# Multi-Modal Biometrics: Applications, Strategies and Operations

Iwasokun Gabriel[1] and Udoh . S[2]

[1] Federal University of Technology

*Received: 8 April 2015 Accepted: 2 May 2015 Published: 15 May 2015*

---

## Abstract

The need for adequate attention to security of lives and properties cannot be over-emphasised. Existing approaches to security management by various agencies and sectors have focused on the use of possession (card, token) and knowledge (password, username)-based strategies which are susceptible to forgetfulness, damage, loss, theft, forgery and other activities of fraudsters. The surest and most appropriate strategy for handling these challenges is the use of naturally endowed biometrics, which are the human physiological and behavioural characteristics. This paper presents an overview of the use of biometrics for human verification and identification. The applications, methodologies, operations, integration, fusion and strategies for multi-modal biometric systems that give more secured and reliable human identity management is also presented.

---

***Index terms***— biometrics, human identity management, human verification and authentication, security, multi-modal.

# 1 Introduction

iometrics refers to human characteristics and traits related metrics [1]. They are the distinctive, measurable and naturally endowed characteristics used to label and describe individuals. Any of the human physiological or behavioural characteristics is a biometric provided it satisfies some criteria that include universality, uniqueness, permanence, collectability, performance, acceptability and circumvention [2,3]. Universality implies that every individual should possess the characteristic while uniqueness means that no two persons should be the same in terms of the characteristics. Permanence denotes that the characteristics should be invariant with time. By collectability, quantitative measurement of the characteristic must be possible and with ease while performance refers to achievable identification/ verification accuracy with different working or environmental conditions. Acceptability indicates the extent to which people are willing to accept the characteristic while circumvention refers to how difficult it is for fraudulent techniques to fool a system that is based on the characteristic. The relative comparison of the performance of the existing biometric characteristics based on these criteria is presented in Table 1 [4]. Physiological characteristics (shown in Figure **??**) are related to the shape of the body and incluttern Recognitionde fingerprint, palm prints, face, deoxyribonucleic acid (DNA), hand geometry, iris recognition, retina and odor/scent. Behavioural characteristics (also shown in Figure **??**) include handwriting (typing rhythm), signature, gait and voice which are all related to the pattern of behaviour of a person. The traditional human identity management methods which include possession (such as identity and smart cards) and knowledge (such as Personal Identification Number (PIN) and password) based human identification schemes suffer various limitations including theft, forgery, unauthorized access and forgetfulness. Several private and public organizations often consider strengthening their knowledge-based security systems using longer and dynamic (changing) passwords, which often requires individuals documenting their passwords in unsecured manners. The compromise of a re-used password on different systems may lead to theft, privacy intrusion and other consequences [5]. Biometric-based human identity management systems have emerged as reliable, secure and dependable solutions to these limitations and have been deployed in numerous government and private applications [6]. The high confidence and success levels recorded for biometric-based systems have been attributed to some advantages that biometrics maintain over other methods. The advantages include strict and direct covert observation of biometric information, nonsharability, not-transferable and regeneration within short period when damaged or mutilated. In addition, biometrics-based systems are very easy to use, very friendly and repudiation-proof [7].

Table **??**: Comparison of various biometric characteristics (A=Universality, B=Uniqueness, C=Permanence, D=Collectability, E=Performance, F=Acceptability, G=Circumvention, H=High, M=Medium, L=Low)

A biometric system that is based on a single characteristic is called a uni-modal system while multimodal biometric systems rely on multiple characteristics to function. Uni-modal biometric systems rely on the evidence of a single source of information for human authentication and they are susceptible to the following limitations [8][9][10][11][12][13] for a small proportion of the population leading to very identical biometric characteristics (such as facial appearance) as may be observed for mother and daughter, father and son and identical twins. It impacted negatively on a biometric system by increasing its False Match Rate (FMR). (f) Non-invariant representation: This is an intra-class variation arising from varied interactions of the user with the sensor. It may be due to angular, translational, pressure, pose and expression variations when a characteristic is repeatedly captured on a sensor. Other sources include the use of different sensors during enrolment and verification, changes in the ambient environment conditions and the inherent changes arising from wrinkles or scars in the biometric trait. These variations usually increase the False Non-Match Rate (FNMR) of a biometric system.

(g) Spoofing: Some biometric systems (especially those based on facial images) can be imitated or forged.

Multi-modal approach to human authentication and verification has been considered as the most reliable method for the elimination of these limitations. Multi-modal biometric systems integrate two or more types of biometric characteristics for consolidation and meeting stringent performance requirements. Most importantly, it is extremely difficult for an intruder to spool multiple biometric traits simultaneously [5,11]. This paper presents the motivations, strategies and limitations of fingerprint, voice, iris and other biometrics modes for human identity management. Synopses of the integration techniques, fusion levels and scenarios, modes of operations and evaluation strategies of multimodal systems are also presented.

# 2 II.

# 3 Unimodal Biometric Systems

A uni-modal biometric system comprises of any of the biometrics shown in Figure **??** and contains five integrated components conceptualized in Figure 2 [12,14]. The enrolment component is a sensor that acquires the biometric data and converts into a digital format. The image-processing unit uses specified algorithms to enhance the image and extracts meaningful feature set to form a biometric template. The biometric database is a repository of the extracted templates, which are necessary data for future reference from several images. The matching unit is responsible for performing algorithm-based comparison of a reference biometric image with the template image in the database and generate a matching score. The decision component uses the results from the matching component to make a system-level decision.Characteristics A B C D E F G Face H L M H L H L Fingerprint Iris H H H M H L H Retina H H M L H L H Signature L L L H L H L Voice M L L M L H L Facial thermogram H H L H M H H DNA H H H L H L L

