A New Approach for Security System based on Multi-Biometric Parameter

Mr. Pund Kishor Jagannath[1], Prof. V. S. Bhatlavande[2]

[1] *Student, VLSI and Embedded System, Siddhant College of Engineering, Sudumbare, Pune 412109, Maharashtra, India*

[2] *Asst. Prof., VLSI and Embedded System, Siddhant College of Engineering, Sudumbare, Pune 412109, Maharashtra, India*

ABSTRACT

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Multimodal biometric systems are becoming more and more popular, they have more accuracy as compared to unimodal biometric systems. On the other hand these systems are more complex. By using different Biometrics parameter we can create security system, which will be useful for the person's identification and authentication and also for access control. This security system can be used anywhere as per the requirement of the user. For keeping the things confidential people needs security system, that security system should not be known or recognizable to anyone. As the Biometric parameters i.e. human characteristics and traits can allow people identification and authentication, it is used for security purpose globally. Researchers are working on the different biometric parameters which can be used for the creation of the security system. We discuss here different types of multimodal biometric systems, different decision fusion techniques used in these systems. We discuss their feasibility and advantage over unimodal biometric systems & some of the future directions of biometrics system.

Keyword : - *Biometric, confidential, authentication, multimodal, unimodal.*

1. INTRODUCTION

In recent years, the increasing interest in security system has led to the creation of numerous and very diverse initiatives focused on a various biometric parameters such as physical (Fingerprint, Face, Iris, Ear, Retina, Hands) and behavioral (Walking, signature, typing patterns) etc. Now days, whole word is facing a problem of insecurity in case of things, in case of documentation, in case of jewelry, in case of Banking etc. There are number of things which are insecure because of increased in the hacking and thieves. As the technology is getting advance new techniques are proposed for the security. The study of automated identification and verification of person with the help of human's physical or behavioral characteristics and traits is called as biometric. Biometrics parameter has advantage that it has no risk of forgetting, losing it, getting it stolen, getting is copy, being used by anyone else. And it has properties like Universal, Uniqueness, Permanence and Collectability. Now again question arises that why to go for biometric? Answer is that it is more secure because of its simplicity and easiness. In this only the intended person has the access control for the authentication. For this various methods or parameters are used for it s uch as face, iris, fingerprint, ECG or key, password, magnetic card or smartcard. Because of unique features biometric parameters are mostly used in various security now a day's which is playing a very important role in that field.

The security of a system has three primary components - authentication, authorization, and accountability. Authentication is the most fundamental of these three elements because it comes first. In the information technology domain, authentication means either the process of verifying the identities of communicating equipment, or verifying the identities of the equipment's users which are primarily humans. Biometric systems are becoming popular as a measure to identify human being by measuring one's physiological or behavioral c haracteristics. Biometrics identifies the person by what the person is rather than what the person carries, unlike the conventional authorization systems like smart cards. Unlike the possession-based and knowledge-based personal identification schemes, the biometric identifiers cannot be misplaced, forgotten, guessed, or easily forged. Despite these inherent advantages, the wide scale deployment of biometrics-based personal identification has been hindered due to several reasons: Firstly, the less than desirable accuracy in several application domains, for example, face recognition. The accuracy of face recognition is affected by illumination, pose and facial expression [1]. Secondly, the biometric system cannot eliminate spoof attacks. Thirdly, some persons cannot provide the required standalone biometric, owing to illness or disabilities [2]. The multimodal biometric systems provide advantage over the conventional Unimodal biometric systems in various ways, we discuss this in the coming section, summarizing here we put the limitations [3] of Unimodal biometric systems as:

1. Susceptibility of biometric sensors to noise. This can lead to inaccurate matching, as noisy data may lead to a false rejection.
2. Unimodal systems are also prone to interclass similarities within large population groups e.g. In case of identical twins, facial feature leads to inaccurate matching, as bad data may lead to a false rejection.
3. Incompatibility with certain population. Elderly people and young children may have difficulty enrolling in a fingerprinting system, due to their faded prints or underdeveloped fingerprint ridges.
4. Finally, Unimodal biometrics is vulnerable to spoofing, where the data can be imitated or forged. e.g. rubber fingerprints can be used for spoofing, hence liveness tests are required.

2. BIOMETRICS

Biometrics is related to the human characteristics and traits. Biometrics authentication is mostly used in computer science for identification and access control for security purpose. It is also used to identify individuals in groups that are under security. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric characteristics are often classified as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the human body. Examples include, but are not limited to fingerprint, ECG, face recognition, ear recognition, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a human being, including but not limited to typing rhythm, walking style, and speech. Since biometric parameters are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric parameters raises privacy concerns about the ultimate use of this information.

