Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 73 (2014) 26015-26019

ISSN: 2229-712X

Multiple biometric systems: design approach and application Scenario

Aranuwa Felix Ola
Adekunle Ajasin University, Akungba Akoko, Ondo State, Nigeria.

ARTICLE INFO

Article history:
Received: 8 June 2014;
Received in revised form:
20 July 2014;
Accepted: 31 July 2014;

Keywords
Multiple biometric,
Authentication system,
Pattern recognition,
Matching accuracy,
Noisy data.

ABSTRACT
Biometric technology has become a basis of an extensive array of highly secure identification and personal verification solutions in our world today. More importantly in the wake of heightened concern about security and rapid advancements in communication and mobility. Significant application areas of biometric systems include security monitoring, access control and authentication, border control and immigration, forensic investigation, telemedicine and so on. When a single trait is used in an application it is referred to as unimodal biometric, while combination of two or more sources or traits in an application is referred to as multiple biometrics. But biometric system that uses a single biometric trait for recognition has this propensity to contend with problems related to non-universality of the trait, spoof attacks, large intra-class variability, and noisy data. Besides, no single biometric trait can meet all the requirements of every possible application, hence the need for multiple biometric system to overcome the limitation of unimodal biometric. The new paradigm is robust against individual sensor or subsystem failures and spoof attack, as it is very difficult to spoof multiple traits simultaneously. In addition, the technological environment is very appropriate because of the widespread deployment of multimodal devices (PDAs, 3G mobile phones, Tablet PCs, laptops etc). The aim of this paper is to present an overview of multiple biometric systems, design approach and application scenario.

Introduction

Multiple biometrics or simply muilti-biometric systems is a biometric technology that combines many type of biometric information or multiple sources to overcome the limitations of single biometric system. Generally, biometrics is referred to as the science of recognizing an individual based on his or her physical or behavioural traits (Akhtar et al, 2011). The technology has emerged as a reliable and effective method for establishing the identity of a person and controlling access to both physical and spaces in our society today. More importantly in the wake of heightened concern about security and rapid advancements in communication and mobility in our environments (Ross and Jain, 2003). Meanwhile, experimental studies have shown that a biometric system that uses a single biometric trait for recognition has this propensity to contend with problems related to non-universality of the trait, spoof attacks, large intra-class variability, and noisy data. Besides, no single biometric trait can meet all the requirements of every possible application (Yadav et al, 2011; Damousis and Argyropoulos, 2012). It is believed that some of the limitations imposed by unimodal biometric systems can be overcome and much higher accuracy achieved by integrating the evidence presented by multiple biometric traits for establishing identity. An ideal biometric characteristic is expected to be universal, unique, permanent, and collectable, (Chibelushi et al, 1999). A characteristic is universal when every person possesses it. A characteristic is unique when no two persons share exactly the same manifestation of the characteristic. A permanent characteristic is one that does not change and cannot be altered. A collectable characteristic is one that a sensor can easily measure or read. A number of biometric characteristics are being used in various applications. Commonly used traits are illustrated in figure 1 below:

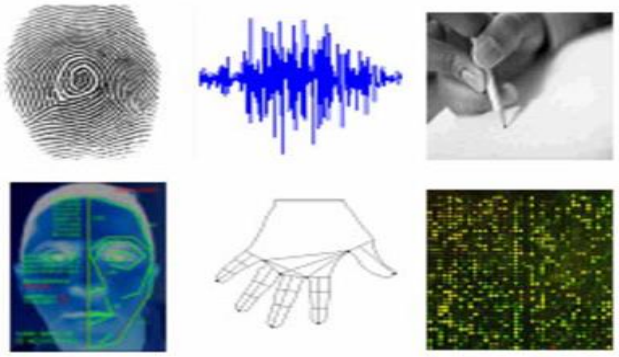


Figure 1: Examples of biometric characteristics that are commonly used: (a) fingerprint (b) voice (c) signature/handwriting, (d) face, (e) hand geometry and (f) chemical composition (body odour) (Shoewu, 2014).

