Proceedings of the International Conference on Intelligent Computing and Communication for Smart World (I2C2SW-2018)
14-15 December 2018

A Survey on Multimodal Biometrics Authentication and Template Protection

Aravindhraj Natarajan
Department of CSE
Bannari Amman Institute of Technology
Sathyamangalam , India
aravindhrajnatarajan@gmail.com

N. Shanthi
Department of CSE
Kongu Engineering College
Perundurai , India
shanthi.moorthi@gmail.com

***Abstract*— Biometric systems occupies a vast space in the field of security systems. Most of the applications make use of biometric systems such as attendance system, locker systems in banks, hospitals, industries, etc. Besides authentication provided by these biometric systems there is also need to protect the templates that are stored in them. This work involves a review of multiple biometrics such as fingerprint, face, hand vein, iris, signature, etc and the techniques used for authentication, fusion and template protection. Different traits and techniques are compared to obtain the most unique and suitable methods for biometric authentication and template protection. This paper also includes the comparison between the unimodal and multimodal biometric systems. Parameters such as Genuine Acceptance Rate(GAR), Equal Error Rate(EER) ,False Acceptance Rate(FAR) and False Reject Rate(FRR) are used to evaluate the various unimodal and multimodal biometric systems.**

Keywords—Query template, GAR, FAR, FRR , EER

I. INTRODUCTION

Biometrics is the measure of biological data. Biometric systems came into existence in the mod 1800s. Even there are evidences reporting the fingerprint markings in the old caves of prehistorical ages. In 1858, Sir William Herschel recorded an imprint on the back of an agreement for every laborer to recognize representatives from other people who may profess to be workers when payday arrived. This was the main recorded orderly catch of hand and finger pictures that were consistently taken for ID purposes. The use of first real time biometric technology began in 1870 as a method to identify individuals by their body measurements by Alphonse Bertillon. In 1892, Galton gave a detailed study about fingerprints. The characteristics that are defined by him are still used today to classify the individuals. This beginning of biometric technology lead to great revolution in the field of security.

Biometrics can be characterized into two noteworthy sorts. They are behavioural characteristics and physical characteristics. Behavioral characteristics includes voice pattern, signature, etc. Physical characteristics refers to fingerprint, hand vein, iris, face, etc. Authentication using these biometrics are employed in most of the governmental organizations, private corporate, etc. They are used in many applications ranging from small attendance systems to high level military security systems for authentication. The reason behind the deployment of biometric systems is the ease of use and their uniqueness. Biometrics have the following set of characteristics[3]

Universality: every person must have a distinct characteristic;

Distinctiveness: One should differ from the other person characteristic;

Permanence: the characteristic ought to be invariant at a timeframe;

Collectability: the characteristic ought to be estimated quantitatively.

At the initial registration stage (enrollment), the biometric templates either single or multiple are captured, pre-processed, processed and stored in the database. Then, after getting registered to the biometric system, the users get authenticated through the verification(testing) stage.

The processed and stored templates are subjected to many attacks [29]. Some of the attacks includes insider attack, non-secure infrastructure, biometric overtness, etc[4]. To overcome these threats, a template protection technique should be applied. There are several types of template preservation techniques such as fuzzy vault[13][16][18], Topology code[38], cryptosystems[1],etc. So, template protection also has a greater importance in the biometric systems.

A. Performance measurement parameters

There are four commonly used parameters such as genuine acceptance rate(GAR), false acceptance rate(FAR), false reject rate (FRR) and equal error rate(EER).

False acceptance rate is the ratio of number of imposters accepted by the system to the total number of imposter attacks.

$$FAR = \frac{Imposters\ \ accepted\ \ by\ the\ system}{Total\ \ no.of\ \ imposter\ \ \ attacks}\ X\ 100 \quad (1)$$

False rejection rate is the ratio of genuine users rejected by the system to the total number of claims made by the genuine user.

$$FRR = \frac{Genuine\ \ users\ \ rejected\ \ by\ the\ system}{Total\ \ no.of\ \ genuine\ \ users\ \ claimed}\ X\ 100 \quad (2)$$

Genuine acceptance rate is defined as the number of genuine users accepted by the system.

$$GAR = 100 - FRR \quad (3)$$

Equal error rate is defined as the chances of being FAR and FRR equal. For a better authentication system, GAR should be high and FAR should be less.

