Comparative Study of Fusion Techniques Performed at Different Levels

Komal[1], Dr. Chander Kant[2]
[1] *P.hd Scholar,* [2]*Assistant Professor*
[12]*Department of Computer Science and Application, K.U. Kurukshetra (Haryana), India*

Abstract- Unimodal biometric based systems suffer from lack of security and efficiency. This leads to advent of the multimodal biometric based system and overcome these deficiencies. Multimodal biometric system uses more than one modality, fuse them using fusion techniques and give secure results. Multimodal system increases the security of the system as it is difficult to spoof more than one modality at a time. For fusion in multimodal biometric system different techniques are used at different levels. In this paper, a background study has been conducted which is based on comparison of different fusion techniques that are commonly used in multimodal biometric systems. It is also discussed in this paper, how various techniques are used at different levels with the main objective to improve the security and efficiency of the system. The main application of this paper is to help the new researchers in understanding the fusion techniques used at different levels in multimodal biometric system.

Keywords- Fusion levels, Fusion techniques, Multimodal, Unimodal Biometric System.

I. INTRODUCTION

Biometric is an automated recognition of an individual based on physiological and behavioural traits such as fingerprint, face, iris, voice, signature etc. Biometric recognition is very reliable and natural mechanism for ensuring that only authorized user can access the system. Biometric recognition is basically a pattern recognition system and it is used to identify or verify a human being [1]. The main objective to authenticate through biometric system is based on the fact that every individual is distinctive and can be easily authenticate by his or her unique physiological and behavioural characteristics. Biometric modalities can be broadly divided into two categories as shown in Fig1:

i) **Physiological modalities:** These are related to the shape or composition of body e.g. finger-print, face, iris, DNA, Palm-print, ear, FKP (Finger Knuckle Print), IKP (Inner Knuckle Print) etc. Every individual on this planet has different physiological characteristics. Even the twins have different fingerprint and iris pattern [2]. So individuals can easily be identify or authenticate by using biometric system.

ii) **Behavioural modalities:** These are related to the behaviour of a person e.g. voice, signature, gait etc. behavioural modalities are not very secure when used alone but it can be used in combination with physiological modalities [3]. Using single modality for identification process has high risk of spoofing so better idea for safe process is to combine behavioural modality with physiological modality eg. Face with voice etc [4].

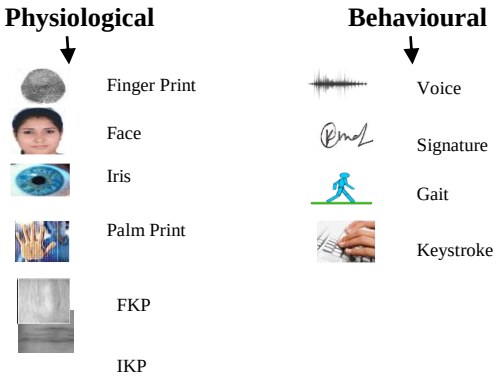

Fig.1: Classification of biometric modalities

Every biometric system uses four common components or modules for the identification or authentication process as shown in the Fig2. Sensor is used for capturing raw data and after scanning converts it into digital form [5]. Then features are extracted and stored in the database. After then matching module match the data with the template stored in the database and finally the decision is taken out [6].

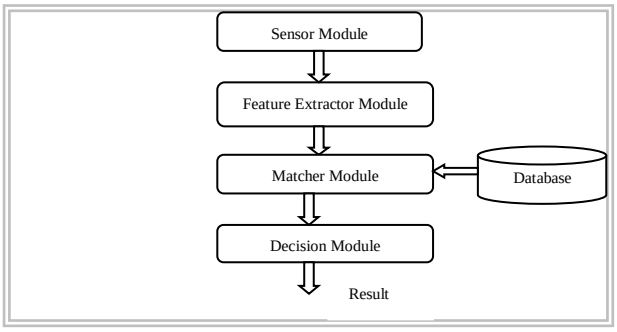

Fig.2: Biometric Modules

A biometric system will use three steps for their regular working: enrolment, storage and comparison [7]. Enrolment is the process where the user's initial biometric samples are collected, assessed, processed, and then stored for future use in a biometric system as shown in Fig3. Now when ever an enlisted individual comes for the live comparison process then that individual either accepted or rejected. An individual is accepted if their live template matches with the one stored in the database otherwise it is rejected as shown in Fig4. These templates can be compared using comparison-based-algorithms.