Generic Biometric Components

A generic biometric system can be viewed as having five important components or modules each of these modules is shown in Figure 2 and described below (Jain, 2008):

(i). **Sensor module:** The sensor module is responsible for acquiring the biometric data from an individual. A suitable biometric reader or scanner is required to acquire the raw biometric data. This module defines the human machine interface and it is pivotal to the performance of the biometric system. For example, a poor machine or poorly designed interface can result in high failure to acquire rate and consequently, low user acceptability.

(ii).**Feature extraction module:** The feature extraction module is responsible for the processes of the data acquired and

Tele:
E-mail addresses: felixaranuwa@gmail.com

extraction of salient features to represent underlying trait. Typically, the acquired data is subjected to a signal enhancement algorithm in order to improve its quality. During enrolment, this feature set is stored in the database and it is commonly referred to as a *template*.

(iii). **Matching module:** The matching module compares extracted features against the stored template to generate match scores. The number of matching features between the input and the template feature sets is determined, and a match score is reported.

(iv). **Decision module:** The decision module uses the match scores to either validate a claimed identity or determines the user's identity.

(v). **System database module:** The system database module acts as the repository of biometric information. During the enrolment process, the salient feature set extracted from the raw biometric sample (i.e , the template) is stored in the database possibly along with some biographic information (such as name, personal identification number, address etc) characterizing the user. In addition, there is the need for generic networking and programming interfaces for interconnections between the capture device, the verification and storage components of the system into which the biometric system may have to be integrated.

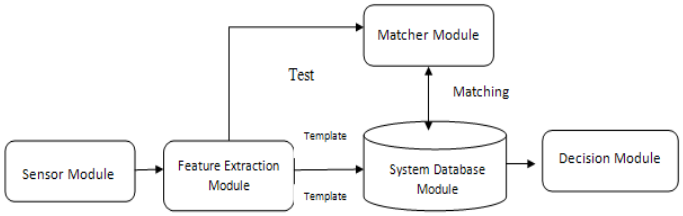


Figure 2: showing a Generic Module of Biometric System

General Architecture of Biometric System

A typical biometric system is essentially a pattern recognition system that acquires biometric data from an individual, extract a salient features set from the data, compares this feature set against the feature sets stored in the database, and execute action based on the result of the comparison (Ross and Jain , 2007). The general architecture of a biometric system can be divided into two categories (Jain and Ross, 2004): (1) verification (also referred to as authentication in this paper), and (2) identification. The two distinct mode of operation (enrolment and verification) in an authentication system is sketched in Figure 3.

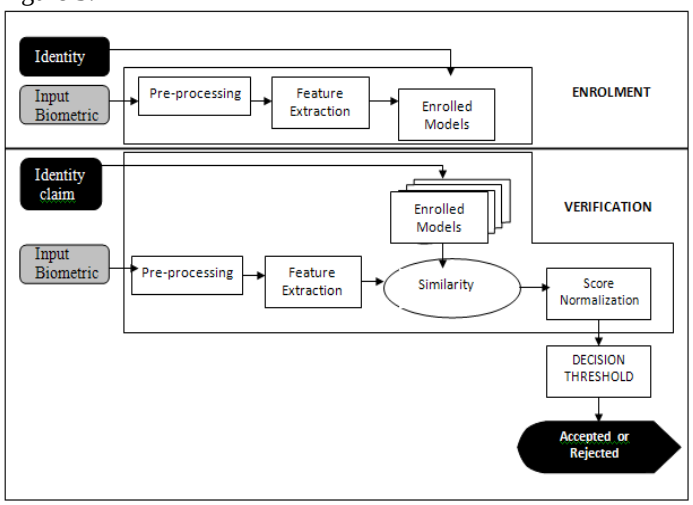


Figure 3: Diagram of the Enrolment and Verification modes in Authentication System (Jain et al, 2004)

Verification and Identification in Biometric System

In verification applications, the users are known to the system through enrolment or training process. In such applications, a user provides a biometric sample and some biometrics reference information about a person are stored in a database. The system validates a user identity by comparing the captured biometric data with his biometric template stored in the system database. An individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name or a smart card and the system conducts a *one to one* comparison to determine whether the claim is true or not. The verification task is a two category classification problems, (Ross et al, 2004; Agrawal, 2007). This can be viewed as follows: Given an input query feature set X and a claimed identity I, determine if (X, I) belongs to T or F, where T indicates that the claim identity is true (genuine user) and F indicating that the claim identity is false (imposter). To determine its category, X is matched against Y, the stored biometric template of user I. The resulting decision rule can be expressed as,

$$(X,I) \in \begin{cases} T \text{ if } S(X,Y) >= Th \\ F \text{ Otherwise} \end{cases} \quad (1)$$

Where S represents the function that measures the similarity between X and Y, and Th is the predefined threshold. The value S(X, Y) is a match score between the feature vector of the query and the stored template corresponding to identity I of the person being verified.