II. UNIMODAL BIOMETRIC SYSTEMS

A. *Unimodal Biometric systems*

An unimodal biometric system deals with single biometric trait for authentication purposes. It may use any one of the physical or behavioral biometrics. Unimodal systems generally have four modules[22]. They are

- Sensor Module
- Feature Extraction Module
- Matcher Module and
- Storage Module.

Sensor module senses and obtain the user input which is any one of the biometric feature. The obtained input is an image and it is preprocessed to get a clear image. Feature extraction module extricates the details focuses from the acquired information. Not all the parts of image is taken into account for authentication process. Only certain features alone are extracted from the image.

In the enrollment phase, obtained highlights are put away in the database. This is the work of the storage module. In the verification phase, matcher module plays out the coordinating between the query template and the stored template. These sequences of steps are shown in the Fig.1

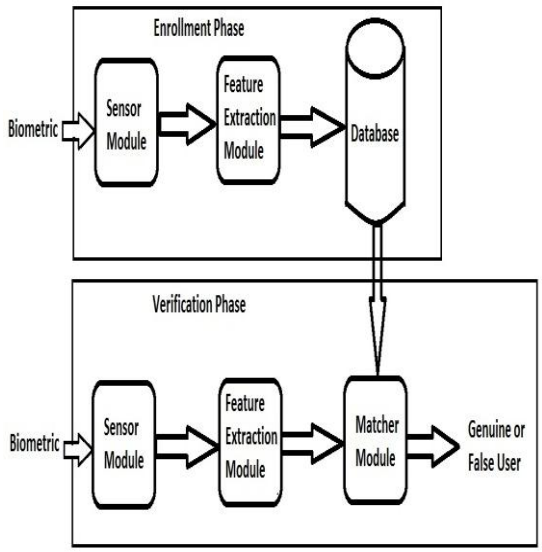

Fig.1. Unimodal Biometric System

B. *Fingerprint*

Wencheng Yang et al.,(2014) proposed fingerprint authentication and template protection. Delunay quadrangle method is used to authenticate a user and topology code generated from each quadrangle helps in protecting the template. In this method only the encrypted templates are stored in the database and they are only used for verification purpose. Local features extracted from the delunay quadrangle is encrypted by the Pinsketch .The topology code extracted from each quadrangle is also encrypted with key to ensure security. Thus ,template with two level encryption is put away in the database and this results in the template protection. The parameters such as FAR, FRR and ERR are used to evaluate the system.

Paper [11] enforces that the biometric systems should have both authentication and template protection. Helper data ought not uncover any data about the biometric. A computational approach with security analysis has been suggested to protect the template. Multibiometric system considering fingerprints of different fingers is considered. Decision level fusion has been carried out to fuse the different biometric templates. Hash functions are used for template protection. EER , FAR and FRR are utilized to assess the system. Results shows that multimodal biometric systems are accurate than single biometric system.

Fuzzy vault is a cryptographic system to ensure the biometric formats [9]. Record multiplicity attack has been prevented using the fuzzy vault technique which takes input as minutiae points of fingerprint. Fingerprint pre-alignment is done to resist the leakage of information. Thus the finger print based fuzzy vault protects against record multiplicity and information leakage. GAR and FAR are used to evaluate the system. Fuzzy vault provides good security against the brute-force attack and false-accept attack. Fuzzy vault along with helper data to protect the fingerprint image had been proposed in [36].

C. *Hand vein*

A hand vein biometric including dorsal and palmar vein has been actualized in [20]. Vein design attributes are known for their uniqueness, steadiness and insusceptibility to fakes. Score level combination is utilized to join dorsal and palmar highlights of hand vein which utilizes the scores produced by individual matchers of the both. Hand vein images are captured and features are extracted first. Independent component analysis technique is used to represent the features because it reduces the dimensionality of the captured image. The scores are used to authenticate the user. FRR and FAR are the parameters used to assess the framework and the outcomes demonstrates that multimodal combination gives better FAR and FRR.

