International Journal of Scientific & Technical Development
(A Peer-Reviewed Bi-Annual Journal) ISSN: 2348-4047

# BIOMETRIC SECURITY USING MULTI-BIOMETRIC

***Dr. Surender Kumar**
Head, P.G. Department of Computer Science Sri Guru Teg Bahadur Khalsa College, Sri Anandpur Sahib
(An Autonomous College) Punjab (India) drsurender.sgtb@gmail.com

**Abstract**
Biometric systems are used for uniquely identification and verification of a person by their physiological or behavioural features. Multi-biometric system are in interest due to their advantages in improving the matching accuracy, increasing population coverage, deleting spoofing attacks and imparting fault tolerance to biometric applications. Unimodal system rely on the evidence of a single source of information whereas multi-biometric systems, if consolidate multiple sources of biometric evidences. The integration of evidences is known as fusion. In a multi-biometric system, source of biometric information used various biometric traits that can be fused and the different fusion schemes are used to enhance the security. In this paper different security mechanism are derived and find that multi-biometric system is the best Biometric Security system as compared to Unimodal Biometric System.

Keywords:Biometric, Uni-biometric, Multi-biometric, Fusion.

## 1. Introduction

The need for the reliable user authentication techniques in the wake of heightened concerns about security and advancements in networking, communication and mobility etc. Biometric system can either is used for Identification or verification of an individual. Traditionally, authentication methods using passwords (knowledge based security) and ID cards (possession based security) have been used to restrict access to applications. However these systems are vulnerable to attacked and security can be breached. According to Satyavarapu et al. attacks on biometric authentication system can be generally divided into some categories. There are attacks at the user interface, attacks at the Interfaces between modules, attacks on the modules attacks on the template database. Biometric systems refers to the automatic recognition of individuals based on their physiological and behavioral characteristics. Physiological characteristics (fingerprint, iris, hand geometry, face, as well as samples of DNA etc.) use measurements from the human body. Behavioural characteristics (signature, keystroke, voice etc.) use dynamic measurements based on human actions [1]. These are uni-biometric which rely on the evidence of a single source of information for authentication, which have to maintain with a variety of problems such as (noise in sensed data, inter-class similarities, and intra class variations, etc). It occurs that a single biometric is not sufficient to meet the variety of requirements described by several large scale authentication systems possible solution to compensate for the false classification problem due to inter- class similarities and intra class variations can be found in the fusion of biometric systems or experts [2]. Which refers as Multibiometric. This system which fuse information from multiple biometric sources can be classified into different categories: Multi-sensor systems, Multi-modal systems, Multi-sample systems, Multi-instance system, Multi-algorithm systems. Depends on the level of information that is fused, the fusion schemes can be classified as the levels are sensor level, feature level, score level, and decision level fusion. There are wide variety of applications whereas a biometric system with multiple levels of security is desirable. In this paper [3], an efficient biometric security using multibiometric has been proposed to ensure the different level of security.

## 2. Related work:

M.Thieme [4] proposed an overview of single and multiple caharacteristics based biometric systems, includes the performance of physiological characteristics (such as fingerprint, hand geometry, iris, face recognition, DNA, etc.) and behavioural characteristics (such as gait, signature dynamics, keystroke dynamics, voice etc.). The fingerprints, iris image and DNA based multimodal systems and their performances are analyzes in terms of accuracy, security, reliability. The pros and cons of multiple feature based biometric approaches published and analyzed in this paper.

Ameya K. Naik [5] In this paper we present a novel Joint Encryption and Compression (JEC) technique for transmission of biometric data over a wireless channel. The method gives advantages such as the reduced data processing, security and recognition accuracy. The security of the biometric data is ensured by means of water marking followed by random bit shuffling. The watermarking process involves embedding one fingerprint in formation in his/her compressed face image. The advantage of the proposed method is that the overall data rate can be minimized while simultaneously maintaining good quality reconstruction.

Kamal A. El Dahshan [6] In this paper fusion of fingerprint, iris and face traits are used at score level in order to improve is accuracy of the system. Scores which find out from the classifiers are normalized first using the min-max normalization. Then sum, product and weighted sum rules are used to acquire fusion. Experimental results show that multimodal biometric systems out perform unibiometric systems and weighted sum rule gives the best results comparing with sum or product methods.