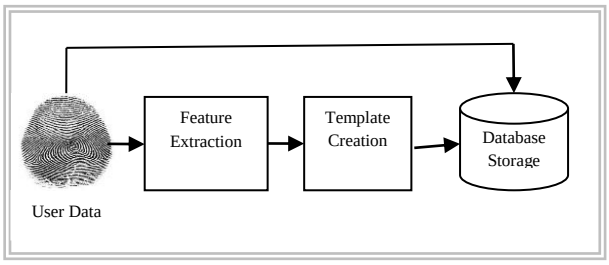

Fig.3: Enrolment Process in Biometric System

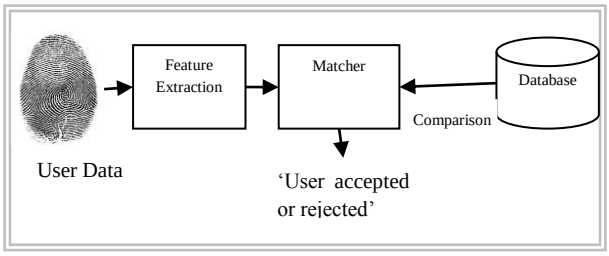

Fig.4: Identification Process in Biometric System

1.1 Performance Parameters

Different parameters can be used to rate the performance of a biometric factor, solution or application. Two most common performance metrics are **False Acceptance Rate** (FAR) and the **False Rejection Rate** (FRR).

- **False Acceptance Rate (FAR)**

It refers to the possibility where an unauthorized user is accepted by the authentication biometric system as an authenticated person.

- **False Reject rate (FRR)**

It is the probability for an authorized person is rejected by the biometric machine as an unauthenticated person. It measures the percentage of incorrectly rejected valid users.

False Accept Rate is also called False Match Rate, and False Reject Rate is sometimes referred to as False Non-Match Rate as shown in Fig5**.**

- **Crossover Error Rate (CER)**

It is the rate where both accept and reject error rates are equal. CER is also called Equal Error Rate (EER). Devices with lowest EER are most accurate [8].

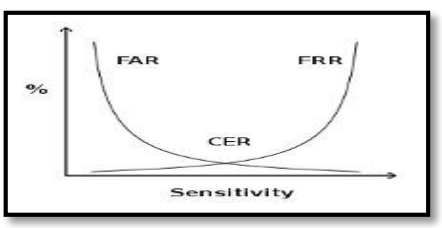

Fig.5: Graphical Representation of FAR and FRR Errors, Indicating CER

- **Failure to Enroll Rate (FER)**

Failure to Enrollment Rate FER is the rate at which attempts to create a template from an input is unsuccessful. It can be defined as the probability that a user attempting to enroll itself but unable to do so. The reason for this is low quality inputs [9].

1.2 Multimodal Biometric System

Unimodal biometric system faces many problems such as Non universality, Lack of individuality, Circumvention etc. Sensor might encounter some problem issues due to some noise or inefficient light present. Sometimes Features extracted from biometric characteristics of different individuals can be quite similar. For example, Due to genetic factors, many individual can have similar facial characteristics (e.g., father and son, identical twins, etc.). Unimodal biometric system is venerable to spoof attacks. So there is need of more secure or efficient system and this leads to advent of multi-modal biometric system. It is based on merging of more than one biometric trait. The main reason of merging is to increase the accuracy and recognition rate. In multimodal biometric systems, failure of any one trait may not seriously affect the authentication process as other trait can successfully work. Reduction in failure to enrol rate is the major advantage of this system [10].

1.3 Fusion Levels

Information Fusion can be classified in two major types: Fusion-Before –Matching and Fusion-After-Matching as shown in Fig6 [11]. Fusion-Before Matching consists of combination of raw data before applying any matching algorithms or classifier. On the other hand, Fusion-After-Matching consists of combination of information after all classifier or algorithms decisions are obtained [12].

