International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4

ISSN: 2454-4248
412 – 416

A Review Of Multilevel Multibiometric Fusion System

Modi Jay
Department of Electronics and Communication
Sarvajanik College of Engineering & Technology
Surat, India
j28795@gmail.com

Neeta Chapatwala
Department of Electronics and Communication
Sarvajanik College of Engineering & Technology
Surat, India
neeta.chapatwala@scet.ac.in

***Abstract*—** Biometric systems allow automatic person recognition and authenticate based on the physical or behavioral characteristic. In recent years, researchers have paid close attention to the design of efficient multi-modal biometric systems due to their ability to withstand spoof attacks. Sometimes single biometric traits fail to extract relevant information for verifying the identity of a person. Therefore, combining multiple modalities, enhanced performance reliability could be achieved. If the security level increases then multi-level fusion techniques are used. This paper discusses the many fusion levels: algorithms, level of fusion, methods used for integrating the multiple verifiers and their applications.

Keywords- *Biometrics; unimodal system; multimodal system; fusion levels.*

*****

I. INTRODUCTION

The development of the internet has determined the apparition of some problems such as computer theft, viruses, spoofing, and so on. That affect the productivity and the industries and individual persons. Thus, security became more important and necessary. Biometric features can be classified as: physiological (fingerprint, face, iris, etc.) and behavioral (voice, gait, signature, writing style etc.)[2]. Physiological or behavioral feature may be used as a biometric verifier as long as it satisfies table 1[2]:

TABLE I. Biometric System Characteristics [16]

Characteristic	***Description***
Distinctiveness	Any two people should have discrete representation of the characteristic
Universality	Every individual should have this characteristic
Permanence	The characteristic should undergo no or very slight variance over time.
Collectability	There must be a way to convert the characteristic into data points.
Performance	Refers to standard expected rates of execution and accuracy.
Acceptability	Indicates the amount of support from people for using the system in their daily lives.
Circumvention	Refers to how easily the system can be compromised.

Biometric systems divided into two types: unimodal and multimodal system [1, 2]. Unimodal biometric systems can be overcome by including multiple sources of information for install identity [3]. There are mainly 4 fusion levels available; (1) sensor level, (2) feature level, (3) match score level and (4) decision level defined based on the type of information needed to be fused [2].

A. BIOMETRIC SYSTEM

Biometric systems divided into two types: unimodal and multimodal biometric system [1, 2]. Unimodal biometric systems depend on single evidence is used for information about the recognition and authenticate person [2]. A basically unimodal biometrics system runs in two modes: verification and identification [2]. Processes are discrete in nature. Verification, it means mapping with initially scanned factor and a previously scanned factor. Identification, it means mapping with initially scanned factor is run across a database of templates to find a match. Thus, verification is a one-to-one relationship system while identification is a one-to-many relationship system. Unimodal biometric systems tolerate several problems like noise in sensed data, Intra-class variation, Spoof attack, Non-universality and others [1].

- Non-universality: Single source it might not be useful for some user authentication. (e.g. iris)
- Noisy data: low lighting on the user biometric trait.
- Intra-class variations: sometimes the presence of wrinkles, cuts in the fingerprint can make a variation in the output and user can incorrectly communicate with the sensor.
- Spook attack: Forgery in hand signature is the best example for this.

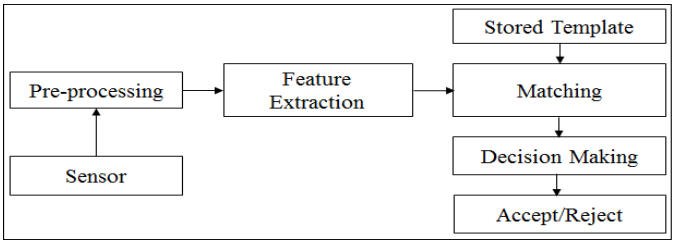

Figure 1. Block diagram of Biometric system [2]

 ISSN: 2454-4248
412 – 416

In show figure 1 basic block diagram of the biometric authentication system. Biometric system divided into 4 module: the sensor module, feature extraction module, a matching module, decision module. In sensor module sense the different biometric trait samples are captured using different sensor or cameras. In feature extraction module all individual biometric traits feature value are extracted. Matching module is used for comparing storage template and the user template and generates individual score. Final decision module is used for taking a final decision person is authenticated or not based on criteria.