Mouad. M. H. Ali [7] proposed an overview of a current multimodal biometrics research based on fingerprint and palm-print. It described the pervious study for each modal distinctly and its fusion technique with another biometric modal. The basic biometric system consists of four stages: 1)The sensor which is used for enrollment & recognition the biometrics data. 2)the pre-processing stage which includes the enhancement and segmentation of Region-Of-Interest ROI. 3) The features extracted from the output of the pre-processing and every modal of biometrics having different type of features. 4) The matching stage is to compare with the acquired feature with the template in the database. Finally, the database which stores the features for the matching stages.

**3. Unimodal Biometric System:**

The unimodal biometric rely on the evidence single source of information for authentication (eg. Single fingerprint face) [8]. Unimodal systems have to contend with a variety of problems such as :

Noise in sensed data: A fingerprint image with a cut, injury or voice sample altered by cold are example of noisy data. It could result from defective or improperly sensors (eg. by the dirt on a fingerprint sensor).

Inter-class similarities: In a biometric system comprises of a wide variety of users, there may be interclass similarities (overlap) in the feature space of multiple users.

Intra-class variations: In which variations are typically caused by a user who is incorrectly interacting with the sensor (eg. Incorrect facial pose).

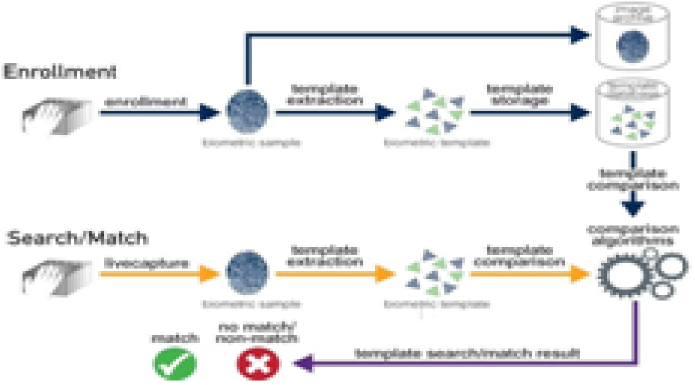

Figure 1: Unimodal biometric system.

Non-universality: The biometric system may not be able to acquire the meaningful biometric data from the subset of users (eg. fingerprint biometric system may extract incorrect minutiae features from the fingerprint of certain due to poor quality of ridges).

Spoof attacks: This attack is especially relevant information when using the behavioral characteristic.

**4. Multi-biometric system:**

The term multibiometric [9] denotes the multiple source of biometric information are used which various sources that fusion the different type of information. (eg. Fingerprint and face of same person). Multibiometrics has addressed some issues related to unimodal biometrics such as follow as:-

- Non–universality or the insufficient population coverage (to reduce failure to enroll rate which increase population coverage).
- It becomes increase difficulty for an imposter to spoof multiple biometric traits of a legitimately enrolled the individual.
- Multibiometric systems also efficiently address the problem of noisy data (illness affecting voice, scar affecting fingerprint).

**Classification of Multi-biometric:[1]**

A multibiometric system [10] performs recognition based on the evidences obtain from the multiple sources of biometric information. It is depending on the nature of sources, multibiometric system can be classified into five categories. Table 2 below illustrates the five categories by the simple case of using 2 of something.

Table 2: The comparison between the different multibiometric systems (categorized on the basis of sources of evidences) [11].

| Category | Modality | Algorithm | Biometric tarit (eg. Fingerprint,iris etc.) | Sensor |
|---|---|---|---|---|
| Multi-sensor | 1(always) | 1(usually)a | 1(always, and same instance) | 2(always) |
| Multi- | | | | |
| algorithm | 1(always) | 2(always) | 1(always) | 1(always) |
| Multi-instance | 1(always) | 1(always) | 2 instances(-subtypes) of 1 body trait(eg. Left and right index finger | 1(usually)b |

| | | | | |
|---|---|---|---|---|
| Multi-sample | 1(always) | 1(always) | 2 samples of 1 biometric trait(eg. 2 fingerprints of same finger) | 1(always) |
| Multi modal | 2(always) | 2(always) | 2(always) | 2(usually)c |

**aException:** It is possible that two samples from separate sensors are processed by using separate "Feature extraction" algorithms and then through a common comparison algorithm, making this one or two completely different algorithms.

**bException:** This case may be using two individual sensors each capturing one instance.

**cException:** A multimodal system with a single sensor used to capture two different modalities (eg. A high resolution image used to extract face and iris).

**Multi-sensor systems:** multiple sensor systems a single biometric trait is captured using multiple sensors order to extract different information. For instance, in face recognition, the results of 2D and 3D recognition technologies can be combined to increase overall recognition accuracy [12].