1.3.1 Fusion-Before-Matching

When the biometric information is integrated before applying any template matching algorithms, is called Fusion Before Matching. It is also called Pre-Classification-Fusion [13]. It is categories into two futher levels:

1) **Sensor Level Fusion:** Sensor level fusion involves combining raw information from two sensors. This type of fusion can be appropriate for multi sensor and multi sample systems [14]. For example, if two biometric samples are taken from face scanner, these two are combined to form a result. The instances might be taken from different source or a single source. But it is important that raw data to be fused are of same type, eg. two image taken from two different camera which will be fused need to be of same resolution. Sensor level fusion is also called Data level or Image level fusion.

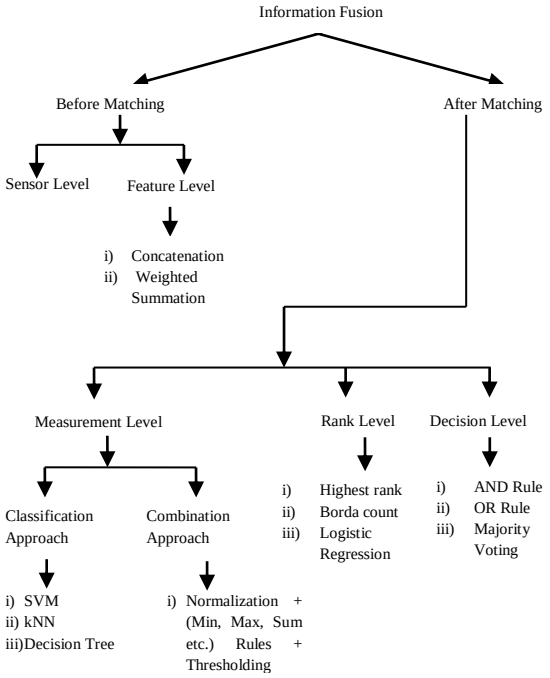

Fig.6: Information Fusion Levels

2) **Feature Level Fusion:** Feature level fusion includes combining different feature set from different modalities into single feature vector. If the feature sets are compatible with each other than it is reasonable to concatenate two feature set into one vector and if they are not compatible than several reduction, normalization or transformation techniques are used to making them compatible. Min-Max, median etc. normalization techniques are used to map the feature set into common domain. For reduction in dimensions, transformation techniques are used like Forward Sequential Selection; Backward Sequential Selection etc [15]. if the features vectors are homogeneous then resultant feature set is calculated as an average of weight of all features extracted individually. On the other hand, if feature vectors are not homogenous then concatenation can be done to get the final or resultant feature vector. Homogenous feature vector can be obtained if multiple instances of the single modality are used and non homogenous obtained if different modalities are used at the input time [16]. Concatenation process can't be performed if feature vectors used are not compatible with each other. For example Eigen face values can't be concatenate with fingerprint minutiae points.

Biometric authentication systems that combine information at the early stage are more effective as compared to systems that integrate at the later levels. Because quality of information degrade as it flow form sensor to decision level [17].

However, integration at feature level is difficult to perform for the following causes:

1. Concatenation of two or more feature vector might produce a feature vector which has large dimensionality. This leads to 'curse of dimensionality' problem.
2. Many commercial authentication system might not provide the right to all feature vectors that they are using in their security systems. Because of this, many researchers prefers the Fusion After Matching.'

1.3.2 Fusion-After-Matching

When the biometric information is integrated after applying matching algorithms, is called Fusion-After Matching. It is also called Post Classification Fusion. It is further categories into 3 types:

1) **Measurement Level Fusion:** Measurement level fusion includes the combination of scores provided by the match score module for different input feature vectors in the database. This type of fusion is also called match score level fusion. This type of fusion can be classified by two different approaches and these approaches are based on how the match score is processed. One is by classifying the feature vector and another is by combining the feature vector. One most significant feature in this type of fusion is the normalization of the match score [19]. Normalization of the match score is necessary to maintain the compatibility between the match score generated by two different modalities.

2) **Rank Level Fusion:** It is the method of combining more than two identification results from two different modalities, to improve the efficiency or reliability of the system. There are three different techniques to combine the rank obtained from different matchers: Highest rank method, Borda count method and Logistic regression method [20].

3) **Decision Level Fusion:** In this type of fusion, integration of the information occurs when each system makes the decision about the identity of the person based on the input data of the person. This is abstract level fusion where Boolean functions are used some of used Boolean functions are majority voting, AND rule, OR rule etc [21]. This is the simplest form of the fusion because this uses only the final output of the different modalities.

