Multimodal Biometrics it is: Need for Future Systems

Ashish Mishra
Assistant Professor ,
Department of Computer Science,. GGCT, Jabalpur, [M.P.]

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. 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.

I. INTRODUCTION

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 characteristics. 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.

II. MULTIMODAL BIOMETRICS SYSTEM

Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a verification / identification system. Identification based on multiple biometrics represents an emerging trend. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. One is that different biometric modalities might be more appropriate for the different applications. Another reason is simply customer preference.

The International Committee for Information Technology Standards (INCITS) Technical Committee M1, Biometrics, and researchers have described methods for performing multi-biometric fusion [4]. In general, the use of the terms multimodal or multi-biometric indicates the presence and use of more than one biometric aspect (modality, sensor, instance and/or algorithm) in some form of combined use for making a specific biometric verification/identification decision [4].

The goal of multi-biometrics is to reduce one or more of the following:

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)
- Susceptibility to artifacts or mimics

To further the understanding of the distinction among the multi-biometric categories [4], [5] they are briefly summarized in the following:

Multimodal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example, a system combining face and iris characteristics for biometric recognition would be considered a "multimodal" system regardless of whether face and iris images were captured by different or same imaging devices. It is not required that the various measures be mathematically combined in anyway. For example, a system with fingerprint and face recognition would be considered "multimodal" even if the "OR" rule was being applied, allowing users to be verified using either of the modalities.

Multi-algorithmic biometric systems take a single sample from a single sensor and process that sample with two or more different algorithms. The technique could be applied to any modality. Algorithms can be designed to optimize performance under different circumstances.

Multi-instance biometric systems use one sensor (or possibly multiple sensors) to capture samples of two or more different instances of the same biometric characteristics. For example, systems capturing images from multiple fingers are considered to be multi-instance rather than multimodal. However, systems capturing, for example, sequential frames of facial or iris images are considered to be multi-presentation rather than multi-instance. This is whether or not the repeated captured images are combined at the image (feature) level, some other level of combination or a single image is selected as the one best used for pattern matching.

Multi-sensorial biometric systems sample the same instance of a biometric trait with two or more distinctly different sensors. Processing of the multiple samples can be done with one algorithm or some combination of multiple algorithms. For example, a face recognition application could use both a visible light camera and an infrared camera coupled with specific frequency (or several frequencies) of infrared illumination.

For a specific application in an operational environment, there are numerous system design considerations, and trade-offs that must be made among factors such as improved performance (e.g. verification or identification accuracy, system speed and throughput, robustness, and resource requirements), acceptability, circumvention, ease of use, operational cost, environment flexibility and population flexibility. Especially for a large-scale identification system, there are additional system design considerations such as operation and maintenance, reliability, system acquisition cost, life cycle cost and planned system response to identified susceptible means of attacks, all of which will affect the overall deployability of the system.

III. ASPECTS OF MULTIMODAL BIOMETRIC SYSTEMS

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.

IV. FUSION IN MULTIMODAL 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 improve the performance of the system; the different levels of fusion are shown in Fig. 1. as follows.

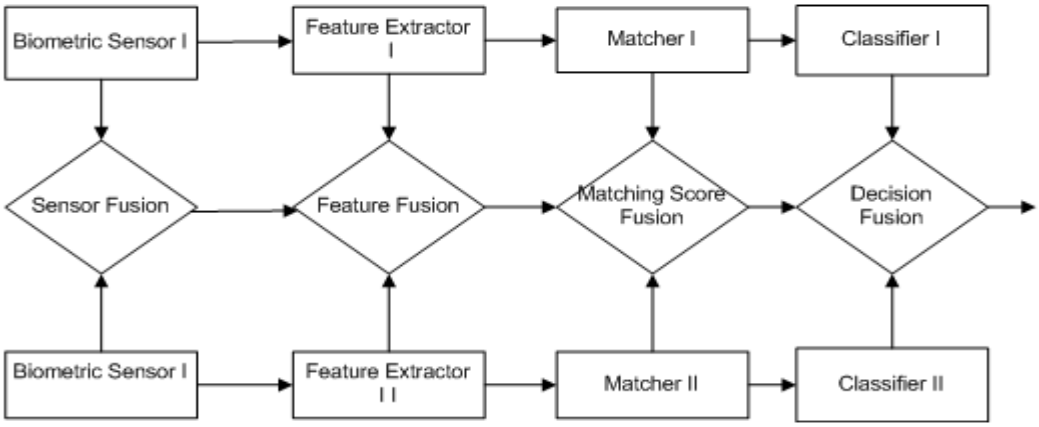

Figure 1. Fusion levels in Multimodal Biometric Systems

V. MULTIMODAL BIOMETRIC SYSTEMS ARCHITECTURES

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. 2.