**Multi-sample system:** multiple samples, readings of the same biometric are collected during the enrollment and recognition phases (eg. A number of fingerprint readings are taken from same finger).

**Multi-instance system:** multiple instances means the use of the same type of raw biometric are collected (eg. fingerprint from two or more fingers).

**Multi-algorithm system:** multiple algorithm systems process the same biometric sample using by the multiple algorithm. They can use the multiple feature sets (i.e multiple representations) extracted from the same biometric sample or multiple matching schemes operating on a single feature set.

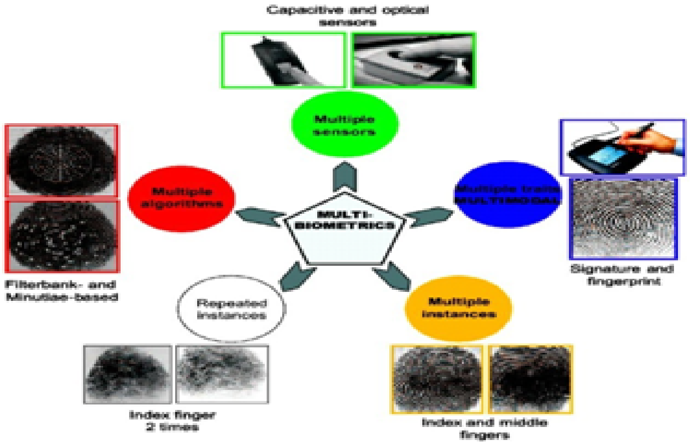

Figure 2: Different types of multibiometric

**Multi-modal system:** multiple modal system is the combine two or more different biometric traits for establish identity. Multimodal system have the several advantages better recognition rate from achieved combining different modalities. Higher performances improvement can be expected by using physiological traits (eg. finger and iris ) than using behavior traits (eg. Voice and lip). Multimodal system also address the problems of noisy data [13].

The advantages of using the multimodal biometric system instead of conventional unimodal biometric system[14] are as follows as:

1. Multimodal biometric system is capable to maintain a high threshold recognition checks, which results is reduced False accept rate (FAR).
2. Reduce the risk of admitted an impostor.
3. The combination of more than one modality causing reduced inter-class similarities and the intra-class variations in individuals.
4. Multimodal biometric system deter spoofing because it is not possible for an impostor to spoof more than one biometric trait.

This figures shows the block diagram of multi-modal system.

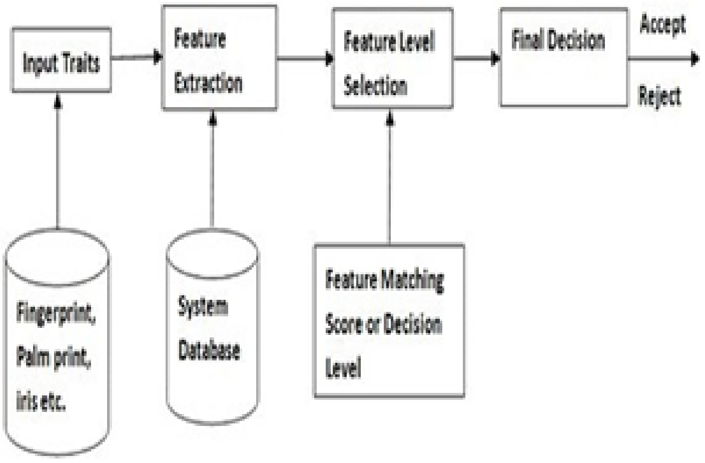

**Figure 3: Block diagram of Multi-modal system**

This system contains four modules. They are: sensor modules, feature extraction module, matching module, and decision module.

## 5. Fusion in multimodal biometric system:

A mechanism that combines the feature sets from each biometric channel is the called as biometric fusion. The amount of information available decreases after each level of processing in different modules of a biometric system. The raw data represents the richest source of information whereas the final decision just contains an abstract level of information [15].

The various levels of fusion are categorised as: 1) Pre-classification or fusion before matching[16][17].2) Post- classification or fusion after matching [18][19]. This categorization is based on the fact that the amount of information available for fusion is reduced once the matcher. Fusion before matching can take place at the sensor level or feature level is pre-classification. Fusion at score level, and decision level occur after matching module is post-classification. We discuss the various levels of fusion in multi biometric system.