In identification applications, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a *one to many* comparisons to establish an individual identity or fails if the subject is not enrolled in the system database. In this application, the subject does not claim any identity but determine identity. The identification problem may be stated as follows: given an input query feature set *X*, determine the identity I_k, $k \in \{1,2\ldots\ldots N, N+1\}$, where $I_1, I_2, \ldots\ldots I_N$ are the N identities enrolled in the system, and I_{N+1} indicating the reject case. To determine the individual's identity, the decision rule can be expressed as,

$$X \in \begin{cases} I_M \text{ If } M = max_k \{S(X,Y_{Ik}) \text{ and } S(X,Y_{IM})\} >= Th \\ I_{M+1} \text{ Otherwise} \end{cases} \quad (2)$$

Where *S* represents the function that measures the similarity between *X* and Y_{Ik}. Y_{Ik} is the biometric template corresponding to identity I_k, and *Th* is the predefined threshold. The value $S(X,Y_{Ik})$ is a match score between the feature vector of the query and the stored template corresponding to identity *I* of the person being identified. The above described identification as the open-set identification. Another one is closed set identification in which the user is known to exist in the database. There is never a reject case in the closed set identification. The enrolment, verification and identification process details are as illustrated in Figure 4.

Design Issues and Approaches in Multimodal Biometric System

The following key issues needed to be considered in designing and applying biometric systems in any application (Deravi, 1999)

- **Robustness:** It is important to consider how robust the system is to fraud and impersonation. Such fraud can occur at the

enrolment stage as well as at the verification stage. Using more than one biometric modality can help combat fraud and increase robustness. Also the system should be robust to small variations of the users' biometrics over time. For this, an adaptive system that gradually modifies the stored templates may be used.

- **Acceptability:** The technology must be socially acceptable and easy to use during both the enrolment and comparison phases. The users would not accept a system that may threaten their privacy and confidentiality or that might appear to treat them as potential suspects and criminals.
- **Speed and Storage Requirements:** The time required to enrol, verify or identify a person is of critical importance to the acceptability and applicability of the system. Ideally, the acceptable verification time should be of the order of one second or faster. The storage requirement for the templates is also an important issue, especially if the templates are to be stored in magnetic stripe or smart cards.
- **Integration:** The hardware platform on which the system is to be implemented is a key concern. The software, hardware and networking requirements should ideally be compatible with existing systems, allowing the biometric system to be integrated to the existing infrastructure. The system cost should be reasonable and the maintenance costs should be understood.
- **Legal issues:** This also have to be considered in relation to biometric systems, since there are concerns over potential intrusions into private lives by using biometric systems. Legal issues must be considered for any potential application and appropriate measures must be taken. A clear public stance on the issue of privacy in relation to biometric technologies is required to ensure broad public acceptance.

