Multi-Modal Biometric System: An Approach towards Security Management in Vulnerable Location

D.O. Njoku[1], S.A.Okolie[1], F.N. Eluemelem[1], I.A. Amaefule[2]

[1]*Department of Computer Science, Federal University of Technology Owerri, Owerri, Nigeria*
[2]*Department of Computer Science, Imo State University, Owerri, Nigeria*

Abstract— **This paper has presented a review on multimodal biometric system with a view of applying same in the enhancement of secuirty management in vulnerable location. The review is on the use of biometric features to ensure adequate security. It considered various schemes and their individual strengths and weaknesses. However, more emphasis was given to multimodal biometric system. A Multimodal biometric system is a biometric scheme that uses more than one modality in making verification and authentication as well as identification . The challenges of single trait biometric systems can be addressed by multimodal biometric system. Several multimodal biometric systems combining different features have been proposed in literature and in practice for security and access control purposes. After considering other biometric options proposed in literature by taking into account factors such as ease of use, convenience of user, reliability, cost and response time, a multimodal biometric scheme that combines fingerprint and face features was proposed for stakeholders authentication to augment security management in vulnerable environment such as Internally Displaced persons (IDP) camp. This way, stakeholders can be properply identified and managed. The proposed system will be evaluated by testing on database after a good number of fingerprints and face images of stakeholders have been enrolled. Subsequently, matching modules will be run to check performance. It is believed that equipping IDP camp where there are high chances of invaders, for sexual abuses and other social vices with multibiometric metric system by taking record of number of persons in such place, will provide robust security system with easy tracking of an intruder and will also ensure adequate sharing and management of resources and intervention aids within the camp.**

Keywords-: **Authentication, Face features, Fingerprint, Identification, Multimodal biometric, Vulnerable location**

I. INTRODUCTION

The world as a complex place has been impacted today by increasing use of technology to advance security in homes, communities, cities, companies, and over information and communication technology device. As it is today, it will be much difficult to authentically identify a person who is in an online interaction or transaction occurring hundreds of thousands times per day using conventional methods. These conventional methods or older identity authentication methods such as keys, personal identification numbers (PINs) badges could easily be lost, forged or stolen thereby resulting to false authentication and resulting implications [1]. Certainly, these conventional methods are not reliable [2]. Rather than depend on such older methods of obtaining someone's identity, which rely on external objects or memorized codes, a method of human anatomical characteristics have been proposed in literature and in practice. This method of using human anatomical characteristics to automatically recognize and analyze biological and behavioral traits and patterns for the purpose of identity authentication is called biometrics.

Biometric is defined in [3][4] as automatic recognition and analysis of individuals based on their distinctive physical and other traits, for example fingerprints, DNA, irises, voice patterns, facial patterns and hand gesture. The technique involves obtaining biological as well as behavioral biometric characteristics during a process called enrolment by using specialized sensors and peculiar feature extraction algorithms to generate and store biometric template [3]. As a result of its tremendous accuracy and speed, biometric technology has become a viable alternative to conventional methods of identity authentication [2]. A biometric technology can quickly recognize and analyze biological as well as behavioral features of human. During the process of recognition, anatomical features serving as query biometric inputs, are compared against data set (or stored template) of approved or disapproved persons so as to either grant or deny access using matching algorithm [1][3].

A broad and most general definition given by Gad et al [1] is that biometric system as automated methods of verifying and / or recognizing the identity of human being based on the categories:

i. Physiological biometrics such as facial, hand and hand vein infrared thermo gram; odor; Ear; hand and finger geometry; fingerprint, face, retina, Iris, palm print, voice, and DNA [6],
ii. Behavioral biometrics which comprises gait, keystroke, signature that detect the human actions [7] and
iii. Human electrocardiogram (ECG) signal which is considered as one of biometric traits employed in recognition and authentication of person [8]. The latter category has been coined and referred to as behaviour-metrics to describe it by some researchers [9].

As an identity authentication system for secured access and permission, Biometric has been evolutional and gaining wide spread acceptance. However, no single biometric system is sufficient enough as each has its pros and cons [10]. In fact, any recognition based on the use of one modality (unimodal system) may probably not be sufficiently robust or may not be acceptable to a certain user group or in a specific situation or instance [11]. This highlights the need to combine various modalities together to realize systems that are more reliable and accurate.

Unimodal biometric system use single biometric trait for identity authentication or recognition purposes. They are subject to many practical problems such as non-universality noisy sensor data, intra-class variation, restricted degree of freedom, unacceptable error rate, failure to-enroll and spoof attacks [11]. This can be achieved by the techniques of multimodal biometric system which offer a feasible method to solving the problems that are associated with unimodal biometric system [11][12]. The multimodal biometric systems use various biometric traits or modalities at the same time to authenticate the identity of a person [11][13].

The combine biometric traits methods give better performance with respect to false acceptance and false rejection rate [10]. The system's accuracy increases geometrically. Also, when compared to a unimodal biometric system, the requirements for storage, the time for a multimodal biometric system is higher [10][14]. The important processes associated with multimodal biometric system are acquisition of image, extraction of feature, fusion and matching. An effective fusion scheme determines the success of multimodal biometric system. There are various levels for performing fusion. These includes, as outlined in [15][10]: a). Fusion at the data or feature level, b). Fusion at the match score level, c) Fusion at the decision level.

Biometric systems were initially made available in the 1970s for law enforcement agencies for identifying criminals through fingerprint recognition [16][17]. However, with the increased threats to buildings or rooms containing information technology (IT) infrastructures, documents filling etc [17], advances have been made recently in the areas of biometric technologies. This has increased the applications of biometric systems into the physical and logic control domains [4] [16-19].

Physical access control ensures that only authorized persons have access to vulnerable places, building or rooms etc. Also for logic access controls, protection of the computers, network facilities and information systems from threats of unauthorized access [17] is ensured. Biometric systems have also been implemented due to cost reduction of device [19]. These technologies can be applied at various levels which include public (or national) or private (corporate) domain. Besides, they can be incorporated within an individual customer's goods [17]. As an example, the Nigerian voter's card provided by the Independent National Electoral Commission (INEC) uses the fingerprint biometric technologies to identify and authenticate eligible voters. In addition, the National Identity Management Commission (NIMC) which provides national ID card ensures that a person's identity and citizenship can be ascertained or verified based on fingerprint. Also, the use of such applications has been deployed in the Nigerian banking sector where customers are made to provide their identity through biometric verification to secure their Account numbers in different banks to a common database through bank verification Number (BVN). In the United States (US), entrances into its nuclear power plants are only allowed based on hand geometry recognition [19][17]. Also, in Nigeria, the National Youth Service Corps (NYSC) scheme requires the corps members to undergo biometric identification process based on fingerprint technology that helps to identify and fetch out irregular members.

There is difference between the various biometric system based on the underlying technologies complexities and performance [17-19]. Every biometric technology has its strength and limitations, and the choice depends on the application [20]. As such it is usually difficult to have a biometric technology that meets all technical requirements [17]. Hence, in deploying a biometric system, a comprehensive study on the performance trade-off and risk management is essential in information security policy and decision making before and during implementation. The main objective of a trade-off analysis [17] is to ascertain the requirement of the security access control applications so as to assist in identifying the right biometric solution. Also, the challenges of technical design and operation identified in the risk management analysis help in defining additional or alternative security control for effective information security governance [17][21].

This paper reviews biometric system and projected a strategy that will enhanced and strengthened security management and to extension adequate sharing of resources managing people in vulnerable environment especially internally displace persons (IDP) camps.

