AUGMENTED SECURITY THROUGH MULTIMODAL BIOMETRIC SYSTEM

Mohamed Basheer.K.P, Research Scholar, Dept. of Computer Science, Jamal Mohammed College, Thiruchirappalli,

Abstract

Biometrics is a technique by which an individual's identity can be authenticated by applying the physical or behavioral trait. Physical traits, like fingerprints, face, iris etc. are based on physical characteristics which are generally inherent and stable. Behavioral traits, like voice, signature or keystroke dynamics etc. on the other hand, is a quantifiable characteristics. That is obtained over time and is subject to deliberate alteration. Unimodal biometric systems developed for each of these biometric features may not always meets the required performance. The methods are analyzed to integrate the various features together to acquire a multi-modal biometric system. The recent research reveals that multi-modal biometric system is more effective in authentication. The objective of this paper is to highlight the importance of the use of multimodal biometrics in the area of secure person authentication. This study provides a different perception to use biometrics as a highest level of network security with the fusion of multiple biometric modalities.

Key Words: *Biometrics, Unimodal Biometrics, Multi-modal Biometric System, Fusion Levels.*

1. INTRODUCTION

A biometric system measures one or more physical or behavioral characteristics including fingerprint, palm-print, face, iris, retina, ear, voice, signature, gait, hand-vein information of an individual to determine or verify his identity. These characteristics are referred by different terms such as traits, indicators, identifiers, or modalities [1]. A Biometric system is an identification system based on the use of different biometric features of individuals by the analysis of physiological characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements for authentication purposes or behavioral characteristics. Authentication systems setup with one biometric modality may not be sufficient for the pertinent application in terms of properties such as universality, distinctiveness, acceptability etc. Unimodal biometric systems are lacking operational advantages pertaining to the performance and accuracy [2]. 100% accuracy may not achieve in unimodal systems on account of the limitations such as the noise in the sensor data, intra-class variations, inter-class similarities, lack of universality, interoperability issues, spoof attacks and other vulnerabilities. Accuracy in biometrics is measured in terms of 'error rates'. The two mainly used error rates are False Acceptance Rate (FAR) and False Rejection Rate(FRR). Multi-modal biometric system is a refined system of unimodal system incorporating the remedial measures for the drawbacks faced in unimodal biometric system.

2. MULTI-MODAL BIOMETRIC SYSTEM

Multi-modal biometric is a system that combines the results obtained from more than one biometric feature for the purpose of personal identification. Multi-modal biometric systems are more reliable because many independent biometric modalities are used. By the use of multiple number of biometric modalities may result highly accurate and secure biometric identification system, as unimodal biometric system may not provide accurate identification due to non-universality. For example, since few percentages of people can have worn, cut or unrecognizable prints, finger-print biometric may produce erroneous results. In Multi-modal biometric Systems, failure of any one technology may not affect seriously the individual identification as other technologies can be successfully employed. Hence the spoofing can be minimized drastically; thus improving the efficiency of the overall system. The reduction in failure to enroll (FTE) rate in multi-modal evaluation is very significant and which is one of major advantages of this system. A common biometric system mainly involves the following major modules [3] - sensor module, feature extraction module, matching module and decision making module. Each of these modules is described below.

2.1 Sensor module

At sensor module a suitable user interface incorporating the biometric sensor or scanner is needed to measure or record the raw biometric data of the user. This raw biometric data is captured and then it is transferred to the next module for feature extraction. The design of the sensor module influences the various factors like cost and size.

2.2 Feature extraction module

At feature extraction module the quality of the acquired biometric data from the sensor is assessed initially for further processing. Thus generating a synoptic but

indicative digital representation of the underlying traits or modalities. After extracting the features it is given as input to the matching module for further comparison.

2.3 Matching module

The extracted features when compared with the templates in the database generate a match score. This match score may be controlled by the quality of the given biometric data. The matching module also condensed a decision making module in which the generated match score is used to validate the claimed identity.

2.4 Decision making module

Decision making module identifies whether the user is a genuine user or an impostor based on the match scores. These are used to either validate the identity of a person or provides a ranking of the enrolled identities for identifying an individual.