4)

1.4 Multimodal Fusion Techniques

There are certain fusion techniques as shown in Fig7 that can be categorized into three types: Rule based, Classification based and Estimation based techniques.

Categorization of techniques is basically based on the structure of these techniques and depends on the problem areas, like parameter estimation issue can only be solved by the estimation based technique. If the problem based of observation then rule based or classification based techniques can be used to solve the problem. These three techniques are explained below:

1.4.1 Rule Based Techniques

Rule based fusion techniques include an array of some basic rules that combine information. Some rule based techniques are used in multimodal such as Sum and Product based fusion (Linear Weighted), Min-Max (Majority voting), OR-AND based fusion [22]. Custom defined rule based techniques are depends on the application perspective.

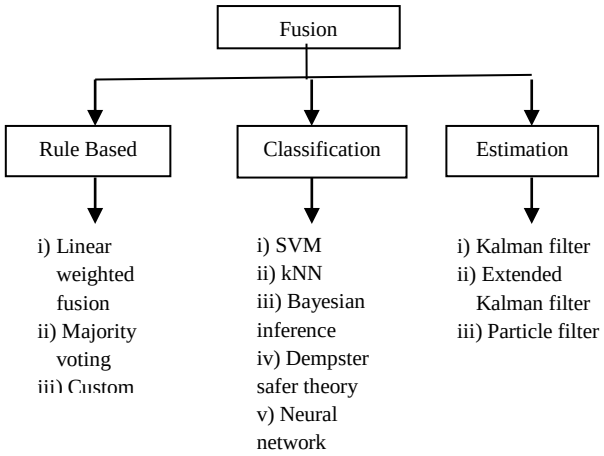

Fig.7: Categorization of Fusion Techniques

1.4.2 Classification Based Technique

These types of techniques include an array of classification methods which can be utilized for classification of observations obtained into one of the pre defined class. Some of the techniques in this group are Support Vector Machine (SVM), k Nearest Neighbour (kNN), Bayesian inference, Dempster safer theory, neural network etc [23].

These techniques can be further divided into two types: Discriminative and generative models. These models depend on the perspective of machine learning. SVM and neural network both are discriminative whereas Bayesian inference is generative representation.

1.4.3 Estimation Based Techniques

These type of techniques include Kalman filter, Extended Kalman filter and Particle filter. These techniques are mostly used for better estimation of the state of moving entity that is based on multimodal information [24]. For tracking the object position, it requires the fusion of multiple modalities like audio and video.

II. RESEARCH RELATED TO MULTIBIOMETRIC SYSTEM

The making of this paper has an extensive background study of the technique proposed in this area. A more robust multibiometric system have low False Acceptance Rate (FAR) and False Rejection Rate (FRR) but accuracy rate must be high. FAR,FRR and accuracy rate of different fusion techniques are compared in table 1.

In [25], presented a multi-biometric system that fused face and palm prints modality at the feature level. Researcher believe that fusion at feature level gives more precise results in comparison to fusion at other levels, because feature level has high quality of information and quality degrades as it flows from feature to decision level. The GAR of the unimodal system using palm print as a modality is about 81.48% and system with face modality has GAR about 88.88%. When these modalities fused together, it will substantially increase accuracy of the system up to 95% with FAR of 0.5% and FRR of 1.2%.

In [26], researcher used the combination of Iris and Fingerprint at feature level. Eyelashes and eyelids are removed to avoid the situation of image inconsistencies in the snap shot of iris and then further processed. Core and delta points are extracted using Gabor function. Gabor filter is used for feature extraction from fingerprint and iris and then they are fused. The final match score is generated by Hamming Distance. This system is tested on 50 people. The proposed system has less execution time and the accuracy rate is very good, which is nearly 90%. The FAR and FRR of the system is also very low. The fingerprint of recognition and detection is done using singularity for detection and the iris recognition is done using the centre circular region. Speed of the proposed system is 5 times quicker than other system but it has large computational cost. So, the system was tested within budget which was 2 to 3 times faster as compared to its counter parts.