D. *Voice*

A two-stage authentication method which uses the biometric transformation and biometric cryptosystems is proposed in [15]. Original voice captured is projected using random matrix at the enrollment phase. Principal component analysis or biohashing is used to generate the codebook for cancellable transformation of the template. Fuzzy vault technique is used here to encrypt the template where the chaff vectors are added additionally and it is stored in the database. Same techniques are applied to the query voice template and matching is done by measuring the Euclidean distance between the query template and encrypted code book. FAR and FRR are the parameters used to evaluate the system.

E. *Iris*

An authentication scheme which derives a secret key is from an individual's biometric is proposed [1]. Combining biometrics and cryptographic techniques is called as crypto-

biometric scheme. The template is projected into a polynomial and secret key derived from the biometric template is hidden in the polynomial. In verification phase, polynomial is reconstructed using Lagrange Interpolation Process to obtain the secret.GAR,FAR and FRR are used to evaluate the system.

F. Mouse Dynamics

Paper [34] investigates the continuous authentication biometric system. Mouse dynamics are considered as the biometric templates. It examines the distinctive blends of fusion and score boosting strategies. These systems can likewise be connected to other biometric modalities. Features such as speed of action, direction, types of action and distance travelled are extracted. The techniques such as Support Vector Machine(SVM) and Artificial Neural Networks(ANN) are used to classify them. The parameters such as Average Number of Genuine Actions(ANGA) and Average Number of Imposter Actions(ANIA) are are utilized to assess the execution of the system. The outcomes demonstrates that no bonafide clients get bolted by the system.

G. Touch Dynamics

Multimodal biometric authentication using touch dynamics in touch enabled mobile phones is proposed in [37]. Touch dynamics has been used for continuous authentication. Particle Swarm optimization(PSO) and Radial basis function network techniques are utilized for feature extraction. Touch dynamics are characterized by timing of touch points, coordinates and touch pressure. FAR and FRR are utilized to assess the execution of the system.

Touch screen input is used as biometric to authenticate users on the smart phones[21]. Touch actions that are captured are horizontal sliding and vertical sliding actions. The classifiers K-NN and Support Vector Machine(SVM) are used to classify the user as a genuine or intruder. Genuine user is identified by matching the templates at the continuous authentication phase. EER, FAR and FRR are utilized to assess the system performance.

H. Signature

In order to eliminate the compromise of templates, a framework that applies random projection for the biometric trait and keys to secure them by generating a revocable template has been proposed in [30]. It uses arithmetic hashing for the key derived from the user given password. Then the existing stored template and the query template are verified. FAR and FRR are utilized to assess the execution of the system.

I. Sole Pressure

A biometric authentication method which uses the pair of left and right sole pressures while walking has been discussed in [35]. The pair of left and right sole pressures are obtained using a mat type load distributor. The features are then extracted from the footprints which are obtained from the load distribution of the frame. Fuzzy rules are then applied to calculate the similarity between the query template and the stored template. FAR and FRR are used to evaluate the performance of the system.

J. Face

Protection of face images using feature transformation and bio crypto systems is developed in [31].In the feature transformation phase, the biometric template is transformed using transformation function, F with key, K and it is stored in database. Biometric cryptosystems creates a protected key. Mistake adjusting code and the produced key is connected on biometric layout to get the assistant information. Face pictures are dissected in this method and the outcomes demonstrates a reduction in mistake rate and increment in exactness.

K. Limitations of Unimodal Systems

Unimodal biometric systems have some of the drawbacks such as[2]

- Noisy Data
- Intra-class variation
- Inter-class similarity
- Non Universality
- Spoof attacks

Noisy data are those which contains unwanted data in the original data. Intra-class variations refers to the difference in images that are obtained during the authentication and enrollment stage. It may occur due to misplacements in the sensors. Inter-class similarities refers to the similarity of images between the two different persons. Same features cannot be obtained for certain people due to their age, inability, etc which is called as non universality. Intruders can spoof original traits and obtain a duplicate copy and it is called as spoof attack.

