Indian Journal of Science and Technology, *Vol 8(32), DOI: 10.17485/ijst/2015/v8i32/91488, November 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Survey of Multi-Biometrics and Fusion Levels

Khalaf Emad Taha and Sulaiman Norrozila

University Malaysia Pahang, Kuantan - 26300, Malaysia;
pcc13010@stdmail.ump.edu.my, norrozila@ump.edu.my

Abstract

The verification of the identities of individuals is becoming an increasingly important requirement in a variety of applications based on specific physiological or behavioral features. Most biometric systems that are currently in operation usually utilize a single biometric trait which called Uni-biometric systems. Other systems are called Mutli-biometrics systems which are utilize, or are capable of utilizing, more than one physiological or behavioral characteristic for enrolment either in verification or identification mode. It is generally believed that by integrating various biometric traits into one single unit, the limitations of uni-biomatic systems can be alleviated. Given that several biometric sources usually compensate for the weaknesses of single biometric fusion techniques has dealt primarily with the fusion at the score matching level.

Keywords: Biometric System, Fusion, Multi-Biometric, Uni-Biometric

1. Introduction

A biometric considered as a pattern recognition problem which is uses to identify authorized person based on specific physiological or behavioral features[1]. Industry has engaged with academic and research institutions in the goal to standardized biometric formats and traits[2]. Most of the current biometric systems employ a single biometric trait this kind of biometric system called unimodel, while the system that employs more than one trait is called multi-biometrics[3]. Examples of behavioral characteristics are gait, signature, and voice. Physical characteristics include: fingerprint, Palmprint, iris, DNA, hand geometry, ear, retina and face[4]. After the pre-processing of the biometric sample like dental, fingerprint, face, iris etc, an algorithm extracts the unique features derived from the biometric sample and converts it into template in the database. A number of anatomical and behavioral body traits can be used for biometric recognition (see Figure 1). It can be divide into two type as below[5,6]:

- Physiological attributes: These attributes identify the person on the basis of anatomical traits such as face, fingerprint, iris, palmprint, DNA, hand geometry and ear shape. Biological features are strong durable "link" between the person and identity and these qualities cannot be easily lost, forgotten, shared, or forged. Biological systems require the user to be present at the time authentication and it can also be used to deter users from making false claims disclaimer. For these reasons, adopting of biometric systems is increased in a number of government and civilian applications.
- Behavioral attributes: based on the analysis of the behavior of an individual while he is performing a specific task, example gait, signature, keystroke dynamics and voice. the vocal tract shape affects to some characteristics of human voice such as pitch, tenor and nasality, while characteristics such as word or phoneme pronunciation are learned[6].

Other characteristics can provide some information about the identity of a person such as gender, ethnicity, age, eye color, skin color, scars and tattoos, these characteristics called "Ancillary characteristics" also called "soft biometric characteristic" because they do

* *Author for correspondence*

not provide sufficient evidence to precisely determine the identity[7].

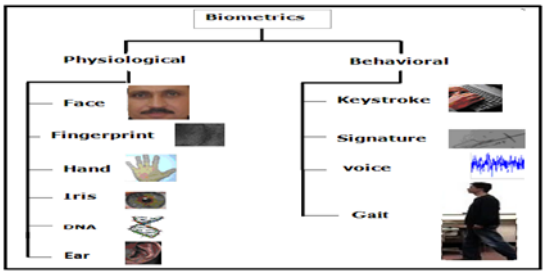

Figure 1. Biometrics System Type.

