cisdi Journal

Computing, Information Systems & Development Informatics Journal
Vol. 11 No. 2, 2020 - www.isteams.net/cisdijournal

Structural Approach and Application Scenario in Multiple Biometrics System

Aranuwa, F.O.
Department of Computer Science
Adekunle Ajasin University,
Akungba – Akoko, Ondo State, Nigeria
E-mail; felix.aranuwa@aaua.edu.ng
Phone: +2347031341911

ABSTRACT

The challenges of remembering multiple passwords, personal identification numbers (PINs) and maintaining multiple authentication tokens which can be easily forgotten, forged or stolen in the traditional personal identification systems led to the emergence of biometric technology. The technology is based on the fact that humans' physiological and behavioural characteristics are unique and can be used to uniquely recognize or identify an individual. When a single trait or characteristic 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 system. Meanwhile, study have revealed that 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 the conventional mode. The new paradigm is quite robust particularly against individual sensor/subsystem failures and spoof attacks, as it is very difficult to spoof multiple traits simultaneously in a single application. Additionally, the technological environment is very appropriate because of the widespread deployment of multimodal devices (PDAs, 3/4/5G mobile phones and technologies, Tablet PCs, laptops, and so on). However, the issues of design and approach to effective and efficient deployment of the system remain a challenge. Hence, the aim of this paper is to present a general overview of multiple biometrics, its system structure, explore key design issues, approaches and application scenarios for efficient multiple biometrics system.

Keywords: Biometric Technology, Unimodal Biometric, Multiple Biometrics, Design Approach, Password, Biometric Traits, Verification and Identification.

CISDI Journal Reference Format
Aranuwa, F.O. (2020): Structural Approach and Application Scenario in Multiple Biometrics System. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 11 No 2, Pp 63-76. Available online at www.computing-infosystemsjournal.info

1. BACKGROUND TO THE STUDY

Today, biometric technology is rising as an advanced layer to many personal and enterprise security systems. The technology has emerged as a reliable and effective method for establishing the identity of a person and access control to both physical and spaces, more importantly in the wake of heightened concern about security and rapid advancements in communication and mobility in our society today. Major application areas of biometric systems include security surveillance, authentication, border control and immigration, forensic investigation, telemedicine and so on. According to [1], biometrics is referred to as the science of recognizing an individual based on his or her physiological or behavioural characteristics. Top benefits of biometric technology are authentication, privacy or data discretion, authorization or access control, data veracity, and non-repudiation.

The technology promises to be the more reliable and secure means of authentication owing to the fact that it uses human distinctive characteristics [2]. Table 1 and Figure 1 show different biometric traits (characteristics), their corresponding modalities, and commonly used biometric characteristics respectively.

TABLE 1: BIOMETRIC TRAITS AND CORRESPONDING MODALITIES

S/N	Trait	Modality
1	Facial Pattern	Physiological
2	Fingerprint	Physiological
3	Palm Print	Physiological
4	Hand Geometry	Physiological
5	Retina and Iris patterns	Physiological
6	Signature pattern	Behavioural
7	Voice	Behavioural
8	Gait (walking pattern)	Behavioural

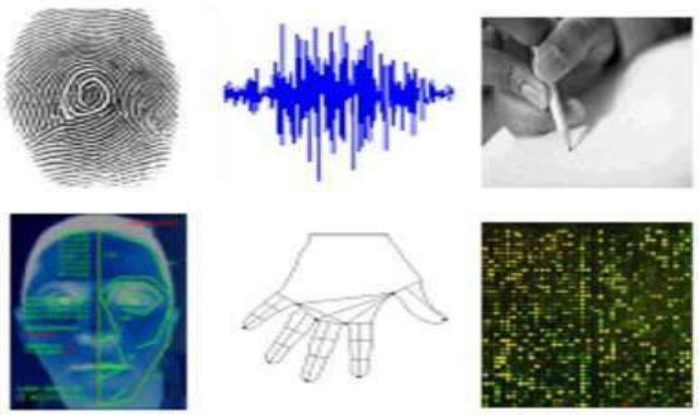

Figure 1: Examples of commonly used biometric characteristics: (a) fingerprint (b) voice (c) signature/handwriting, (d) face, (e) hand geometry and (f) chemical composition (body odour) [3].