III. MULTIMODAL BIOMETRIC SYSTEMS

Multimodal biometric innovation utilizes in excess of one biometric identifier to look at the identity of the individual. Multimodal biometrics frameworks are viewed as more solid and productive than the unimodal frameworks [23]. If one of the trait is unable to identify , other traits can be used to identify and verify the user. It also overcomes spoof attacks by applying template protection methodologies such as fuzzy vault[9], watermarking[10][26], cancellable biometric cryptosystems[19],etc.

Multimodal biometric system consists of five modules[32] such as follows

- Sensor Module
- Feature Extraction Module
- Fusion Module
- Matcher Module
- Storage Module

Sensor module is similar to unimodal system where as here multiple sensors are used to capture multiple biometric features. All the caught pictures through sensor are preprocessed and just required highlights are obtained from the picture. It is performed by the feature extraction module. Features obtained from multiple biometrics are combined to frame a solitary template called as fused template which is performed by the fusion module. Matcher module and storage module functions similarly like the unimodal system

but here they take the input as the fused template having multiple characteristics.Image fusion takes a major importance in multimodal biometric system because all the actions are performed only on the fused template. There are three main types of fusion and they are [6]

- Feature level fusion
- Matching score level fusion
- Decision level fusion

In feature level fusion, the highlights separated from various modalities are fused into single template[7].

In matching score level fusion, scores obtained from different classifiers for different modalities are combined and checked for the score with higher level[14].

Decision level fusion joins the consequences of matching module whether genuine or false matching is obtained[27].

Multimodal biometric system can be depicted with its modules in the Fig.2.

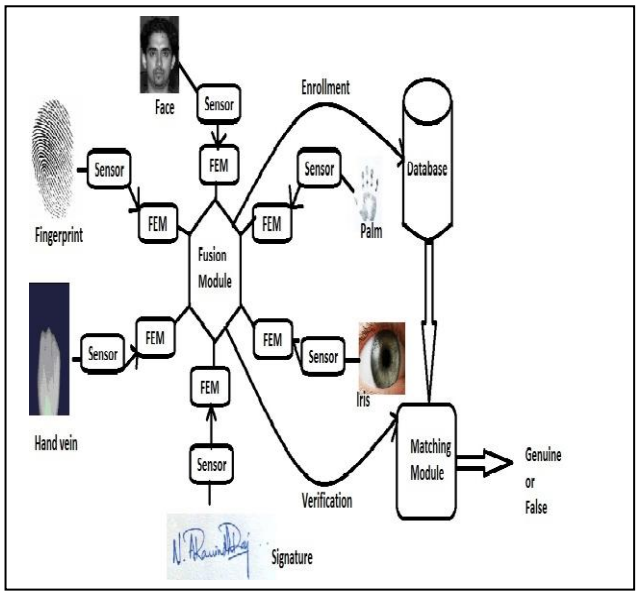

Fig.2. Multimodal Biometric System

A. *Face and Ear*

Templates are protected from the compromises that are made eventually or accidentally using multimodal biometric cancellable fusion[23]. The multimodal biometric cancelable fusion secures all the characteristics of template even if the templates are compromised. As storing of encrypted templates consumes more time, templates are subjected to cancellable transformations.

Face and Ear templates are chosen in this technique. The biometric template is split into n blocks and Random Projection Matrix is generated. Then, project each ear image utilizing arbitrarily anticipated face block. After projection they are fused based on features. Accuracy has been checked against GAR and FAR.

Feature level fusion has been applied using principal component analysis to the multimodal biometrics(Li Yuan et al., 2014). Face and Ear melded genuine esteemed format is changed over to paired layout utilizing non-invertible transformation. Binarization transform is used which randomly generates matrix and Gram-Schimdt is applied to get orthogonal matrix. The binary template is encrypted by means of fuzzy commitment. FRR, FAR and EER are used to evaluate the performance.