2. Biometric History

In many cases throughout history of the biometric is the recognition of palm prints and fingerprints, the oldest method of biometric identification with their history until at least 6000 BC the first recorded use of fingerprints the law was referred by the ancient Assyrians, Babylonians, Japanese and Chinese for signing certificates. In ancient Babylon, fingerprints were used on clay tablets for business. The survey of handprints was the only way to distinguish an illiterate another because they could not write their own name. As a result, the impressions of the hands of those who could not receive a name, but got the best of a color hand on the back of an acceptable form of identification contract[8]. The English began with fingerprints in 1858 William Herschel decided his handprint on the back of a contract in order to scare the people of the facsimile of the signature to impress. Finally, it has become customary to require handprints, and after a while, only the pressure of the right index and middle fingers. He believed that the contract as if it will be mandatory just signed. As his collection of fingerprints grew up, he began to discover that none of inked impressions were the same. He realized that fingerprints are unique to the individual and to the same everywhere, individual life[9] stayed. In the 1870s, an anthropologist and the receptionist Police in Paris, France, named Alphonse Bertillon tried the problem on the basis of his system to the assertion that the measurement of adult bone does not resolve to change after the age of twenty year old. The method was to identify people by. Measurements that the height of a person, arm length and the width of the head, the length of the individual fingers, the length of the forearm, etc. calipers He developed a method of multiple measurements of the body, which is named after him and is called Bertillon Ages. His system has been used worldwide by police, but it quickly disappeared when it was discovered that some people share the same measures in parts of the body[10]. In the late 19th century, Francis Goldstein wrote a detailed study of fingerprints in which he presented a new classification system with prints of all ten fingers. After Galton calculations were 1 in 64 billion chance of two distinct impressions, even. Galton identified characteristics of fingerprints which are identified (minutiae) which[11] are essentially the same today, still in use. This classification of minutiae is often referred to as Galton details. Also in the 1890s, police in Bengal, India, under British policeman Edward Richard Henry started with fingerprints to identify criminals. As an Assistant Commissioner of the Metropolitan Police, Henry founded the first fingerprint files of the UK in London in 1901[12]. In 1905, the US Army began using fingerprints. Two years later, the US Navy began using fingerprints and Marine Corps joined the following year. In the next 25 years, an increasing number of law enforcement personal identity[8] The use of fingerprints as a means of joining. Frank Burch in 1936 the concept of using the iris pattern can be proposed as a method, a person[13] can be seen. Some of the earliest work on face recognition system can be panorama of the 1960s at a company called Research in Palo Alto, California predicted. This type of research is then referred to as artificial intelligence, by Woody Bledsoe, was a pioneer in the field of automated reasoning. His method called "human face recognition and machine" using a technique known as feature extraction. In the late 1960s, Robert P. Miller started patents, United States Patent Office for a device that measures the properties and characteristics unique features for comparison and identification (ID) study[10] was adopted. Goldstein 1970, Harmon and Lesk used 21 specific subjective markers such as hair color and lip thickness to automate the recognition, it can be manually calculate this measure[11]. In 1974 was a year of break through for automated biometric data, such as hand geometry at the University of Georgia campus food service areas to get started. Both Stanford Research Institute at the National Physical Laboratory in the United States and Britain signed detection systems[12] started. In 1985, one of the first scanning systems of the retina to secure access to a Department of Defense facility at the Naval Postgraduate School in use. In the mid-1980s, the State of California to finger printing as a requirement for all license applications. The first

organization of the biometric industry, International Biometric Association (IBA), founded in 1986-1987. Iris recognition technology in the 1980s by John Daugman was developed at the University of Cambridge. Other new technologies in the production of commercially available include arcograph face and the face recognition system[12]. 1987 River develop an algorithm obtained a patent for the human iris identification approach[13] and in the same year was the recognition Sok Gek solution visual form of objects classified by hierarchical syntax extraction in which objects and then reduce the binary thin line image and distinguish chief Moving from a wide range of where moving objects in a family environment[14]. In 1998, the International Biometric Industry Association (IBIA) in Washington, DC was founded to advance as a professional association of non-profit industry, common global interests of the biometric industry. The National Biometric Security Project (NBSP) was established in 2001 in response to the events of September 11, 2001, and the need to accelerate the development and deployment of biometric technologies[15]. In April 2002 Staff Paper Technology palmprint and IAFIS skills to palmprint identification services (IS) Advisory Council Subcommittee CJIS policy (PDB) has been submitted. The Joint Working Group then moved "for strong support for planning, costs and the development of an integrated latent print function with the palm of the CJIS Division of the FBI. This should be seen as an attempt on the same parallel lines passing IAFIS developed and integrated into the CJIS technical skills" as a result of these and other supporting evolving business needs of the prosecution, said the initiative Next Generation FBI IAFIS (NGI). An essential part of the NCI initiative is the development of the needs and the use of an integrated national PalmPrint service. Show law enforcement authorities at least 30 percent of prints lifted the knife handles crime scenes, gun grips, steering wheels and windows - are palm, not your fingers. For this reason, detection and scanning latent palm become an area of increasing interest in the application of the law. National service PalmPrint is based on improving the ability of law enforcement to provide a complete set of biometric data[16] exchange developed.