The two major mode of operation in multi-modal biometric systems are serial mode and parallel mode. In serial mode of operation, multiple sources of information is not acquired simultaneously, that is the user goes through stage by stage authentication process. Thus the recognition time is improved in serial mode as decision is made before getting all the traits. But in the case of parallel mode of operation, recognition is performed by acquiring multiple sources of information simultaneously [4]. This will reduce the efficiency of the system and in turn cause inconvenience to the user. Thus both modes of operations have its own advantages and disadvantages. Study reveals that combined use of both modes may result a system which provides high efficiency and user convenience. A simple block diagram for multi-modal biometric system is shown in Fig-1

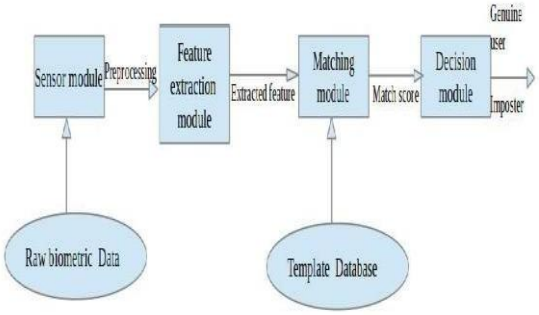

Fig-1: Block diagram of multi-modal biometrics system

By employing the information available in any of the modules like sensor level, feature extraction level, matching level and Decision making level, fusion can be developed in multi-modal biometric system like sensor level fusion, feature level fusion, matching score level fusion and decision level fusion. The different biometric identifier used in the multimodal biometric system, their information from the individual identifier is taken together and can be fused at different levels of fusion such as fusion at sensor level, fusion at feature level, fusion at matching score level and the fusion at decision level [5].

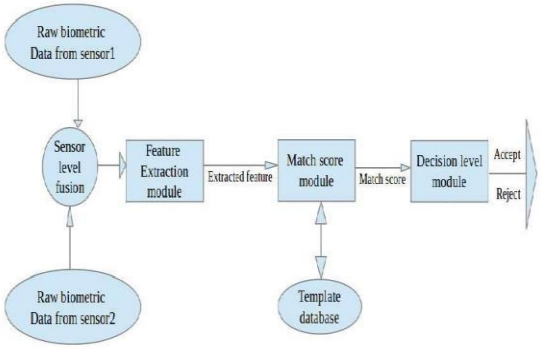

Fig-2. Sensor level fusion

Fig-2 shows the fusion at Sensor level which involves combining raw data from various sensors and this fusion can be appropriate for multi-sample and multi-sensor systems. In this method, the multiple modalities must be compatible with feature level in the raw data and must be known in advance or estimated accurately.

Feature level fusion shown in Fig- 3 refers to combining the different feature sets extracted from multiple biometric modalities into a single feature vector. If the features extracted from multiple biometrics are independent of each other and involve the same type of measurement scale, it is reasonable to concatenate the two vectors into a single new vector. The new fused feature vector will have higher dimensionality and thus increase the discriminating power in feature space. Feature reduction techniques or feature selection schemes may then be employed to extract a small number of significant features from a larger set of features. In some cases when feature sets are not compatible, concatenation is not possible, for example with incompatible fingerprint minutiae and eigen-face coefficients.

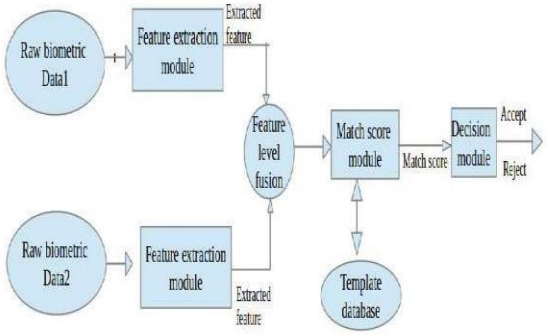

Fig-3: Feature level fusion

Matching score level fusion shown in Fig-4 refers to the combination of similarity scores provided by a matching module for each input features and template biometric feature vectors in the database. This method is also named as measurement level fusion or confidence level fusion. The matched score output generated by biometrics matchers

provide the required information about the input pattern after the raw data and the feature vector representations. Matching score fusion can be classified by the two different approaches which are based on how the match score isprocessed either by classifying the feature vector or by combining the feature vector [6]. Normalization of the match score is a significant factor to be considered in this fusion, because of the dissimilar match score generated by the multiple modalities. Several researchers have proposed various normalization techniques in the literature.