B. *Iris and Voice*

Applying transformations to the biometrics is called as cancellable biometrics[5]. Multiple biometrics with cancellable transformations is subjected to decision level fusion. The multiple biometrics are classified by individual N classifiers and their outputs are provided to the decision module. KNN classifier is used to classify the genuine and non –genuine users. Cancellable transformations can be done through Biohashing, Interpolation and Bioconvolving. Iris and Voice templates are considered in this methodology. Accuracy and Standard Deviation of voice and iris templates in classification are measured.

C. *Face and Fingerprint*

Punam Bedi et al.,(2012) used watermarking technique to provide a secure authentication system. Particle Swarm Optimization(PSO) is utilized to do the watermarking of the biometric image. Face picture of an individual is watermarked with the unique finger impression of a similar individual to acquire the intertwined single format. PSO selects the best discrete cosine transform coefficients in the face image for embedding the watermark. Peak Signal Noise Ratio(PSNR), Structural Similarity Index(SSIM) and Normalized Correlation(NC) are the parameters utilized to evaluate the system performance. PSNR,SSIM and NC are compared against cover and watermarked images where PSO technique outperforms other watermarking techniques.

A two phase confirmation system utilizing watermarking is done to address the validation problem[10]. Face highlights are inserted into unique mark pictures of a similar person. At the primary phase of verification , the believability of information is built up by checking the validness of removed examples. Wavelet quantization based watermarking approach is proposed to circulate watermark vitality on critical DWT coefficients of unique mark pictures. Information Credibility utilizes Support Vector Machine(SVM) and multimodal biometrics utilizes Sparse Reconstruction based Recognition and score level combination. Peak Signal Noise Ratio(PSNR), Structural Similarity Index(SSIM) and Bit Error Rate(BER) are the parameters used to assess the framework execution.

In [39], author proposed a watermarking method for multimodal biometric framework including face and unique mark. In this strategy, thumbnail highlights of the face picture is watermarked into the unique mark picture. In verification, the thumbnail highlights of face picture in the query template is coordinated with the thumbnails of the stored template.

D. Face and Iris

Face and Iris highlights are intertwined to shape a combined template[40]. Fisher Discriminant analysis has been used to construct a fused template. Neural network with radial basis function is utilized to coordinate the separation between the element vectors of the inquiry format with the put away layout to group the client as certified or faker.

E. Fingerprint and Iris

Multimodal biometric system involving finger print and iris had been proposed in [17]. It uses matching score to identify the user as a genuine or imposter. Scores are coordinated by minmax, z-score and hyperbolic tangent and combination of scores is finished by methodologies, for example, minimum score, maximum score, simple sum and user weighting.

A cryptographic system involving fingerprint and iris was developed in [12]. The fingerprint features such as bifurcation, ending points and orientation points are extracted and they are concatanated with iris features obtained using wavelet transformation.

This is called as feature level fusion. In the verification phase, same fusion is applied for query template and it is matched by measuring the hamming distance between the query template features and stored features.

In [8] they have also presented a review about multimodal biometric systems involving fingerprint and iris. Feature level fusion is done to fuse both the templates. In addition to authentication, the security of the fused template is enhanced using the fuzzy vault and fuzzy commitment technique. Fuzzy vault technique along with symmetric algorithm was discussed in [28] for fingerprint and iris.

F. Face and Speech

In [33], the author says that joining at least two characteristics yields preferable acknowledgment results over utilizing a solitary qualities for validation. Systems, for example, support vector machine(SVM), fisher linear discriminant analysis , Bayesian classifier and so on are analyzed in this work. It is demonstrated that SVM and Bayseian classifier beats than other arrangement strategies for user acknowledgment.

G. Face,Fingerprint and Palmvein

A Multimodal biocryptosystem had been proposed in [25]. It uses fingerprint image and face image to be encoded into a single image using the palm vein as a secret key. Fingerprint image is encrypted using palmvein as a key and it is embedded into face image. During verification, the reverse process is done to authenticate a person.

H. Face, Ear and Signature

A novel approach of decision fusion of multimodal biometrics utilizing social network analysis has been formulated in [24]. Dimensionality reduction, classifier choice and aggregated decision making are the issues in multimodal biometric systems. Social Network Analysis overcomes all these issues. Feature extraction is done using the Fischer Linear Discriminant Analysis(FLDA). Social networks are developed dependent on the likeness and connection of highlights among the classes. K-NN method is used for classification and after that decision fusion is done. Face , Ear and Signature are the biometrics are employed in this system. GAR and FAR are the parameters used to evaluate the system.