3. Related Works

Many research findings have been reported in the area of information fusion to multibiometric. Duca et al.[17] propose an algorithm based on Bayes theory in order to fuse individual experts opinions. The modalities used in their system are face and speech for each person involved. Experimental results show that fusion improves accuracy over the uni-biometric systems by reaching success rates of 99.5%. Hong and Jain[18] utilize the benefit of fast recognition in Face systems and a drawback of reliability by using fusion to utilize the reliability of fingerprint recognition and performance of face retrieval. The integrated system overcomes the limitation of face recognition and the fingerprint verification process. Their systems works very well in terms of response time and it meets the accuracy requirements. However, Chatzis et al.[19] used information fusion of personal authentication modality. At the decision level, fusion takes place using fuzzy k-means and fuzzy vector quantization algorithm and median radial basis function. Their simulation results shows that median radial basis function outperform other fuzzy function for biometric recognition especially with two modalities A multi-view face and gait recognition system was proposed by Shakhnarovich et al.[20] using an image-based visual hull. Image sequences captured from multiple cameras are passed to an unmodified face or gait recognition algorithm, the proposed algorithm shows an integrated face and gait recognition provides improved performance over a single modality of one of them alone. Feature level fusion has been applied on several samples as presented in[21]. Ross and Govindarajan[22] discuss fusion at the feature level in three different scenarios and the results are encouraging. They use hand and face biometric as a case study. Fusion of gait and face for human identification has been studied by Kale et al.[23]. They implement a decision level fusion in order to combine expert's decisions from multiple modalities. Gait recognition was used as a filter to reduce the sample space for identification for face recognition. They also implement a score level fusion for both modalities as another approach of information fusion. Face and speech have been studied by[24-26] and the results indicate that performance improvement can be achieved only if the soft biometric traits are complementary to the primary biometric traits. Face, fingerprint and hand geometry also have been experimented by Ross[2]. Multi-sensor fusion has been studied for fingerprint verification by Marcialis and Roli[27]. In their work, they implement a sensor level fusion using optical and capacitive sensors. The result outperforms single sensor fingerprint recognition

systems. Chang et al.[28] however uses the 2D and 3D images of face to build their datasets, they involve 198 persons face in their study. They used match score level in order to get a decision of identification and their conclude that 2D and 3D have similar recognition performance when considered individually, however combining 2D and 3D results using a simple weighting scheme outperforms either 2D or 3D alone, combining results from two or more 2D images using a similar weighting scheme also outperforms a single 2D image, and combined 2D+3D outperforms the multi-image 2D result. Dass et al.[29] is an ideal setting for combining multiple modalities adjustment values using the likelihood ratio calculated using the generalized density estimated from scores of the agreement and the real scam. They claim that parts of the score distributions be discrete nature; Thus, the estimation of continuous density distribution may be inappropriate. They present two approaches to combining evidence based on generalized density: i) the product rule, assumes independence between individual modalities, and ii) copula models, the dependence between the matching scores of view multiple modalities. Fierrez-Aguilar et al.[30,31] provide a signature line verification system with information on both local and global fusion at decision. We show experimentally that the experts of the machine on the basis of local information exceed the system on the basis of a comprehensive analysis when enough training data is available. Conversely, it should be noted that the entire analysis is appropriate in the case of the small size of the training set. The two proposed systems are also shown that additional recognition information is successfully exploited with notes merger decision level. In[32], Campbell presents an approach to combine Support Vector Machine with speaker detection using generative and discriminative approaches by mapping a whole speech utterance onto a fixed length vector. Ho[33] uses a multiple classifier system and rank level fusion to solve the problems of recognition of the difficult shapes with sets of overcrowded classrooms and noisy input, because it allows the simultaneous use of arbitrary length descriptors and classification methods. That can be taken by the classifiers, such as the list of the classes is represented, so that they are comparable between the different types of classifiers and different instances of a problem. However, in[34], Woods et al. apply the multiple classifiers using local accuracy estimates of each individual classifier's in a small region of feature space surrounding an unknown test sample and they suggest a methodology for determining the best mix of individual classifiers. Lu[35] applies the multiple classifiers for face recognition and it outperforms individual classifiers. This technique however can be applied to protect privacy as it proposed as a framework by Yanikoglu and Kholmatov[36]. Decision-level fusion has also been applied in many different samples for verification. Prabhakar and Jain[37] studied the effect of that scheme in fingerprint verification and they achieve 5% better accuracy. Fierrez-Aguilar[38] Fusion strategy applied to the Roman scores based on quality measures for multimodal biometric authentication. The proposed merging function is adapted made an authentication request based on the estimated quality of the detected biometric signal at this time at any time.

4. Biometric Systems

The basic steps of any typical authentication biometric system comprises four steps (Figure 2):

- Data collection: Capturing a biometric sample (raw data of a biometric characteristic before pre-processing) from a claimant, who wants to proof his/her identity. If there is no reference template in the database, the person must first register the biometric characteristic (e.g. a fingerprint) to be included into the database. This process is called enrollment. If the person is already enrolled, the process is called authentication (verification or identification) which means establishing confidence in the truth of the determination[39].
- Feature extraction: After the pre-processing of the biometric sample, an algorithm extracts the unique features derived from the biometric sample and converts it into biometric data so that it can be matched to a reference template in the database[40]. The feature extraction shown as third block in Figure (2) refers to extract the features.
- Template database: In the case of enrolment biometric data are stored in a template database. In the case of authentication, biometric data are matched against a reference template from the template database.
- Matching and Deciding: In the matching stage, biometric data are matched (compared) with data contained in one (verification) or more (identification) reference template(s) to score a level of similarity[39]. The acceptance or rejection of biometric data is dependent on the scored level of similarity in the matching stage, falling above or below a defined threshold. The threshold is adjustable so that the biometric

system can be more or less strict, depending on the requirements of any given biometric application[39]. Figure 2 Basic building blocks of a generic biometric system.