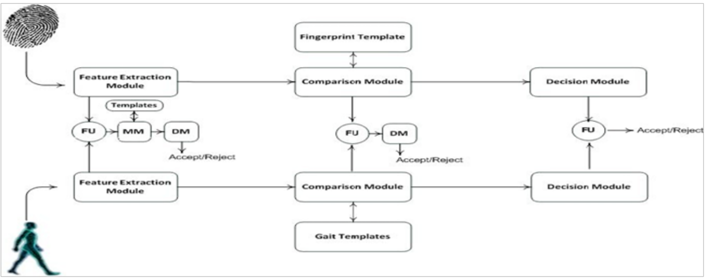

Figure 4: Different fusion levels

Pre-classification or fusion before matching:

**Sensor level fusion:** It requires the raw biometric data to be acquired from multiple sensors which can be further processed and integrated to generates new data from which features can be extracted. Sensor level fusion [20] refers to combine of the raw data obtained using multiple compatible sensors or snapshots of a biometric using a single sensor. The block diagram is shown in figure 5.

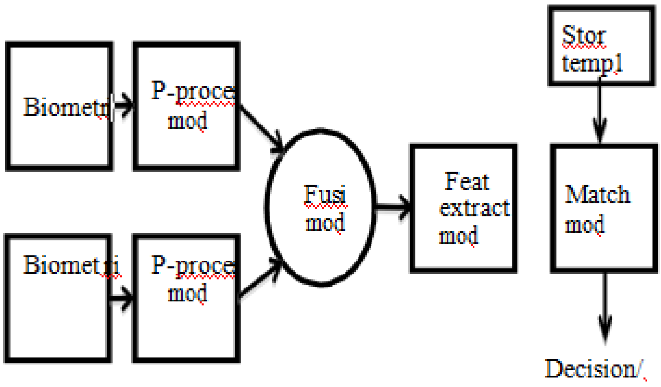

Figure 5: Sensor level fusion

**Feature level fusion:** In which, [21] feature sets originating from multiple information source integrated into a new feature set. For homogeneous sets (eg. Multiple measurements of a person hand geometry), fusion can be achieved by calculating the weighted average of individual feature vectors. For non-homogeneous sets (eg. Features of different modalities like face and hand geometry), a single feature set can be obtained by the concatenation. The block diagram representing the flow of feature level fusion in figure 6.

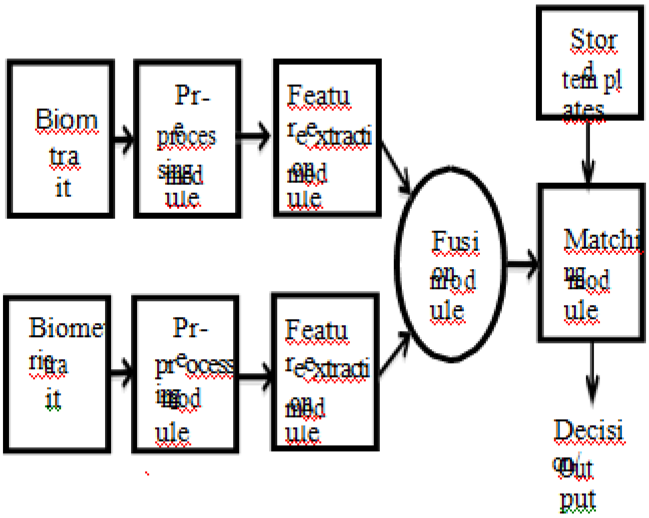

Figure 6: Feature level fusion

Post-classification or Fusion after matching:

**Score level fusion:** In which [22][23] different biometric matchers provides match score denoting the degree of similarity between the input and template vectors. These match score are consolidated to reach the final recognition system (eg. similarity score, distance score). It is also called as fusion at confidence level or measurement level. After the sensor and feature level information, match score contain the richest information about the input biometric sample. The block diagram representing the general flow of information in a match score level fusion scheme is shown in figure 7.