II. Overview of biometric systems

In order for a biometric system to be practical and reliable, it should satisfy the requirements/characteristics specification [5][22] [23]

a) Universality (availability): Each individual should possess the characteristics. Availability is determined by the "failure to enroll" rate.
b) .Distinctiveness: It states that any two persons should sufficiently possess different characteristics. It is determined (or measured) by the False Match Rate (FMR), which is also called "Type (II) error".

c) Permanence (robustness): It is expected of the characteristics to be stable (with respect to the matching features) for a given period of time. A measurement of robustness is the False Non-Match Rate (FNMR) also known as “Type (I) error”.

d) Collectability (accessible): This characteristic is measured quantitatively and easy to image using electronic sensor. It can be quantified by the “through put rate” of the system.

e) Performance: This means achieving recognition accuracy, speed, and the resources required to the application.

f) Acceptability: It means that the population of particular user and the public in general, should have no objections to the measuring/collection of the biometric characteristic. In fact, the acceptability of a biometric system is a measure of rolling carryout on the device users.

g) Resistance to circumvention: It means testing and proving how the system can withstand fraudulent techniques easily.

No one single biometric trait is best. Each of the biometric features has its strength and limitation and the act of choosing which to use depends on the application. Also, each biometric characteristic can be used in authentication and/ or identification purpose [24][5]. A surprisingly difficult task is predicting the “false acceptance” and “false reject” rates, system throughput, user acceptance, and cost saving for operational systems from test data [5]. Similarly, it is impossible to state that a single biometric modality will be sufficiently robust for all application, or be acceptable to a particular user group or in particular situation or instance [11].

A. Basic Structure of Biometric System

In a biometric authentication system, there are five major components [26]: Sensor feature extractor, template database, matcher, and decision module. Figure 1 shows the basic structure of a fingerprint recognition system which is the same for all such system [1]. Also, Fig. 2 shows the components of a biometric system whose operation according to Ahmad et al. [17], mainly involves two phases namely enrollment and recognition [19][26].

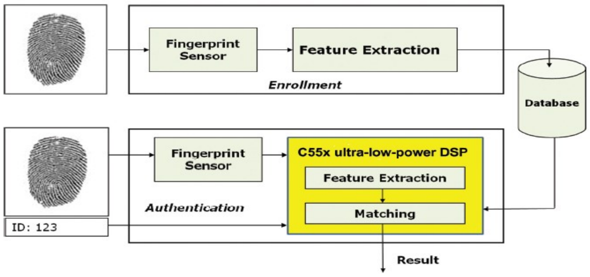

Fig. 1 Block diagram of fingerprint recognition system [1]

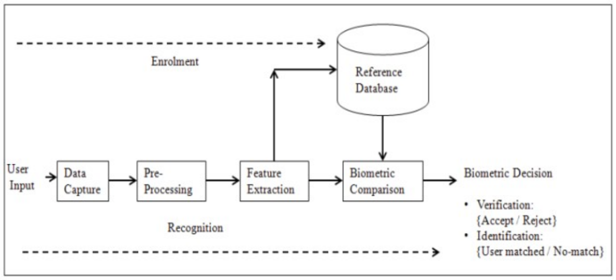

Fig. 2 Components of a biometric system [17]

On the other hand, Borkar [1] opined that a typical biometric system is comprised of four major subsystems; sensing, feature extraction, template matching and output.

a) *Sensing:* The sensing or input element is a sensor that interfaces between the user and the biometric system. It scans and captures the biometric traits or characteristics of the user and the converts the captured imaged into Digital information [1][25]. The sensing device might in corporate a camera, CMOS or optical sensor, or a high-performance charge couple device (CCD) of the Texas Instrument (TI) [1]. It might use a microphone in the case of voice-based identification systems while other types of sensing device like thermal and capacitive sensors could be used as well in other applications.

b) *Feature Extraction:* The scanned and captured biometric data is processed by the feature extraction module. Many of the authentication systems are based on computationally complex algorithms like image and voice processing, and as such the needs for the system’s processing capacities can be a challenging task. During the feature extraction stage, the processor extracts the salient information (feature set) from the sensor, for example, the image of a face during a facial scan [1][25] that helps to distinguish between various users. That is, the feature extraction module (or processor) extracts data points to generate a “template” or a model of the user’s unique biometric traits. In some other applications, a quality assessment module which determines whether the scanned biometric trait sufficiently qualify for further processing is ensured before the feature extract or, during enrollment, the extracted feature set is stored in a database as a template indexed by the user [27].

c) *Template matching*: In application such as access control, for example, the biometric system might compare the template of a fingerprint presented at an authentication station with those stored in a database of templates of users who are granted access [1]. In a situation that the template is not in the database, the user cannot be identified and is not allowed access. Data storage depends on the size of the database, and it can be achieved in solid state memory located in the authentication station, which is either integrated with the digital signal processor (DSP) or external to it, or the database may be stored in a remote server that is accessible via a secured link of communication (B.

d) *Matcher and Decision Module (Output):* Once the matching template process has been completed by the biometric systems processor, that is, template search and comparison algorithms, it then gives output results. According to Borkar [1], based on the finding of the system, certain action is likely to occur. For instance, the output might be connected directly to a mechanical device which opens a door or the result might be sent via a wireless connection and displayed on a screen for review by a security agent. Consequently, maintaining the security of the template database is not a trivial issue, since it could be geographically distributed and with millions of records contained therein. The matcher module, which is usually on executable instruction that accepts two biometric feature sets (from the template and query, respectively) as input and output [25], and establish a match score showing the similarity between the two sets. At the end of decision module generates the identity decision and then initiates a response (output) to the query.

B. Common Single Biometric System

1) Fingerprint biometric:

The applications of fingerprinting matching were the first and still are the most commonly used biometric system [1]. Fingerprint is the pattern of ridges and valleys on the tip of a finger [9] that is deployed for identity authentication of person or group of persons. It has become the most common and popular recognition method because of its distinctive universality, permanence, uniqueness, accuracy and low cost [1][9] and as such has been seen as a relatively simple method and the leading biometric technology.

According to Maltoni et al [28] and Mahesh and Govindarajulu [9] there is an evidence of archaeological study that Assyrians and Chinese ancient civilizations have deployed fingerprints a form of identification since 7000 to 6000 BC. Today, fingerprint recognition techniques can be broadly categorized as Minutiae-based, Ridge Featured-based, correlation-based and gradient based. With the majority of the automatic fingerprint authentication and identification systems using methods based on minutiae points [9]. Fingerprint biometric systems offer some advantages such as very high accuracy, economical, widely developed biometrics, very user friendly (easy to use), small storage space for biometric template (database), and standardized.

2) Face Biometric:

The face recognition as a biometric trait serves as an important alternative for choosing and developing an optimal biometric system [9]. It does not require physical contact with an image capturing device like camera and this is advantage. A face authentication or recognition system requires no advanced hardware as it can be used with existing image as it can be used webcams etc. Hence, it can be considered as a major alternative in the development hybrid biometric systems.

Quite a number of techniques have been proposed and presented in literature for face recognition. Such algorithms or techniques can be categorized into; geometric feature-based and appearance-based.

3) Iris biometric:

The iris is well protected thin circular diaphragm and the colours part which lies between the rear of the cornea and the lens of the human eye. Iris recognition technique identifies a person by mathematically analyzing the peculiar pattern of the iris and matching (making comparison) with an existing database template. The overall performance of iris biometric system is determined by the accuracy of conversion of iris features into iris code [2]. However, identity recognition in iris biometric is significantly affected when scanning images are not perfect as a result of lightening motion, blur, or even physical problems like occluded irises, etc [9]. Some drawbacks associated with iris biometrics are intrusive, requiring large (or many) storage (or memory) for data, more experience etc.