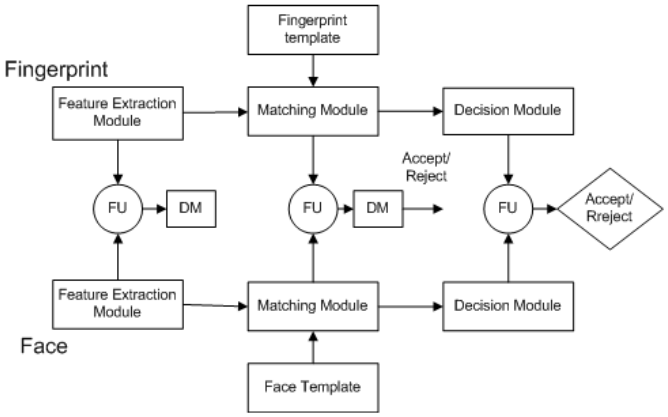

Figure 2. Multimodal Biometric System using Face & Fingerprint. (FU-Fusion, DM – Decision Module)

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. 3 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.

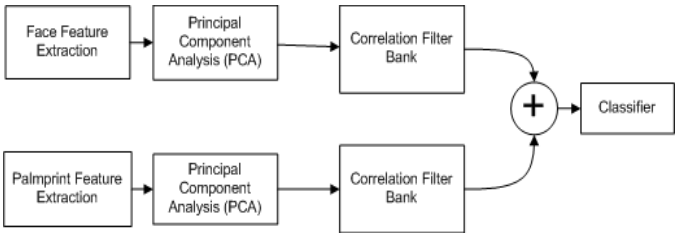

Figure 3. Correlation Filter Bank based Fusion [9]

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. 4 Shows the reliability based fusion for Speech & Face biometrics.

In [11] F. Yang & M. Baofeng have discussed two multimodal biometric systems based on fingerprint, palm-print and hand-geometry, 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 pre-processing 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.

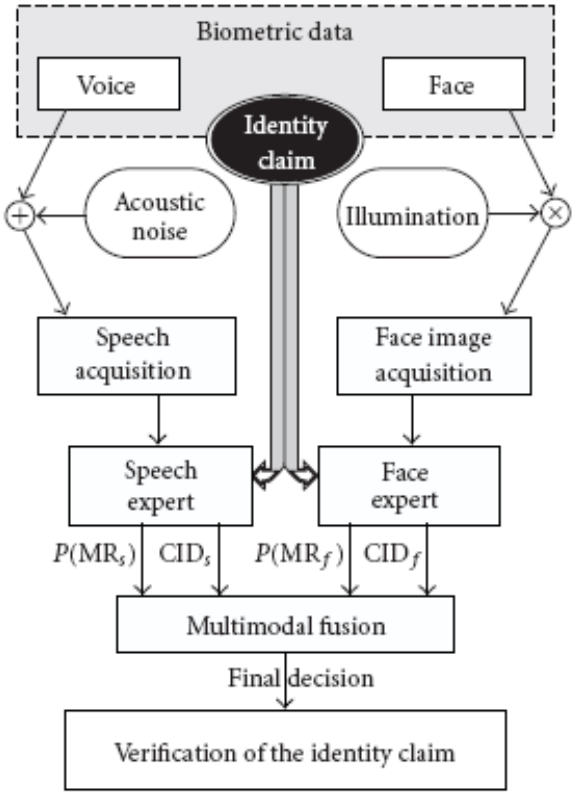

Figure 4. Multimodal Biometric System with reliability information [10]

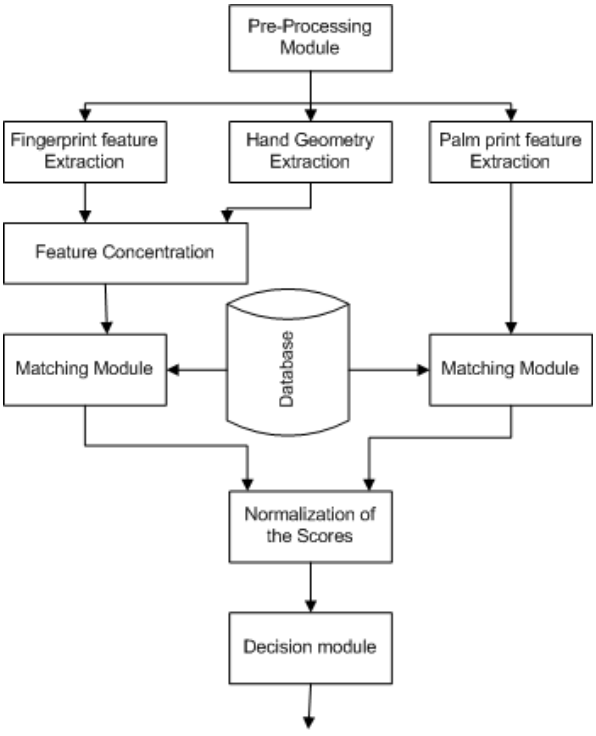

Figure 4. Multimodal Biometric with Palm & Fingerprint Fusion [11]

