2nd International Conference on Science, Technology and Management
University of Delhi (DU), Conference Centre, New Delhi (India)
27 September 2015, www.conferenceworld.in, www.icstmdu.com
978-81-931039-6-8

MULTI-BIOMETRIC SYSTEMS: A SURVEY AND RESEARCH DIRECTION

Punit Chaudhary

[1]*Student, Computer Science & Engineering,*

University of Engineering and Management, Jaipur (India)

ABSTRACT

Multi-biometrics is an exciting and interesting research topic. It is used to recognizing individuals for security purposes; to increase security levels. The recent research trends toward next biometrics generation in real-time applications. Also, integration of biometrics solves some of unimodal system limitations. However, design and evaluation of such systems raises many issues and trade-offs. A state of the art survey of multi-biometrics benefits, limitations, integration strategies, and fusion levels are discussed in this paper. Finally, upon reviewing multi-biometrics approaches and techniques; some open points are suggested to be considered as a future research point of interest.

Keywords: Biometrics; Multimodal Biometric Systems; Fusion Levels; Recognition Methods; Authentication.

I. INTRODUCTION

Authentication (identifying an individual using security system) of users is an essential but, difficult accurate and secured practical authentication technology. Traditional techniques for user authentication could be categorized as :

(1) Token based techniques (i.e. key cards and smart cards) and

(2) Knowledge-based techniques include text-based and picture-based passwords (often mix of username and password).

Due to vulnerabilities in above methods (It could be easily transgressed or lost or forgotten); Traditional techniques are considered to be not reliable or secure, and are not presently sufficient in some security application zones. The primary advantage of biometrics over these methods is that it cannot be misplaced, forgotten or stolen. Also, it is very difficult to spoof biometric traits . Due to greater accuracy and higher robustness of biometric recognition.

In the most general definition, "**Biometric technologies**" is defined as an automated methods of verifying and/or recognizing the identity of a living individual based on two categories :

(1) ***Physiological biometrics*** include (Facial, hand and hand vein infrared thermogram, Odor, Ear, Hand and finger geometry, Fingerprint, Face, Retina, Iris, Palm print, Voice, and DNA) , and

978-81-931039-6-8

(2) ***Behavioral biometrics*** like (Gait, Keystroke, Signature) which measure the human actions. Also, human electrocardiogram (ECG) signal is considered one of Biometric features used in individual recognition and authentication.

Depending on the application context, biometric systems may operate in two modes: verification mode and identification mode. Through *verification mode*, the system verifies the identity by comparing the enrolled biometric trait by a stored biometric template in the system (1:1). This mode is used for positive recognition, and it aims to prevent the multiple individuals from using the same identity. In the *identification mode*, the enrolled sample is then compared with existing templates in a – central – database (1: M) . A database search is crucial and needed. The identification mode is critical in negative recognition applications, which aims to prevent a single user from using multiple identities. Negative identification is also known as screening. Obviously, verification is less computationally expensive and more robust compared with identification. On the other hand, the latter is more convenient and less obtrusive.

Multi-biometric systems distinguished over traditional uni-biometric systems as it addresses the issue of non-universality and noisy data. Multi-biometric systems can facilitate the indexing of large-scale biometric databases. Also, it becomes not easy for an impostor to spoof all the biometric traits of an authorized enrolled person

The rest of this paper is organized sequentially as follow: Section II will overview the biometrics characteristics followed by section III to discuss the unimodal biometrics' drawbacks. Next, Section IV will discuss the multi-biometrics advantages and limitations, categories, and integration scenarios. After that, section V is to discuss biometrics quality performance and metrics. different fusion levels before and after matching, depended on theses metrics, will be discussed in section VI. Benefits and drawbacks for each approach will be declared with evidence of previous research. Moreover, section VII will show the design issues and trade-offs related to any multi-biometric recognition system. Finally, Section VIII suggests some open points for further investigation and research.