An ideal biometric characteristic is expected to be universal, unique, permanent, and collectable [4]. 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. 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. Meanwhile, study have revealed that 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 [5]; [6]. 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 conventional mode.

By description, multiple biometrics is described as biometric technology that combines more than one form of biometric information or source for greater recognition efficiency and security. The new paradigm is quite robust particularly against individual sensor/subsystem failures and spoof attacks, as it is very difficult to spoof multiple traits simultaneously in a single application [7]. The system structure of a generic biometric and multiple biometrics system are succinctly discussed in section 4 of this paper.

2. STATEMENT OF PROBLEM

Multiple biometrics paradigm relatively is a technology developed to overcome the limitations of unimodal biometric system. The paradigm combine evidences from multiple biometric sources or traits capable of offering considerable improvements in reliability and better performance. However, the issues of design and approach to effective and efficient performance of the system attract research attention.

3. OBJECTIVE

The main objective of this study is to present a general overview of multiple biometrics and its system structure, explore key design issues, approaches and application system scenarios.

4. METHODOLOGY

4.1 System Module for Generic Biometrics System

A generic biometric system can be viewed as having five important components or modules [8]. Each of these modules is depicted in Figure 2 and discussed as follows:

(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 rate and consequently low user acceptability.

(ii) **Feature extraction module**: The feature extraction module is responsible for the processing of the data acquired and extraction of salient features to represent underlining traits. 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) **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's identity. 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.

(v) **Decision module**: The decision module uses the match scores to either validate/determines a claimed identity either to accept or reject the claimed identity.

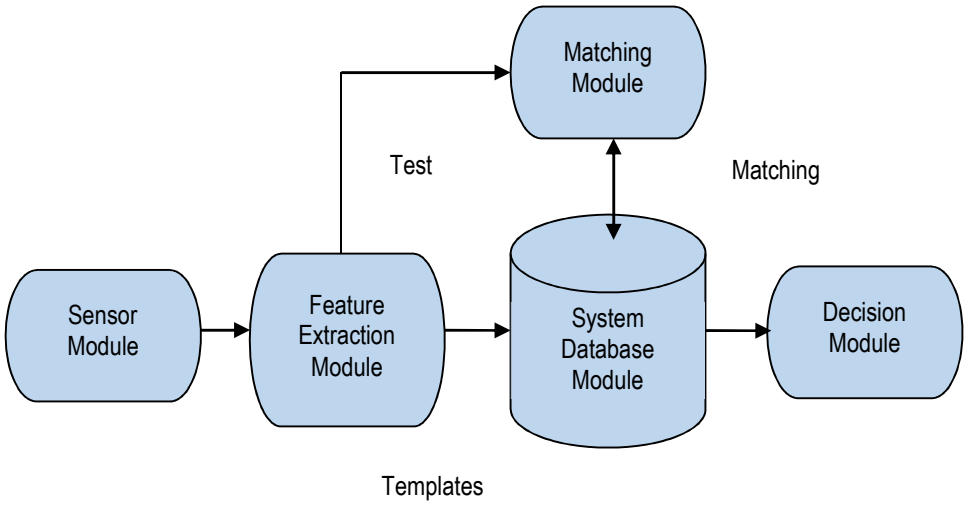

Figure 2: showing a Generic Module of Biometric System

4.2 Enrolment and Verification Process in Biometric Authentication 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[10]. The general architecture of a biometric system can be divided into two categories [11]. They are: (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.