4) Other biometric:

All the single biometric characteristics discussed so far are unimodal system and are relative economical and less expensive. There are other common biometrics that are reliable but expensive. These are: Palm-print, DNA and Retinal scanning. There are also others like voice and signature that are less expensive but without much dependable [9]. An ill health such as a cold can change a person’s voice; this will render absolute authentication difficult or impossible. Signature authentication is developed to identify people based on the traits of their peculiar or unique signature. Due to this, users who do not sign their names in a consistent manner may have difficulty enrolling and authenticating in signature authentication [9].

So far the various unimodal biometric systems have been discussed. The next is to look at the limitation of the limitations of unimodal biometrics.

C. Limitations of Single Modal Biometrics

Single modal (unimodal) biometrics systems are known to have associated limitations. For instance, the Iris recognition suffers from certain problems such camera distance, eyelids and eyelashes occlusion, lenses and reflections [7] [29][30][5].

The face recognition suffers from the effect of face changes, overage and instability and twins face features similarity. Also, fake faces from mobiles as examples and masks use in attacking system [5] impact seriously on face recognition. For the case of fingerprint, the fingerprint may have some cuts, burns and small injuries temporary or permanent. More so, there are fake fingers made from gelatin and /or silicon a capable of attacking the fingerprint based recognition system. Cold can change a user's voice and thereby leading to voice problems and tape recording may be used for system hacking purpose [9][31].

The DNA includes sensitive information related to individuals' genetic and performing the test is quite an expensive exercise. Hand geometry cannot be used for a large population because it is not distinctive enough. Hence, it is not suitable for the purpose of identification [32].

Gait is sensitive to body weight and unstable. It is not employed for large population and not reliable enough [5].

Signature biometric is not universal and varies with time. Offline (static) signatures can be forged, while online (dynamic) signatures cannot be used in critical application for documents verification (such as governments' documents and bank cheques).

Generally, recognition based on any of the above biometric traits alone cannot guarantee perfect or sufficient robust recognition performance [5][11]. Also, the biometric system (either an authentication system or an identification system) is vulnerable to the outrider or unauthorized person at various locations [33][5]. Hence a more improved system that is less disadvantageous and more reliable is a combined multiple modalities.

Since the unimodal biometrics depends on the evident of single source of information for authentication, they may not achieve the desired performance requirements because of the error rates they have [23][34]. These systems are generally prone with the following drawbacks:

a) *Noise in sensed (collected) data:* defective or improperly maintained sensor (for example, accumulated dirt on fingerprint sensor) may produce deformed and noisy data leading to error in matching [5][35]. This could be as a result of injuries, voice changes as a result of cold or illness, wearing of glasses which alters iris recognition performance, poor illumination in face sensing, positioning during capture and faulty sensors [5][35-37].

b) *Distinctiveness:* This problem is categorized into intra class variation arises when a user incorrectly interacts with the sensor for example; the physical make up or incorrect facial pose of the user like wrinkles due to ageing, grown beard or hair the face and other facial expression render single trait biometrics less reliable [5][35]. On the other hand, inter-class variation arises due to similarity (overlap) in the feature sets of multiple users. For instance, when there is no significant difference between two persons, the false match rate (FMR) increases.

c) *Spoof attack:* It means the use of false biometric trait to gain access by faking the biometrics of the authentic or authorized user. As stated in [5], artificial fingers/fingerprint can be employed to spoof the authentication system. This type of attack is readily common using behavioural traits.

d) *Non-Universality:* It is the inability of the unimodal biometric system to acquire meaningful biometric data from a population of users due to deficiency in some of biological traits, physical; abnormalities and culture [5][35]. For instance, a reasonable percentage (say 6%) of the population of users to be enrolled may have sears or cuts in fingerprints. This may lead to the extraction of incorrect minutiae features from them.

The limitations and drawbacks of single trait biometrics have been discussed so far. The single trait (or unimodal) biometrics also suffer some other drawbacks such as insufficient population coverage, lack of individuality, lack of invariant representation, and susceptibility to circumvention [5][38]. These problems or drawbacks cause higher False Reject Rate (FRR) and False Accept Rate (FAR) [6][22][39].

D. Multimodal Biometric Systems

These systems make use of more than one biometric traits simultaneously to authenticate a user identity [11][13][35]. It has become an emerging due to the fact that more than one biometric trait are combined to study the recognition and authentication performance of multimodal system. The attraction of research study and subsequent implementation for practical purposes is due to increase in identification/authentication speed and accuracy that multi-biometric offer some drawbacks associated with unimodial biometric system have been taken care of by the use of multimodal biometric system [5][35][40]. The benefits offer by multimodal systems over unimodal systems are discussed as follows:

a) *Accuracy of Recognition:* When compared to the unimodal biometric system, multimodal biometric system has better accuracy [41]. It is expected of the multimodal biometric system to more accurate and reliable as a result of the multiple, biometric traits independency, and difficult to forge all of them ([6][34]. As the combined biometric identifiers provide some additional evidence about identity authentication claim, more confidence in result can be guaranteed. For instance, similar signature patterns may be possessed by two persons, in which case, the signature verification system will produce large False Accept Rate (FAR) for that system [5]. Addition of face recognition system with the signature verification system may eliminate the problem and reduce the FAR [5][14]. According to Gad et al [5], experimental results have shown that the accuracy of multi-biometric can reach near 100% in identification.

b) *Privacy:* Multi-biometric improves resistance to certain type of vulnerabilities. The template of biometric system is prevented from stolen as at the time it stores the two characteristics of biometric system in the database [5][43]. Spoof attacks would be more challenge for attacker due to many different biometric identifiers.

c) *Enrollment of Biometric Data:* Multimodal biometrics can solve the problem of non-universality. In a situation where a particular biometric data is unavailable or is of poor quality, other biometric identifier of the multimodal biometric can be employed to capture data. It makes better system operation [41]. Multi biometric is known to provide universal coverage and improves matching accuracy [6][44].

There are basically two categories of multimodal biometric systems; synchronous and asynchronous. The synchronous category is such that two or more biometric combined within a single process of authorization. In the case of asynchronous system, two biometric technologies in sequence (that is one after the other) are used [5][45]. However, multimodal biometrics can operate in three different modes [5][34]:

i. *Serial Cascade Mode:* In this case, a modality is examined before the modality is investigated. There is the possibility of the overall recognition duration to decrease as the total number of possible identities before using the next modality could reduce [5].

ii. *Parallel Mode:* This mode of operation is such that the data sensed or captured from multiple modalities are employed in concurrent way to perform recognition. The results are then combined for making final decision.

iii. *Hierarchical Mode:* The classifiers are combined in a hierarchy-tree like-structure. This mode is preferred when expecting a large number of classifiers.

The multimodal biometric system uses more than one biometric trait for recognition and authorization purposes. Recognition systems employing multiple biometric traits are designed to operate in one of the integration scenarios as follows [5]:

a) *Multi Sensor System:* More than one sensor is employed for extracting data from individuals. For example, using a thermal infrared and a visible light camera to capture the face or using an optical and a capacitive sensor to capture the fingerprints [46][35].

b) *Multi modal:* Here, more than one physiological and behavioral trait is used for identification of users. Example, information obtained using face and voice features or others can be integrated to establish the identity of the user [5][45]. It requires multiple sensors with each sensor sensing different biometric traits and such this making can make it to be more costly.

c) *Multi-Instance System:* This is case whereby multiple instances of biometric characteristics are captured. For example, images of the left and right irises can use for iris recognition. Also, multiple instances of index finger the physiological or behavioral trait such as left and right index finger, may be combined.

d) *Multi-Algorithm systems:* In this process, more than one algorithm is used for feature extraction to improve the matching and recognition performance. Example is using principal component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminant Analysis (LDA) for facial feature extraction [35].

e) *Multiple Sample System:* This method uses multiple samples of the same biometric trait for individual enrollment and recognition. For example, in the process of using frontal face, the left and right profiles are also captured. Multiple impression of the same finger and multiple samples of a voice can be combined.