# 4 Global Journal of C omp uter S cience and T echnology

Volume XV Issue II Version I Year ( )G 2015 a) Fingerprint Verification System

Fingerprint is an impression that is formed through deposit of minute ridges and valleys when a finger touches a surface. Facts exist that the ridges and valleys do not change for lifetime no matter what happens and in a case of injury or mutilation, they reappear within a short period. The five commonly found fingerprint ridge patterns are arch, tented arch, left loop, right loop and whorl (Figure 3) [15,16]. The uniqueness of friction ridges implies that no two fingers or palm prints are exactly alike [17]. Fingerprint identification involves making a comparison between two or more fingerprints to determine if they originated from the same finger under some threshold scoring rules. Human verification based on fingerprint was then carried out electronically by extracting the fingerprint patterns after scanning the inked image with high-resolution page scanners. In recent years, the need for fast and reliable fingerprint verification systems has necessitated the shift from the ink card method to live scan devices, which are categorized into optical sensors [18,19], electrical sensors [18][19][20] and ultrasonic sensors [18,21,22]. Fingerprint image enhancement is performed to remove the enrolment attracted noise and it requires a number of processes including normalization, segmentation, ridge orientation and frequency estimation, filtering, binarization and thinning. Several algorithms had been proposed in [20,[23][24][25][26][27] for these processes. Existing fingerprint feature extraction algorithms include Crossing Number [19,[27][28][29][30], Adaptive Flow Orientation [31], Orientation Maps [32], Gabor Filter [33], Mathematical Morphology [34] and Minutiae Maps and Orientation Collinearity [35]. Others are Poincare Index [36][37][38][39], Curvature [40] and Multi-Resolution [41]. Several studies on fingerprint matching have produced several algorithms that are correlation, minutiae and ridge feature-based [42][43][44][45][46][47][48][49][50]. Fingerprint matching algorithms were also proposed in [51][52][53] on the basis of Delaunay triangulation (DT) in computational geometry.

The matching of two minutiae sets based on these algorithms is usually posed as a point pattern matching problem and the similarity between them is proportional to the number of matching minutiae pairs. Although the minutiae pattern of each finger is quite unique, contaminants and distortion during the acquisition and errors in the minutia extraction process result in a number of missing and spurious minutiae.

Due to difficulty in obtaining minutiae points from poor quality fingerprint images, other ridge features like the orientation and the frequency of ridges, ridge shape and texture information have formed the bedrock for several fingerprint matching algorithms. However, several of these methods suffer from low identification capability. In correlation-based fingerprint matching, the template and query fingerprint images are spatially correlated to estimate the degree of similarity between them. If the rotation and displacement of the query with respect to the template are not known, then the correlation must be computed over all possible rotations and displacements, which is computationally very expensive. Furthermore, the presence of non-linear distortion and noise significantly reduce the global correlation value between two impressions of the same finger. To overcome these problems, correlation is locally done around the high curvature, minutia information and other interesting regions of the fingerprint image. One main shortcoming for fingerprint identification systems is that the presence of small injuries and burns may cause disproportionate results due to presence of false minutiae points. In fact, injury, whether temporary or permanent, can interfere with the scanning process. For example, bandaging a finger for a short period of time can impact the fingerprint scanning process. Ordinarily, a burn to the identifying finger could make the fingerprint identification process fail [54][55] while daily work can also affect or sometimes damage some of fingerprint ridges.

# 5 b) Voice/Speaker Recognition

Voice is a combination of physiological and behavioural biometrics [2,56,57] and it is the natural means of communication for human beings. While speech recognition is concerned with the interpretation of what the speaker says, speaker recognition focuses on verifying the speaker's identity [58]. The two are based on the analysis of the vibrations created in the human vocal tract which is unique in shape, larynx, size and so on and also determines the resonance of the voice across individuals. A voice recognition system uses a microphone to record the voice, which is digitised for authentication. The speech can be acquired from the user enunciating a known text (text dependent) or speaking (text independent) [4]. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase while text-independent voice recognition system recognizes the speaker independent of what is said. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud [57]. The first task of an Automatic Voice/ Speaker Recognition system is the collection of speech samples that contain the discriminating features and their vectors from the speakers. Features are then extracted from collected speech samples base on any of the existing voice feature extraction methods which include Spectral Centrod, Spectral Roll Off, Spectral Flux and Mel Frequency Cepstral Coefficient (MFCC). The extracted features are then trained to extract feature vectors from the speech signals of several speakers and building the MFCC vectors, which is a small codebook that represents all the vectors in the minimum mean square sense. The spectral distance between testing utterance feature and code vectors obtained during training is then determined and the utterance is classified to its nearest speaker [59][60][61].

Voice/speaker recognitions have been used in variety of assistive contexts, including home computers and various mobile, public and private telephone services [11]. This is attributed to non-use of specific grammar and language independent natures; hence allowing callers to speak a particular phrase in any language of choice [62]. In addition, voice needs inexpensive equipment for capturing and can be deployed with ease for applications where other biometric modes experience difficulties [63]. Despite having lots of potentials and its growing popularity, voice/speaker recognition technologies are still not easily employed for individuals (such as older adults) with speech or communication disorders [64]. Human emotion is so unstable that accurate simulation or recognition of voice at different emotional states is highly impractical [65]. Furthermore, human voice is generated through a complex process of interactions among several body parts, especially the lungs, larynx and mouth and a temporarily or permanent damage to any of these body parts can lead to a voice disorder with significant effect on the identification process. The possibility of hacking into a system using a tape recording is another problem [10].