II. BIOMETRICS OVERVIEW

A biometric system to be practical and reliable should meet the specified requirements/characteristics *Universality (availability),* each person should have the characteristic. Availability is measured by the "failure to enroll" rate. *Distinctiveness:* It declares that any two persons should sufficiently have different characteristic. It is measured by the False Match Rate (FMR), also known as "Type (II) error". *Permanence (robustness),* the characteristic should be stable (with respect to the matching features) over a period of time. Which means the stability over age. Robustness is measured by the False Non-Match Rate (FNMR), also known as "Type (I) error" . *Collectability (accessible),* the characteristic can be measured quantitatively, and easy to image using electronic sensors

Which biometric characteristic is best? Each biometric feature has its own strengths and weaknesses and the choice typically depends on the application. Accordingly, each one could be used in authentication and/or identification applications. Predicting the "false acceptance" and "false rejection" rates, system throughput, user acceptance, and cost savings for operational systems from test data, is a surprisingly difficult task.

Biometric Characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial Thermogram	H	H	L	H	M	H	L
Hand Vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand Geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H

Table I. Comparison of biometric characteristics .

III. UNIMODAL BIOMETRICS LIMITATIONS

Any single modal biometric has limitations. For example, iris recognition suffers from some problems like camera distance, eyelids and eyelashes occlusion, lenses, and reflections. Face changes overages and unstable, and twins may have similar face features. Also, fake faces from mobiles as example, and masks used to attack the system . Fingerprint may have some cuts, burns, and small injuries temporary or permanent . Moreover, fake fingers made from gelatin and/or silicon have ability to attack the fingerprint-based recognition system . Cold leads to voice problems and a tape recordings may be used to hack the system. The fingerprint of DNA needs several hours to be obtained. Besides, DNA includes sensitive information related to genetic of individuals and the test is quite expensive to perform . Hand geometry is not distinctive enough to be applied to a large population. Thus, it is not suitable for purpose of identification. Gait is sensitive to body weight and not stable; it is not used for large population and not reliable enough . The unimodal biometric rely on the evident single source of information for authentication (e.g., single fingerprint, face) . Single modal biometric traits may not achieve the desired performance requirements; as they have plenty of error rates. These systems have to contend with a variety of problems such as:

 Noise in sensed data; defective or improperly maintained sensors (i.e. accumulation of dirt on a fingerprint sensor) could produce deformed and noisy data. For instance, a cold has effects on the voice, wearing glasses alters iris recognition performance, variations in light or illumination in face sensed …etc.

 Distinctiveness (Intra-class variations and Inter-class similarities); Biometric trait is expected to be varied significantly across two persons. Intra-class variations occur when a user interacts with the sensor incorrectly (e.g., incorrect facial pose). Also, characteristics of the individuals are formed with the large inter-class similarity (overlap) in the feature sets of multiple users.

 Non-universality; means the non-ability of the biometric to acquire meaningful biometric data from a group of users due to the poor quality and consistency of the acquired biometric data as a result to error or a fault in the sensor. For example, many of population (about 4%) may have scars or cuts in fingerprints. As a result, a fingerprint biometric system, may extract incorrect minutiae features from them. Also, user-sensor interaction is adjustment incorrectly. Of course, this may give undesired matching result.

 Spoof attacks; a fake traits or biometrics of the authorized user are enrolled and saved in the template database; an imposter person may attempt to spoof these sensed data when the traits are used. As in , artificial

fingers/fingerprint can be used to spoof the verification system. This type of attack is common when using behavioral characteristics.

IV. MULTI-BIOMETRICS AS A SOLUTION

Biometric fusion has a history of more than 30 years . More than one biometric combined to investigate high performance multi-biometric recognition system. Multi-biometrics has addressed some issues related to unimodal this make it has some benefits over unimodal biometrics such as recognition accuracy, privacy, and biometric data enrollment.

Recognition accuracy*:* Its accuracy is better as compared to the unimodal biometric system . The multi-biometric system is expected to be more accuracy and reliability due to the multiple, biometric traits independency, and difficult to forge all of them. As the combination of each of the biometric identifiers offers some additional evidence about the authenticity of an identity claim, one can have more confidence in the result. For example, two persons may have the similar signature patterns, in which case, the signature verification system will produce large FAR for that system. Addition of face recognition system with the signature verification system may solve the problem and reduce the FAR. Experiments have shown that the accuracy of multimodality can reach near 100% in identification.