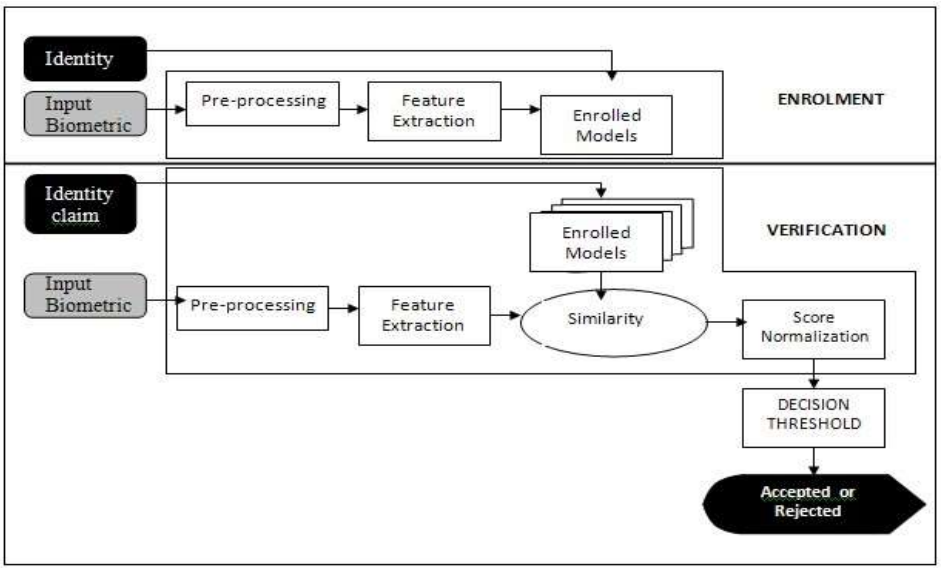

Figure 3: Diagram of the Enrolment and Verification modes in Biometric Authentication System [11].

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 reader, personal identification number or a user name 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, [11;12]. 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.