# 6 c) Iris Recognition

The iris begins to form in the third month of gestation with patterns that depend on the initial environment of the embryo. It is unchangeable after the age of two or three and highly distinct among individuals, hence making it a unique feature. The iris is isolated and protected from external environment and it is impossible to surgically modify it without unacceptable risk to vision [55]. It appears as a circular diaphragm located between cornea and lens of the human eye and controls the amount of light entering through the pupil. The average diameter of iris is 12 mm and pupil size can be 10% to 80% of the diameter [11,66,67]. Iris recognition identifies a person by analyzing the "unique" random and visible patterns within the iris of an eye to form an iris code that is compared to iris templates in a database. Its often involves the process of image acquisition (which involves capturing of highquality iris image while remaining non-invasive to the human operator), iris localization (which involves the detection of the edges and pupil of the iris) and normalization of the size of the iris region. Normalization

# 7 Global Journal of C omp uter S cience and T echnology

Volume XV Issue II Version I Year ( ) G is for ensuring consistency between eye images despite the stretching of the iris induced by the pupil's dilation. It also involves unwrapping of the normalized iris region into a rectangular region, extraction of discrimination features in the iris pattern, so that a comparison between templates can be done and encoding of iris features using wavelets to construct the iris code to which input templates are compared during matching [68,69]. Challenges that are currently facing iris recognition include growing difficulty for distance larger than a few meters and it requires absolute cooperation from the individual to be identified [55]. It is also susceptible to low performance for poor quality images [70].

# 8 d) Face Recognition

Sometimes, faces are used in un-attended authentication applications, which are developed for human recognition by several organizations including universities, government and private agencies such as banks. Many of these organizations have facial images stored in large databases making many commercial and law-enforcement applications feasible given a reliable facial recognition system. Success in computing capability over the past few years have facilitated the development of several face-based recognition systems with simple geometric models or sophisticated mathematical representations and matching processes [55,71,72]. Face recognition systems detect patterns, shapes, and shadows in the face, perform feature extraction and recognition of facial identity. In the broader view, it encompasses all types of facial processing such as tracking, detection, analysis and synthesis. Existing techniques for face recognition include eigenfaces (Figure 4) and fisher-faces, which use the image of the whole face as raw input and are based on principal component analysis with higherorder statistics. Other techniques depend on extracting and matching certain features from the face, such the mouth and eyes. Some other approaches use data from the whole face as well as specific features to carry out the recognition [2,73]. While face recognition is nonintrusive, and may experience high performance and user acceptance in controlled environments, robust face recognition in non-ideal situations continues to pose challenges [74,75]. Facial images of a person can be collected with little cooperation and may perform with very high error rates when deployed in the real world, especially for long-range recognition [55]. Facial recognition systems may also underperform when identifying the same person with different illuminations, smiling, makeup, occlusion, pose, gestures, age, and accessories (moustache, glasses) conditions [2,11].

# 9 e) Gait Recognition

Gait analysis focuses on the systematic study of animal locomotion, more specifically, the study of human motion, augmented by instrumentation for measuring body, its mechanic and the activity of its muscles [76]. The gait of a person can be extracted without the user knowing they are being analysed and without any cooperation from the user in the information gathering stage. It can be captured at a distance, does not require high quality images and it is difficult to disguise [77]. Gait analysis is used to assess, plan, and treat individuals with conditions affecting their ability to walk while gait recognition is the process of identifying individuals based on their walking characteristics and it encompasses quantification and interpretation. Quantification is concerned with the introduction and analysis of measurable parameters of gaits while interpretation involves drawing various conclusions about health, age, size, weight, speed, and so on from gait pattern. Gait recognition involves the capturing of human walking image, pre-processing of the raw image, extraction of gait features (main leg angle and frame) and feature recognition. Existing feature extraction techniques include Hidden Markov Model (HMM) and an Exemplar-based HMM [78], Radon transform with Linear Discriminant Analysis (LDA) [79], Support Vector Machine (SVM) [80], Principal Components Analysis (PCA) and Maximization of Mutual Information (MMI) [81]. The block diagram for gait recognition system is presented in Figure 5.

# 10 G

Recent gait recognition approach involves having a physical device, such as an accelerometer, attached to one's physical body to collect data about one's gait. The new sensor-based approaches, however, give up gait's potential to identify from a distance [82]. Difficulty in deliberately copying someone else's way of walking remains one of the strong motivations for gait recognition [64]. However, being a biometric, an individual's gait will be affected by certain factors including drugs and alcohol (which affect the way in which a person walks) and physical changes such as pregnancy, accident, disease and severe weight gain or loss. It is also affected by mood and clothing [74]. In addition, gait recognition is still in its infancy and has not face severe or thorough tests, especially for potential attacks [83].

# 11 f) Signature Recognition

A signature is the dynamics of a person's handwritten and comprises of special characters and flourishes, which in several cases, make them unreadable. Intra-personal variations and differences make the analysis of signatures as complete images rather than letters and words important and unique. This also accounts for the wide acceptance of signatures by government, legal, and commercial transactions as a method of verification [75]. Signature recognition technology consists primarily of interconnection of a pen, specialized writing tablet and local or central computer for template processing and verification. In the enrolment process, an individual is requested to sign his or her name several times on the tablet. The robustness of the enrolment template is a direct function of the quality of the writing tablet that is utilized. A high quality writing tablet will capture all the behavioural variables (timing, pressure, and speed) of the signature, whereas a lower end writing tablet may not. The constraints faced in signature acquisition include the clause that signature cannot be too long or too short. Too long signature causes too much behavioural data which results in difficulty in identifying consistent and unique data points while too short signature experiences shortage of data that increases the rate of false acceptance. Furthermore, same type of environment and conditions (standing, sitting, arm position, etc) is needed for the completion of the enrolment and verification processes. The extraction of the unique features such as the time and speed utilized for signing, the pressure applied from the pen to the writing tablet, the overall size of the signature and the quantity and the various directions of the strokes in the signature proceeds the enrolment phase. The biggest advantage that signature recognition offers is its very high resistance to imposters. Although, a wide range of signatures can be forged, it is still very difficult to "mimic" the behavioural patterns associated when signing. Compared to other biometric technologies, signature recognition is non-invasive and as a result, experiences high acceptance rate with no privacy rights issues. More importantly, the dynamics of signature can be changed during cases of hacking or stolen templates. In terms of weaknesses, a person's signature changes with time and is highly affected by the physical and emotional conditions of the signatories. More importantly, successive signatures by the same person can show significant differences resulting in increased error rates [2,55].