Biometric data enrollment: Multimodal biometric systems can address the problem of non-universality. In case of unavailability or poor quality of a particular biometric data, other biometric identifier of the multimodal biometric system can be used to capture data. For example, a face biometric identifier can be used in a multimodal system (involves fingerprint of general labors with lots of scars in the hand).

4.1 Multimodal Categories

Multi-biometric systems have two basic categories: synchronous and asynchronous. In synchronous, two or more biometrics combined within a single authorization process. On the other hand, asynchronous system uses two biometric technologies in sequence (one after the other) . Multimodal biometric systems can operate in three different modes:

 Serial Mode (cascade mode) – each modality is examined before the next modality is investigated. The overall recognition duration can be decreased, as the total number of possible identities - before using the next modality - could be reduced

 Parallel Mode – sensed/captured data from multiple modalities are used in concurrent way to perform recognition. Then the results are combined to make final decision.

 Hierarchical Mode – individual classifiers are combined in a hierarchy -tree like- structure. This mode is preferred when a large number of classifiers are expected. B. Multi-Biometrics Integration Scenarios

Recognition systems using multiple biometric traits are designed to operate in one of the integration scenarios as below:

1**) Multi-sensor systems**

The information of the same biometric obtained from different sensors are combined for all. For example, complementary information corresponding to fingerprints can be acquired using different types of sensors (like optical and capacitive sensors). Information obtained are then integrated using sensor level fusion technique.

2**) Multi-modal systems**

More than one biometric trait is used for user identification. For example, the information obtained using face and voice features or other can be integrated to establish the identity of the user. This can be more costly; because it requires multiple sensors with each sensor sensing different biometric characteristics. But, the improvement in performance is substantial.

3) **Multi-instance systems**

Multiple instances of a single biometric trait are captured. For example, images of the left and right irises can be used for iris recognition. Also, fingerprints from two or more fingers of a person may be combined or one image each of the same person may be combined. If a single senor is used to acquire these images in a sequential manner, the system can be made really cost effective, as it does not require multiple sensors. Moreover, it does not incorporate additional feature extraction and matching modules.

4) **Multi-sample systems**

Multiple samples of a same biometric trait are used for the enrollment and recognition. For example, along with the frontal face, the left and right profiles are also captured. Multiple impression of the same finger, and multiple samples of a voice can be combined. Multiple samples may overcome poor performance. But, it requires multiple copies of sensors, or the user may wait a longer period of time to be sensed or a combination of both.

5) **Multi-algorithm systems**

Multiple different approaches to feature extraction and matching algorithms are applied to a single biometric trait. Final decision obtained if any of the matching fusion technique can be applied on the results obtained using different matching algorithms. These systems are more economical as no extra device is required to capture the data. But, these are more complex because of application of different algorithms.

6) **Hybrid systems**

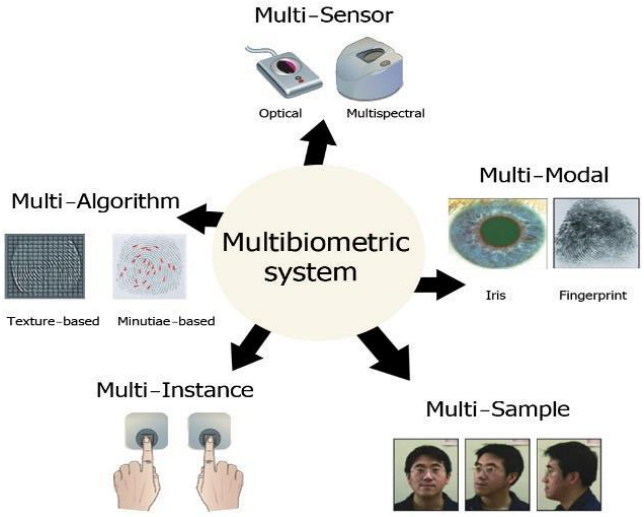
It is a system which integrates more than one of the above mentioned multi-biometric systems. For example, two face recognition algorithms can be combined with two fingerprint recognition algorithms. Such a system will be multi-modal and multi-algorithmic system. Moreover, if multiple sensors are used to obtain these images, then it will be multi-sensory, and if multiple instance of the finger is used, it will be multi-instance system also.

Both of hybrid systems and multi-modal systems can be desired by using multiple modalities. However, the rest can be achieved with the only help of even single modality.