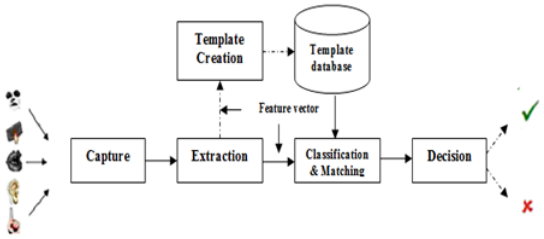

Figure 2. Basic building blocks of a generic biometric system.

5. Properties of Biometrics

Biometric systems are widely implemented worldwide for boarder control, restricted access of privileged information, secured online banking systems, and social insurance programs and so on. Although, uni-biometric systems (biometric systems based on single source of evidence) are widely deployed and used, they have several limitations that hinder their reliability and make them less reliable in identification and authentication applications. Some of these limitations are outlined below[41]:

◦ Accuracy: Noisy sensor data, non-universality, inter-class similarity and lack of invariant representation.

◦ Scalability: If the number of data samples, N, is large, identification becomes an issue.

◦ Security and Privacy: Spoofing can take place in many traits such as fingerprint, signature and voice.

In response to these limitations, multibiometric systems have been recently introduced as an improved means for person's identification and recognition purposes. Such systems rely on multiple evidence rather than single biometric evidence[41]. By integrating multiple biometric samples or multiple traits, more efficient and reliable systems can be devised. Information fusion has been proposed to achieve the integration of the multiple biometric traits at different stages of multibiometric systems[42,43]. It should be noted that the resulting systems can be either be hybrid or simple systems depending on the type of information fusion strategy being adopted and applied. Figure 3 shows the major differences between uni- and multi-biometric systems. The integration of several biometric samples and/or traits is made possible only by the incorporation of the information fusion module which highlights the importance of the latter module in the successful development of multibiometric systems since uni-modal could be considered in an ensemble but without allowing possible an improved matching and recognition performance.

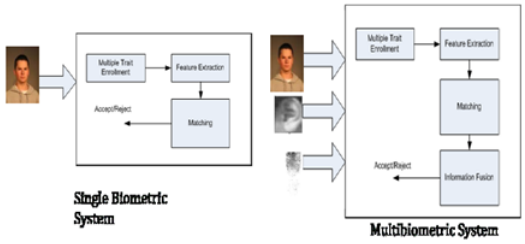

Figure 3. Single Biometric System vs. Multibiometric System.

Multimodal biometric systems can be designed to operate in five different modes[41]: 1) Multiple-Sensor Mode: In this mode, the raw biometric data is acquired from multiple sensors, processed and integrated to generate new data from which features can be extracted, Needless to notion the increased hardware, software and computational costs caused by such integration. However, the incorporation of sources from multiple sensors significantly improves the segmentation and registration procedures in addition to improving the matching accuracy[41]. 2) Single-Biometric Multiple-Representations Mode: In these systems, the same biometric data is processed using multiple algorithms at the mapping and feature levels. For instance, a multiresolution algorithm based on texture analysis and a minutiae-based algorithm can operate on the same fingerprint image in order to extract diverse feature sets that would greatly improve the performance of the overall system. This mode is characterized by its cost efficiency since it does not require the use of multiple sensors. Furthermore, the user is not required to interact with multiple sensors thereby enhancing user convenience and comfort. It does require the introduction of new feature extractor and/or matcher modules which may increase the computational requirements of the system[44]. 3) Single-Biometric Multiple-Units Mode: Multiple instances of the same biometric trait are considered in this mode. For example, the left and right irises of the same person are considered

for fusion and further processing. Systems pertaining to this mode generally do not necessitate the introduction of new sensors nor do they entail the development of new feature extraction and matching algorithms and are, therefore, more cost efficient than those systems belonging to the previous mode. In some cases, a new sensor arrangement might be necessary in order to facilitate the simultaneous capture of the various units[44].

4) Single-Biometric Multiple- snapshots Mode: In this mode, a single sensor is used to capture multiple snapshots of the same biometric trait. A mosaicing scheme may then be used to assemble the multiple impressions and create a composite image. One of the main issues in this mode is the determination of the number of samples or snapshots that have to be acquired from an individual. It is important to well capture the variability, as well as the typicality, of the individual's biometric data in the captured samples[41].

5) Multiple-biometrics Mode: Multibiometric systems requiring more than one modal are classified under this mode. For instance, the iris and fingerprint of the same person can be used for the matching, identification and recognition purposes. Systems belonging to this mode are usually known as multimodal biometric systems[2].