# 12 g) Hand Geometry Recognition

Hand geometry of individuals is based on the shape of their hands and it is a stable biometric whose physical characteristics are not susceptible to major biological changes (except for conditions of arthritis, swelling, or deep cuts). Hand geometry recognition has been among the oldest and has established itself as a viable technology. During a hand geometry-based recognition, the subject's hand is placed onto a platen which then captures the ridges (black images) and valleys (white images) of the top and sides of the hand. Moderately unique features which include the finger thickness, length and width, the distances between finger joints, the hand's overall bone structure and so on are located in the structure of the images. Hand geometry recognition is often seen as one of the easiest to use, administer and environmental friendly biometric technologies. It is the least susceptible to privacy rights issues primarily because of its simple enrolment and verification procedures. Hand geometry is not distinctive, especially when applied to a large population. Thus, it is most suitable for purposes of verification rather than identification. Hand geometry may not be an ideal biometric to use for a population, which includes children whose hand-geometry template may vary during their growth period [84]. In addition, most hand-geometry systems perform with procedures that restrict the positional freedom of the hand [55,85].

# 13 h) Palm Print Recognition

Just like fingerprint recognition, palm print technology uses the information presented in a friction ridge impression for human identification. This information combines ridge flow, ridge characteristics, and ridge structure of the raised portion of the epidermis. The data represented by these friction ridge impressions allows a determination that corresponding areas of friction ridge impressions either originated from the same source or could not have been made from the same source. The uniqueness and high permanence levels of fingerprint and palm print have been used as a trusted form of identification. However, palm recognition has been a slower automated system due to limitations in computing capabilities and live-scan technologies. Palm identification, just like fingerprint identification, is based on the aggregate information presented in a friction ridge impression. A palm recognition system is designed to interpret the flow of the overall ridges to Year ( ) G assign a classification and then extract the minutiae detail as a subset of the total amount of information obtained from a coordinated search of a large repository of palm prints. Minutiae information includes the flow of the friction ridges, the presence or absence of features along the individual ridge paths and their sequences as well as the intricate detail of a single ridge. Minutiae are limited to location, direction and orientation of the ridge endings and bifurcations (splits) along a ridge path [86].

# 14 i) Deoxyribonucleic Acid (DNA) Recognition

DNA is a well-known double helix structure present in every human cell. DNA fingerprint is produced as a robust and unchangeable (by surgery or any other known treatment) human attribute which is the same for every single cell of a person. The molecular structure of DNA can be considered as a zipper with the letters: A (Adeline), C (Cytosine), G (Guanine) and T (Thymine) representing each tooth and with opposite teeth forming one of two pairs, either A-T or G-C [87]. The sequence of letters along the zipper determines the DNA information [2,88] and presents unique differences in the DNA fragments and molecules resulting in different biological pattern between individuals. DNA is widely used in the diagnosis of disorders, paternity tests and criminal identification and very high level of success and accuracy has been reported [55]. The use of DNA however experiences computational complexity with enormous time requirements. It is often considered as a violation of privacy and not always unique between monozygotic twins [11,57].

# 15 III.

# 16 Multi-Modal Biometric Systems

Some of the limitations imposed by unimodal biometric systems can be addressed through multimodal sources (MMS) of information for establishing identity [89]. MMS are expectedly more reliable due to their multiple, (fairly) independent pieces of evidence [90]. They also provide stringent performance requirements imposed by various applications and also address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they facilitate a challengeresponse mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition [91]. A generic biometric system is presented in Figure 6 with four important modules; namely sensor, feature extraction, matching and decision modules [91,92].

The sensor module captures the trait (raw biometric data), while the feature extraction module processes the data to extract a feature set that is a compact representation of the trait. The main function of the matching module is to generate the matching scores based on comparison of the extracted feature set with the templates in the database by a classifier. Based on a matching score, the decision module rejects or confirms a claimed identity. Important considerations for the design of multi-modal biometric system include architecture, choice of biometric modality, total number of modalities, level of accumulation of evidences, level and methods for fusion, safety and user friendliness and cost versus the matching performances. Others are level of security and reliability, mode of operations, assigning weights to biometrics and multimodal database [11,93]. Challenges confronting multimodal biometric systems include failure of sensors to show consistency in various operating environments, poor design due to lack of proper understanding of biometric technologies and public confidence. Other challenges are complex and unverifiable matching algorithms, misleading results due to poor scalability and lack of standard guidelines for auditing biometric system and records [94].

# 17 a) Fusion levels

In a multi-modal biometric system, information reconciliation may be attained via the fusion of the raw data, extracted features or the matching scores. Information may also be obtained at the decision levels. While fusion at the data or feature level is performed when either the data or the feature sets originating from multiple sensors/sources are fused, fusion at the match score level involves an integration of the scores obtained by multiple classifiers pertaining to different modalities. When the final information is obtained from the fusion of different decision levels, the final output of the multiple classifiers is consolidated using majority voting or any other suitable method [95]. Biometric systems that integrate information at an early stage (using features set) perform better than those that perform integration at a later stage [91,92]. This is attributed to the richer information offered by the features when compared to the matching score or the output decision of a matcher. However, in practice, fusion at the feature level is difficult to achieve due to complexities that trail the task of providing a common feature set for various modalities. Fusion at the decision level on its own is believed to be rigid due to its limited information. Thus, for its relatively easy access, fusion at the match score level is usually preferred.