Despite the fact that multi-biometrics have proven to be more promising than unimodal systems, some limitation still exist such as noise in the biometrics like scratches in the fingerprint and lens mark in iris that can lead to increase False Reject Rate (FRR) [5]. In multi-biometrics, failure of one biometric will result to the whole system failing [47]. Also, multi-biometric system may be more expensive and complicated as a result of the additional hardware requirement and matching algorithms required. There is a greater demand for computational power and storage [42]. Current research has shown the essence of multi-modal biometrics systems in enhancing network security to people. However, it requires more efforts and research to overcome some types of attacks like spoof attack, substitution attack, Trojan horse attack, transmission attack, template database attack and decision attack [5][24]. Figure 3 shows the different types of multi-modal biometric systems.

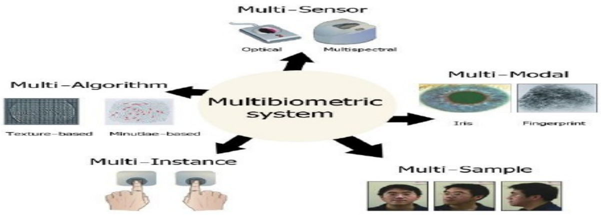

Fig. 3 Different types of multi-modal biometric system [23]

E. Abbreviations and Acronyms

The performance of a biometric system can be measured in two main phases, which are enrollment and recognition/authentication [17] [26] [19]. The various quality performance measurement of a biometric system helps in comparing systems and motivating the progress [31]. Jain et al. [4] has outlined the recognition accuracy of a biometric system based on performance measurement to include: False Reject Rate (FRR) and False Accept Rate (FAR) [5][16][17]. The most common performance metrics of biometric systems are briefly discussed below [4][5].

a) *False Reject Rate (FRR):* This is also known as Type I error or False Non Match Rate (FNMR) [18][19][26]. It describes the likelihood that a legitimate user is rejected by the system [17]. In other words, it gives an emulous interpretation of two biometric measurements from the same persons such that it appears that they are from two different people as a result of large intra-class variations. Ti is measures of the percentage of valid inputs being rejected [5]. The FRR is defined given by Eq. (1) [5][41]:

$$\%\mathrm{FRR} \quad = \frac{\mathrm{T_{Greject}}}{\mathrm{T_{Gsubmit}}} \times 100 \qquad (1)$$

where $\mathrm{T_{Greject}}$ is the total number of genuine test pattern rejected, and $\mathrm{T_{Gsubmit}}$ is the total number of genuine test submitted to the system in order to achieve good performance, FRR must be low.

b) *False Accept Rate (FAR) or False Match Rate (FMR):* This entails mistaking the biometric measurements obtained from two different individuals as if they are from the same person as a result of inter-use similarity. It is a measure of percentage of invalid matches. The FAR is expressed by Eq. (2) [5].

$$\%FAR = \frac{T_{Faccept}}{R_{Fsubmit}} \times 100 \qquad (2)$$

where $T_{Faccept}$ is total number of forgeries accepted and $R_{Fsubmit}$ is total number of forgeries submitted to the system test. In a good authentication system this rate must be low [5]. The average of the FRR and FAR is called the Average Error Rate (AER) [5].

c) *Genuine Acceptance Rate (GAR):* It is sometimes used as biometric performance measurement. It is the percentage of the likelihood that a genuine individual is recognized as a match [7]. A valid user GAR can be obtained Eq. 3 [5]:

$$\%GAR = 1 - \%FRR \qquad (3)$$

d) *Equal Error Rate (EER):* It is used summarize the biometric system performance that is defined at the point where FRR and FAR are equal. Biometric system with the lower EER, is the more accurate and precise [5][42]. The ERR is also called the Type (III) error.

e) *Failure to capture (FTC):* It is also known to in biometric literatures a failure to Acquire (FTA) Rate [17]. FTC represents the percentage by which the biometric device fails to automatically capture a characteristic correctly when presented [5]. This often occurs when system deals with a signal of insufficient quality [41].

f) *Failure to enroll rate (FER or FTE):* It represents the number of times in percentage a user cannot enroll in the recognition system [5]. It is used to measure the universality aspect of a biometric system, is a figure that shows the cost effectiveness of a biometric system [17].

g) *Template capacity:* It is the maximum number of data sets that can be input to the system [5][41]

The performance metrics discussed are usually represented using graphs such as Receiver Operating Characteristic (CMC), Score Histogram (SH) and Cumulative Match Characteristic (CMC)[5] [14]. The ROC graph is obtained by plotting the values of FAR against FAR at various operating points on a linear or logarithmic or semi-logarithmic curve [5]. Detection Error Trade off (DET) is a common variation, which is obtained via normal deviation lies on both axes [5][41].The CMC is used to summarize the identification [5]. The SH curve on the other hand, plot the frequency of the scores for matches and non-matches over the match score range [5].

F. Multimodal Biometric Fusion

In order to support the advantages and reduce the draw backs of the single biometric trait, multimodal biometric fusion combines the distinguished trait from different biometric features [34]. The basic concern of information fusion is to selection of technique for carrying out the fusion.

The objective of fusion is to come up with an appropriate function which can optimally combine the information given by the biometric subsystem [5][7].

The fusion scheme in multimodal biometrics can be classified as sensor level, feature level, match score level, rank level and decision level [5][22] as shown in Fig. 4. The process can be subdivided into two main categories as presented in [5][14]: prior to matching fusion and after matching fusion. Figure 5 shows these fusion level possibilities at each module. The hybrid fusion is achieved by mixing two or more of these fusion levels.

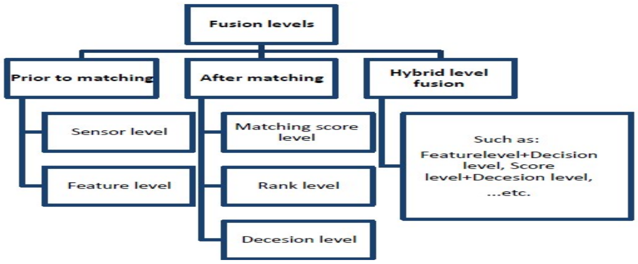

Fig. 4 Different fusion levels [5]

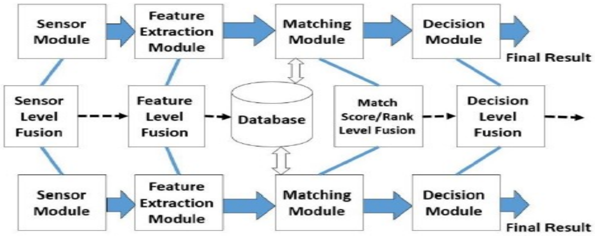

Fig. 5 Prior to matching and after matching fusion levels related biometric system modules [5][14]

1) *Before matching fusion:*

In this category fusion combines evidences before matching. Classification in this aspect can be achieved considering two different categories as follows:

Sensor level fusion: in this case, multiple sensors are used multiple snapshots of the same biometric trait are taken using a single sensor [35]. The concept is that a new biometric data is generated by combing raw data taken from multiple sources. Then, a trait can be obtained (or extracted). A single sensor or different compatible sensors such as fingerprint, iris scanner, etc., represents the samples of the single biometric trait sensed [5][39].

Sensor level fusion can be useful to multi-sample system that captures many snapshots of sample biometric. It has a lot of information when compared to other types of fusion [5]. It is estimated to enhance the recognition accuracy. The problem of noise in sensed data due to improper maintenance is solved in sensor fusion [22].