Unlike the first four modes where multiple sources of information are derived from the same biometric trait, in the last mode, useful biometric information is derived from different biometric traits. However, fusion at the matching score level seems to be the logical choice as it is relatively easy to access and combine scores presented by the different modalities[44]. Furthermore, incorporating the fusion process at earlier stages of the multibiometric system is more effective. In summary, the main advantages of multibiometric systems are outlined below[41]: * Improve accuracy. * Address the issue of non-universality problem. * Provide flexibility to the user. * Reduce the effect of noisy data. * Provide the capability to search a large database in computationally efficient manner. * Resistant to spoof attacks. * Fault tolerant systems.

Each of the above-mentioned features mitigates one or some of the limitations found in uni-biometric systems. Table 1, gives a comparative summary of the various biometric traits with respect to key factors such as universality, performance, acceptability and distinctiveness.

Table 1. Comparison of various biometric technologies (H=High, M=Medium, L=Low)

Biometrics	Universality	Uniqueness	Permanence	Collectability	performance	Acceptable	Circumvention
Face	H	L	H	H	L	H	L
Fingerprint	H	H	H	M	H	M	H
HandGeometry	M	M	M	H	M	M	M
Keystroke	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear	M	M	H	M	M	H	M

6. Levels of Fusion

Multimodal biometric systems overcome several practical problems of single-biometric systems, like noisy sensor data, non-universality and/or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks[41]. The procedure by which information from multiple biometric traits is consolidated is called biometric fusion, which is the critical component in multimodal biometrics.

The Figure 4 show the layout of a bimodal biometric system it illustrate the various levels of fusion for combining two (or more) biometric systems. The three possible levels of fusion are (a) fusion at feature extraction level (b) fusion at matching score level (c) fusion at decision level.

- Feature level: The raw data captured from each sensor will be used to build a feature vector, which uniquely identifies a given person in the feature space. Combining more feature vectors results in one vector with higher dimensionality and may increase the probability of correctly identifying a person.
- Match Score level: Fusion at the match score level is typically more effective than fusion at the decision level. Each single-modal biometric system measures and calculates its own match score. Match scores are a measure of the similarity or distance between features

derived from a presented sample and a stored template. A match or non-match decision is made based on a certain decision threshold. For example, one approach is to construct a score vector using the match scores from each biometric modality, then a trained classifier will decide one of two classes: "Accept" (genuine user) or "Reject" (imposter user) based on the score vector.

- Decision level: Fusion at this level is the least informative. Each biometric system makes a decision and then those decisions are combined, usually using majority voting scheme. Some methods to weight the decisions from each biometrics are also used. Apart from the above, fusion is possible at the raw data level or the rank level. Fusion at the score level is considered to be the most common approach due to the ease in accessing and combining the scores generated by different matchers[45].

Fusion at Score Level: Fusion techniques at the score level can be divided into three categories. The transformation-based score fusion will normalize the match scores to a common domain prior to combining them. Choice of the normalization scheme and combination weights is data-dependent and requires extensive empirical evaluation. In a classifier-based score fusion, scores from multiple matchers will be treated as a score vector, therefore, a classifier can be constructed to discriminate genuine and imposter scores. In this case, biometric fusion is considered as a typical classification problem. Density-based score fusion is usually based on the likelihood ratio test. Based on the Neyman-Pearson theorem, if the underlying densities of genuine and imposter scores are explicitly known, the likelihood ratio fusion.

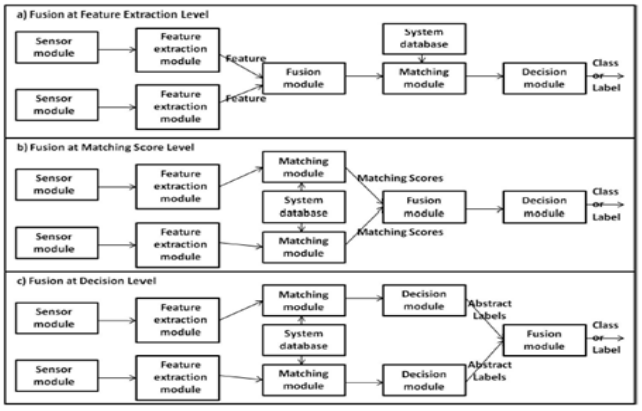

Figure 4. The biometric fusion could be implemented at various levels: a) fusion at feature level; b) fusion at match score or rank level; c) fusion at decision level.

This figure is based on[46]. Technique will provide the highest Genuine Accept Rate (GAR) for a fixed False Accept Rate (FAR)[47]. However, the underlying densities of scores cannot be exactly estimated in practice. In this work, a common transformation-based score fusion technique, namely, the sum rule has been used to obtain all the Receiver Operating Characteristic (ROC) curves summarizing the fusion performance. As mentioned earlier, a score normalization scheme is required prior to merging the scores from different modalities into a single scalar score. Based on an empirical evaluation, Jain et al.[45] found that the min-max normalization scheme followed by a simple sum of scores fusion resulted in a superior GAR than other normalization and fusion techniques for the dataset used here. So the same process is used in this work.