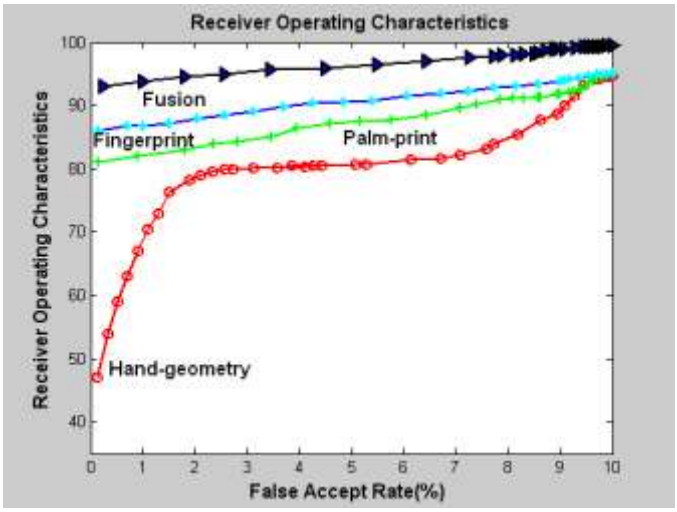

Figure 4. Results for system [11] shown in Fig. 5.

Result for "State-of-the-art" Error Rates Fig.4

	Test	Test Parameter	False Reject Rate	False Accept
voice	NIST [2000]	Text Independent	10-20%	2-5%
Face	FRVT [2002]	Varied lighting, outdoor/indoor	10%	1%

VI. AGEING ADAPTATION FOR MULTIMODAL BIOMETRICS

Another Important aspect is to be discussed is the ageing of human being. In [12] authors have proposed a n algorithm for ageing adaptation for multimodal biometrics.

The current biometric system enroll human being by capturing biometric trait over a very short span of time (hardly minutes or hours) , the databases used for testing are collected over a time of few weeks to months. Biometric features such as face, voice, signature

and gait change gradually with time. This may be due to ageing, illness or any other environmental factor. As discussed above the on the field biometric systems do not consider this aspect while enrolling and it is not practical also to take samples over the period of few months or years.

The solution is to re-enroll complete feature set after certain time, authors have proposed an adaptive feature set updating algorithm for multimodal biometrics which will take care of this thing and the update procedure will be secure and gradual over the time. This algorithm is proposed for only multimodal biometric systems having at least one feature which has high degree of permanence, this include fingerprint, iris and retina.

The architecture of system is given in Fig. 5, this shows two channels, one for dependent biometric trait (Face, Voice Signature) and one for independent biometric trait (Fingerprint, Iris, Retina, Palm-print), the adaptive feature set update module is implemented separately and takes input from final decision and independent channel matching score. This architecture is useful for future biometric system for adapting to human ageing.

Further we discuss efforts towards normalization of programming and hardware platform for biometrics. A common framework is the need of future biometric systems for seamless integration.

