switzerland, pp. 408, 2002.
[25] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari, "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
[26] P.U. Lahane, Prof. S.R. Ganorkar, "Efficient Iris and Fingerprint Fusion for Person Identification", International Journal of Computer Applications (0975 – 8887), Volume 50– No.17, July 2012.
[27] C.Hesher, A.Srivastava, G.Erlebacher, "A novel technique for face recognition using range images" in the Proceedings of Seventh International Symposium on Signal Processing and Its Application, 2007.
[28] T. A. M. Kevenaar, G. J. Schrijen, M. vanderVeen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in Proc. AutoID, 2005, pp. 21–26.
[29] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9,pp. 1081–1088, September 2006.
[30] T. A. M. Kevenaar, G. J. Schrijen, M. vanderVeen, A. H. M. Akkermans,and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in Proc. AutoID, 2005, pp. 21–26.
[31] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9,pp. 1081–1088, September 2006.
[32] Anil k .Jain,Karthik Nandakumar and Abhishek Nagar, " Biometric Template Security ", Eurasip journal on advances in signal processing,2007.