Many different aspects of human physical, chemistry or behavior can be used for biometric authentication. Convenient biometric use dependent on the application. Certain biometrics parameter will be better than oth ers based on the required levels of convenience and security. No single biometric will meet all the requirements of every possible application.

2.1 Features of Biometrics security System.

1) Unique, Uniqueness which means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.

2) Highly measurable, Measurability (collectability) relates to the ease of accretion or measurement of the trait. In addition, obtained data should be in a form that permits subsequent processing and extraction of the relevant feature sets.

3) Performance is good, which relates to the accuracy, speed, and robustness of technology used.

4) Highly universal, Universality means that every person using a system should possess the characteristics.

5) Highly acceptable, Acceptability relates to how well individuals in the pertinent population accept the technology such that they are willing to have their biometric attribute captured and assessed.

2.2 Challenges of Biometrics security systems

Biometrics security systems face some main challenges, these are high initial cost, time consuming, knowledgeable person required for its use, somewhat complex. The main intention of this research is to design and implement a security system using Biometrics parameter which can give access control for the recognition and authentication of a person to the system. The security system requires number of sensors depending on the level of security that is to be required by user.

3. ASPECTS OF MULTIMODAL BIOMETRICS SYSTEM

Multimodal Biometric systems have following advantage over Unimodal biometric systems

1. Systems are resistant to intra class similarity of data like facial feature. They combine more than one modality causing reduced intra-class similarity.
2. Noise resistance- Multimodal systems are more resistant to noise as compared to Unimodal biometric systems, as they have more than one modality more data is available for matching.
3. Less vulnerable to spoofing, as it is difficult to spoof more than one modality simultaneously.

As these are clear advantage we have to fight with following issues when it comes for implementation of multimodal biometric security system

1. Interpretability – various systems using multimodal features must follow uniform rules for classification, these rules are not yet standardized.
2. Implementation Cost – Systems use more hardware and computational resources causing increased setup cost.
3. Reduced matching levels – Better decision fusion algorithms are required to attain higher matching levels in combination of biometric traits than the individual matching level.

All the above issues are being addressed by various researchers worldwide and this can lead to design of better Multimodal biometric systems in future.

4. FUSION IN MULTI-BIOMETRIC SYSTEMS

In multimodal biometrics we use more than one biometric modality; we have more than one decision channels. We need to design a mechanism that can combine the classification results from each biometric channel; this is called as biometric fusion. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths and diminish the weaknesses of the individual measurements. Fusion at matching score, rank and decision levels have been extensively studied in the literature [6][7]. Multimodal Biometrics with various levels of fusion: sensor level, feature level, matching score level and decision level.

A. ***Sensor level Fusion***: In sensor Fusion we combine the biometric traits coming from sensors like Thumbprint scanner, Video Camera, Iris Scanner etc, to form a composite biometric trait and process.

B. ***Feature Level Fusion***: In feature level fusion signal coming from different biometric channels are first preprocessed, and feature vectors are extracted separately, using specific fusion algorithm we combine these feature vectors to form a composite feature vector. This composite feature vector is then used for classification process.

C. ***Matching Score Level***: Here, rather than combining the feature vector, we process them separately and individual matching score is found, then depending on the accuracy of each biometric channel we can fuse the matching level to find composite matching score which will be used for classification.

D. ***Decision level Fusion***: Each modality is first pre-classified independently. The final classification is based on the fusion of the outputs of the different modalities.

Multimodal biometric system can implement any of these fusion strategies or combination of them to improv e the performance of the system; the different levels of fusion.

5. MULTI-MODAL BIOMETRIC SYSTEM ARCHITECTURE

Here we discussed some of the existing architectures. In [8] Jain and Ross has discussed a Multimodal biometric system using Face & Fingerprint, they have proposed various levels of combinations of the fusion this system is shown in Fig. 1