II. MULTIMODAL BIOMETRICS

In unimodal system, any one trait of a person is taken and considered for authentication. But in multimodal systems utilizes more than one biometric trait of a person is taken into account. The unimodal biometric systems had the disadvantage of noise image into the data, spoofing, non-universality, interclass variation and is also not reliable. The fingerprints can easily manipulate, the signatures can be forged, and also a voice of any particular person can be imitated. Thus, the developers focused on multimodal biometrics system. In this multimodal biometric system used more than one biometric as initial stage then fused all individual biometric traits so these systems are more secure and safe as compared to the unimodal system. In this, the data from different biometrics are captured and pre-processed. Then from each of the biometrics, features are extracted and matched with the stored templates in the database [4]. Different authors have used different traits of a person to get the result. But there are also facing challenges in many sights of its execution. The developer has defined some challenges as follow: (1) multimodal systems are difficult to design [14], (2) user acceptance is quite low [15], (3) requires a higher level of investment [16] and (4) the performance trade-off [16]. Multimodal system design needs to consider various questions such as what number of factors to be used and which factors to be used. Furthermore, the proper threshold has to be initialized the factors to certify acceptable levels of False Accept Rate(FRR), False Reject Rate(FAR) and also find Genuine Accept Rate(GAR).

Application:

It is classified in three categories depending on the potential of the solution provided by the systems:

- Strong potential: physical access, criminal ID, civil ID;
- Moderate potential: network/PC access, ATM;
- Modest potential: telephony, surveillance, e-Commerce.

III. FUSION LEVELS

There are many fusion techniques used for combining the different modalities used in the multimodal system. Fusion of these modalities is an important, critical and crucial step. In multimodal biometric Fusion levels are classified into Fusion before matching module and after matching module. In this fusion classification sensor levels and feature level are used before the matching module while score level and decision levels are used after the matching module. Each fusion levels has their own advantages and disadvantages. The four fusion levels are described as below:

A. Sensor Level

Sensor level is the first type of fusion level. In this level raw data capture using different sensors or cameras. Multiple samples are taken in same biometric (e.g. Face and iris image capture from different cameras). Also, multiple sensors are used for multiple biometric (e.g. fingerprint, finger vein, and finger-knuckle-print using multiple sensors). Fusion of multiple images can take either at pixel, signal or at the feature level. Its signal to noise ratio and raw data resolution is higher [2] but security level is lower [3].

B. Feature Extraction Level

Feature extraction level is the second part of the fusion levels. In this case, fusion is operated in parameters stage. In this level, all the biometric traits are recorded and then individual traits features are extracted separately. Feature level fusion prepares to combine feature from multiple cameras, sensors, samples, traits, at different interval of time and to get the resultant feature vector. Biometric traits have rich information and fusion of features is concede to be more impressive compared to other fusion levels. Feature level information also useful about not only discards the inutility but also store discriminate information. In this case, need to care according to different sensors for different traits. This fusion approach reinforces characteristic but it needs to improve about selected parameters. It is accurate with better recognition [7] but it is more time-consuming and memory requirement.

C. Score level

Score level fusion is used after the matching module. In this level, a match score is obtained from a biometric matcher. It simply likelihood ratio between the feature vector and the stored template feature vector. For individual biometric traits match scores are combined and new match score is derived. Equality scores are generated for each biometrics and that are fused simultaneous. Score level approach discovers scores given by every individual developer. In this scores are combining using different ways such as min-max, sum-rule, and arithmetic average method. It's easy to process and also architecture is easy to implement [4]. The only drawback is need of normalization [8].

ISSN: 2454-4248
412 – 416

D. Decision level

Decision level is the final level of the fusion classification. And its level is used after the matching module. In this case, fusion operates in decision stage: each unimodal system gives their individual notification about acceptation/rejection of user asking for the global system. These binary responses are dealt with by a supervisor who has a global view of different opinions and makes the final decision. All individual traits decision is in binary form. The final decision obtained based on different system match scores depends 'AND' and 'OR' logic operator, majority vote or the theory of Dempster Shafer method [2]. It is framework is simple and clear from a mathematical point of view [3]. The common analysis of small and contains rigid information content.