IV. ANALYSIS

TABLE I. ANALYSIS

Biometric(s)	Author(s)	Techniques and Algorithms	Parameters
Fingerprint	Wencheng Yang et al.,(2014)	Delunay Quadrangle method for authentication and Unique Topology code	FAR: 0 -0.1%, FRR : around 2% and EER: 1.07%
	Cai Li et al.,(2015)	Decision Level Fusion, Hash Functions, Delaunay Triangulation and Shamir's Secret Sharing Scheme	FAR and FRR
	Benjamin et al.(2015)	Fuzzy Vault	GAR:79% and FAR
Hand vein	Maleika Heenaye et al.(2012)	Independent Component Analysis(ICA) and Score Level Fusion	FAR:0.02% and FRR:0.35%
Voice	Hua-Hong Zhu et al.,(2012)	BioHashing for transformation, Random Projection and Fuzzy vault	FAR:0.07-0.08% and FRR is same as fuzzy vault technique
Iris	R. Alvarez Marino et al.,(2012)	Fuzzy Extractor	GAR: 90.33%, FAR: 4.42% , FRR: 9.67%
Mouse Dynamics	Soumik Mondal et al.,(2015)	SVM(Support Vector Machine), ANN(Artificial Neural Network)	ANGA(Average No. of Genuine Actions) ANIA(Average No. of Imposter Actions):70
Touch Dynamics	Weizhi Meng et al.,(2015)	Particle Swarm Optimization and Radial Basis Function Network	FAR :3.82% and FRR: 4.76%
	Mario Frank et al., (2013)	KNN(K –Nearest Neighbor) and SVM(Support Vector Machine)	EER: Inter Session:2% - 3%Intra Session: 0% Inter week Session: < 4%
Signature	Salman et al.,(2015)	Keyed Random Projection, Arithmetic Hashing	EER : SVC:6.2+/-8.59%, SUSig:4.08+/-19.1%, SigComp:5.24%
Sole pressure	Takeda et al.,(2011)	Fuzzy logic	FAR: 0.196% and FRR: 11.82%
Face	Sanaa et al., (2010)	Private Chaos based template protection Algorithm	Accuracy and Error rate
Face and Ear	Padma Polash Paul et al., (2014)	Cancelable Feature Fusion Random Projection Matrix	Accuracy: 96%
	Li Yuan et al., (2014)	Fuzzy Commitment Random Projection	FRR, FAR and ERR:8.95%
Iris and Voice	Anne et al., (2013)	KNN, Biohashing, Interpolation and Bioconvolving	Accuracy and Standard Deviation of voice and iris templates in classification
Face and Fingerprint	Punam Bedi et al., (2012)	Particle Swarm Optimization	PSNR(Peak Signal Noise Ratio) SSIM(Structural Smilarity Index) NC(Normalized Correlation)
	Bin Ma et al., (2014)	Wavelet Quantization based water marking	PSNR: 48 dB(Low Profile) & 42dB(High Profile),SSIM and BER(Bit Error Rate):5%
	Won-gyumKim et. al(2009)	Watermarking	PSNR
Face and Iris	Wang et. al.,	-	FAR and FRR
Fingerprint and Iris	Kamer Vishi et. al.,	Score level fusion	EER=3.30 %
	Ashish P. Palandurkar et. al.,(2013)	Fuzzy commitment	-
	S. Sowkarthika et. al.,(2013)	Double Encryption, Fuzzy vault	FRR:0.1% FAR: 0.06%
Face and speech	Souheil Ben-Yacoub et. al.,(1999)	Bayesian classifier SVM-polynomial Fisher classifier	EER:1.9%
Face, Fingerprint and Palm vein	B.Prasanalakshmi et. al.,(2011).	-	EER: 25%, FAR:25%, FRR:25%, GAR:75%
Face, Ear and Signature	Padma Polash et al., (2013)	Fisher Linear Discriminant Analysis(FLDA) and Social Network analysis	GAR:100% And FAR :5%