In [27], multiple instances of iris are used and fused at the decision level. Proposed system is robust to occlusion and outside noise. This robustness increases the efficiency of system to a great level. The proposed Scarcity based Multi Biometric Recognition (SMBR) technique gives an accuracy of 95.7 without error and 95.6 with error.

In [28], multimodal biometric system combined palm print and face at feature level. Fusion process at feature level give more precise result because it believe that feature level contains more rich and relevant information about input image. Accuracy rate of unimodal system with palm-print is about 81.48% while system with face modality is 88.88% when fused together, accuracy rate will increase up to 95% with FAR of 0.50 and FRR of 1.20%.

In [29], combined palm print and iris at feature level fusion. It has a very high accuracy rate of 99.2% with rejection rate of 1.6% only. The proposed security system is based on the wavelet technique. All the feature vectors attained are different in size, so the live feature vectors are matched with stored templates by kNN (k Nearest Neighbor) classification technique.

In [30], combined palm print and fingerprints at feature level wavelet techniques. Min-Max normalization technique is used to make the feature vector into common domain. Accuracy of the proposed system was 98.43 with false rejection rate of 0.9% and false acceptance rate of 1.02%. Proposed system can face problem or increase Failure to Enrol (FTE) rate if the person to be enrolled does not have hands because both input modalities are based on the hand of an individual.

In [31], combined fingerprint and palm print modalities at match score level in a multimodal biometric authentication system. Gabor filter is used for feature extraction and get accuracy of 87%. This system has FAR of 0.2% and FRR of 1.1%. One drawback of this system is that both the modalities used are related with hand. So, a person without hand and an aged person with wrinkle on their hand can cause hindrance in proper image acquisition through sensor.

In [32], proposed a system which fused finger print and iris at the matching score level. This system is a two-level approach in which input modalities are match with stored templates at level-I and if don't match only then level-II is set-up. This system has an accuracy rate of 97% with FAR rate of 1.23% and FRR of 2.46%.

In [33], proposed a multi-modal biometric that included iris and fingerprints at decision level. Fuzzy logic is used with

fusion which results in better performance and has accuracy rate of 98% with 2% FAR and FRR. This accuracy rate is very high for the multimodal system that uses fusion at decision level.

In [34], proposed a system that used multi-algorithmic method for feature extraction. Finger print is used as a modality and hybrid wavelet technique us used for feature extraction. Accuracy rate of this system is 86.4% when FAR and FRR are taken as 0%. It believes that multi-algorithmic method doesn't give accuracy rate as high as other technique like multi-instance, multi-sensor etc. In [35], proposed a multimodal system that includes face and ear modality at the matching score level. Principle component analysis (PCA) algorithm is used for extracting features from the input modalities. With this approach, overall accuracy of the system is 94.4%. Experimental evaluation implemented using Matlab tool.

In [36], proposed a multimodal biometric system which includes face and fingerprint recognition using logical AND operators at decision-level fusion. Recognition rate of unimodal face and finger print biometric system is 90.8%and 94% respectively. This rate increases up to 97.20% when multimodal biometric system is used. Both FAR and FRR have been reduced to 0.00 and 2.20% respectively and makes the system more robust.

In [37], decision level fusion is used with hybrid wavelet feature extraction method. Iris and Fingerprint are used as modalities in the system. This system has an accuracy rate of 84.2% with FAR and FRR of 0%.

In [38], a Multimodal system is proposed that fuses three modalities like fingerprint, retina and finger vein. Cryptography technique is also used after fusion to improve the performance. Implementation work has been done using Matlab. The proposed system has accuracy rate of 95.3% and FAR of 0.01%.

In [39], a multi-biometric fusion of fingerprint and signature is performed at the feature extraction level. Minutia fingerprint technique and Scale Invariant Feature Transform SIFT technique are used to extract the feature vectors. Sum rule is used for the fusion process. This fusion scheme decreased the FAR and FRR of the system to 0.09 and 0.02 respectively and increases system accuracy to 99.65.

In [40], proposed multimodal system was based on decision level fusion of face and fingerprint. Fuzzy logic has been applied after fusion to improve the efficiency of the system. The proposed system is successful in overcoming the drawbacks of individual sensors. Individually face and finger print unimodal system has accuracy of 94% and 94.6% respectively. But proposed system improves the accuracy rate to 99.5% with FAR of 2.40% and FRR of 2.00%.