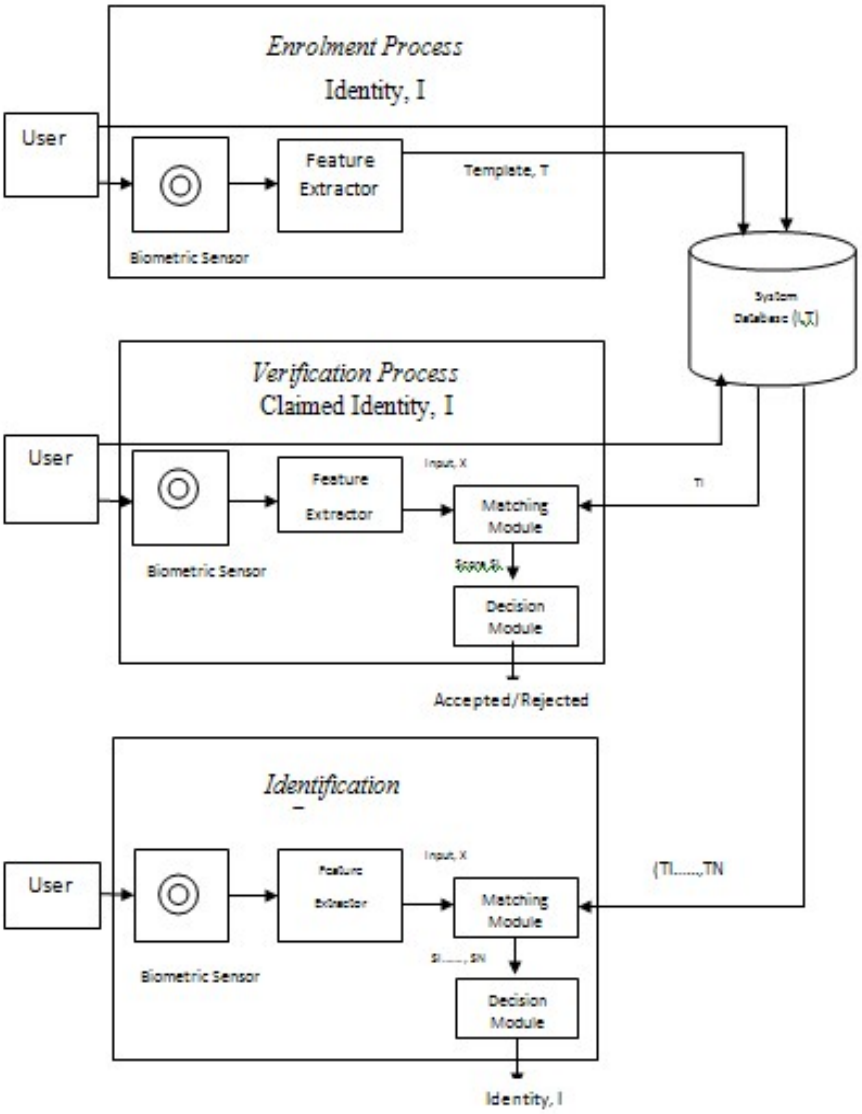

Figure 4: Enrolment, Verification and Identification Processes [12]

4.3 Key Design Issues in Biometric Systems

The following key issues needed to be considered in designing and applying biometric systems of any application [13]:

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 enroll, 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. Ideally, a clear public stance on the issue of privacy in relation to biometric technologies is required to ensure broad public acceptance.

4.4 Structural Approach in Multiple Biometrics System

Design decisions in multiple biometrics system have an intense contribution on the performance of the system. Though they are strongly dependent on the application scenario, but the following approaches must be sturdily considered (i) the system structure, (ii) the system scenarios (iii) fusion levels, that is the level at which the evidence is accumulated, and (iv) the methods of information integration or fusion.

4.4.1 System Structure Classifications in Multiple Biometrics System

The structure of a multiple biometrics 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 classified into three main categories: (i) Serial also known as cascading (ii) Parallel and (iii) Hierarchical [14; 15]. Their choice of deployment of any of these structure depends on the application requirements. User friendly and less security critical applications like bank ATMs can use a cascaded multiple biometrics system. On the other hand, parallel and hierarchical 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 is easy and supports 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 biometrics 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 multiple 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 [16]; [17].

In the hierarchical structure, different classifiers are combined into a tree-like structure. It exploits the different discriminating power of the different groups of features, but has not actually received much attention from researchers and designers. The three structures are depicted in Figure 5.