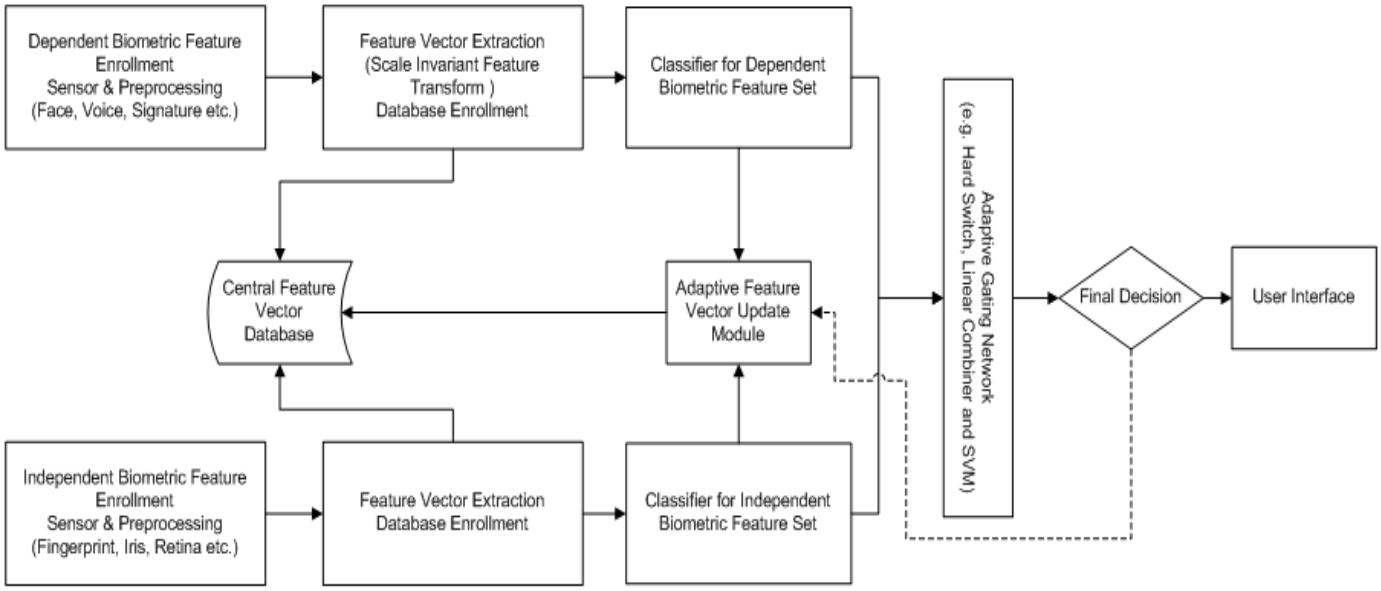

Figure 5. Multimodal Biometric System using Adaptive Feature Vector Update mechanism.

VII. BioAPI

BioAPI (Biometric Application Programming Interface) is a key part of the International Standards that support systems that perform biometric enrollment and verification (or identification). It defines interfaces between modules that enable software from multiple vendors to be integrated together to provide a biometrics application within a system, or between one or more systems using a defined Biometric Interworking Protocol (BIP) [13][14] as shown in Fig. 6.

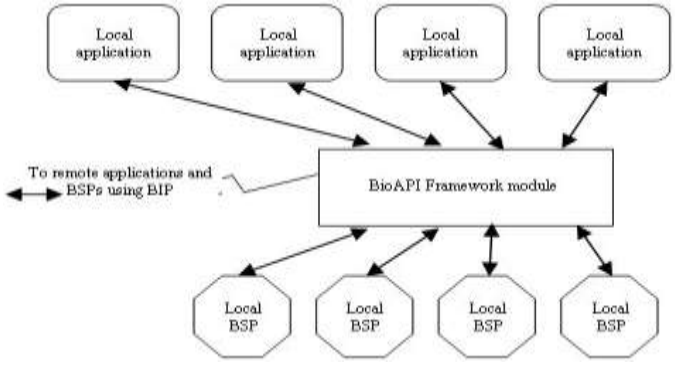

Figure 6. BioAPI architecture

Biometrics (measurements of physical characteristics of a person) are increasingly being used to provide verification of the identity of an individual, once they have been enrolled (one or more of their physical characteristics has been measured). Computer systems that perform biometric enrollment, verification, or identification are becoming increasingly used. The BioAPI specification enables such systems to be produced by the integration of modules from multiple independent vendors.

The BioAPI Consortium was founded to develop a biometric Application Programming Interface (API) that brings platform and device independence to application programmers and biometric service providers. The Consortium is a group of over 120 companies and organizations that have a common interest in promoting the growth of the biometrics market.

BioAPI is dedicated to developing a specification for a standardized Application Programming Interface (API) that will be compatible with a wide range of biometric application programs and a broad spectrum of biometric technologies. The API description defines how application programmers and biometric solution vendors write to the common BioAPI interface. The BioAPI runtime framework will allow applications to interoperate with various biometric solutions.

Security considerations will be central to the development of both the application and device levels of the BioAPI standard. Besides BioAPI other identification and authentication standards also exixt which incorporate biometrics, such as CDSA/UAS, PAM/XSSO, and MS CAPI.

It is also expected that future biometrics applications will use multiple biometric modalities (for example, fingerprint, iris, and face), both to improve the accuracy of identification and to cope with people that are missing a finger, or have disability problems that prevent use of iris or face recognition

Another ISO/IEC JTC1/SC37 Standard - BioAPI Interworking Protocol (BIP) - specifies an enhancement of the BioAPI Framework that essentially maps all API calls into network messages (defined using ASN.1) to provide a distributed BioAPI system. BIP is also being progressed as a Recommendation in ITU-T as Joint text with ISO/IEC [15].

VIII. 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.

This is ensured by the normalization efforts like BioAPI which are aimed towards development of a common framework for biometrics systems. We can expect more robust, effective and accurate biometric system for the near future.

REFERENCE

[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-978-1-4244-2175-6

[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

[13] http://www.bioapi.org/index.asp, 10/01/2009

[14] http://en.wikipedia.org/wiki/BioAPI, 10/01/2009

[15] BioAPI Specification Version 1.1, March 16, 2001, Developed by the BioAPI Consortium