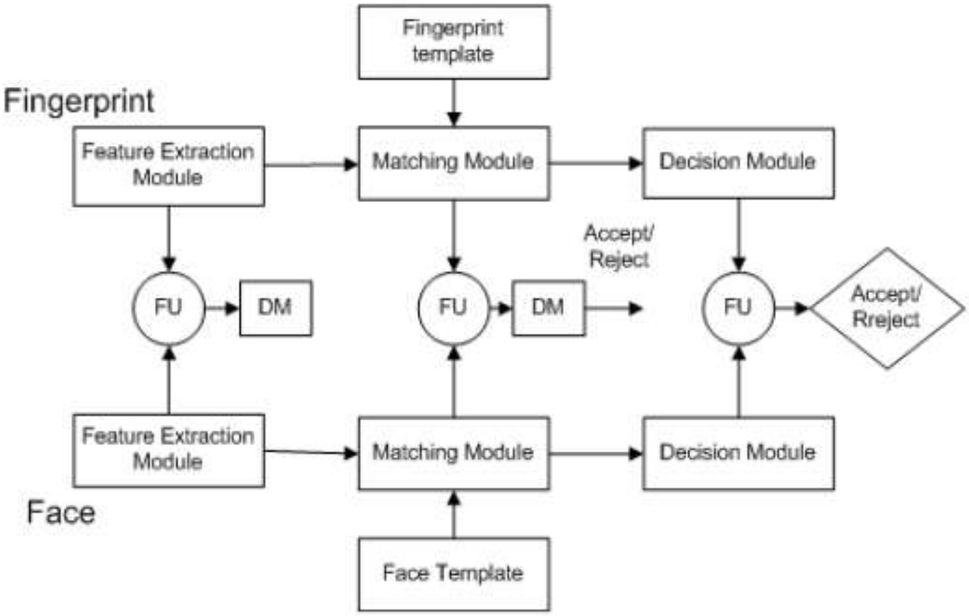

Figure1. Multimodal Biometric System using Face and Fingerprint (FU- Fusion DM-Decision module)

Yan and Zang [9] have proposed a correlation Filter bank based fusion for multimodal biometric system; They used this approach for Face & Palmprint biometrics. In Correlation Filter Bank, the unconstrained correlation filter trained for a specific modality is designed by optimizing the overall original correlation outputs. Therefore, the differences between Face & Palmprint modalities have been taken into account and useful information in various modalities is fully exploited. PCA was used to reduce the dimensionality of feature set and then the designed correlation filter bank (CFB) was used for fusion. Fig. 2 Shows the fusion network architecture proposed by them, the recognition rates achieved are in the range 0.9765 to 0.9964 with the proposed method.

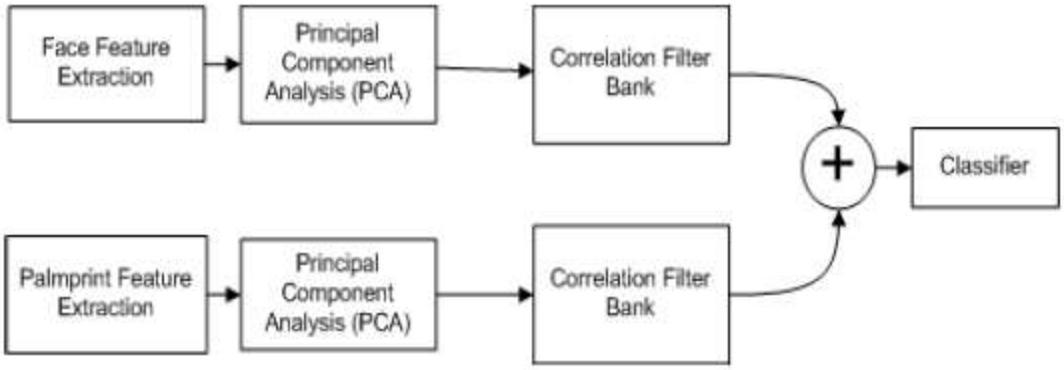
Face Feature Extraction
Principal Component Analysis (PCA)
Correlation Filter Bank
+
Classifier
Palmprint Feature Extraction
Principal Component Analysis (PCA)
Correlation Filter Bank

Figure2. Correlation Filter Bank Fused Fusion

K. Kryszczuk, J. Richiardi have presented an reliability based information fusion model for multimodal biometrics [10]. They have used Bayesian network for modality decision reliability estimation. This method has been used for Face & Speech biometrics and a better fusion was obtained. Fig. 3 Shows the reliability based fusion for Speech & Face biometrics.