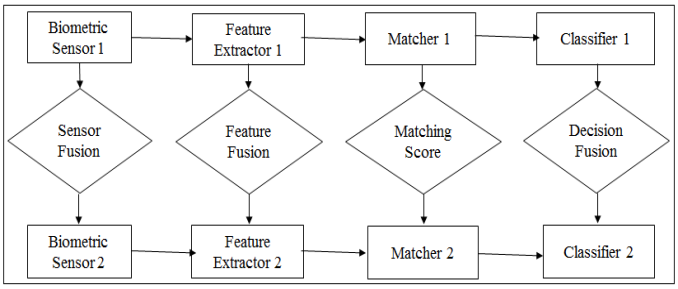

Figure 2. Block diagram of fusion levels in multimodal biometric systems [2]

IV. RELATED WORK

Lots of work has been done on multimodal biometrics system. In this Table 2 describe the different authors work done in this area. Here the developers have used different biometric traits then fused using discrete fusion algorithm and fusion levels. Hybrid fusion levels technics are also included in this table 2.

Score level fusion is attempted for three multimodal datasets like I.I.T. Delhi, PolyU, XM2VTS [4]. This all datasets including different biometric traits then implemented using available dataset and enhance the result using Frank t-norm algorithms [4]. Score level fusion method also implemented using sum rule, product rule, hamacher t-norm [7]. Similarly, decision level fusion are used Fvc2000 dataset for their implementation work using logical AND-rule [5]. Sometime many researcher used their own datasets created and then implement [9]. Hybrid score level and decision level fusion combine then take individual decision and that decision fused using fuzzy system [6]. Hybrid Feature, Score and Decision level Fusion by combining three fusion classifiers like Local Binary Pattern Histogram (LBPH), modular Principal Component Analysis (mPCA) and sub-pattern Principal Component Analysis (spPCA) with a decision rule [10].

TABLE 2. Different Biometric Traits and the Levels Used for their Fusion

References	Biometric Traits use	Used Algorithms	Dataset	Methods of Fusion
[4]	Hand geometry , Palm-print , Hand vein	Frank t-norm	IITD PolyU XM2VTS	Score level
[5]	Finger vein, Iris	AND rule	fvc2000	Decision level
[6]	LI FKP, LM FKP, RI FKP, RM FKP	t-norm, PSO, Adaptive fuzzy decision level fusion	Polytechnique uni., HongKong	Score level & adaptive decision level
[7]	Palmprint , dorsal hand veins	Sum rule, product rule, hamacher t-norm, frank t-norm	I.I.T. Delhi, Bosphorus	Feature level & score level
[8]	Finger knuckle, finger vein	FFF Optimization, Repeated line tracking, k-SVM	I.I.T. Delhi, SDUMAL-HMT	Feature level & score level
[9]	Fingerprint, Face, Speech	Minutia, Eigenface, HMM and LPC	Own dataset created	Decision Level
[10]	Face, Iris	Local Binary Pattern Histogram (LBPH), modular Principal Component Analysis (mPCA) and sub-pattern Principal Component Analysis (spPCA) as	ORL, CASIA	Hybrid Feature, Score and Decision level Fusion n by combining three fusion classifiers with a decision rule

 ISSN: 2454-4248
412 – 416

		local methods and Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) as global method		
[11]	Iris, Fingerprint	Gabor wavelets, Chain Code based feature extractor with contour following to detect minutiae	Own created	Score Level
[12]	Iris, Palmprint	Walsh, Haar, Kekre, Slant, Hartley, DCT and DST transform, Query Execution Module	Palacky University, Hong Kong University (PolyU)	Score Level, Feature Level

V. CONCLUSION

Biometric authentication will never be completely secure, but still it is one of the best security methods. Biometric system is used to increases the efficiency, accuracy, and robustness. Previously while performing fusion technique, sensor and feature levels makes the information fusion very complex, while score and decision levels gives a reliable information content. Biometric system does not satisfy performance as per requirement so system performance improvement proves to be big challenge. This article introduces various biometric methodology, also contains various fusion level with the different methods. The score level fusion Frank t-norm method ensures better performance gain compared to other methods such as sum rule, min-max, etc. While in decision level fusion And-rule is more suitable and also easy to implement, this makes the biometric system more secure if both score level and decision level techniques are fused.