In [41], proposed a multimodal system for fusion of the fingerprint and face biometric at the match score fusion level. For feature extraction face and fingerprint unimodal system uses scale invariant feature transform (SIFT) algorithm and the hamming distance to measure the distance between key points.

It has been observed that the multimodal system has a higher accuracy of 92.5% compared to the face and finger print unimodal system at 90% and 82.5% respectively. The system has FAR of 3.75% and FRR of 7.50%.

1n [42], proposed a multi-biometric authentication system based on face and iris fusion at match score level. Features of face are extracted using 2D wavelet transform while iris features are extracted using 2D Gabor filter. Proposed system has an accuracy of 99% which is very good as compared to other authentication systems.

Table 1: Accuracy rates at different Fusion Level

References	year	Fusion level used	Modality used	FAR %	FRR%	Accuracy %
[25]	2011	Feature extraction level	Face and palm-print	0.50	1.20	95
[26]	2012	Feature extraction level	Iris and finger-print	0.00	4.30	90
[28]	2012	Feature extraction level	Palm-print and face	1.20	0.50	95
[29]	2012	Feature extraction level	Palm-print and iris	0.00	1.60	99.20
[30]	2012	Feature extraction level	Finger-print and palm-print	1.02	0.90	98.43
[34]	2014	Feature extraction level	Finger-print and palm-print	0.00	0.00	86.40
[39]	2016	Feature extraction level	Finger-print and signature	0.09	0.02	99.65
[31]	2013	Match score level	Palm-print and finger-print	0.20	1.10	87
[32]	2013	Match score level	Finger-print and iris	1.23	2.46	97
[35]	2014	Match score level	Face and ear	0.00	0.00	94.40
[38]	2016	Match score level	Finger-print, retina and finger veins	0.01	0.01	95.30
[41]	2017	Match score level	Finger-print and face	3.75	7.50	92.50
[42]	2018	Match score level	Face and iris	--	--	99
[27]	2012	Decision level	Multiple instances of iris	0.01	0.00	95.70
[33]	2013	Decision level	Iris and finger-print	2.00	2.00	98
[36]	2015	Decision level	Face and finger-print	0.00	2.20	97.20
[37]	2014	Decision level	Iris and finger-print	0.00	0.00	84.20
[40]	2017	Decision level	Face and finger-print	0.00	4.00	96.00

III. CONCLUSION AND FUTURE WORK

Multi-biometric systems are already being used in many corporate and national security based organizations. Multimodal biometric system is deployed in many large scale biometric applications for e.g. FBI-IAFIS (Federal Bureau of Investigation – Integrated Automated Fingerprint Identification System) and UIDAI (Unique Identification security of India) system in India. In the paper, various fusion techniques are discussed which can be applied at any fusion level.

Fusion can also be performed at two or more than two levels in one multi-biometric system. It will increase the performance of the system but it might increase the complexity of system. Fig8 shows comparison of accuracy rates of different level of fusions performed on various modalities.

It is observed that fusion of more than two modalities increases the performance but it will also increase the complexity level of the system. The accuracy percentage range is between 85%-99% range, which is very desirable.

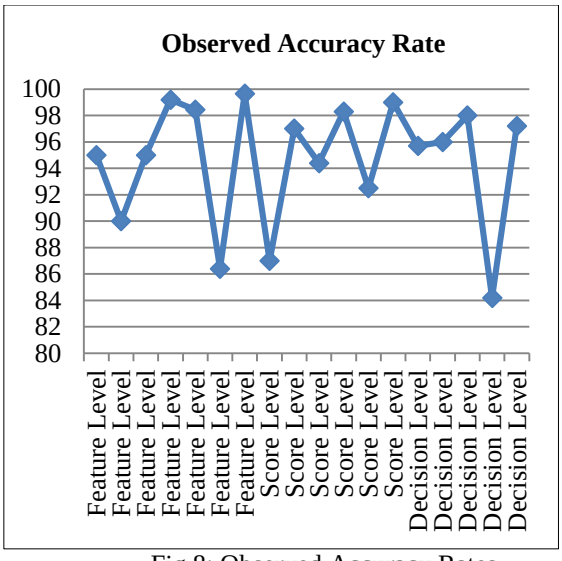

Fig.8: Observed Accuracy Rates

The amount of information at sensor or feature level is more accurate or relevant than at decision level because it goes on decreasing as proceeds from sensor to decision level. So, a multimodal system that fuses information at an early stage

will yield more promising results. But at the sensor level fusion have many problem of improper interaction of the user with the sensor; noise in sensed data because of improper maintenance etc. Work can be done in this area to make fusion at the initial levels easy by removing these problems. Such type of improvement will lead to the development of more secure and accurate multi-biometric system.