Performance Measures: Usually, the performance of a biometric system can be measured in terms of two error rates, False Accept Rate (FAR) and False Reject Rate (FRR)[48]. The FAR refers to the errors that occur when a system mistakes the biometric measurements from two different individuals to be from the same person. In statistics, FAR is the probability of a type-II error. The FRR refers to the errors that the biometric system mistakes two biometric measurements from the same person to be from two different people. FRR is the probability of a type-I error. FAR and FRR are also called as False Match Rate (FMR) and False Non-Match Rate (FNMR), respectively, in some literature. To understand the performance of a biometric system, a plot of FAR vs. FRR is usually used. This is known as a Receiver Operating Characteristic (ROC) curve. ROC curves present a non-dimensional, basic technical performance measure for comparing two or more biometric systems. It can also display the trade-offs between FAR and FRR over a wide range of thresholds. In this study, ROC curves are plotted as GAR (Genuine Accept Rate) vs. FAR, where GAR is the complement of FRR (GAR = 1-FRR). Equal Error Rate (EER) can also be used to give a threshold independent performance measure of a biometric system[41]. It is the point where the FAR equals the FRR. In the other words, EER is the error rate occurring when the decision threshold of a system is set so that the proportion of false rejections is approximately equal to the proportion of false acceptances. In Figure 5, the EER of the hand-geometry scores in the MSU database is about 10:7%. Figure 6 provides an example of a multimodal biometric system that can demonstrate a better recognition performance than using a single biometric. This example employs the simple sum of scores as the fusion scheme, and the min max normalization technique is used for transforming the

match scores from face, fingerprint and hand-geometry into a common domain before fusion.

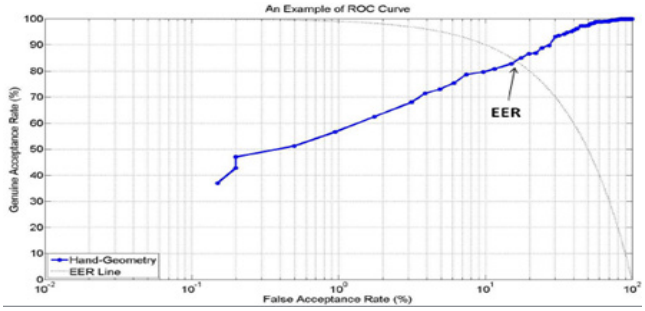

Figure 5. Example of the ROC Curve (GAR vs. FAR) for Hand-Geometry scores in the MSU database.

Most techniques for score level fusion are designed for a complete score vector, where the scores to be fused are assumed to be available. When any of the scores are missing, these techniques cannot be invoked. Incomplete score vectors can occur under different conditions. There are many causes for missing data such as the failure of a matcher to generate a score (e.g., a fingerprint matcher may be unable to generate a score when the input image is of inferior quality), the absence of a trait during image acquisition (e.g., a surveillance multibiometric system may be unable to obtain the iris of an individual), and sensor malfunction, where the sensor pertaining to a modality may not be operational (e.g., failure of a fingerprint sensor due to wear and tear of the devic4. There are several methods to deal with missing data as pointed out earlier. However, some practical constraints have to be dealt with when it comes to bio-metrics. Compared with most studies that adopts the entire dataset for the analysis,

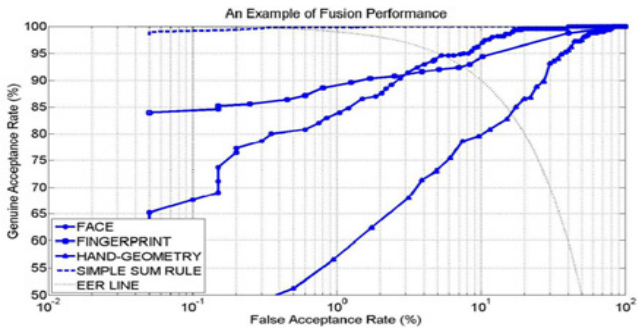

Figure 6. Example of ROC curves for three single-modal biometrics in the MSU database and the simple sum fusion.

A static set of training, in the context of biometrics preferred (a) the attribution to this whole set of changes dynamically over a fixed set, and (b) can easily handle both complete and incomplete because it is based on the vector set of test scores. scoring on a vector-by-vector of vectors independence than the attribution process a batch process where all scores are missing at the same time the accused are. That understood, scoring only captured part of this vector and a set of training can be used for the allocation. Independent vectors can not be added to any other information. Gene-expression data or other data mining applications is usually no problem as there were a large number of variables are used, less than 5 modes involve multimodal biometrics systems. That is why, among other things, a detailed framework for the merger[49] is possible models, the combination of methods sharp mind, the more likely they are to be effective multimodal biomet-RICS. On the other hand, some of the imputation methods such as Bayesian Network (BN), more variables[50] and which can calculate the probabilistic relationships between them, biometrics can not be in an environment Summary and Conclusions.