2.2 Limitation of Multi-biometrics System

Some lacks are still found such as noise in the biometrics like scratches in the fingerprint and lens mark in iris, this will lead to increase the (FRR). Moreover, the accuracy of the multi-biometric enrollment and multi-biometric identification need to be improved. In multi-biometrics, failure of one biometrics will make the whole system to fail. In addition, multimodal biometric systems, may be more expensive and complicated due to the requirement of additional hardware and matching algorithms, and there is a greater demand for computational poser and storage. Recent research has revealed that multi-biometric systems can increase the security level as a means to enhance network security to people who are encouraged to use biometric systems in this field. However, it need more efforts and research to face some types of attacks such as: spoof attack, replay attack,

substitution attack, Trojan horse attack, transmission attack, template database attack, and decision attack. Next section will list the performance metrics that distinguish between the multi-biometrics techniques.



The different types of multi-biometric system

V. QUALITY PERFORMANCE AND METRICS

Various quality performance metrics measure the performance of any biometric authentication techniques. It helps comparing systems and motivating the progress . The most common performance metrics of biometric systems are described below :

False Accept Rate (FAR) or (False Match Rate (FMR)): Mistaking the biometric measurements from two different persons to appear as if they are from the same person due to large inter-user similarity. It measures the percent of invalid matches. The FAR is defined as in (1):

(1) **FAR %=(TFaccept/TFsubmit) *100**.

Where, *TFaccept* is total number of forgeries accepted and *TFsubmit* is total number of forgeries submitted to the system test. In a good authentication system this rate must be low.

False Reject Rate (FRR) or (False Non-Match Rate (FNMR))*:* Mistaking two biometric measurements from the same person to appear that they are from two different persons due to large intra-class variations. It measures the percent of valid inputs being rejected. The FRR is defined as in (2):

(2)FRR%=(TGreject/TGsubmit)*100.

Where *TGreject* is the total number of genuine test pattern rejected, and *TGsubmit* is total number of genuine test submitted to the system. This must be low to achieve good Performance. The average of the FRR and FAR is called the Average Error Rate (AER).Genuine Acceptance Rate (GAR) sometimes used, which is the percentage of the likelihood that a genuine individual is recognized as a match. GAR of a valid user can be obtained by equation (3)

3) GAR%=1-FAR %.

Equal Error Rate (EER): For a simple empirical measure, it is used to summarize the performance of a biometric system that is defined at the point where False Reject Rate (FRR) and False Accept Rate (FAR) are equal . System with the lower EER, is the more accurate and precise . The EER is also called the type (III) error.

Failure to Capture (FTC): denotes the percentage of times the biometric device fails to automatically capture a biometric characteristic when presented correctly. This usually happens when system deals with a signal of insufficient quality.

Failure to Enroll Rate (FER or FTE): denotes the percentage of times users cannot enroll in the recognition system. Data input is considered invalid due to poor quality.

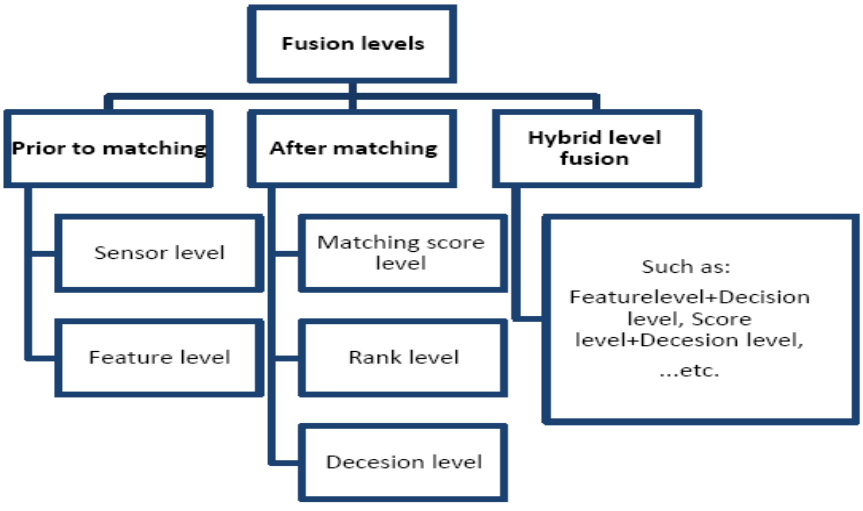
Template Capacity: It is the maximum number of sets of data which can be input in to the system .