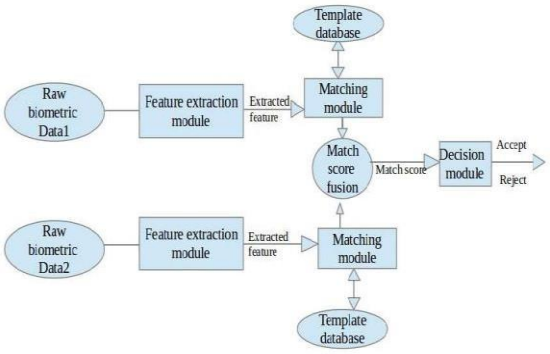

Fig-4: Matching score level fusion

In decision level fusion as shown in Fig-5, the information integration occurs when each biometric system makes an independent decision about the identity of the user or verifies the claimed identity. This fusion level is the simplest form of fusion because this uses only the final output of the individual modalities. For decision level fusion different methods like 'AND' and 'OR' rules, Majorityvoting, weighted majority voting, Bayesian decision fusion, the Dempster-Shafer Theory of Evidence and Behavior Knowledge Space are proposed in the literature.

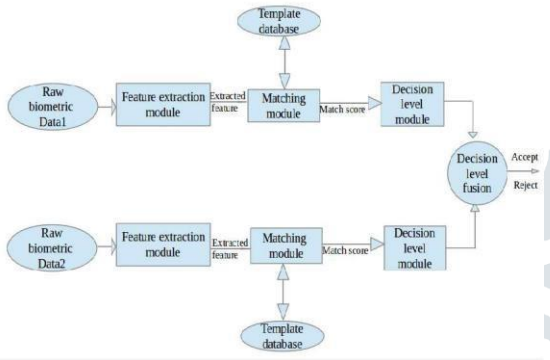

Fig-5: Decision level fusion

3. COMPARISON OF VAROIUS BIOMETRIC TECHNOLOGIES

Personal characteristics of a physical or a behavioral trait satisfying the seven properties like Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability, and Circumvention can be termed as a biometric [8]. Universality means every individual should have the biometric trait. Distinctiveness ensures that no two individuals should be identical in terms of the biometric traits. Permanence means the biometric trait of an individual should be sufficiently invariant over a period of time. Collectability (measurability) means it should be easily measurable without any inconvenience to the user. Performance relates to accuracy, speed of the technology used. Acceptability means the user acceptance without objection to the collection of the biometric and Circumvention relates to the ease with which the biometric trait can be deceived.

Brief comparisons of the different biometric identifier in terms of those seven features are shown in the Table-1.

Table-1: Comparison of various biometric technologies

Biometric identities / Character-istics	Finger-scan	Facial-scan	Iris-scan	Hand-scan	Retina-scan	Signature-scan
Universality	Moderate	More	More	Moderate	More	Less
Distinctiveness	More	Less	More	Moderate	More	Less
Permanence	More	Moderate	More	Moderate	Moderate	Less
Collectability	Moderate	More	Moderate	More	Less	More
Performance	More	Less	More	Moderate	More	Less
Acceptability	Moderate	More	Less	Moderate	Less	More
Circumvention	Moderate	More	Less	Moderate	Less	More

In the Table-1 'more' indicates that the particular biometric identifier is having very good performance, whereas poor performance in the evaluation criteria is represented by 'less' and average performance in the evaluation criteria is represented by 'moderate'. From the Table-1 it is evident that for every biometric trait have merits and demerits in each of the seven characteristics. Hence on account of the above limitations it is better to use more than one biometric identifier.