Most of biometric systems used in real applications are unimodal, which means they rely on only one area of identification. So, they are not reliable enough like the systems that use more than one attributes, such as collecting voice and face or palmprint for two hands to the same person, this system known" multi-biometrics system". Multi-biometrics systems are fusing separate information or separate features to provide integrate information. That make the systems more reliable recognition of individuals, also if don't enable to obtains for required data to any traits, the other traits enough led the system more is become more especially when used more than two traits reliable.

7. References

1. Preeti, Rajni, Physical Security: A Biometric Approach, *International Journal of Engineering And Computer Science*, 2014; 3(2):3864-68,
2. Group, I. B. Retrieved 2014 May 12: Available from: www.biometricgroup.com.
3. Aly OM, Onsi HM, Salama GI, Mahmoud TA. A Multi-modal Biometric Recognition system using feature fusion based on PSO. *International Journal of Advanced Research in Computer and Communication Engineering*. 2013 November; 2(11).

4. Griaule Biometrics, *Book-Understanding Biometrics*. 2012.
5. Sabareeswari TC, Lenty Stuwart S. Identification of a Person using Multimodal Biometric System. *International Journal of Computer Applications*. 2010; 3(9):0975-8887.
6. Shoa'a JadAllah, AbdulAziz Manal**.** Biometrics in Health Case Security System, Iris-Face Fusion System. *International Journal of Academic Research*. 2011; 3(1):11-19.
7. James W. *Introduction to Biometrics,* book in Library of Congress Control Number. 2011; p. 942231.
8. History of Fingerprinting, Home page. Last visited 30th January, 2011: Available from: http://www.fingerprinting.Com/history–of–fingerprinting.php.
9. Tohn V. *Biometrics technology and verification system*, book library of congress car at aloging. 2009.
10. Miller RP. Finger dimension comparison identification system. *US Patent*, No. 3576538. 1971.
11. Goldstein AJ, Hill M, Harmon NJ, Leon D., Lesk AB. Identification of Human Faces. *Proc. IEEE*. 1970; 59(5):748-60.
12. Chawki JM, Abdel Wahab MS. Identity Theft in Cyberspace: Issues and Solutions. *Lex Electronica, (Printemps/ Spring.* 2006; 11(1) *Available from: http://www.lexelectronica.org/articles*.
13. NSTC, *biometrics History*, book issue from National Science and Technology. 2006.
14. National Center, Individual Biometrics: Iris Scan. *Available from: http:// ctl.ncsc.dni.us/biomet%20web/BMIris.html*. 2005.
15. National Biometric Security Project. *Biometric Technology Application Manual*, Biometric Basics, Updated Summer. 2008; 1.
16. Adekunle O G. Dermatology Division, University College Hospital: Jan-June, Finger nail plate shape and size for personal identification a possible low technology method for the developing world-Preliminary report. *African Journal of Health Sciences*. 2005; 12(1-2):13-20.
17. Duc B. Bigun ES, Bigun J, Maitre G and Fischer S. Fusion of audio and video information for multi modal person authentication. *Pattern Recognition Letters*. 1997; 18(9):835-43.
18. Hong L, Jain AK. Integrating Faces and Fingerprints for Personal Identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1998; 20(12):1295-1307.
19. Chatzis V, Borse AG, Pitas I. Multimodal Decision-Level Fusion for Person Authentication. 1999; *SMC-A(29)*(6):674.
20. Shakhnarovich G, Lee L, Darrell T. Integrated Face and Gait Recognition From Multiple Views, cvpr, *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'01)*. 2001; 1:439.
21. Chibelushi CC, Mason JSD and Deravi F. Feature-level Data Fusion for Bimodal Person Recognition. Dublin, Ireland: *Proceedings of the Sixth International Conference on Image Processing and Its Applications*. 1997 July; 1:399-403.
22. Ross and Govindarajan R. Feature Level Fusion Using Hand and Face Biometrics. Orlando, USA: *Proceedings of SPIE Conference on Biometric Technology for Human Identification II*. 2005 March; 5779:196-204.
23. Kale AK, Chowdhury R, Chellappa R. Fusion of Gait and Face for Human Identification. Montreal, Canada: *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*. 2004 May; 5:901-04.
24. Ben-Yacoub S, Abdeljaoued Y and Mayoraz E. Fusion of Face and Speech Data for Person Identity Verification. *IEEE Transactions on Neural Networks*. 1999 September; 10(5):1065-75.
25. Sanderson C, Paliwal KK. Information Fusion and Person Verification Using Speech and Face Information. *Technical Report IDIAP-RR 02-33*, *IDIAP*. 2002 September.
26. Jain K, Nandakumar K, Lu X and Park U. Integrating Faces, Fingerprints and Soft Biometric Traits for User Recognition. Prague, Czech Republic: *Proceedings of ECCV International Workshop on Biometric Authentication (BioAW)*. 2004 May; LNCS 3087:259-69.
27. Marcialis GL and Roli F. Fingerprint Verification by Fusion of Optical and Capacitive Sensors. *Pattern Recognition Letters*. 2004 August; 25(11):1315-22.
28. Chang KI, Bowyer KW and Flynn PJ. An Evaluation of Multimodal 2D+3D Face Biometrics. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2005 April; 27(4):619-24.
29. Dass SC, Nandakumar K and Jain AK. A Principled Approach to Score Level Fusion in Multimodal Biometric Systems. Rye Brook, USA: *Proceedings of Fifth International Conference on Audioand Video-based Biometric Person Authentication (AVBPA)*. 2005 July; p. 1049-58.
30. Fierrez-Aguilar J, Nanni L, Lopez-Penalba J, Ortega-Garcia J and Maltoni D. An On-line Signature Verification System based on Fusion of Local and Global Information. Rye Brook, USA: *Fifth International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA)*. 2005 July; p. 523-32.
31. Fierrez-Aguilar J, Garcia-Romero D, Ortega-Garcia J, and Gonzalez Rodriguez J. Bayesian Adaptation for User-Dependent Multimodal Biometric Authentication, *Pattern Recognition*. 2005 August; 38(8):1317-19.
32. Campbell WM, Reynolds DA and Campbell JP. Fusing Discriminative and Generative Methods for Speaker Recognition: Experiments on Switchboard and NFI/TNO Field Data. Toledo, Spain: *Odyssey: The Speaker and Language Recognition Workshop*. 2004 May; p. 41-44.
33. Ho TK, Hull JJ and Srihari SN. Decision Combination in Multiple Classifier Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1994 January; 16(1):66-75.
34. Woods K, Bowyer K and Kegelmeyer WP. Combination of Multiple Classifiers Using Local Accuracy Estimates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1997 April; 19(4):405-10.
35. Lu X, Wang Y and Jain AK. Combining Classifiers for Face Recognition. Baltimore, USA: *IEEE International Conference on Multimedia and Expo (ICME)*. 2003 July; 3:13-16.
36. Yanikoglu B and Kholmatov A. Combining Multiple Bio-