Usually, the above performance metrics are expressed using different graphs such as Receiver Operating Characteristic (ROC), Score Histogram (SH), and Cumulative Match Characteristic (CMC) [9]. Receiver Operating Characteristic (ROC) curve: There is a trade-off between FAR and FRR in every biometric system. In fact, both of them are functions of the system threshold (t); if it is declined to make the system achieves higher tolerance to input variations and noise, then FAR increases. On the other hand, if it is raised to make the system more secure, then FRR increases accordingly . The ROC plot is obtained by graphing the values of FAR against FRR, at various operating points (thresholds) on a linear or logarithmic or semi-logarithmic curve. Detection Error Trade off (DET) is a common variation, which is obtained via normal deviate scales on both axes .

VI. LEVELS OF FUSION IN MULTIMODAL BIOMETRICS

Multimodal biometric fusion combines the distinguished aspect from different biometric features to support the advantages and reduce the drawbacks of the individual aspects . The fundamental issue of information fusion is to determine the type of information that should be fused and the selection of method for fusion . The goal of fusion is to devise an appropriate function that can optimally combines the information rendered by the biometric subsystems.

In multimodal biometrics, the fusion scheme can be classified as sensor level, feature level, match score level, rank level, and decision level [4] as shown in figure (2). The process can be subdivided into two main categories: prior-to-matching fusion and after matching fusion [33]. Figure (3) [9], shows these fusion levels possibilities at each module. The hybrid one is mixing two or more from these level fusions



Categories of different fusion levels

6.1 Prior to Matching Fusion

Fusion in this category integrates evidences before matching. This can be classified into two different categories as follows:

1**) Sensor level fusion**

Principles- A new biometric data generated by merging the raw data obtained from multiple sources. Then, trait can be extracted. A single sensor or different compatible sensors like fingerprint, iris scanner, etc., represents the samples of the single biometric trait sensed. This level of fusion is also known as data level fusion or image level fusion (for image based biometrics).

Discussion- Sensor level fusion can benefit multi-sample systems which capture multiple snapshots of the same biometric . Compared to other fusion types, it has a lot of information. It is projected to improve the recognition accuracy. Sensor fusion addresses the problem of noise in sensed data because improper maintenance of sensors . However, raw images are either not available or the information available from the different sources is not compatible.

2) Feature level fusion

Principles- The correlated feature sets extracted from different biometric channels (modalities) can be fused by using specific fusion algorithm forming a composite feature set, passed to the matching module. This done after normalization, transformation and reduction schemes The goal of feature normalization is to modify the location (mean) and the scale (variance) of the feature value via a transform function in order to map them into a common domain. (e. g. Min-max normalization, Median normalization...etc.) . Transformation or Feature Selection is algorithm use to reduce the dimensionality of the feature set. (e. g. Sequential forward selection, Sequential backward selection, Principal Component Analysis (PCA), etc.) .

6.2 After Matching Fusion

Prior to matching fusions sometime don't involve multiple modalities. Also, the fusion of data set is more complex, and it is not good to ignore any data. After matching fusion integrates evidences of after matching module. This can be classified into three different categories:

1**) Matching score level fusion**

Principles- Individually, Extracted feature vectors (generated separately for each modality) are compared with the templates enrolled in the database for each biometric trait in order to generate the match scores [. Output set of match scores are fused to create composite matching score (single scalar score). This fusion technique is also known as confidence level or measurement level fusion.

The matching scores cannot be used or combined directly; because these scores are from different modalities and based on different scaling methods. Score normalization are required, by converting the scores into common similar domain or scale.

2) **Rank level fusion**

Principles- In this new fusion approach, each classifier associates a rank with each enrolled trait to the system (a higher rank indicating a good match). It consolidates multiple unimodal biometric matcher outputs, and determining a new rank that would help in estimating the final decision. Generally, the rank level fusion is adopted for the identification rather than verification. Here, the working procedures are: first, generate a rank of

identities sorted with all modalities. Second, by help of any method of fusion, the ranking for each individual available for different modalities fused. Finally, the identity with the lowest score is the correct identified one.