IV. REFERENCES

[1]. Maheswari MAP, Ancy S, Devanesam KEP. Biometric identification system for features fusion of iris and fingerprint. Recent Research in Science and Technology. 2012; 4(6):1–4.

[2]. Choudhari P, Hingway SP, Sheeja S, Suresh, Wagh A. Fusion of iris and fingerprint images for multimodal biometric identification. IOSR Journal of Engineering. 2014 Aug; 4(8):1–4.

[3]. Marasco E, Johnson P, Sansone C, Schuckers S. Increase the security of multi biometric systems by incorporating a spoofing detection algorithm in the fusion mechanism, Springer Berlin Heidelberg, Italy; 2011; 309–318.

[4]. Barde S, Khobragade, Singh R. Authentication Progression through Multimodal Biometric System, International Journal of Engineering and Innovative Technology. 2012 Sep; 2(3):255–258.

[5]. Kant, C. and Jain, R. (2015). Attacks on Biometric System: An Overview. International Journal of Computer Science and Application, 3(2): 1090-1094.

[6]. Obied, A. How To Attack Biometric System In Your Spare Time. International Journal Of Scientific & Technology Research. 2011; 4(1): 1-9.

[7]. He M, Horng S, Fan P, Run R, Chen R, Lai J, Khurram M, Octavius K. Performance evaluation of score level fusion in multimodal biometric systems.. 2009 Nov:1–12.

[8]. Peng D, Zuo X, Wu J, Wang C, Zhang T. A Kalman Filter based information fusion method for traffic speed estimation. Power Electronics and Intelligent Transportation System (PEITS); 2009.

[9]. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems For Video Technology. 2004; 14(1):4–20.

[10]. Mishra, A.. Multimodal Biometrics it is: Need for Future System. International Journals of Computer Application. *2010;* 3(4): 28-33.

[11]. Sanderson C, Paliwal KK. Information fusion and person verification using speech and face information. Research Paper IDIAP-RR 02-33, IDIAP; 2002.

[12]. Sankar SP, Dinakardas CN. Multimodal biometric authentication system based on high level feature fusion approach. European Journal of Scientific Research. 2012; 84(1):55–63.

[13]. Thomas T, Babu HK. A novel fake detection system for biometric modalities. International Journal of Advanced Research in Computer Science and Engineering. 2015; 5(4):439–44.

[14]. Gudavalli, M. Babu, A. V. and Kumar, D. S. Multimodal Biometrics–Sources, Architecture and Fusion Techniques: An Overview, IEEE: International Symposium on Biometrics and Security Technologies. 2012; 27-34.

[15]. Soliman H, Mohamed AS, Atwan A. Feature level fusion of palm veins and signature biometrics. International Journal of Video and Image Processing and Network Security. 2012 Feb; 12(1):1–12.

[16]. Mahoor MH. A multimodal approach for face modelling and recognition. IEEE Transactions on Information Forensics and Security. 2008 Sep; 3(3):431–40.

[17]. Ben-Yacoub S, Abdeljaoued Y, Mayoraz E. Fusion of face and speech data for person identity verification. IEEE Transactions on Neural Networks. 1999; 10(5):1065–75.

[18]. Ross A, Jain AK. Information fusion in biometrics. Pattern Recognition Letters. 2003; 24(13):2115–25.

[19]. Jain A, Nandakumar K, Ross A. Score normalization in multimodal biometric systems. Pattern Recognition Society. 2005:2270–85.

[20]. Ho TK, Hull JJ, Srihari SN. Decision combination in multiple Classifier systems. Pattern Analysis and Machine Intelligence. 1994 Jan; 16(1):66–75.