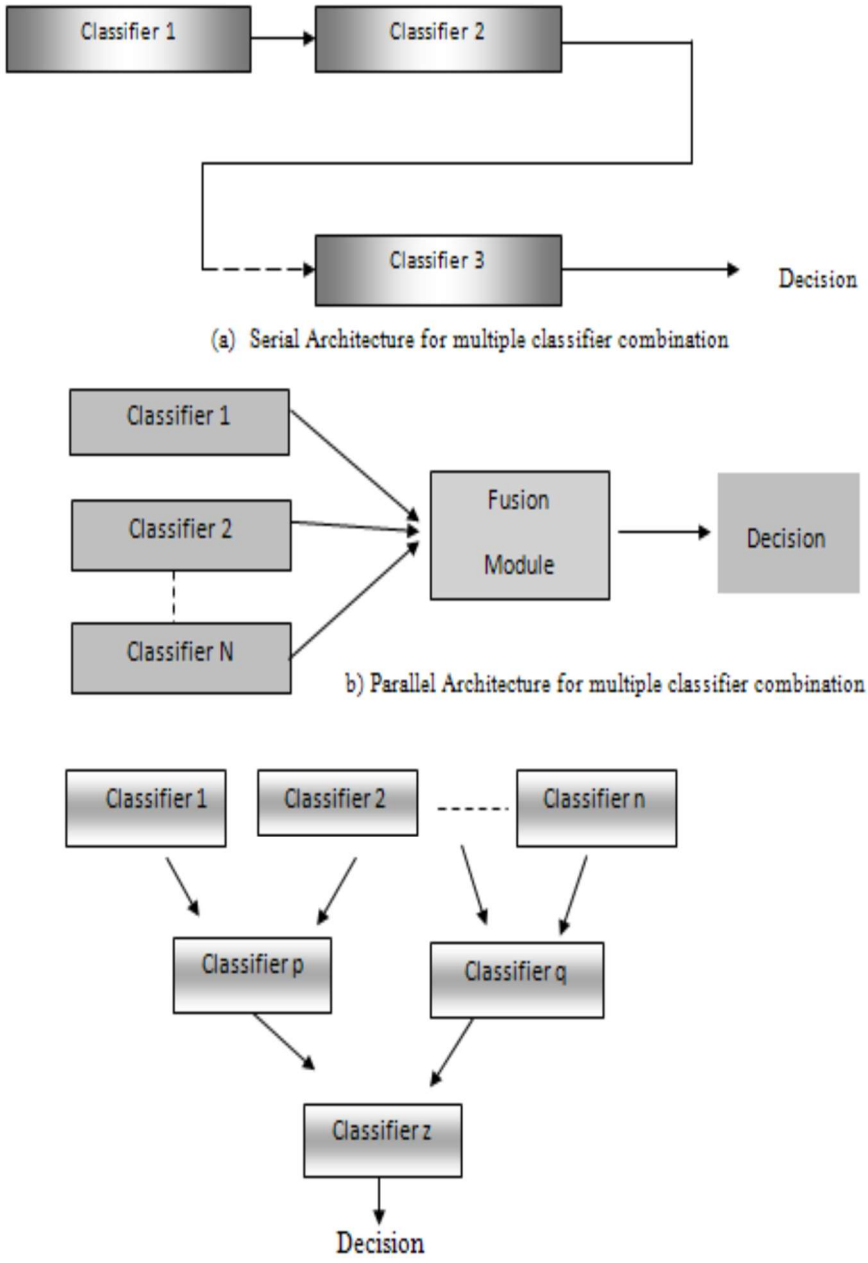

Figure 5: System Structures for Multiple Biometric System [15]

4.4.2 System Application Scenarios in Multiple Biometrics System

Scenario in a multi-biometric system can be classified into one of the following six categories, [18]: multiple sensors, multiple instances, multiple representations, multiple samples, multiple traits (modalities) and hybrid systems. See figure 6 for different application scenarios of multiple biometrics system.

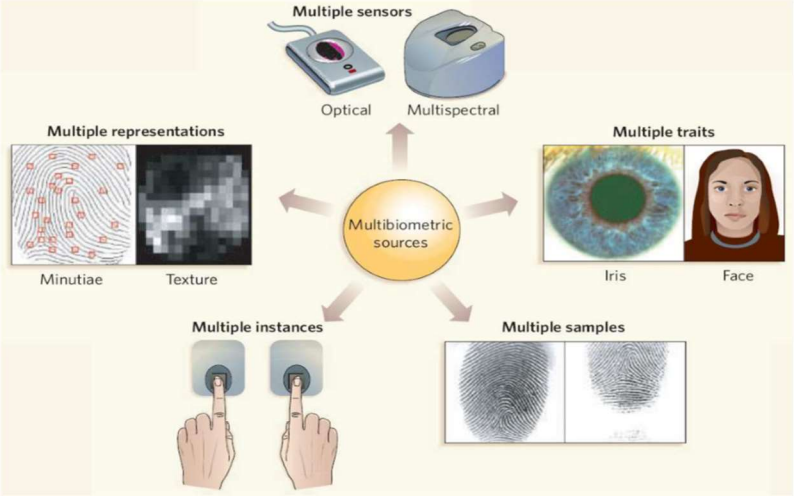

Figure 6: Different Scenarios in Multi-biometrics System [18]

Multiple sensors system:

In a multi-sensors system, a single biometric modality is acquired using a number of sensors, (for instance, using 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.

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.

Multiple representations system

In this type of system scenario, 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, it is 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.

Multiple Samples system
In this type of 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).

Multiple Traits (Multimodal systems)
In this system scenario multiple traits also known as multimodal system, multiple biometric modalities are combined to establish the identity of a person based on the evidence from these modalities, (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. The number of traits used in specific application may also be restricted by practical considerations such as the cost of dimensionality, deployment, enrolment time, throughput time etc.

Hybrid systems:
The term hybrid describes systems that integrate a subset of the five scenarios discussed above. For instance, 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. The computational complexity of this system may be high unless a multi-levels system is employed.