3**) Decision level fusion**

Principles- The final decision - in multimodal biometric systems - is formed from obtaining individually separate decision of different biometric modalities using different techniques include behavior knowledge space, majority voting, , weighted voting, AND rule, and OR rule. Decision level fusion is also named abstract level fusion; because it is used when there is access to only decisions from individual.

6.3 Hybrid Level Fusion

Tri-level fusion scenarios (different fusion in different levels of the system) can be investigated to make the system faster and significantly reduce the error rate. The fusion of level increased the performance. In 2007, C. Lupu et al. [65] fused fingerprint, voice and iris. Next year 2008, S. Asha et al. [7] combined fingerprint with mouse dynamics. In 2011, Parallel Feature Extraction with the help of SIFT, SIMD, and HMA techniques was used by Anukul Chandra Panda et al.[66] to fuse multiple iris. Next in 2013, Gandhimathi Amirthalingam, and Radhamani. G. [5] used fuzzy vault to implement multimodal system based on Face and ear traits.

VII. DESIGN AND IMPLEMENTATION OF MULTI-BIOMETRICS RECOGNITION TRADE-OFFS

Generally, any biometric recognition system architecture is related to software-based techniques and hardware-based techniques. The obstacles here is to satisfy all challenges requirement such as: user friendly, fast (i.e. the system must identify individuals in real time), low cost, high performance, less intrusive, fraud prevent and high fake detection rate . Briefly, design issues in multi-biometrics include :

- Choosing the biometric modalities and number of traits (defining and estimation of each modality reliability is still open research issue).
- Choosing the best samples for a particular biometric.
- Fusion level and fusion methodology.
- Fusion scenario and common strategy.
- Learning weights of individual biometric for users
- Cost versus performance and accuracy versus reliability trade-offs.
- Verification and/or identification system for application.
- Expert features selection difficulties.

In order to optimize the multi-biometric recognition benefits, the issues of system design firstly should be understood better; so the more effective design methodology and system architecture can be developed. For instance, to decide whether combining multiple biometrics or combining multiple samples of the same trait is better, to achieve economic system. In addition, privacy issues should be considered, and compromising between accuracy and coverage.

VIII. MULTI-BIOMETRICS - DISCUSSION AND RESEARCH DIRECTION

Several research directions arise from the work proposed in this topic. There are some issues and open questions still need some efforts. We suggest the following tasks and discussion as future work that would significantly improve the security or other performance metrics of multi-biometric systems. Below is a hot point in this field still under research.

8.1 Multi-data Database / Real dataset

A dataset is not a research result in itself but, a well-designed one can facilitate the research. Many researchers are putting efforts in fusing multimodal biometrics. There are different approaches for biometric fusion. One approach is to use heterogeneous database (i.e. one biometric trait from one database and other trait from another database). But this approach is not reflecting the performance of multimodal users. The other approach, is to use homologous database. It means different biometrics from the same person. Only few multimodal databases are available publicly. BANCA and XM2VTS includes face and voice biometrics. BIOMET which includes face, voice, fingerprint, hand and signature. BIOSEC includes fingerprint, ace, iris and voice. SDUMLAHMT is a homologous database which includes face images from 7 angles, finger print images, gait videos, iris images. But these databases have some limitations. Homologous multi-biometrics dataset should be complete (contains all the biometrics for large population) for future research testing and multi-biometric system evaluation.

8.2 Soft Multi-biometrics

Using multiple biometric identifiers in a single system will increase the identification or verification times and hence, cause more inconvenience to the users and increase the overall cost of the system. Thus, soft biometric is introduced in 2004 to obtain the same recognition performance without causing any additional inconveniences to the users by incorporating it (soft biometric identifiers) to the primary multimodal systems. Soft biometric identifiers include gender, ethnicity, height, weight, eye color, skin color, hair color, etc. Two key challenges need to be addressed to incorporate soft biometrics into the traditional multimodal biometric framework. The first challenge, is the automatic and reliable extraction of the soft biometric information without causing inconveniences to the users, and the second challenge, is to combine optimally this information with the primary biometric identifier to achieve the best recognition performance.