metrics to Protect Privacy. Cambridge, UK: *Proceedings of ICPR Workshop on Biometrics: Challenges arising from Theory to Practice*. 2004 August.
37. Prabhakar S and Jain AK. Decision-level Fusion in Fingerprint Verification. *Pattern Recognition*. 2002 April; 35(4):861-74.
38. Fierrez-Aguilar J, Garcia-Romero D, Ortega-Garcia J and Gonzalez-Rodriguez J. Adapted user-dependent multimodal biometric authentication exploiting general information. *Pattern Recognition Letters*. 2005 December; 26(16):2628-39.
39. Claus V. *Brandenburg (Havel)*, Germany: Biometrics and ID Management COST 2101 European Workshop, *Bio ID 2011* March 8-10. 2011.
40. Anil JK. *New York*, Boston, Dordrecht, London, Moscow: Michigan State University: Biometrics Personal Identification in Networked Society. 2002.
41. Ross, K. Nandakumar, and A. K. Jain. Springer: *Handbook of Multibiometrics*. 2006.
42. Snelick R, Uludag U, Mink A, Indovina M and Jain AK. Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2005 March; 27(3):450-55.
43. Ulery B, Hicklin AR, Watson C, Fellner W and Hallinan P. Studies of Biometric Fusion. *Technical Report IR 7346*, NIST. 2006 September.
44. Ross AK, Jain. Information Fusion in Biometrics, *Pattern Recognition Letters*. 2003 September; 24(13):2115-25.
45. Jain A, Nandakumar K and Ross A. Score normalization in multimodal biometric systems. Pattern Recognition. 2005; 38(12):2270-85.
46. Jain A. Ross A and Prabhakar S. An introduction to biometric recognition. *In IEEE Transactions on Circuits and Systems for Video Technology*. 2004; 14:4-20.
47. Nandakumar K, Chen Y, Dass S and Jain A. Likelihood Ratio Based Biometric Score Fusion. *In IEEE Transactionson on Pattern Analysis and Machine Intelligence*. 2008; 30(2):342-47.
48. Ross A and Jain A. Information fusion in biometrics. *In Pattern Recognition*. 2003; 13:2115-25.
49. Fatukasi O, Kittler J and Poh N. Estimation of missing values in multi-modal biometric fusion. In IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS). 2008.
50. Friedman N, Geiger D and Goldszmidt M. Bayesian Network Classifiers. *In Machine Learning*. 1997; 29(2-3):131-63.