# 18 b) Fusion Scenarios

As shown in Figure 7, existing multi-modal biometrics fusion scenarios depend on the number of traits, sensors and feature sets and are classified into the following categories: The existing biometrics fusion algorithms include Score Normalization [1,102], Minimum Average Correlation Energy Filter [105], Neyman-Pearson (Product) Rule and Gaussian Copla Models [108], Principal Components Analysis (PCA), Fisher's Linear Discriminate Methods [109] and Geometry Preserving Projection [106] Modes of Operation The existing modes of operation for a multimodal biometrics scheme are serial, parallel and hierarchical which are presented in Figure 8. The output of one modality is traditionally used to determine if the next modality will be used in the serial mode. This implies that simultaneous acquisition from multiple sources of information (such as multiple traits) is not required and final decision could be made with any modality. For the parallel mode, simultaneous acquisition of multiple modalities takes place and final decision is based on the integration of information (output) from the various modalities. The hierarchical scheme combines individual classifiers in a treelike structure and it is only applicable for large number of classifiers [91,102,110].

# 19 c) Integration Strategies

Fusion at the feature and matching score levels are the two major strategies for the integration of multimodal systems. Fusion at the feature level is accomplished through the concatenation of two compatible feature sets before a feature selection or reduction technique is employed for handling any dimensionality problem [91]. The authors in [1,12,102,105,111,112] had carried out detailed studies on fusion at the match score level. Base on robust and efficient normalization techniques [9,59,102,106,112,113,116], scores from multiples matchers are transformed into a common domain prior to consolidating them. In the context of verification, the feature vector is constructed using the matching scores output of the individual matchers and then classified into accept (genuine user) or reject (impostor) [91]. Fusion of individual matching scores generates a single scalar score that is used for taking the final decision [116,117]. General strategies for combining scores from multiple classifiers include principal component analysis [109], majority voting [95], behaviour knowledge space method [118], weighted voting based on the Dempster-Shafer theory of evidence ??119], AND/OR rules [120] and Score normalization [121]. Others are simple sum rule [89], weighted product, bayes' rule, mean fusion, Linear Discriminant Analysis [LDA], k-nearest neighbour [KNN] and hidden Markov model ??HMM].

# 20 e) Evaluation Strategies

The evaluation of multi-modal biometrics systems provides basis for establishing their performance and adequacy levels.

Benchmarked evaluation strategies include False Rejection Rate (FRR), False Acceptance Rate (FAR), Receiver Operating Characteristics (ROC) Curve, Equal Error Rate (EER), Cumulative Match Curve (CMC) and Average Matching Time (AMT). If an imposter score exceeds the threshold, it results in a false accept, while genuine score that falls below the threshold results in a false reject. FRR is therefore the rate of occurrence of a scenario of two biometrics (same mode) from the same source (subject) failing to match and FAR is the rate at which two biometrics (same mode) from different sources (subjects) are found to match. An ROC curve measures the overall performance of a multi-modal biometric system base on the plot of FRR against FAR for all possible matching thresholds. In the ideal case, both FAR and FRR should be zero and the genuine and an 'acceptable' ROC curve presents a step function at imposter distributions should be disjoint. In such cases, the zero FAR. On the other extreme, if the genuine and imposter distributions are equal, then the ROC curve is a line segment with 45o slope and an end-point at zero FAR. In practice, the ROC curve falls between these two extremes [122]. For each matching threshold i, EER is presented as the value at which FAR (i) and FRR (i) are equal. CMC is another indicator that is similar in nature to ROC curve [123,124].

# 21 Conclusion

The motivations, methodologies, strengths and weaknesses of the physiological and behavioural modes for human identity management had been presented. The integration, fusion and evaluation strategies for multi-modal approach to human identity management are also presented. Multi-modal biometric systems have performed well in addressing the problems of unimodal systems by combining information from different sources and improve the systems performance, raise the scope, discourage spoofing, and promote indexing. Improved performance has been noticed with uncorrelated traits and integration of parameters that are user's specific in multimodal systems. Without doubt, the widespread deployment of biometric systems in government and private establishments across the world will offer more secured and reliable human identity management.

# 22 Global

[1] [2] [3]


[3]Multi-Modal Biometrics: Applications, Strategies and Operations

Figure 1:

2

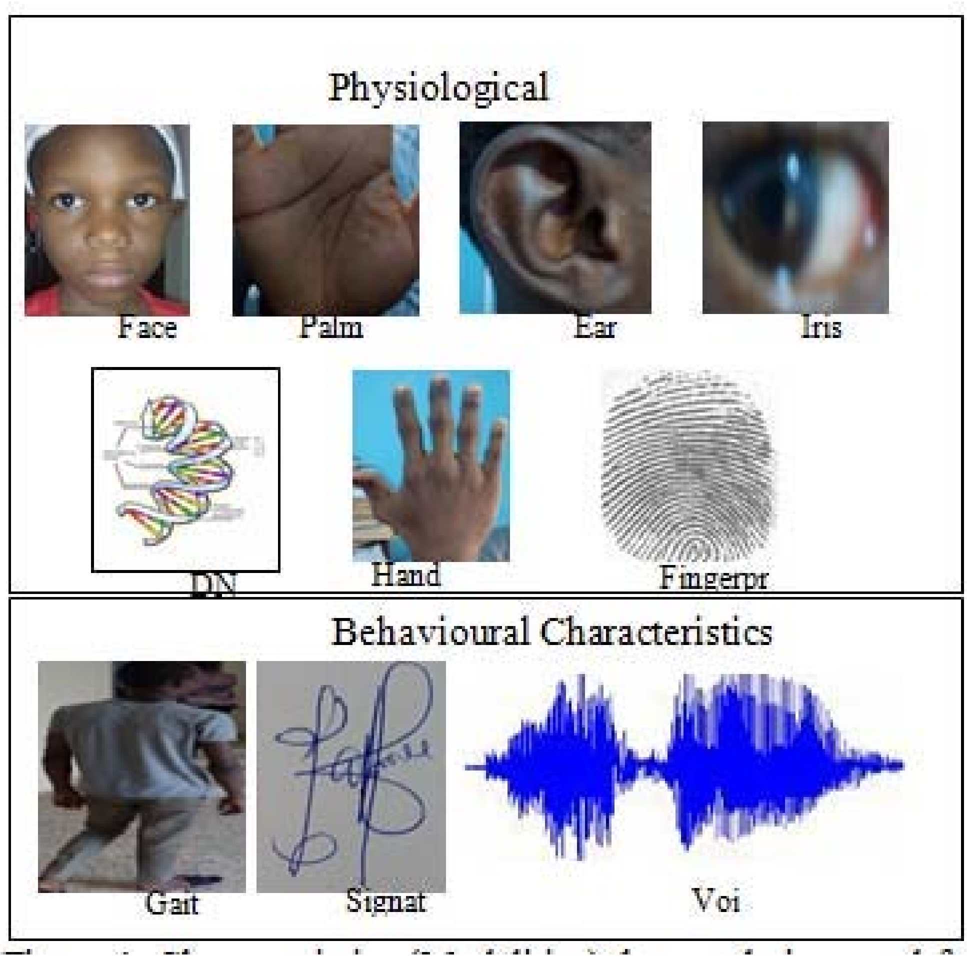


Figure 2: Figure 2 :

3

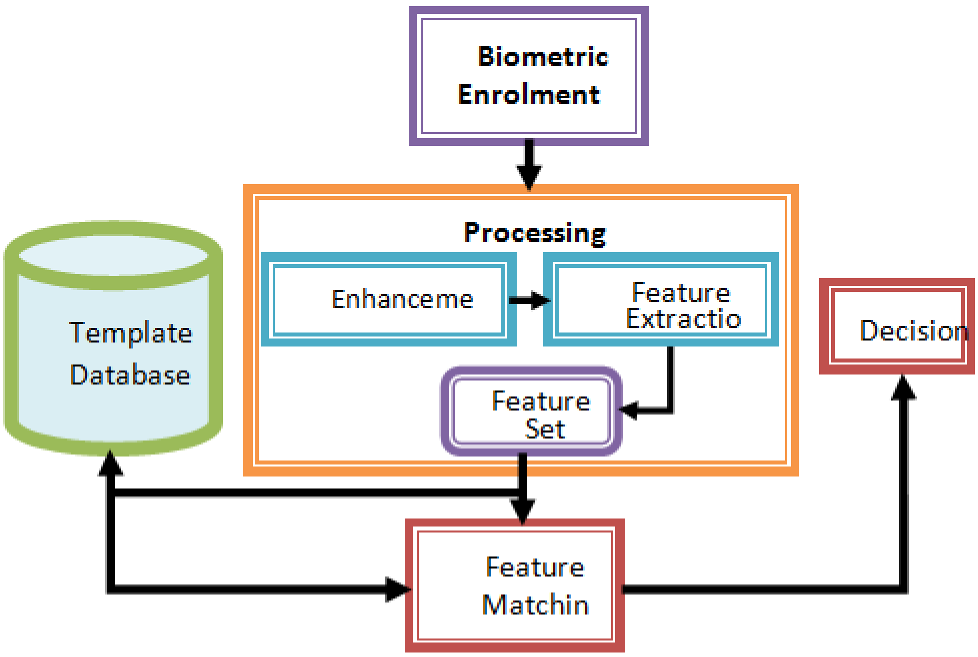


Figure 3: Figure 3 :

4


Figure 4: Figure 4 :

5


Figure 5: Figure 5 :

6


Figure 6: Figure 6 :

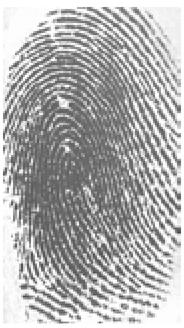

Figure 7:

**7**

Figure 8: Figure 7 :

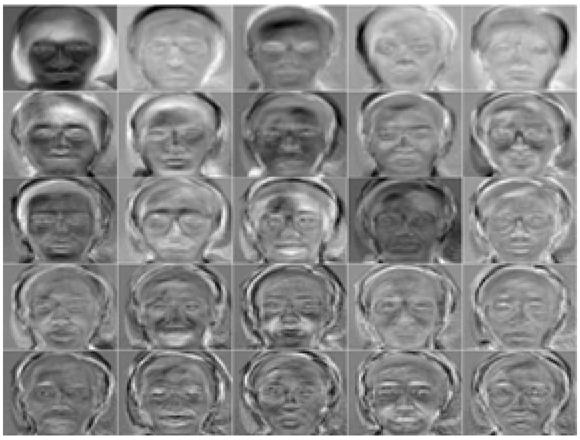

Figure 9: Global

**8**

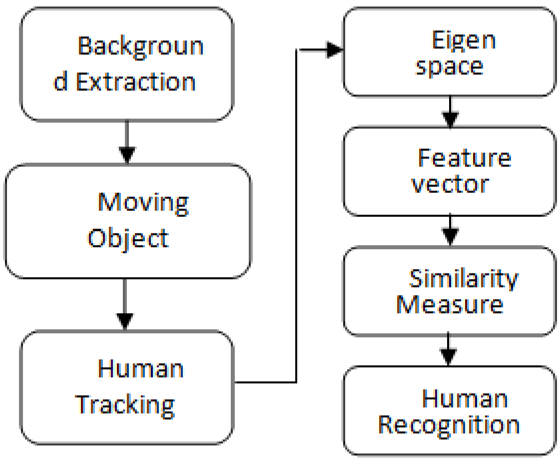


Figure 10: Figure 8 :