Feature level fusion: in this case, different biometric algorithms are fused together to extract a simple feature by applying normalization, transformation and reduction techniques [35]. The feature sets which are correlated are extracted from multiple biometric modalities and are fused by employing specific algorithm to form a composite feature set that is passed to the matching module [5][32][34]. This takes place after normalization, transformation and reduction schemes [14]. The objective of feature normalization is to modify the location (mean) and the scale (variance) of the feature value via transform function so as to map into a common domain, etc. [5]. To reduce the dimensionality of the feature set, transformation or feature selection algorithm is used for example, sequential forward selection, sequential backward selection, principle component analysis [23].

Final feature vectors can either be uniform (Homogenous) or non-uniform (heterogeneous) [5]. The feature sets are from different algorithms and modalities, and as such, the combination of feature set may have some problems [34][39][5]. In established relationship between the features of these biometric systems must not be well known, and features of structurally incompatibility are common. Also, concatenating two feature rectors might cause dimensionality problem [22].

2) *After matching fusion:*

Prior to matching fusion sometime do not involve modalities [5]. Also, data set fusion is more complex, and it is not good to neglect any data [39]. After matching fusion can be classified into three categories:

Matching score level fusion: In this case, feature vectors extracted individually (that is separately generated for each modality) are compared with the templates enrolled in the data base for each biometric trait so as to generate the match scores [5][34]. Composite matching score (single scalar score) is created by fusing the output set of match scores [5][22]. This fusion technique is also called confidence level or measurement level fusion. Different methods such as density, transformation, and classified base score fusion are used to achieve this fusion level [39].

In using or combining of match scores, score nominalization is required by converting the scores into common similar domain or scale. This is done because the matching scores cannot be used or combined directly due to the fact that these scores are from different modalities and based on different scaling methods. The score normalization can be performed with different techniques such as piece wise linear normalization discovered by Slobodan Ribaric and Ivan Fratric [5].

Fusion application at this level is preferred as it is easy to acquire and fuse matching scores of different biometrics [5][6]. It offers best set of information about the biometric data [5]. Nevertheless, complexity is more [39]. Much work has been done using matching score level fusion. According to Gad et al [5], it is the most studied fusion method so far which takes a look at the similarity/distance score for fusion. However, the similarity/distance score are required to be normalized before combining because they can be in different ranges [42]. The choice of inappropriate normalization method results to very low recognition performance rate [22]. For example, the match score generated by the face, fingerprint and hand modalities of a user combined via the simple sum rule to obtain a new match sure, after which it is used for making final decision [5][7].

Rank level fusion: In this fusion method, every classifier associates a rank with each enrolled trait to the system (a higher rank is an indication of good match). Many single trait biometric matcher outputs are consolidated and a new rank that would help in estimating the final decision is determined [22][34]. Generally, the rank level fusion is used for identification rather than verification (or authentication) [5]. The working procedures are carried out as follows: first, generate a rank of identities sorted with all modalities; secondly, by the help of any fusion method, each available individual ranking for different modalities are fused. Finally, the lowest score is the correct identified one [5][39].

Decision level fusion: The final decision in multimodal biometrics is formed from decision obtained from independent decision of different biometric modalities using different methods which include behaviour knowledge space, majority voting, weighted voting, AND rule, and OR rule [7][5][34]. This fusion level is also called abstract level because it is used when there is access to only decisions from individual [7][39].

The method mostly used for decision level fusion is the majority voting. The input sample with agreed in majority of matchers is given the identity. AND/OR rules are rarely used because they combine two different matchers, so this sometimes degrade performance of the system [5]. AND combination improves the FAR while, OR combination improves the FRR [5]. The main benefit of the majority voting method is that no prior knowledge about the matcher is required and it does not require training for final decision making [5][48].

Decision level fusion techniques are well studied for biometric systems unlike rank level fusion. However, decision level fusion techniques are not too flexible due to limited amount of information, which can lead to the possibility of having a tie [5][22]. It only considers single information for fusion, which has a high chance of producing enough recognition result [7][34]. Since it has a less amount of features or scores information of different modalities, it is very easy to implement [39]. This fusion level is less preferred in multi biometric system implementation

3) *Hybrid level fusion:*

Tri-level fusion cases (different fusion in different levels of the system) can be studied to make the system faster and significantly reduce the error rate. The fusion of level increased the performance [5]. Previous studies have been carried out regarding this fusion level. Lupue et al [49] combined fingerprint, voice and iris, Asha et al [38] combine fingerprint, with mouse dynamics. Panda et al [50] studied the use of parallel feature Extraction with the help of SIFT, SIMD and HMA methods to fuse multiple iris. Fuzzy vault has been used to implement multimodal system based on face and ear traits. Some other previous studies on level fusion can be obtained in [51]-[54].

III. IMPLEMENTED MULTIMODAL BIOMETRIC TECHNIQUES

Mahesh and Govindarajulu [9] studied biometric hybrid system based verification. A hybrid biometric system that uses Fingerprint and face biometrics was proposed considering such factors like ease of use, use convenience, reliability and costing. It maintained that the proposed biometric system efficiency was evaluated by testing on database after on rolling good numbers of fingers, face images. It suggested that the system be test and evaluated on large database. However, in this work, in developing the finger print, two minutiae sets were used for the matching algorithm. Authentication in this method may fail due to the presence of noises in test images. Also, the efficiency of the proposed biometric system is in doubt considering the database used and the fact that no specific area of application was mentioned. Biometric system performance may vary with respect to locations and function of principals. Hence there is need to design them considering the area of application(s).

Stefani and Ferrari [20] presented design and implementation of a multi-modal biometric system for company access control. The main focus was on authentication and its use in a real content within a company security system for regulating the main access and the movement to the different locations inside the company. Two biometric traits which consist of face and iris were chosen for the developed system. The face trait used a technique based on local Binary patterns histograms for recognition, while the iris data analysis was carried out using the Daugham's method. It used a post classification method as its fusion methodology, which then follows the OR rule. The system test evaluation was conducted using AT and T face database and UBIRIS database of irises. However, it maintained that despite the fact that the proposed system was to form a general prototypical system to be implemented in most different contexts, more study is required in order to design proper# strategies that would cope with partially conflicting behaviours. The issue with this work is the use of OR rules in the decision level fusion. This because OR rule combines two different matchers and this sometimes degrade the system performance Gad et al. [5].

Kaur and Singh [10] presented a novel biometric system based on hybrid fusion speech, signature and tongue. It used the Mel Frequency Cepstral Coefficients (MFCC) for feature extraction in speech and in signature feature extraction; Discrete Cosine Transformation (DCT) applied on signature database was used. For the tongue feature extraction, the Scale Invariant Feature Transform (SIFT) algorithm was used. It proposed a hybrid weighted order averaging function for the fusion of extracted features of tongue, speed and signature. For experimental propose, SVC2004 signature database was used f or signature biometric, CMU ARCTIC was used for speech database and pictures capturing digital camera for tongue database. In order to ascertain the accuracy of the system, features sample were collected separately for both noisy environment. In the case of noisy environment, Gaussian noise was added to the system to check the performance of the noisy environment. It maintained that the system record accuracy of 88.75% with 0.06% of False Acceptance Rate (FAR) and with 0.05% of False Rejection Rate (FRR) for non-noisy system.In the case of noisy system, the system recorded 0.05% of FAR and FRR 0.15%.

Atuegwu et al. [35] presented bimodal biometric students attendance system. The system uses student's faces and fingerprint to take attendance. The face feature database is achieved using webcam to capture student's faces. The capture image is preprocessed by converting the colour images to grey scale images, and the images were then normalized to reduce noise. The face feature extraction was carried out using Principal Component Analysis ((PCA) algorithm, while classification was achieved using support vector Machine (SVM). For the fingerprint, features were captured using a fingerprint reader. At the decision level fusion, the logic techniques (OR) was used to fuse the face and fingerprint feature extracted data. It maintained that the implemented system provided a minimum recognition accuracy of 87.83%. However, the short coming of the proposed system is the use of OR as decision level fusion sometimes degrades system performance (Gat et al, 2015).