[21]. Garje PD, Agrawal SS. Multimodal Identification System. IOSR Journal of Electronics and Communication Engineering. 2012; 2(6):1–5.

[22]. Gagandeepkaur, Mittal AK. A new hybrid wavelet based approach for. International Journal of Innovative Research in Science, Engineering and Technology. 2015:19034–43.

[23]. Dhriti, Kaur M. K-nearest neighbor classification approach for face and fingerprint at feature level fusion. International Journal of Computer Applications. 2012; 60(14):13–17.

[24]. Hong L, Jain AK. Integrating faces and fingerprints for personal identification, IEEE Transactions on PAMI. 1998; 20(12):1295–1307.

[25]. Jagadessan K, Duraisamy. Secured cryptographic key generation from multimodal biometrics: Feature level fusion of fingerprint and iris. International Journal of Computer Science and Information Security. 2011; 7(1):296–305.

[26]. Gawande U, Nair SR, Balani H, Pawar N, Kotpalliwar M.A high speed frequency based multimodal biometric system using iris and fingerprint. International Journal on Advanced Computer Engineering and Communication Technology. 2012; 1(2):1–8.

[27]. Shekhar S, Patel VM, Nasrabadi NM, Chellappa R. Joint Sparsity-based robust multimodal biometrics recognition. European Conference on Computer Vision; 2012. p. 365–374.

[28]. Bokade GU, Sapkal AM. Feature level fusion of palm and face for secure recognition. International Journal of Computer and Electrical Engineering. 2012; 4(2):1–10.

[29]. Gayathri R, Ramamoorthy P. Feature level fusion of palm print and iris. International Journal of Computer Science. 2012 Jul; 9(4):1–10.

[30]. Krishneswari K, Arumugam S. Multimodal biometrics using feature fusion. Journal of Computer Science. 2012; 8(3):431–5.

[31]. Dhameliya MD, Chaudri JP. A multimodal biometric recognition system based on fusion of palm print and fingerprint. International Journal of Engineering Trends. 2013; 4(5):1–4.

[32]. Hamad AM, Elhadary RS, Elkhateeb AM. Multimodal biometric personal identification system based on fingerprint and iris. International Journal of Computer Science and Communication Networks. 2013; (4):226–30.

[33]. Abdolahi M, Mohamadi M, Jafari M. Multimodal biometric system fusion using fingerprint and iris with fuzzy logic. International Journal of Soft Computing and Engineering. 2013; 2(6):1–7.

[34]. Bharadi VA, Pandya B, Nemade M. Multimodal biometric recognition using iris and fingerprint. IEEE Transactions; 2014.

[35]. Gambhir A, Narke S, Borhade S, Bokade G. Person Recognition Using Multimodal Biometrics. International Journal of Emerging Technology and Advanced Engineering. 2014; 4(4): 725-728..

[36]. Celik N., ManivannanN., Balachandran W. and Kosunalp S. Multimodal Biometrics for Robust Fusion Systems using Logic Gates. Journal of Biometrics & Biostatistics. 2015;6(1): 1-6.
[37]. Bharadi VA, Pandya B, Nemade M. Multimodal biometric recognition using iris and fingerprint. IEEE Transactions; 2014.
[38]. Jagadiswary D, Saraswady D. Biometric Authentication using Fused Multimodal Biometric. International Conference on Computational Modeling and Security. 2016; 109-116.
[39]. Kataria S, Goel AK. A Hybrid Approach for Biometric Authentication using Fusion of Fingerprint and Signature. International Journal of Scientific Research Engineering & Technology (IJSRET). 2016; 5(1): 35-38.
[40]. Sharma P, Singh K. Multimodal Biometric System Fusion Using Fingerprint and Face with Fuzzy Logic. International Journal of Advanced Research in Computer Science and Software Engineering. 2017; 7(5): 482-489.
[41]. Mwaura GW, Mwangi PW, Otieno C. Multimodal Biometric System:-Fusion Of Face And Fingerprint Biometrics At Match Score Fusion Level. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH. 2017; 6(4): 41-49.
[42]. Asst. Prof. Selim MM, Dr. Mahmoud RO, Muhi **OA.** A Feature level Fusion of Multimodal Biometric Authentication System. JCIT (Journal of Convergence Information Technology). 2018; 13(1): 1-11