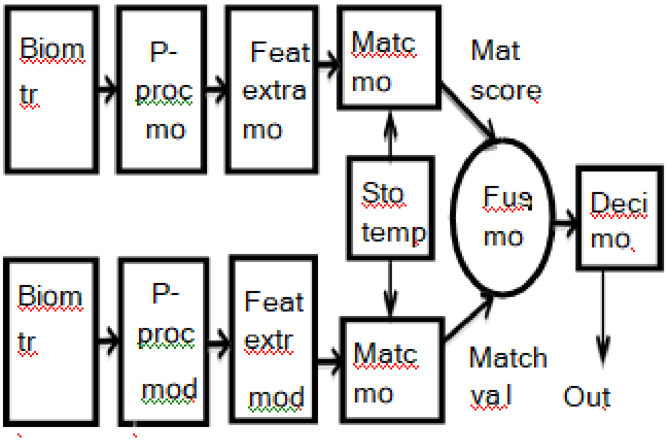

Figure 7: Score level fusion

**Decision level fusion:** Fusion is find out at this level when only decisions output by the individual biometric matchers are available. There is a separate authentication decision is computed for each biometric trait, which is the combined to result in a final vote. The final classification is based on the fusion of output of the different modalities. (e.g. AND ,OR, Majority voting, Bayesian decision fusion)[24]. The block diagram is shown in figure 8.

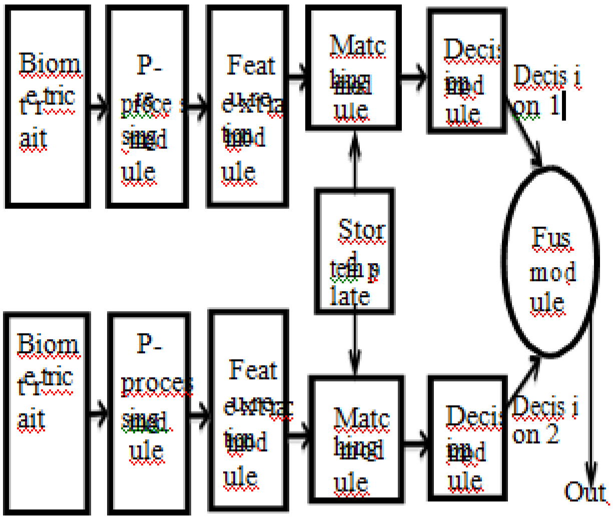

Figure 8: Decision level fusion

### 6. Applications of Multibiometric:

Biometric applications may be categories into three main groups as [25]:

- Forensic applications: These applications are used in criminal investigation, and fraud detection (eg. For parenthood authentication and corpse identification).
- Government applications: These applications including personal documents, such as passports, ID cards, and driver's licences; border and immigration control; social security and welfare disbursement; voter registration and control during elections; e-government.
- Commercial applications: These applications including physical access control; network logins; e-commerce; credit cards; ATM's, mobile phones, device access to computers, facial recognition software; e-health.

### 7. Conclusion:

Multi-biometric system alleviate several of the problems present in unimodal systems. By combining multiple sources of information, the multi-biometric system improve matching performance, deter spoofing, increase population coverage, and indexing. Various fusion levels are possible in multi-biometric system. The most popular one being fusion at the matching score level. Multi-biometric has attracted more interest in recent research.

**References**:

[1] Saritri.B.Patil,"A Study of Biometric Systems: Fusion Technique Application and Challenges" IJCST, Vol.3, 2012.

[2] A.Ross, K.Nandakumar, and A.K. Jain, "Handbook of Multibiometrics", Springer-Verlag edition, 2006.

[3] V. Subbarayudu, and M. Prasad, "Multimodal Biometric System." Paper presented at First International Conference on Emerging Trends Engineering and Technology ICETET. USA: IEEE Computer Society, 635– 6401, 2008.

[4] S.Nanavati, M.Thieme, and R.Nanavati, "Biometrics Identity Verification in a Networked World". Edited by Margaret Eldridge, Adaobi Obi and Micheline Frederick. Canada: John Wiley & Sons, Inc., 2013.

[5] AmeyaK.Naikn,RaghunathS.HolambeJoint Encryption and Compression scheme for a multimodal telebiometric system Neurocomputing 191,69–81,2016.

[6] Kamal A. El Dahshan, Eman A. Karam "Score level fusion for fingerprint iris and face biometrics", International Journal of Computer Applications (0975 – 8887) Volume 111 – No 4, February 2015.

[7] Mouad. M. H. Ali ▯ & A. T. Multimodal Biometrics Enhancement Recognition System based on Fusion of Fingerprint and PalmPrint Gaikwad Global Journal of Computer Science and Technology: F Graphics & vision Volume 16 Issue, 2016.

[8] Nageshkumar.M, Mahesh.PK, and M.N. ShanmukhaSwamy, "An Efficient Secure Multimodal Biometric Fusion UsingPalmprintand Face Image", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[9] Yannis Stylianou, Yannis Pantazis, Felipe Calderero, Pedro Larroy, Francois Severin, Sascha Schimke, Rolando Bonal, Federico Matta, and Athanasios Valsamakis. "GMM-Based Multimodal Biometric Verification", Enterface'05, MONS, Belgium -Final Project Report, 2005.