Poh and Korczak et al. [55] proposed a new hydrid biometric person authentication system using face and voice features. The system is based on many levels of vectors and classifiers. For each of the biometric feature, an extractor, a classifier and a simple negotiation scheme was designed. A sequence of processing algorithms makes up an extractor. Information is extracted using wavelets. The extracted information, called vectors is classified using two separate multilayer perceptions. Simple logic negotiation scheme (AND operator), is used for combing results. The problem with this authentication system is that user's voice can change due to cold or ill-health. Also, the use of AND operator scheme at decision level fusion in multimodalities brings about the combination of different matchers which sometimes reduce the performance of the system.

Negar et al. [56] presented multi-biometric crypto systems based on feature level fusion. It stated that security concerns regarding the stored biometric data is hindering the wide spread public acceptance of biometric technology. The proposed system improved the recognition performance as well as the security of a fingerprint based biometric cryptosystem called fingerprint fuzzy vault. The designed system incorporated minutiae descriptors which capture orientation and frequency information in a multimedia environment, in the vault construction using the fuzzy commitment method.

Falohun et al. [57] designed an access control system using bimodal biometric. Iris and fingerprint traits were employed for gravity access through a secured door that only allowed authorized person(s). MATLAB was used to develop the instructional programme used to implement biometric door access control system. Voting techniques was used to fuse the biometric information from the iris and fingerprints.

Palaniappan et al. [58] considered in priory the feature stability and classification performance of bimodal brain and heart biometrics. Electrical activities obtained from the brain and heart was fused using binaural brain entertainment. It maintained that a greater stability and reliability was achieved from the fusion of the electrical signals coming out from the heart and brain periodically.

Madane and Thepade [59] studied score level fusion based bimodal biometric identification using Thepade's sorted n-ary block truncation coding with varied proportions of iris and palm traits. Iris and palm prints biometrics were fused and a new extraction technique was used to improve the accuracy and reduce the error rate.

Wójtowicz and Ogiela [60] presented a digital image authentication scheme based on bimodal biometric. A fusion of fingerprint and biometric was used to secure digital images. The biometric protection was applied to digital images in watermarks form. Independent component analysis was used to achieve the objective of the work.

Joshi and Kumar [61] considered the design of multimodal biometrics system based on feature level fusion. It fused the wavelet anchored face and signature biometrics. Hamming distance classifier was used for authentication.

Charfi et al. [62] studied bimodal biometric system for hand shape and palm print recognition based on SIFT sparse representation. Two hands shape and palm prints were fused at the feature and decision level by using cascade fusion. It stated that an improved result was obtained compared to the one obtained from existing work pervious work in literature.

Zapata et al. [63] investigated data fusion applied to biometric identification. It referred the state of the art in multimodal biometric with main focus on data fusion. Emphasis was laid on achievement and challenges associated with multimodal data fusion. Also, in Farmanbar and Toygar [64], fusion of features of the face and palmprint biometrics was achieved using match score techniques.

Having reviewed some multimodal biometric schemes proposed in literature for multi-biometric system by taking into account factors such as ease of use, convenience of users, reliability, costing and response time, a multimodal biometric system that combines fingerprint and face features technologies is being proposed for stakeholders authentication for access to facilities in Vulnerable environment such as Internally Displaced Persons (IDPs) camps. The proposed system will be evaluated by testing on database after a good number of fingerprints and face images of stakeholders have been enrolled. Subsequently, matching modules will be run to check performance results.

The general objective will be to develop a system that is required by stakeholders in vulnerable vicinity to manage the security and access control of users in and out of the area. It is desired to grant access to only authorized persons to certain locations in such a facility due to the vulnerability of such place. Specifically, similar systems have been developed and proposed in literature. However, their applications have been in different environment and the techniques of fusion have varied. Two-stage processing for minutiae extraction has been widely employed for fingerprint feature extraction. However, triplet of minutiae is intended to be used in the proposed system to reduce the matching error and improve response time. The Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) have been widely used in literature for face recognition. In the propose system, Locality Preserving Project (LPP) is intended to be used. The LPP preserves local structure of the face image space which is of more significant than the general structure preserved by PCA and LDA.

IV. PROPOSED MULTIMODAL SYSTEM

A. Resarch Design

The flow diagrams in Fig. 6 and 7 are fingerprint and face biometrics development pattern that describe the general feature extraction and authentication process. Figure 8 is a flow diagram of the proposed hybrid biometric system.

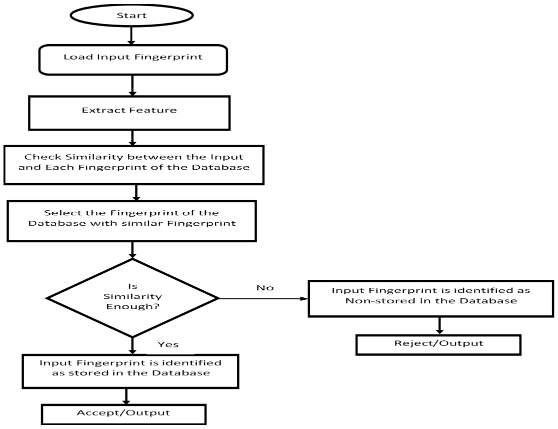
Start
Load Input Fingerprint
Extract Feature
Check Similarity between the Input and Each Fingerprint of the Database
Select the Fingerprint of the Database with similar Fingerprint
Is Similarity Enough?
No
Input Fingerprint is identified as Non-stored in the Database
Reject/Output
Yes
Input Fingerprint is identified as stored in the Database
Accept/Output

Fig. 6 Fingerprint matching recognition flow diagram

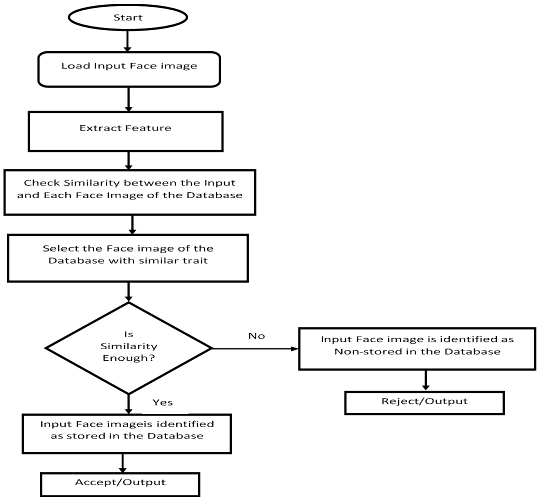
Start
Load Input Face image
Extract Feature
Check Similarity between the Input and Each Face Image of the Database
Select the Face image of the Database with similar trait
Is Similarity Enough?
No
Input Face image is identified as Non-stored in the Database
Reject/Output
Yes
Input Face imageis identified as stored in the Database
Accept/Output

Fig. 7 Face image matching recognition flow diagram

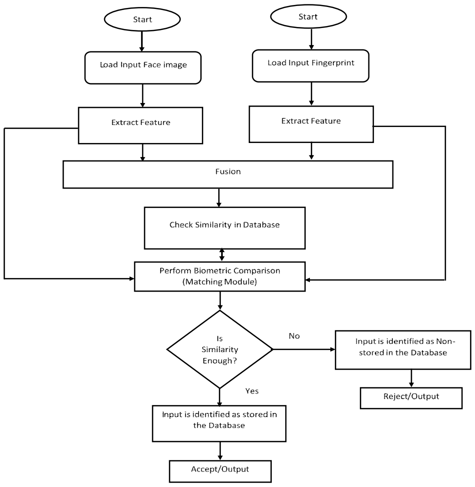
Start
Start
Load Input Face image
Load Input Fingerprint
Extract Feature
Extract Feature
Fusion
Check Similarity in Database
Perform Biometric Comparison (Matching Module)
Is Similarity Enough?
No
Input is identified as Non-stored in the Database
Reject/Output
Yes
Input is identified as stored in the Database
Accept/Output

Fig. 8 Flow diagram of proposed multi-modal biometric

B. Research Method

The proposed system is hybrid biometric technology. It combines fingerprint and facial recognition technologies. Figure 9 shows the block diagram representation of the proposed hybrid biometric system. It is a MATLAB Graphic User Interface (GUI) based solution. It covers all the procedures of a recognition system. It registers stakeholders in IDP camp such as security agents, Non-Governmental Organizations (NGOs) workers, medical practitioners and other authorized persons; takes their schedule visitation to such place like IDP camp and store all information gathered in a database. The user details are to be stored on a well-developed MYSQL database that will be run on reliable and efficient server.