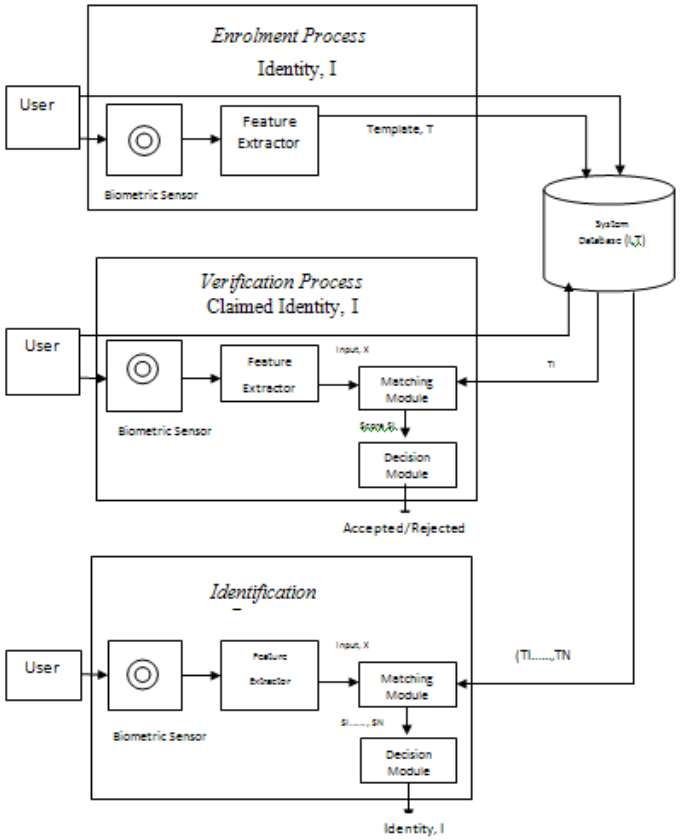


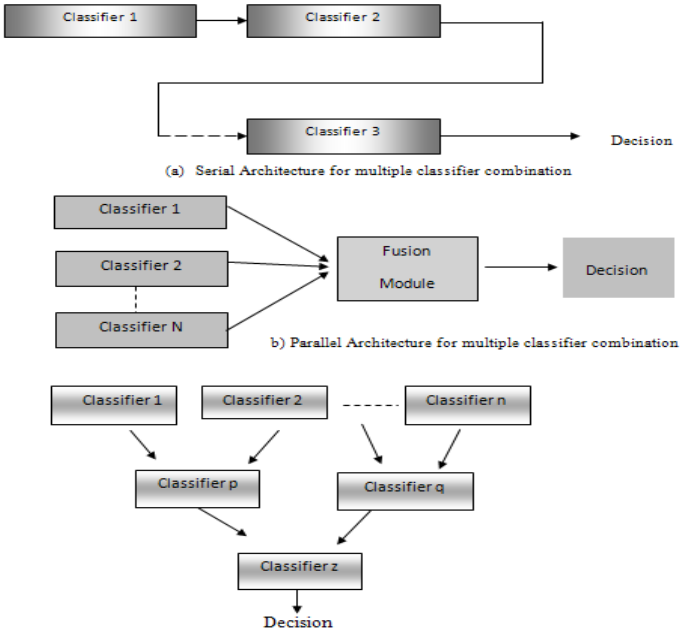
Figure 4: Enrolment, Verification and Identification details of a Biometric System [11]

Design Approach and Application Scenario: the design approach in multiple biometric systems is strongly dependent on the application scenario and this design decisions have an intense contribution on the performance of a biometric system. Multiple biometric systems design in literature can be classified into four parameters namely, (i) system architecture, (ii) the sources and fusion scenarios (iii) the level at which the evidence is accumulated, and (iv) the methods used for the integration or fusion of information.

System Structure of Multiple Biometrics and Application Areas

The structure of a multi-biometric system refers to the sequence in which the multiple traits or sources are acquired and processed. Typically, the structure of a multiple biometric system can be group into three main categories [7, 13]: (i) Serial also known as cascading (ii) Parallel and (iii) Hierarchical, (see Figure 5). The choice of the biometric system design depends on the application requirements. User friendly and less security critical applications like bank ATMs can use a cascaded multiple biometric system. On the other hand, parallel multiple biometric systems are more suited for applications where security is of paramount importance (e.g., access to military installations, and facilities). In the serial architecture, the processing of the modalities takes place sequentially and the outcome of one modality affects the processing of the subsequent modalities. The structural design can improve the user convenience; however, the system may face with the task of identifying the user from a large database.

In the parallel design, different modalities operate independently and their results are combined using an appropriate fusion scheme. A multiple biometric system designed to operate in the parallel mode generally has a higher accuracy because it utilizes more evidence about the user for recognition. Most of the multi-biometric systems have a parallel architecture because of its flexibility and reliability. They are considered more suited for applications where security is of paramount importance [2, 14]. It hierarchical architecture, different classifiers are combined into a tree-like structure. Hierarchical architecture is more flexible architecture that enables the exploitation of the different discriminative power that embedded in different groups of features. But the design of a hierarchical multibiometric system has not received much attention from researchers.