V. CONCLUSION

A study on different biometrics, unimodal and multimodal authentication systems are made. Besides authentication, template protection also grabs a greater attention to enhance the security of the stored templates. Unimodal systems using templates such as fingerprint, face, iris, etc. are existing in most of the current security systems. Studies shows that multimodal biometric systems which involves more than one biometric are more efficient than unimodal systems. Many techniques such as fuzzy vault, fuzzy commitment, bio cryptosystems , etc. are used for preserving templates against intrusion attacks. It is also found that hand vein tends to be more unique and it is hard to alter as it lies underneath the skin. Works related to hand vein authentication also present in less numbers. So, hand vein can be used with any other modality to obtain a multibiometric system. This work leads to the development of multimodal biometric system with template protection using hand vein combining with any other biometric trait.

REFERENCES

[1] Alvarez Marino R , Hernandez Alvarez F , Hernandez Encinas L(2012) "A crypto-biometric scheme based on iris-templates with fuzzy extractors", Elsevier:Journal on Information Sciences, 195 pp.91–102.

[2] Anil K. Jain, Arun Ross (2004) " Multibiometric systems", Communications of ACM, Vol.47, No.1.

[3] Anil K. Jain, Arun Ross, and Salil Prabhakar (2004) "An Introduction to Biometric Recognition", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 1, pp. 4 -20.

[4] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar(2008) "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics.

[5] Anne M.P. Canuto , Fernando Pintro, Joao C. Xavier-Junior (2013) "Investigating fusion approaches in multi-biometric cancellable recognition", Elsevier:Journal on Expert Systems with Applications ,40 , pp.1971–1980.

[6] Arun Ross and Anil Jain (2003) "Information Fusion in Biometrics", Elseveir: Pattern Recognition Letters, 24 ,pp.2115–2125.

[7] Arun Ross and Rohin Govindarajan(2007) "Feature Level Fusion in Biometric Systems".

[8] Ashish P. Palandurkar ,Vinod Nayyar, R. D. Wagh (2013) "Review of Multi-biometric Cryptosystem using Feature level Fusion", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 10.

[9] Benjamin Tams, Preda Mihailescu and Axel Munk (2015) "Security considerations in minutiae-based fuzzy vaults", IEEE Transactions on Information Forensics and Security.

[10] Bin Ma ,Yunhong Wang, Chunlei Li ,Zhaoxiang Zhang , Di Huang(2014) "Secure multimodal biometric authentication with wavelet quantization based fingerprint Watermarking", Springer – Multimedia Tools Application.

[11] Cai Li, Jiankun Hu, Josef Pieprzyk, Willy Susilo(2015) " A new bio-cryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion", IEEE transactions on Information Forensics and Security.

[12] Dr. Ujwalla Gawande, Mr. Kamal O. Hajari , Mr. Yogesh G. Golhar," Novel Cryptographic Algorithm based Fusion of Multimodal Biometrics Authentication system"

[13] Evelyn Brindha V and AM Natarajan (2012)," Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault", Journal of Biometrics & Biostatistics, Vol.3, pp.3-6.

[14] Feifei CUI, Gongping YANG(2011) "Score Level Fusion of Fingerprint and Finger Vein Recognition", Journal of Computational Information Systems 7: 16,pp.5723-5731.

[15] Hua-Hong Zhu, Qian-Hua Hei, Yan-Xiong Li(2012) "A two -step hybrid approach for voiceprint-biometric Authentication on mobile phones", International Conference on Machine Learning and Cybernetics, Xian, pp.15-17.

[16] Ismeet Kaur ,Ajay Mittal and Manvjeet Kaur(2014) "Security Enhancement Techniques of The Fuzzy Vault: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, Issue 6.

[17] Kamer Vishi, Sule Yildirim Yayilgan(2013) "Multimodal Biometric Authentication using Fingerprint and Iris Recognition in Identity Management", Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[18] Karthik Nandakumar and Anil K. Jain(2008) "Multibiometric Template Security Using Fuzzy Vault", BTAS.