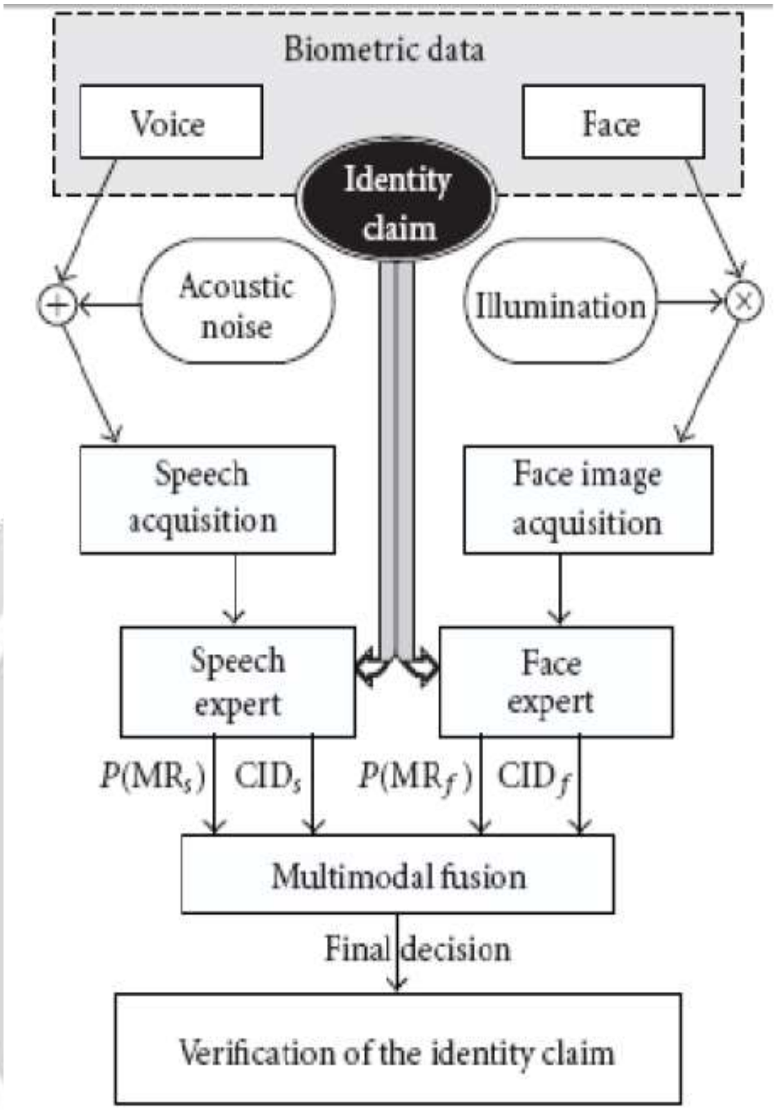

Figure3. Multimodal Biometric system with reliability information [10]

In [11] F. Yang & M. Baofeng have discussed two multimodal biometric systems based on fingerprint, palm-print and handgeometry, whose features can be extracted from the human hand. For one fusion modal, the verification process is organized as follows: image capture; processing; sub-images extraction; five fingerprints classification by SVM (Support Vector Machine) and extracting palm-print and hand-geometry features; matching score normalization; fusion at matching score level by SVM too, finally a decision made. For the other, wavelet transform to extract the features from fingerprint and palm-print is used and hand-geometry feature (such as width and length) is extracted after the preprocessing phase. Feature fusion and mach score fusion are together employed to establish identity. The later system was found to be having better performance. In the model shown in Fig 5. Fingerprint and palm-print employed Discrete Wavelet Transform (DWT) to extract fingerprint and palm print features are connected as a Joint Feature Vector (JFV) at feature lever fusion; matching scores are connected at the matching score level; finally, a decision is made, The results obtained by this model are shown in Fig. 6. , the graph shows the increase in performance as Receiver operating characteristics are high for given FAR for multimodal biometric system based on fusion of palm and fingerprint.