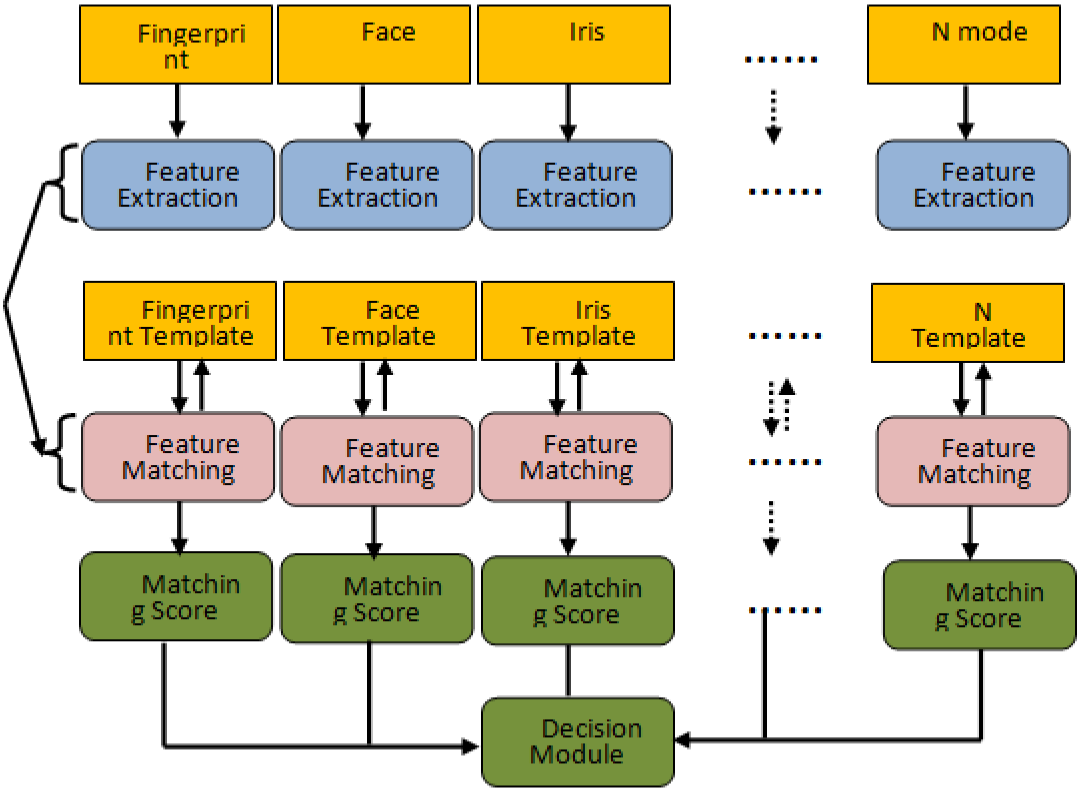
Fingerpri
nt
Face
Iris
N mode
Feature
Extraction
Feature
Extraction
Feature
Extraction
Feature
Extraction
Fingerpri
nt Template
Face
Template
Iris
Template
N
Template
Feature
Matching
Feature
Matching
Feature
Matching
Feature
Matching
Matchin
g Score
Matchin
g Score
Matchin
g Score
Matchin
g Score
Decision
Module

Figure 11:

[Ashbaugh and Ridgeology ()] , D R Ashbaugh , Ridgeology . *Journal of Forensic Identification* 1991. 41 (1) p. .

[Hurst ()] , K Hurst . *NSTC Subcommittee on Biometrics* 2006. (Biometrics Overview. Article 6 of the Data Protection Directive)

[Barde ()] 'A Certificate of Identification Growth through Multimodal Biometric System'. S Barde . *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* 2013. 2.

[Liu et al. ()] 'A Fingerprint Matching Algorithm Based On Delaunay Triangulation Net'. N Liu , Y Yin , H Zhang . *Proceedings of the Fifth International Conference on Computer and Information Technology (CIT'05)*, (the Fifth International Conference on Computer and Information Technology (CIT'05)) 2005.

[Elmir et al. ()] 'A Hierarchical Fusion Strategy based Multimodal Biometric System'. Y Elmir , Z Elberrichi , R Adjoudj . *Proceedings of the International Arab Conference on Information*, (the International Arab Conference on Information) 2013.

[Ross et al. ()] 'A Hybrid Fingerprint Matcher'. A Ross , A K Jain , J Reisman . *Pattern Recognition* 2003. 36 p. .

[Iwasokun et al. ()] 'A Mathematical Modeling Method for Fingerprint Ridge Segmentation and Normalization'. G B Iwasokun , O C Akinyokun , O Olabode . *International Journal of Computer Science and Information Technology and Security (IJCSITS)* 2249 -9555. 2012. 2 (2) p. .

[Weiguo et al. ()] 'A Memetic Fingerprint Matching Algorithm'. S Weiguo , G Howells , M Fairhurst , F Deravi . *IEEE Transactions on Information Forensics and Security* 2007. 2 (3) .

[Soviany et al. ()] 'A Multimodal Approach for Biometric Authentication with Multiple Classifiers'. S Soviany , C Soviany , M Jurian . *World Academy of Science, Engineering and Technology* 2011. 59.

[Labati et al.] *A Neural-based Minutiae Pair Identification Method for Touch-less Fingerprint Images*, R D Labati , V Piuri , F Scotti . 18/06/2014. (unpublished, Available: piurilabs.di.unimi.it/ Papers/PID2035945.pdf)

[Dass et al. ()] 'A Principled Approach to Score Level Fusion in Multimodal Biometric Systems'. S C Dass , K Nandakumar , A K Jain . `http://biometrics.cse.msu.edu/` *IEEE Proceeding of Vision, Image and Signal Processing*, 2003. 150 p. . (Publications/Multibiometric Based Applications)

[Kovoor et al. ()] 'A Prototype for a Multimodal Biometric Security System Based on Face and Audio Signatures'. B C Kovoor , M H Supriya , K P Jacob . *International Journal of Computer Science and Communication* 2011. 2 (1) p. .