[19] Li Yuan(2014) "Multimodal cryptosystem based on fuzzy commitment", IEEE 17th International Conference on Computational Science and Engineering.

[20] Maleika Heenaye, Mamode Khan (2012) "A multimodal hand vein biometric based on score level fusion", Elsevier: International Symposium on Robotics and Intelligent Sensors.

[21] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song(2013) "Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication ",IEEE Transactions On Information Forensics And Security, Vol. 8, No. 1.

[22] Md. Morshedul Arefin, Md. Ekramul Hamid(2014) "A Comparative Study on Unimodal and Multimodal Biometric Recognition", International Journal of Innovative Science and Modern Engineering (IJISME),Vol.3, Issue-1.

[23] Padma Polash Paul, Marina Gavrilova(2014) "Multimodal biometrics using cancelable feature fusion" , IEEE:International Conference on Cyberworlds.

[24] Padma Polash Paul, Marina L. Gavrilova, and Reda Alhajj(2014) "Decision fusion for multimodal biometrics using social network analysis", IEEE Transactions on Systems, Man, and Cybernetics: Systems, Vol. 44, No. 11.

[25] Prasanalakshmi.B , Kannammal.A, Sridevi.R (2011) "Multimodal Biometric Cryptosystem Involving Face, Fingerprint and Palm Vein", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1.

[26] Punam Bedi, Roli Bansal, Priti Sehgal(2012) "Multimodal biometric authentication using PSO based Watermarking", Elsevier:Procedia Technology C3IT 4. pp.612 – 618.

[27] S. Prabhakar, A.K. Jain (2002) "Decision-level fusion in fingerprint verification", Pattern Recognition ,pp.861–874.

[28] S. Sowkarthika , N. Radha(2013) "Securing Iris and Fingerprint Templates Using Fuzzy Vault and Symmetric Algorithm", International Conference on Intelligent Systems and Control (ISCO 2013), pp. 189-193

[29] Salil prabhakar, Sharath Pankanti, Anil K. Jain(2003), "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, pp.33-42.

[30] Salman H.Khan , M.AliAkbar , FarrukhShahzad , MudassarFarooq , ZeashanKhan (2015) "Secure biometric template generation for multi-factor authentication", Elsevier:Journal on Pattern Recognition, 48,pp.458–472.

[31] Sanaa Ghouzali, Wadood Abdul(2013) "Private chaotic biometric template protection algorithm", IEEE Second International Conference on Image Information Processing (ICIIP-2013).

[32] Sanjekar.P.S and Patil.J.B (2013) "An Overview Of Multimodal Biometrics", Signal & Image Processing : An International Journal (SIPIJ), Vol.4, No.1.

[33] Souheil Ben-Yacoub, Yousri Abdeljaoued, and Eddy Mayoraz(1999) "Fusion of Face and Speech Data for Person Identity Verification", IEEE transactions on neural networks, Vol. 10, No. 5.

[34] Soumik Mondal, Patrick Bours(2015) "A computational approach to the continuous authentication biometric system", Elsevier:Journal on Information Sciences 304 pp.28–53.

[35] T. Takeda, K. Kuramoto, S. Kobashi, Y. Hata(2011) "Fuzzy-logic is precise-its application to biometric system", Elsevier:Journal on Scientia Iranica,18 (3), pp.655–662.

[36] Umut Uludag, Anil Jain, "Securing Fingerprint Template: Fuzzy Vault with Helper Data"

[37] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou, "Surveying the development of biometric user Template protection", IEEE Transactions on Communication Survey and Tutorials

[38] Wencheng Yang, Jiankun Hu, and Song Wang (2014) "A Delaunay quadrangle-based fingerprint authentication system with template protection Using topology code for local registration and security enhancement", IEEE transactions on Information Forensics and Security, Vol. 9, No. 7.

[39] Won-gyumKim , HeungKyuLee (2009) "Multimodal biometric image watermarking using two-stage integrity verification", Elsevier: Signal Procesing, 89 ,pp.2385–2399.

[40] YunhongWang, Tieniu Tan, and Anil K. Jain, "Combining Face and Iris Biometrics for Identity Verification"