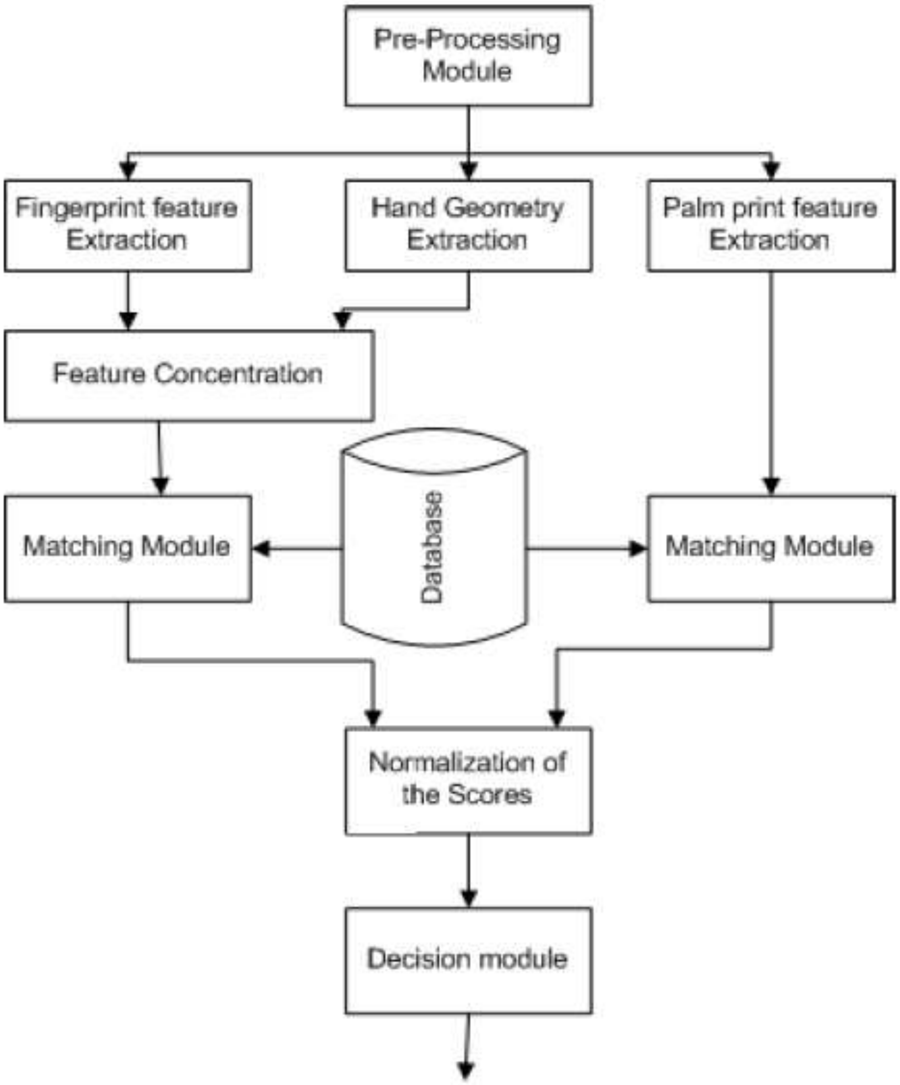

Figure4. Multimodal biometric system using Palm and Fingerprint

CONCLUSION

In this paper we have different aspects of biometric identification systems, their types, current architectures, future architecture and efforts towards the development of common framework for biometric identification. Summarizing we can say that the biometrics systems are effective for human identification and authorization over various levels of implementation , for small to a large population, such systems are difficult to forge and can be made for secure by combining more than one biometric traits , that is multimodal biometric systems. Such systems will become ubiquitous and inevitable in the coming future. We can expect more robust, effective and accurate biometric system for the near future.

REFERENCES

[1] Monrose, F., Rubin, A.D, “Keystroke Dynamics as a Biometric for Authentication” ,Future Generation Computer Systems, Vol. 16, No. 4 (2000) 351-359

[2] G.Feng, K. Dong, D. Hu and David Zhang, "When Faces Are Combined with Palmprints: "A Novel Biometric Fusion Strategy, Proceedings of First International Conference, ICBA 2004, (2004), Springer, 701-707

[3] C. Lupu, V Lupu, “Multimodal Biometrics for Access Control in an Intelligent Car”, 3rd International Symposium on Computational Intelligence and Intelligent Informatics - ISCIII 2007 - Agadir, Morocco, March 28-30, 2007.

[4] Teddy Ko , “Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition”, Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05) ,2005.

[5] “Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability,” November 13, 2002

[6] J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, "Fusion strategies in Biometric Multimodal Verification", Proceedings of International Conference on Multimedia and Expo, ICME 2003.

[7] L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(12), pp. 1295-1307, December 1998.

[8] A. K Jain, A. Ross, “Information Fusion In Biometrics”,Elsevier, Pattern Recognition Letters 24 (2003)

[9]Y. Yan, Y Zang,, “ Multimodal Biometrics Fusion Using Correlation Filter Bank”, IEEE, DOI-978-1-4244-21756

[10] K.Kryszczuk, J. Richiardi, P.Prodanov, and A.Drygajlo, "Reliability-Based Decision Fusion inMultimodal Biometric Verification Systems", EURASIP Journal on Advances in Signal Processing Volume 2007, Article ID 86572

[11] F. YANG, M. Baofeng ,"Two Models Multimodal Biometric Fusion Based on Fingerprint, Palm-print and Hand-Geometry",DOI- 1-4244-1120-3/07, IEEE,2007

[12]H Kekre, V Bharadi , “Ageing Adaptation for Multimodal Biometrics”, Proceedings of International Conference on Computing, Communication & Control, ICAC3’09, ACM-SIGART Conf. ID - 2009-16014