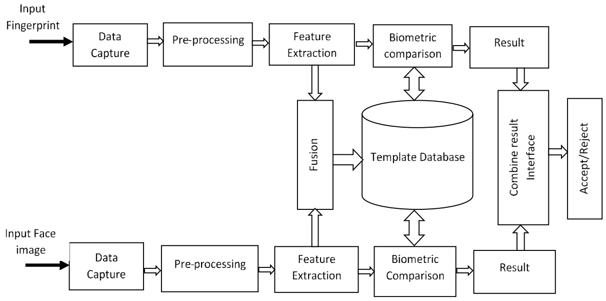

Fig. 9 Block diagram of the Proposed System

V. CONCLUSION

The paper has look at various biometric system. It has presented the strength and weakness of some schemes proposed and implemented in literature and in practice. However, the objective of this paper is to review literature on biometric system with greater attention given to multimodal systems and thereafter proposed a biometric system for user authentication that ensures that access to facilities is given to certain group of individuals in vulnerable environment. This has been significantly covered.

With security becoming a major problem around the world, certain environment and facilities within it such as Internally Displace Persons' (IDP) Camp, seem to be vulnerable. Application of biometric based authentication can ensure secured access control/permission within or around IDP camp and a well augment security through effective identity management. This will help health workers, Non-Governmental Organizations (NGOs), camp security personnel to manage and identify the authentic displaced persons. Secure access permission system for fingerprint privacy protection which combines different biometrics fingerprint and face recognition into a new hybrid system is proposed.

REFERENCES

[1] Borkar, M. (2012). User Identification Systems Leverage Smarter Biometrics Technologies. Texas Instruments, White paper, pp. 1-6.

[2] Manchalwar, A., Manchalwar, A., Inogle, H., & Barman, S. (2016). In's Recognition and Authentication using canny Edge Detection Technique with Hybrid Technology. International Research Journal of Engineering and Technology, 3(3), 1609-1612.

[3] Rampine, E.T.L., & Ngejane, C.H. (2016) a Brief Overview of Hybrid Schemes for Biometric Fingerprint Template security.In proceedings of the 2nd international conference on information systems security and privacy (ICISS P 2016), 340-346.

[4] Jain, A.K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Trans. on Circuits and System for Video Technology, 14(1), 4-20.

[5] Gad, R., El-Sayed, A., El-Fishawy, N., & Zorkay, M. (2015). Multi-Biometric Systems: A State of the Art Survey and Research Directions. International Journal of Advanced Computer Science and Applications, 6(6), 128-138.

[6] Singhal, R., Singhi, N., & Jain, P. (2012).Towards an Integrated Biometric Technique. International Journal of Computer Applications, 42(13), 20-23.

[7] Ross, A.A., Nandakumar, K., & Jain, A.K (2006). Handbook of Multibiometrics, 6, New York: Spring Science and Business Media.

[8] Singh, Y.N., & Singh, S.K. (2012). Evaluation of Electrocardiogram for Biometric Authentication. Journal of Information Security, 3(1), 39-48. doi:10.4236/jis.2012.31005

[9] Mahesh, N.K., & Govindarajulu, P. (2016). Biometrics Hybrid system Based verification. International Journal of Computer Science and Information Technology, 7 (5), 2341-2346.

[10] Kaur, G., & Singh, D. (2015). A Novel Biometric System Based on Hybrid Fusion Speech, signature and Tongue. International, 119 (7), 30-39.

[11] Selvi, S.M., & Chellam, J.A. (2017). Security and Privacy Aware Biometrics. International Journal of Engineering Technology Science and Research, 4 (8), 220-226.

[12] Frischholz, R.W., & Dieckmann, U. (2000). A Multimodal Biometric Identification System. IEEE Computer, 33(2), 64-68.

[13] Monrose, F., & Rubin, A.D. (2000). Keystroke Dynamics as a Biometric for Authentication. Future Generation Computer Systems, 16 (4), 351-359.

[14] Monwar, M., & Gavrilova, M.L. (2009). Multimodal Biometric System Using Rank-Level Fusion Approach. IEEE Transactions on Systems, Man, and Cybernetics, Part Bicybernetics, 39(4), 867-878.

[15] Ross, A., & Jain, A.K. (2004). Multimodal Biometrics: An Overview. Appeared in Proc. Of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224.

[16] Jain, A.K., & Kumar, A.M. (2010). Biometrics of Next Generation: An overview 1.1 Introduction.

[17] Mumtazah, S., Ahmad, S.W., Ali, B.M., Azizun, W., & Adnan, W.A. (2012). Technical Issues and Challenges of Biometric Applications as Access Control Tools of Information Security. International Journal of Innovative Computing, Information and Control, 8(11), 7983-7999.

[18] Jain, A.K., Ross, A., & Pankanti S. (2006). Biometrics: A tool for information Security, IEE Transactions on information Forensics and security, 1 (2), 125-143.

[19] Rhodes, K.A. (2003). Information Security: Challenges in Using Biometrics. US Government Accountability Office, 1-23

[20] Stefani, E., & Ferrari, C. (2017). Design and implementation of a Multi-Model Biometric System for company Access control. Algorithms, 10 (61) 1-10.

[21] Kim, S. (2007). Governance of Information Security: New Security Paradigm of Security Management. Studies in Computational Intelligences (SCI), 57, 235-254.

[22] Radha, N., & Kavitha, A. (2011). Rank Level Fusion Using Fingerprint and Iris Biometrics. Indian Journal of Computer Science and Engineering, 2(6), 917-923.

[23] Almahafzah, H., & AlRwashdeh, M.Z. (2012). A Survey of Multibiometric Systems. International Journal of Computer and Applications, 43(15), 36-43.

[24] Ahuja, M.S., & Chabbra, S. (2011). A Survey of Multimodal Biometrics. International Journal of Computer Science and Applications, 1(2), 157-160.

[25] Jain, A.K., Nandakumar, K., and Nagar, A (2008). EURASIP Journal on Advance in signal processing, special issue on Biometrics, 1-20.

[26] Prabhakar, S., Pankanti, S., & Jain, A.K. (2003). Biometric Recognition: Security and Privacy Concerns. The IEEE Computer Society, 1(2), 33-42. DOI: 10.1109/MSECP.2003.1193209

[27] Jain, A.K., Hong, L., & Pankanti, S. (2000). Biometric: Promising Frontiers for Emerging Identification Market. Comm. ACM, 91-98.