(c) Hierarchical Architecture for multiple classifier combination

Figure 5: System Architecture of Multiple Biometrics (a-c) [13]

Sources and Fusion Scenario in Biometric Modalities

The sources and fusion scenarios in a multi-biometric system can be classified into one of the following six categories, [15]: multiple sensors, multiple algorithms, multiple instances, multiple samples, multiple modalities and hybrid. See Figure 6 for detail illustration:

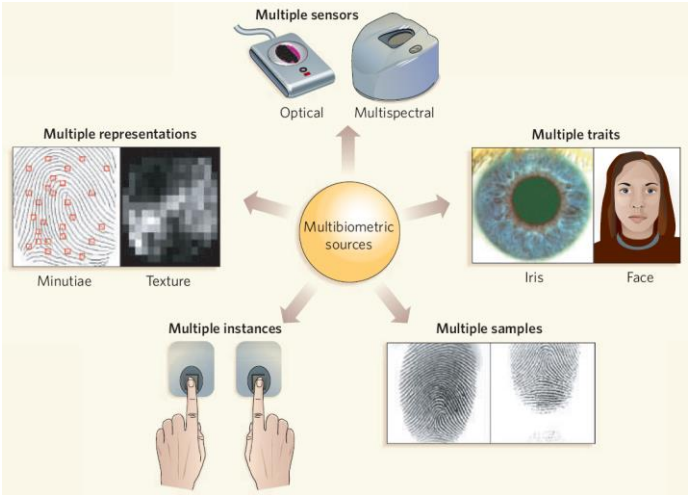


Figure 6: Different Scenarios in Multi-biometrics System [15]

(i). Multiple sensors system:

In a multi-sensors system, a single biometric modality is acquired by using a number of sensors. (for example, optical and multi-spectral fingerprints sensors). The information obtained from the different sensors for the same biometric trait are then combined. The use of multiple sensors, in some instances, can result in the acquisition of complementary information that can enhance the recognition ability of the system.

(ii) Multiple instances system:

This system uses multiple instances of the same biometric body trait, for example, multiple face images of a person obtained under different pose or lighting conditions (left, frontal and right profile of the face). This type of system can be cost-effective if a single sensor is used to acquire the multi-unit data in a sequential fashion. However, in some instances, it may be desirable to obtain the multi-unit data simultaneously, thereby demanding the design of an effective and possibly more expensive acquisition device.

(iii) Multiple representations system

In this system, a single biometric input is processed with different feature extraction and algorithms in order to create templates with different information content. One example of this is processing fingerprint images according to minutiae and texture based representations. These system do not necessitate the deployment of new sensors, hence, are cost-effective compared to other types of multi-biometric systems. But in the other hand, the introduction of new features extraction and matching modules can increase the computational complexity of these systems, (for example, using multiple face matchers like Principal Component Analysis (PCA) and Linear Discriminates Analysis (LDA) together.

(iv) Multiple Samples system

In this system, the same biometric modality and instances is acquired with the same sensor multiple times in order to account for the variations that can occur in the trait (for example, left and right iris images or left and right index finger).

(v) Multiple Traits (Multimodal systems):

In multimodal systems, multiple biometric modalities are combined to establish the identity of a person based on the evidence of multiple biometric traits. (for example, fingerprint and iris). However, the cost of deploying these systems is substantially more due to the requirement of different sensors and, consequently, the deployment of appropriate user interfaces. However, the identification accuracy can be significantly improved by utilizing an increasing number of traits although the curse-of-dimensionality phenomenon would impose a bound on this number. The number of traits used in specific application may also be restricted by practical considerations such as the cost of deployment, enrollment time, throughput time etc.

(vi). Hybrid systems:

The term hybrid describes systems that integrate a subset of the five scenarios discussed above. For example, an arrangement in which two speaker recognition algorithms are combined with three face recognition algorithms at the match and rank levels. Thus, the system having multi-algorithmic as well as multiple modalities in its design.