In summary, the first four scenarios, multiple sources of information are derived from the same biometric trait, while in the fifth scenario, information are 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, while all other potential problems associated with unimodal biometric systems subsist. 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 such as subsystem failure and spoof attacks. However, a multimodal biometric system based on different traits is more robust to noise, address the problem of non-universality of traits, improve the matching accuracy, and provide reasonable protection against spoof attacks. Hence, the development of biometric systems based on multiple biometric traits have received considerable attention from researchers.

4.4.3 Fusion Levels in Multiple Biometrics System
Generally, fusion in biometric systems can take place at six major levels, namely sensor level, feature level, score level, rank level, decision level and hybrid level. The six levels can be broadly categorized into: pre-classification or (fusion before matching) and post classification or (fusion after matching) [6];[19]. Figure 7 illustrated the three most common fusion level possibilities (a) Feature level (b) Match score level and (c) decision level respectively, while Figure 8 shows a broad classification of fusion levels in multi-biometric system.

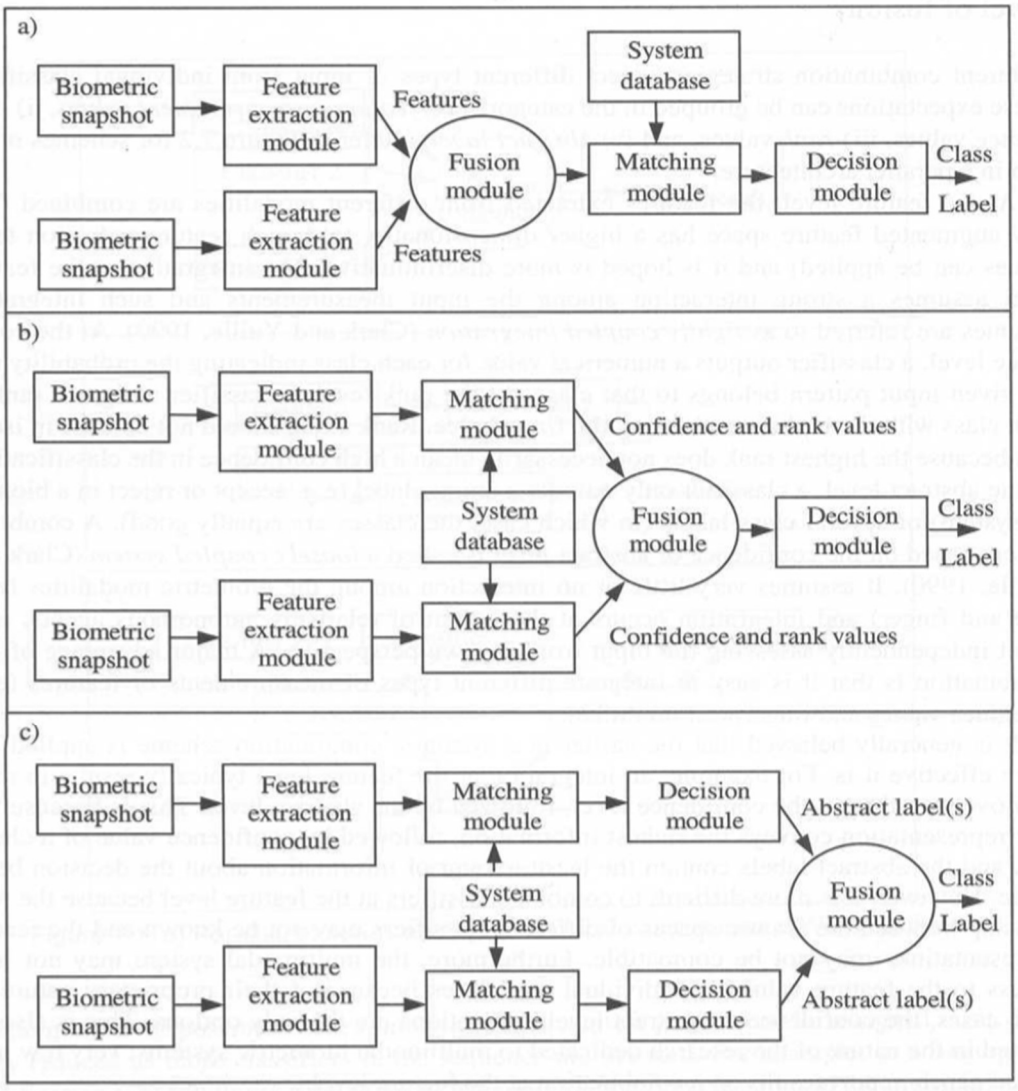

Figure 7. Fusion levels possibilities [20]