8.3 Multi-Algorithms Fusion Methods

Such systems seek to improve the speed, reliability, and accuracy of a biometric system. A variety of fusion methods and approaches have been described in . We suggest new methods and modified algorithms to build and test the multi-biometric system. In, a new robust linear programming method proposed theoretically to fuse multi-biometrics by combining the modalities optimally. The robustness and accuracy have to be practically measured.

Another suggestion is to adopt K-means to cluster data and other advanced clustering methods to offer the best solutions especially when data are influenced by kinds of noise. The new modified feature descriptor Scale Invariant Feature Transform (F-SIFT) algorithm, Incremental Granular Relevance Vector Machine (iGRVM),

Particle Swarm Optimization (PSO), and Hidden Markov Models (HMM) have not been used practically yet as new fusion techniques

8.4 Embedded Hybrid Recognition System

From the above survey, some points noticed as a few research used sensor level fusion; we suggest fusion between physiological and behavioral traits such (iris, fingerprint, face…etc.) with (gait, signature). Fusion between the offline and online signature acts more authentication for critical documents signing. At the same time, the multi-fusion also can be used with multi classifiers and using different fusion levels. The multi-biometric system then may be more complex. This can be resolved by using the parallelism in feature extraction and identification phases, or execution by using H/W devices like Arduino or FPGA or parallel processing elements. In most cases, multi-biometric based security systems need to operate actively in the real-time public network and authentication environment.

IX. CONCLUSION

Multi-biometrics topic has attracted more interest in recent research. It is used to identify individuals based on their physiological and behavioral characteristics for security purposes. Overview of biometrics showed that it is impossible to find the best single biometric suitable for all applications, populations, technologies and administration policies. Also, integration of biometric modalities can solve unimodal system limitation to achieve higher performance.

Benefits and limitations of multi-biometrics discussed as we introduced it as a solution. In this paper, a state of the art survey of integration strategies, and fusion levels prior to matching and after matching are discussed with advantages and disadvantages of each type. However, Design and evaluate the multi-biometric systems raises many issues and trends. Finally, some open points suggested to be considered as a future research and enhance applications.

REFERENCES

[1] . S. Asha and C. Chellappan, "Authentication of E-Learners Using Multimodal Biometric Technology," presented at the Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on, Islamabad, 2008 .

[2]. M. L. Gavrilova and M. M. Monwar, "Current Trends in Multimodal Biometric System Rank Level Fusion," in Pattern Recognition, Machine Intelligence and Biometrics, ed: Springer, 2011.

[3] A. M. Siddiqui, R. Telgad, and P. D. Deshmukh, "Multimodal Biometric Systems: Study to Improve Accuracy and Performance," International Journal of Current Engineering and Technology .

[4] K. Delac and M. Grgic, "A Survey of Biometric Recognition Methods," in Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium, ELMAR-2004, Zadar, Croatia, 2004, pp. 184-193.

[5] M. S. Ahuja and S. Chabbra, "A Survey of Multimodal Biometrics," International Journal of Computer Science and its Applications, vol. 1, no. pp. 157-160, 2011.

[6] A. A. Ross, A. K. Jain, and K. Nandakumar, "Information Fusion in Biometrics," in Handbook of Multibiometrics, ed, 2006 .

[7] N. Geethanjali and K. Thamaraiselvi, "Feature Level Fusion of Multimodal Biometrics and Two Tier Security in ATM System," International Journal of Computer Applications, vol. 70, no. 14, pp. 17-23, 2013.

[8] D. Satyarthi, Y. P. S. Maravi, P. Sharma, and R. K. Gupta, "Comparative Study of Offline Signature Verification Techniques," International Journal of Advancements in Research & Technology, vol. 2, no. 2, pp. 1-6, 2013.

[9] G. Sathish, S. V. Saravanan, S. Narmadha, and S. U. Maheswari, "Multi-Algorithmic Iris Recognition," International Journal of Computer Applications, vol. 38, no. 11, pp. 13-21, 2012.

[10] K. Elumalai and M. Kannan, "Multimodal Authentication for High End Security," International Journal on Computer Science and Engineering, vol. 3, no. 2, pp. 687-692, 2011.