In summary, the first four scenarios, multiple sources of information are derived from the same biometric trait. In the fifth scenario, information is derived from different biometric traits. From these scenarios, it can be deduced that the use of multiple sensors can address the problem of noisy sensor data, but all other potential problems associated with unimodal biometric systems remains. A recognition system that works on multiple units of the same biometric can ensure the presence of a live user by asking the user to provide a random subset of biometric measurements (e.g., left index finger followed by right middle finger). Multiple instances of the same biometric, or multiple representations and matching algorithms for the same biometric may also be used to improve the recognition performance of the system. However, all these methods still suffer from some of the problems faced by unimodal systems. A multimodal biometric system based on different traits is expected to be more robust to noise, address the problem of non-universality, improve the matching accuracy, and provide reasonable protection against spoof attacks. Hence, the development of biometric systems based on multiple biometric traits has received considerable attention from researchers.

Level of Fusion in Biometrics

Fusion in biometric systems generally can take place at four major levels, namely sensor level, feature level, score level and decision level. The four levels can be broadly categorized into: pre-classification or fusion before matching and post-classification or fusion after matching [16]. Figure 7 illustrate fusion level possibilities (a) Feature level (b) Match score level and (c) decision level respectively. Figure 8 shows a broad classification of fusion levels in multi-biometric system.

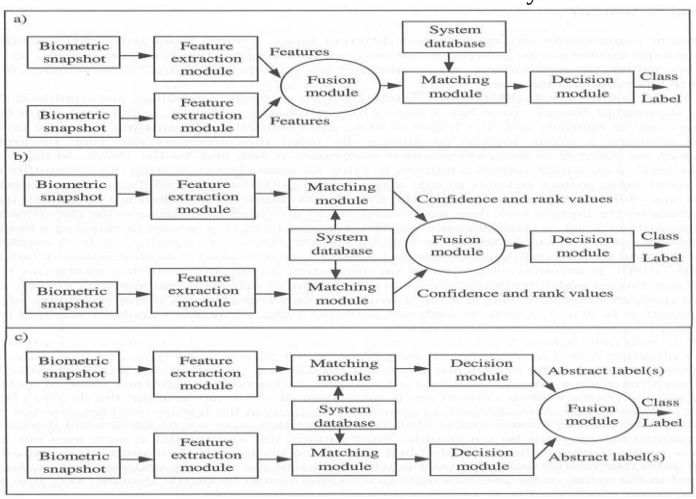


Figure 7. Fusion levels possibilités [17]

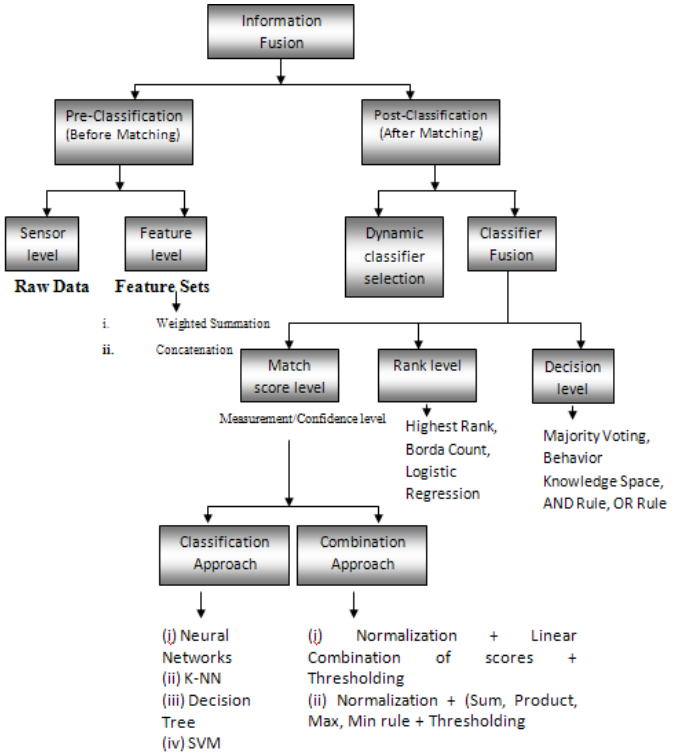


Fig 2.5 Broad Classification of Fusion levels in Multibiometric System [16]

Conclusion

This paper is focused at presenting an overview of multiple biometrics design approach and application scenario. The new paradigm promises an efficient method of establishing the identity of a person over single biometric systems. Additionally, combining the results obtained from multiple traits can significantly improve reliability, accuracy and consequently improve the overall performance of biometric system. Typically, the structure of a multiple biometric system can be group into three main categories (i) Serial also known as cascading (ii) Parallel and (iii) Hierarchical. Meanwhile, the choice of the biometric system design depends on the application requirements. User friendly and less security critical applications like bank ATMs can use a cascaded multiple biometric system. On the other hand, parallel multiple biometric systems are more suited for applications where security is of paramount importance (e.g., access to military installations, and facilities).