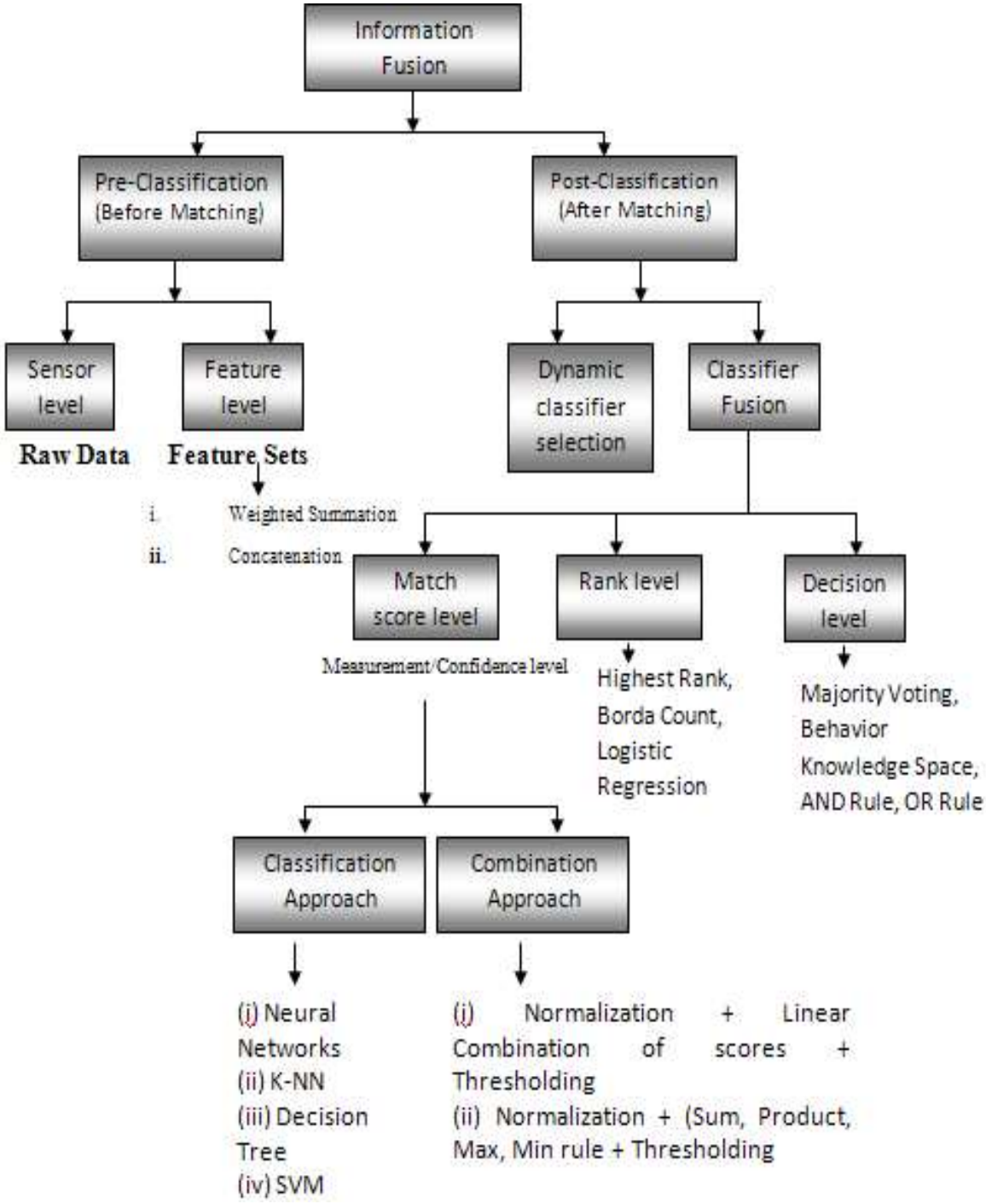

Figure 8: Broad classification of the fusion levels in Multiple Biometrics System [19]