[28] Maltoni, D., Maio, D., Jain, A.k., & Probhakar, S. (2003). Handbook of Fingerprint Recognition. Springer, New York

[29] Feng. G., Dong, K., Hu, D., & Zhang, D. (2004). When Faces are Combined with Palmprints: A Novel Biometric Fusion Strategy. In Proc. Of 1st Int. Conf. on Biometric Authentication, Hong Kong, China, 701-707.

[30] Gad, R., Mohamed, M., & El-Fishawy, N. (2011). Iris Recognition Based on Log-Gabor and Discrete Cosine Transform Coding. Journal of Computer Science and Engineering, 5(2), 19-26.

[31] Karray, F.,Saleh, J.A., Arob, M.N., and Alemzadeh, M. (2007). Multi Model Biometric Systems: A stste of the Art survey. Pattern Analysis and Machine intelligence Laboratory, University of Waterloo, Canada.

[32] Delac, K., & Grgic, M. (2004). A Survey of Biometric Recognition Methods. Proceeding Elmar, 46th International Symposium, ELMAR-2004, Zadar, Croatia, 184-193.

[33] Bhatia, R., (2013). Biometrics and Face Recognition Techniques. International Journal of Advanced Research in Computer Science and and Software Engineering, 3(5), 93-99.

[34] Amirthalingam, G. (2013). A Multimodal Approach for Face and Ear Biometric Fusion System. International Journal of Computer Science Issues, 10(5), 234-241.

[35] Atuegwu, C., Okokpujie, K., & Noma-Osaghae, E. (2017). A Biomodal Biometric Student Student Attendance System. IEEE 3rd International Conference on Electro-Technology for National Development, NIGERCON, 464-471.

[36] Babu, K.G., & Rama Prasad, M.A. (2013).An Effective Approach in Face Recognition Using Image Processing Concepts. Conference Proceedings, 2(8), 215.

[37] Sonsanea, S., Thakura, S. Suthara, P., & Sisodiab, J. (2015). Automated Attendance System. International Journal of Innovative and Emerging Research in Engineering, 2(4). 65-69.

[38] Asha, S., & Chellappan, C. (2008). Authentication of E-Learners Using Multimodal Biometric Technology. International Symposium on Biometrics and Security Technologies, Islamabad, ISBAST, 1-6.

[39]]Meva, D.T. & Kumbharana, C.K. (2013).Comparative Study of Different Fusion Techniques in Multimodal Biometric Authentication. International Journal of Computer Application, 66(19), 28-32.

[40] Kaur, D., Kaur, G., & Singh, D. (2013). Efficient and Robust Multimodal Biometric System for Feature Level Fusion (speech and signature). International Journal of Computer Applications, 75(5), 33-38.

[41] Kalra, S., and Lamba, A. (2014).A Survey on Multimodal Biometric. International Journal of computer science and information Technologies, 5 (2) 2148-2151.

[42] Gavrilova, M.L., & Monwar, M.M. (2011). Current Trends in Multimodal Biometric System Rank Level Fusion. Pattern Rec,ognition, Machine Intelligent and Biometrics, ed. Springer, 657-673.

[43] Wagh, R., & Choudhari, A.P. (2013). Analysis of Multimodal Biometrics with Security Key. International Journal of Advanced Research in Computer Science and Software Engineering, 3(8), 1363-1365.

[44] Meraoumia, A., Chitroub, S., & Bouridane, A. (2012). Multimodal Biometric Person Recognition System Based on his and Palm-Print Using Correlation Filter Classifier Proceeding of the Second International Conference on Communications and Information Technology, Hammamet, Tunisia, 782-787.

[45] Deriche, M. (2008). Trends and challenges in Mono and Multi Biometrics. 2008 First Workshops on image processing Theory, Tools and Applications, 1-9.

[46] Mayhew, S. (2015). History of Biometrics. Available: http://www.bopmetricupdate.com/2015011history-of-biometrics.

[47] Geethanjali, N., & Themaraiselvi, K. (2013). Feature Level Fusion of Multimodal Biometric and Two Tier Security in ATM System. International Journal of Computer Applications, 70(14), 17-23.

[48] Jain, A., Mittal, P., Goswami, G., Vasta, M. & Singh, R. (2015). Person Identification at a Distance via Ocular Biometrics. IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015), Hong Kong, 1-6. doi: 10.1109/ISBA.2015.7126353.

[49] Lupu, C., & Lupu, V. (2007). Multimodal Biometrics for Access Control in an Intelligent Car. International Symposium on Computer Intelligent and Intelligent Informatics (ISCIII'07), Agadir, 261-267.

[50] Panda, A.C. (2011).Parallel Algorithms for Iris Biometrics.M.SC, Department of Computer Science and Engineering, National Institute of Technology, Rourkela, Odisha, India.

[51] Jain, A.K., Nandakumar, K., & Nagar, A. (2013). Fingerprint Template Protection: From Theory to Practice, In Security and Privacy in Biometric, Springer London, 187-214.

[52] Veeramachaneni, K. Osadciw, L; Ross, A; & Srinivas, N. (2008).Decision Level Fusion Strategies for Correlated Biometric Classfiers.IEEE Computer Society Conference on Computer Vision and pattern Recognition Workshops, Anchorage, AK, 1-6.

[53] Almayyan, W. (2012). Performance Analysis of Multimodal Biometric Fusion . De Montfort University, UK.

[54] Fathima, A.A., Vasuhi, S., Babu, N.N., Vaidehi, V., & Tressa, T.M. (2014). Fusion Framework for Multimodal Biometric Person Authentication System. International Journal of Computer Science, 41(1), 1-14.

[55] Poh, N., & Korczak, J. (2001). Hybrid Biometric person Authentication using face and voice features paper presented in the 3rd international conference, Audio and video-based Biometric person Authentication (AVBPA), Halmstad, sweder, 348-353.

[56] Negar, A., Nandakumar, K., & Jain, A.k. (2012).Multibiometriccrytosyterms Based on Feature-level Fusion. IEEE Transactions on information Forensics and Security, 7 (1), 255-268

[57] Falohun, A.S., Fenwa, O.D., & Oke, A.O. (2016).An Access Control System Using Bimodal Biometrics. International Journal of Applied Information Systems, Foundation of Computer Science-FCS, New York, USA, 10(5), 41-47.

[58] Palaniappan, R., Andrews, S., Sillitoe, I.P., Shira, T., & Paramesran, R. (2016). Improving the Feature Stability and Classification Performance of Bimodal Brain and Heart Biometrics. In Advances in Signal Processing and Intelligent Recognition Systems, Springer, Cham, 175-186.

[59] Madane, M., & Thepade, S. (2016). Score Level Fusion Based Bimodal Biometric Identification Using Thepade's sorted n-ary Block Truncation coding with variod proportions of Iris and Palm print Traits. Procedia Computer Science, 79, 466-473.

[60] Wójtowicz, W., & Ogiela, M.R. (2016). Digital Images Authentication Scheme Based on Bimodal Biometric Water making in an Independent Domain. Journal of Visual Communication and Image Representation, 38, 1-10.

[61] Joshi, S.C., & Kumar A. (2016). Design of Multimodal Biometrics System Based on Feature Level Fusion. 10th International Conference on Intelligent Systems and Control (ISCO), IEEE, 1-6.

[62] Charfi, N., Trichili, H., Alimi, A.M., & Solaiman, B. (2016). Bimodal Biometric System for hand shape and palm print Recognition Based on SIFT Spare Representation.

[63] Zapata, J.C; Duque, C.M; Rojas-Idarraga, Y; Gonzalez, M.E, et al. (2017). Data Fusion Applied to Biometric Identification. A Review in Colombian Conference on Computing, Springer, Cham, 721-733.

[64] Farmanbar, M., & Toygar, O. (2016). Feature Selection for the Fusion of Face and Palmprint Biometrics. Signal, Image and Video Processing, 10(5), 951-958.