References

[1] Akhtar, Z and Affrarid, N (2011): "Secure learning Algorithm for Multimodal Biometric Systems against Spoof Attacks". International Conference on Information and network technology IPCSIT vol.4 (2011) © (2011) IACSIT Press. Singapore.

[2] Ross, A., and Jain, A. K., (2003). "Information Fusion in Biometrics". Pattern Recognition Letters, Special Issue on Multimodal Biometrics, 24(13):2115–2125, 2003.

[3] Yadavi. S.S,.Gothwal, J. K. and Singh. R (2011). "Multimodal Biometric Authentication System: Challenges and Solutions". Global Journal of Computer Science and Technology. Volume XI Issues XVI Version 1, September, 2011

[4] Damousis I. G. and Argyropoulos S (2012) : "Four Machine Learning Algorithms for Biometrics Fusion": A Comparative Study. Applied Computational Intelligence and Soft Computing Volume 2012, Article ID 242401, 7 pages. Hindawi Publishing Corporation doi:10.1155/2012/242401

[5] Chibelushi,C C, Deravi, F and Mason, J S.D (1999) : "A Review of Speech-Based Bimodal Recognition – Part 1: Foundations for Audio-Visual Fusion by Machine". Publication in IEEE Transactions on Multimedia, 1999.

[6] Shoewu, O., N.T. Makanjuola, & S.O. Olatinwo. "Biometric-based Attendance System: LASU Epe Campus as Case Study." *American Journal of Computing Research Repository* 2.1 (2014): 8-14.

[7] Jain, A. K. (2008), Microsoft ® Encarta ® 2008 ©, 1993-2007-Microsoft Corporation.

[8] Ross, A. and Jain, A.K. (2007), Human Recognition using Biometrics: An Overview: Annals of Telecommunications, Vol.62, No. 1 pp.11-35.

[9] Jain, A. K and Ross, A. (2004). "Multibiometric Systems". Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1):34–40, January 2004.

[10] Ross, A, Jain, A.K. and Prabhakar, S. (2004): "An Introduction to Biometric Recognition". IEEE Transactions on Circuits and Systems for Video Technology, Special issue on Image and Video-based Biometrics, 14(1): 4-20, January, 2004.

[11] Agrawal , M., (2007): "Design Approaches for Multimodal Biometric System", A Thesis submitted in partial fulfillment of the requirements for the Degree of Master of Technology Department of Computer Science and Engineering, Indian Institute of technology, Kanpur.

[12] Deravi, F. (1999): "Audio-Visual Person Recognition for Security and Access Control" Joint Information Systems Committee, University of Kent at Canterbury, Sept, 1999.

[13] Drygajio, A. (2011), "Information and Communication Security", LIDIAP Speech processing and Biometrics Group, Institute of Electrical Engineering, Ecole Polytechnique Federale de Lausanne (EPFL).http//scgwww.epfl.ch/courses.

[14] Snelick, R, Indovina, M, Yen, J. Mink. A (2005): "Multimodal Biometrics: Issues in Design and Testing National Institute of Standards and Technology Gaithersburg, MD 20899.

[15] Ross A, Nandakumar, K, and Jain A.K (2006). Handbook of Multibiometrics, Springer, New York, USA, 1st edition, 2006.

[16] Sanderson, C and Paliwal, K.K, (2002): "Information fusion and person verification using speech and face information", Research Paper IDIAP-RR 02-33, IDIAP, September, 2002.

[17] Dessimoz, D., Richiardi J., Champod, C. and Drygajlo A (2006): Multimodal Biometrics for Identity Documents: State-of-the-Art Research Report PFS 341-08.05 (Version 2.0), Universite de Lausance June 2006.