4.4.4 Information Integration Methods in Multiple Biometrics System

Researchers at different levels had combined outputs of two or more classifiers in biometric systems and several different techniques such as rule based, statistical methods and machine learning procedures (e.g k-Nearest Neighbor, multi-layer perceptron, decision trees, support vector machine e.tc.) have also been proposed for biometric information fusion [21]. However, four major information fusion techniques based on their pragmatic characteristics, robustness and reliability are comparatively presented in [6].

5. CONCLUDING REMARKS

This study presented a general overview of multiple biometrics system and its structure, explored key design issues, approaches and application system scenarios in the domain. The new paradigm does not only offers an efficient method for establishing identity of a person over single biometric systems, but also provide enhanced security in authentication applications in the domain. Additionally, the new paradigm can significantly improve reliability, accuracy and consequently improve the overall performance of biometric systems. Future studies will consider deployment of the design approaches and their performance metrics, which is an important issue for the adoption of general biometric technologies.

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] French, T. 2012. CIS050-6 Week 6: Biometrics. , Luton Campus, UK: University of Bedfordshire. Available at: http://breo.beds.ac.uk.

[3] Shoewu, O., N.T. Makanjuola, and Olatinwo, S.O. (2014). Biometric based Attendance System: LASU Epe Campus as Case Study." *American Journal of Computing Research Repository 2*(1): 8-14.

[4] Stanley, P., Jeberson, W., and Klinsega V.V. (2009). Biometric Authentication: A Trustworthy Technology for Improved Authentication. 2009 International Conference on Future Networks, , pp. 171-175.

[5] Soliman, H., Mohammed, A. S and Atwan, A, (2012): Feature Level Fusion of Palm Veins and Signature Biometrics, International Journal of Video & Image processing and Network Security IJVIPNS-IJENS Vol. 12No 01, pg 28-39.

[6] Aranuwa, F.O (2020). Information Fusion Schemes for Reliable Biometric System. *American Journal of Biometrics and Biostatistics (AJBB)* 4(1): 001-005. USA. Available at: https://www.scireslit.com/Biometrics/AJBB-ID18.pdf

[7] Choras, R. S (2019). Multimodal Biometrics for Person Authentication DOI: http://dx.doi.org/10.5772/intechopen.85003. Book Chapter pg 1-17

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

[9] 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.

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

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

[12] 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.

[13] Deravi, F. (1999). Audio-Visual Person Recognition for Security and Access Control Joint Information Systems Committee, University of Kent at Canterbury, Sept, 1999.
[14] Jain, A. K. (2008). Microsoft ® Encarta ® 2008 ©, 1993-2007-Microsoft Corporation.
[15] Drygajio, A (2011). Information and Communication Security. LIDIAP Speech processing and Biometrics Group Institute of Electrical Engineering. Ecole Polytechnique Federale de Lausanne (EPFL) http//scg.www.epfl.ch/courses.
[16] Ross, A., and Jain, A. K., (2003). "Information Fusion in Biometrics". Pattern Recognition Letters, Special Issue on Multimodal Biometrics, 24(13):2115–2125, 2003.
[17] 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.
[18] Ross A, Nandakumar, K, and Jain A.K (2006). Handbook of Multibiometrics, Springer, New York, USA, 1st edition, 2006.
[19] 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.
[20] Dessimoz, D., Richiardi J., Champod, C. and Drygajlo A (2006). Multimodal Biometrics for Identity Documents: Stateof-the-Art Research Report PFS 341-08.05 (Version 2.0), Universite de Lausance June 2006.
[21] 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.