Table-2: Strength and Weakness of different Biometric Identities

Biometric-Identifier	Strengths	Weakness
Finger-scan	High level of accuracy, easy to use, flexibility	Performance can deteriorate over time, unable to enroll some percentage of users
Facial-scan	Able to operate without user cooperation	Changes in physiological characteristic reduce matching accuracy
Signature-scan	Resistant to imposters	Lead to increased error rates
Hand-scan	Reliable core technology, stable physiological characteristic.	Limited accuracy
Retina-scan	Highly accurate	Difficult to use
Iris-scan	Resistance to false matching	Difficult of use

The strength and weakness of different biometric identities [7] are also listed in the Table-2. Hence the selection of combination of biometric identity can be made easy by the perusal of the given table, which in turn helps to develop an accurate and high performance biometric identification as well as authentication.

4. RELATED WORK

The unimodal biometric system is most widely used in various applications. On account of the limitations raised by the unimodal biometric system many users resorted to multimodal biometric system in order to provide maximum level of accurate authentication[8]. Effective utilization of the advantages of multiple biometric traits is applied to enhance the performance in many aspects including accuracy, noise resistance, and universality, spoof attacks, and reduce performance degradation in huge database applications. Nowadays, new algorithms and applications of multi-modal biometrics are emerging tremendously. The most commonly used biometrics is face, that is, either as a single trait or combined with other trait as multi-modal biometrics. Face combined with other biometrics at different levels of fusion.

Besbes et al. [9] proposed a multi-modal biometric system which enhanced recognition accuracy and population coverage by using iris and fingerprint. Shahin et al. [10] proposed a high security system by fusing hand veins, hand geometry and fingerprint. Kumar and Ravikanth [11] proposed an approach for personal authentication using both finger geometry and dorsal finger knuckle surface features provides a high performance in person authentication. Chandran et al. [12] investigated and proposed a method to improve the performance by combining iris and fingerprint. Chin et al. [13] proposed a method at feature level which integrate palm print and fingerprint and a series of preprocessing steps are applied on palm and finger print to increase efficiency and for feature extraction of 2D by using Gabor filter at feature level. Sheetal Chaudhary and Rajender Nath proposed a system by integrating palmprint, fingerprint and face based on score level fusion [14].

Fan Yang and Baofeng Ma proposed a method to establish an identity by combining different modalities like fingerprint, hand geometry, palm print using feature and match score fusion [15]. Muhammad Imran Razzak et. al.
[16] proposed a multi-modal recognition system using the biometric traits like face and finger vein. This system effectively reducing the error rates like FAR (False Acceptance Rate) and improving GAR (Genuine Acceptance Rate). Table-3 shows the individual results of various works using multi-modal systems that have been implemented and deployed, using different fusion levels and different algorithms [17].

Table 3: Different interpretations of quality in biometrics from literature

Modality Fused	Level of Fusion	Interpretation
Iris and palm-print[18]	Fusion at score level fusion	Gives high accuracy
Fingerprint and face[19]	Fusion done at match- score level with weighted sum method	Excellent method giving higher performance
Voice and palm print[20]	Fusion at matching score level	Accuracy is 98% and error rates are reduced
Using combinations of various modalities.[21]	Fusion at matching score level	Higher accuracy in score level than decision level
Face, Ear and Gait[22]	Fusion at matching score level	Higher accuracy
Face & Palm-print[23]	Fusion at low level	Makes system more robust.
Finger-print , knuckle-print and palm-print[24]	Fusion at Feature level	Improved matching accuracy and searching efficiency
Face and both irises[25]	Fusion at Score level	Better performance by using Support Vector Machine.

From the literature survey it is inferred that the different fusion levels and combinations of different biometric modalities are being fused by different researchers are for accurate personal identification. Also the performance metrics used for quality-based multi-modal biometric system, fusion approaches must be carefully selected as the precision in personal identification or verification rate may be affected. All performance metrics are not made applicable for all the four fusion levels. There is a scope for better evaluation framework for biometric quality assessment metrics by correlating with the available fusion schemes. Also computational cost in the development of quality assessment approach shall be reduced.

5. CONCLUSIONS

Though there are many multi-modal biometric systems in practice for authentication of a person, selection of appropriate modal, choice of optimal fusion level and redundancy in the extracted features are still some of the shortcomings faced in the design of multi-modal biometric system that needs to be addressed. The different approaches

that are possible in multi-modal biometric systems, the suitable fusion levels, and the integration strategies that can be chosen to consolidate information were discussed here. The combination of more than one biometrics can apply to enhance the security. Performance and the advanced security level made the multi-modal biometric systems popular in these days

REFERENCES

[1] A.K.Jain, Arun A Ross, Karthik Nandakumar, Introduction to Biometrics, Foreword by James Wayman, Springer, ISBN 978- 0 – 387 –77325 – 4.