[10] Sunil Chawla and Aashish Oberoi, Robust algorithm for iris segmentation and normalization using hough transform. Global Journal of Business Management and Information Technology, 1:69–76, 2011.

[11] Dzati Athiar Ramli, Salina Abdul Samad, AiniHussain,"A Multibiometric Speaker Authentication System with SVM Audio Reliability Indicator", IAENG International Journal of Computer Science, 36:4, IJCS-3, 2008.

[12] Arun Ross and Rohin Govindarajanb, "Feature Level Fusion Using Hand and Face Biometrics", SPIE

Conference on Biometric Technology for Human Identification II, Volume, 5779, pp.196-204(Orlando, USA) March 2005.

[13] J.G. Daugman, "High Confidence Visual Recognition of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence 2011.

[14] Haryati Jaafar et al.”A Review of multibiometric System with Fusion Strategies and Weighting Factor” / International Journal of Computer Science Engineering (IJCSE) ISSN: 2319-7323, vol. 2 No. July 2013.

[15] Soh, J.Deravi, F and Triylia,A.,”Multibiometrices and data fusion standardization”, in Encyclopedia of Biometrics, S.Z.Li and A.K.Jain, New York, Heidelberg:Springer,2009.

[16] Noorjahan KhatoonIRACS “Multimodal Biometrics: A Review” International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 3, No.3, June 2013

[17] R.Tronci, G,Giavinto and F.roli, ”Dynamic score selection for fusion of multiple biometric matcher”, proc 14 IEEE International Conference on Image Analysis and Processing, ITALY, 2007.

[18] KalyanVeeramachaneni, Lisa Osadciw, ArunRoss, and NishaSrinivas, “Decision-level Fusion Strategies for Correlated Biometric Classifiers”, Biometric Authentication, Springer 2004.

[19] Federico Castanedo” A Review of Data Fusion Techniques” The Scientific World Journal Volume, Article ID 704504,19, 2013.

[20] Maya V. Karki & Dr. S. Sethu Selvi “Multimodal Biometrics at Feature Level Fusion using Texture Features” International Journal of Biometrics and Bioinformatics (IJBB), Volume (7), Issue (1), 2013.

[21] George Chellin Chandra. J and Rajesh. R.S., “Performance Analysis of Multimodal Biometric System Authentication”, IJCSNS 290 International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.

[22] S.Mohan Prakash, P.Betty, K.Sivanarulselvan, ”Fusion of Multimodal Biometric using Feature and Score level Fusion” International Journal on Application in Information and Communication Engineering, Volume 2: Issue 4: April 2016.

[23] Emanuela Marasco (et.al) Increase the security of multibiometric systems by incorporating a spoofing detection algorithm in the fusion mechanism.”2010.

[24] Yannis Stylianou, Yannis Pantazis, Felipe Calderero, Pedro Larroy, Francois Severin, Sascha Schimke, Rolando Bonal, Federico Matta, and Athanasios Valsamakis. “GMM-Based Multimodal Biometric Verification”,

Enterface’05, MONS, Belgium -Final Project Report, 2005

[25] W.Yang, J. Hu, S. Wang, and C. Chen, “Mutual dependency of features in multimodal biometric systems,”

Electron. Lett., vol. 51, no. 3, pp. 234–235, Feb. 2015

[26] Anil K.Jain, KarthikNandakumar and Abhishek Nagar, Review Article Biometric Template Security, Department of Computer science and Engineering, Michigan State University, 3115 Engineering Building, East Lansing, M148824, USA, 2007.

[27] Meng-Hui Lim, Sunny Verma, Guangcan Mai, Pong C. Yuen, Learning discriminability-preserving histogram representation from unordered features for multibiometric feature fused-template protection, Pattern Recogn., 60, Elsevier pp. 706–719, 2016.

[28] Sasidhar K. [Et Al.] Multimodal Biometric Systems – Study To Improve Accuracy And Performance [Journal]. - [S.L.] : International Journal Of Computer Science & Engineering Survey (Ijcses), Vol.1, 2010.

[29] Gurpreet Singh et al,”Review On Fingerprint Recognition: Minutiae Extraction and Matching Technique” International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 10, 2014.

[30] Ashish Mishra “Multimodal Biometrics it is: Need for Future Systems” Volume 3 – No.4, International Journal of Computer Applications (0975 – 8887), June 2010.