ACKNOWLEDGMENT

I am too much gratefulness the support and help of my Prof. Neeta Chapatwala, Assistant professor of Electronics and Communication Department at Sarvajanik College of Engineering and Technology Surat, India in completing the research on Multilevel Multibiometric Fusion System.

REFERENCES

[1] K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, 2004.

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

[3] Qian Tao and R. Veldhuis, "Hybrid fusion for biometrics: Combining score-level and decision-level fusion," 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 1-6, 2008.

[4] Madasu Hanmandlu, Jyotsana Grover, Ankit Gureja, H.M. Gupta, Score level fusion of multimodal biometrics using triangular norms, In Pattern Recognition Letters, Volume 32, Issue 14, Pages 1843-1850, 2011.

[5] Sudhamani, M. J., M. K. Venkatesha, and K. R. Radhika. "Fusion at decision level in multimodal biometric authentication system using Iris and Finger Vein with novel feature extraction." In India Conference (INDICON), 2014 Annual IEEE, pp. 1-6, 2014.

[6] Jyotsana Grover, Madasu Hanmandlu, "Hybrid fusion of score level and adaptive fuzzy decision level fusions for the finger-knuckle-print based authentication," Applied Soft Computing, Sciencedirect Volume 31, Pages 1-13, 2015.

[7] Chaudhary, Gopal, Smriti Srivastava, and Saurabh Bhardwaj. "Multi-level fusion of palmprint and dorsal hand vein." Information Systems Design and Intelligent Applications. Springer, Volume 3, Pages 321-330, 2016.

[8] S. Veluchamy and L. R. Karlmarx, "System for multimodal biometric recognition based on finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier," in IET Biometrics, vol. 6, no. 3, pp. 232-242,2017.

[9] Anil Jain, Lin Hong, YatinKulkarni "A Multimdoal Biometric system using fingerprint, face and speech" Proc. International Conference on Audio and video based biometric person authentication (2nd)", pp. 182-187, 1999.

[10] V. Azom, A. Adewumi, and J.-R. Tapamo, ``Face and iris biometrics person identification using hybrid fusion at feature and score-level," in Proc. Pattern Recognit. Assoc. South Africa Robot. Mechatronics Int. Conf. (PRASA-RobMech),pp. 207_212, Nov. 2015.

[11] S. Sangeetha, N. Radha "A New Framework for IRIS and Fingerprint Recognition Using SVM Classification and Extreme Learning Machine Based on Score Level Fusion" Proceedings of 7th International Conference on Intelligent Systems and Control (ISCO 2013).

[12] Thepade, Sudeep D., Rupali K. Bhondave, and Ashish Mishra. "Comparing Score Level and Feature Level Fusion in Multimodal Biometric Identification Using Iris and Palmprint

ISSN: 2454-4248
412 – 416

Traits with Fractional Transformed Energy Content." In Computational Intelligence and Communication Networks (CICN), 2015 International Conference on, pp. 306-311. IEEE, 2015.

[13] Khalifa, Anouar Ben, and Najoua Essoukri Ben Amara. "Bimodal biometric verification with different fusion levels." In Systems, Signals and Devices, 2009. SSD'09. 6th International Multi-Conference on, pp. 1-6. IEEE, 2009.

[14] Oviatt, S., Cohen, P., Wu, L., Duncan, L., Suhm, B., Bers, J., Holzman, T., Winograd, T., Landay, J., and Larson, J.: 'Designing the user interface for multimodal speech and pen-based gesture applications: state-of-the-art systems and future research directions', Human-computer interaction, 15, (4), pp. 263-322, 2000.

[15] Ribaric, S., Ribaric, D., and Pavesic, N.: 'Multimodal biometric user-identification system for network-based Vision, Image and Signal Processing, 150, (6), pp. 409-416, 2003.

[16] Kumar, Kunal, and Mohammed Farik. "A review of multimodal biometric authentication systems." International Journal of Scientific & Technology Research 5, no. 12 (2016).