[2] K.Sasidhar, Vijaya L Kakulapati. et. al. Multimodal Biometric Systems –STUDY To Improve Accuracy And Performance, IJCSES, Vol.1, No.2, November 2010.

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

[4] A. Ross and R. Govindarajan, Feature level fusion using hand and face biometrics, Proc of SPIE Conference on Biometric Technology for Human Identification II. vol. 5779, pp. 196-204, 2005.

[5] Mini Singh Ahuja, Sumit Chabbra, A Survey of Multimodal Biometrics, International journal of Computer Science and its Applications, [ISSN 2250 – 3765].

[6] A. K. Jain, A. Ross, S. Prabhakar, An Introduction to Biometric Recognition, IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004.

[7] Samir Nanavati, Michael Thieme, Raj Nanavati, Biometrics Identity Verification in a Networked World, A Wiley Tech Brief, Wiley Computer publishing, ISBN – 0471-09945-7

[8] Soyuj Kumar Sahoo, Tarun Choubisa and S. R. Mahadeva Prasanna, Multimodal Biometric Person Authentication: A Review IETE Technical Review | Vol 29 | Issue 1 |JAN-FEB 2012

[9] Besbes, F, Trichili, H. ; Solaiman, B. Multimodal Biometric System Based on Fingerprint Identification and Iris Recognition Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference

[10] Shahin MK, Badawi AM, Rasmy ME (2008). A Multimodal Hand Vein,Hand Geometry and Fingerprint Prototype design for High Security Biometrics, CIBEC'08

[11] Kumar, A, Ravikanth C, Personal Authentication Using Finger Knuckle Surface, Information Forensics and Security, IEEE Transactions on (Volume:4 ,Issue: 1) , 2009

[12] Chandran GC, Rajesh RS, Performance Analysis of Multimodal Biometric System Authentication, Int. J. Computer. Sci. Network Security, (2009) 9: 3

[13] Chin YJ, Ong TS, Goh MKO, Hiew BY (2009). Integrating Palmprint and Fingerprint for Identity Verification, Third International Conference on Network and System Security

[14] Sheetal Chaudhary , Rajender Nath. A Multimodal Biometric Recognition System Based on Fusion of Palmprint, Fingerprint and Face. International Conference on Advances in Recent Technologies in Communication and Computing. 978-0-7695-3845-7/ 2009 IEEE

[15] Fan Yang,Baofeng Ma. A New Mixed Mode Biometrics Information Fusion on Fingerprint, Hand-geometry and Palm Print. 4th international Conference on Image and Graphics. 7695-2929-1/07 IEEE

[16] Muhammad Imran Razzak, Muhammad Khurram Khan, et.al. Multimodal Biometric Recognition Based On Fusion Of Low Resolution Face And Finger Veins, ICIC International 2011 ISSN 1349-4198, pp. 4679–4689

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

[18] Hariprasath, S, Prabakar, T.N, Multimodal biometric recognition using iris feature extraction and palmprint features, Advances in Engineering Science and Management (ICAESM), 2012 International Conference on 2012

[19] N. Gargouri Ben Ayed, A. D. Masmoudi and D. S. Masmoudi, "A New Human Identification based on Fusion Fingerprints and Faces Biometrics using LBP and GWN Descriptors," in Proc. of 8th International Multi-Conference on Systems, Signals and Devices (SSD), Sousse, pp. 1-7, 22-25 March 2011.

[20] P. K. Mahesh and M. N. S. Swamy, A Biometric Identification System based on the Fusion of Palmprint and Speech Signal, in Proc. of International Conference on Signal and Image Processing (ICSIP), Chennai, pp. 186-190, 15-17 Dec. 2010.

[21] M. Hanmandlu, A. Kumar and V. K. Madasu, Fusion of Hand Based Biometrics using Particle Swarm optimization, in Proc. Fifth International Conference on Information Technology: New Generations (ITNG), pp. 783-788, 2010.