[Yu et al. ()] 'A Study on Gait-Based Gender Classification'. S Yu , T Tan , K Huang , K Jia , X Wu . *IEEE Trans. Image Process* 2009. 18 (8) p. .

[Delac and Grgic ()] 'A survey of biometric recognition methods'. K Delac , M Grgic . *46th International Symposium*, 2004. 2004. 2004. p. . (Proceedings Elmar)

[Ahuja and Chabbra] 'A Survey of Multimodal Biometrics'. M S Ahuja , S Chabbra . *International Journal of Computer Science and its Applications* p. .

[Gu et al. ()] 'Action and gait recognition from recovered 3-d human joints'. J Gu , X Ding , S Wang , Y Wu . *IEEE Trans. Syst* 2010. 40 (4) p. . (Man, Cybern. B)

[Iwasokun et al. ()] 'Adaptive and Faster Approach to Fingerprint Minutiae Extraction and Validation'. G B Iwasokun , O C Akinyokun , B K Alese , O Olabode . *International Journal of Computer Science and Security* 2011. 5 (4) p. .

[Ratha et al. ()] 'Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images'. N Ratha , S Chen , A K Jain . *Pattern Recognition* 1995. 28 (11) p. .

[Asha and Chellappan ()] 'Adaptive Multimodal Biometric Authentication using Fingerprint, Palmprint and Voice Biometrics'. S Asha , C Chellappan . `http://www.Europeanjournalofscientificresearch.com` *European Journal of Scientific Research* 1450-216X. 2013. 95 (1) p. .

[Setlak ()] 'Advances in fingerprint sensors using RF imaging techniques'. D R Setlak . *Automatic Fingerprint Recognition Systems, N. Ratha and R. Bolle*, (New York) 2004. Springer-Verlag.

[Nageshkumar and Shanmukhaswamy ()] 'An Adaptive Multimodal Biometric Recognition Algorithm for Face Image using Speech Signal'. M Nageshkumar , M N Shanmukhaswamy . *International Journal of Computer Applications* 2010. 7 (1) .

[Tico and Kuosmanen ()] 'An algorithm for fingerprint Image Post-processing'. M Tico , P Kuosmanen . *proceedings of the 34th Asilomar Conference on Signals*, (the 34th Asilomar Conference on Signals) 2000. 2 p. .

[Jain et al. ()] 'An Introduction to Biometric Recognition'. A K Jain , A Ross , S Prabhakar . *IEEE Transactions on Circuits and Systems for Video Technology*, 2004. 2004. 14.

[Phillips et al. ()] *An Introduction to Evaluating Biometric Systems*, P J Phillips , A Martin , C L W M Przybocki . 2000. IEEE. National Institute of Standards and Technology

[Sanjekar and Patil ()] 'An Overview of Multimodal Biometrics'. P S Sanjekar , J B Patil . *Signal & Image Processing*, 2013. 4.

[Andrej et al. ()] Kisel Andrej , Alexej Kochetkov , Justas Kranauskas . *Fingerprint Minutiae Matching Without Global Alignment Using Local Structures, INFORMATICA, Institute of Mathematics and Informatics*, (Vilnius) 2008. 2011. 19 p. .

[Albert and Ganesan ()] 'Applications of Principal Component Analysis in Multimodal Biometric Fusion System'. T A Albert , S Ganesan . http://www.europeanjournalofscientificresearch.com, Access03/03/2013 *European Journal of Scientific Research* 2012. 67 (2) p. .

[Ortega-Garcia et al. ()] 'Authentication gets personal with biometrics'. J Ortega-Garcia , J Bigun , D Reynolds , J Gonzalez-Rodriguez . *Signal Processing Magazine* 2004. 21 (2) p. . (IEEE)

[Ratha and Bolle ()] *Automatic Fingerprint Recognition Systems*, N Ratha , R Bolle . 2004. New York: Springer-Verlag.

[Bebis et al.] G Bebis , T Deaconu , M Georgiopoulos . http://fmi.dreamlords.org/ *Fingerprint Identification Using Delaunay Triangulation*,

[Weaver ()] 'Biometric authentication'. A C Weaver . *Computer* 2006. 39 (2) p. .

[Gafurov et al. ()] 'Biometric gait authentication using accelerometer sensor'. D Gafurov , K Helkala , T Søndrol . *Journal of Computers* 2006. 1 (7) p. .

[Jain et al. ()] 'Biometrics-Personal Identification'. A Jain , B Ruud , P Sharath . http://www.amazon.com/Biometrics-Personal-Identification-Networked-Society/dp/0387285393.Accessed24/08/2013 *Journal of Networked Society* 1998. Kluwer Academic Publishers.

[Simpson ()] 'Biometrics: Issues and Applications'. I Simpson . *6th Annual Multimedia Systems*, 2006. Electronics and Computer Science, University of Southampton

[Hong and Jain ()] 'Classification of Fingerprint Image'. L Hong , A K Jain . http://www.cse.msu.edu/biometrics/Publications/Fingerprint/clas.pdf.Accessed24/06/2012 *Proceedings of Eighth Scandinavian Conference on Image Analysis*, (Eighth Scandinavian Conference on Image AnalysisKangerlussuaq, Greenland) 1999.

[Lu et al. ()] 'Combining Classifiers for Face Recognition'. X Lu , Y Wang , A K Jain . *Proceedings of IEEE International Conference on Multimedia and Expo (ICME)*, (IEEE International Conference on Multimedia and Expo (ICME)Baltimore, MD) 2003. 3 p. .

[Daugman] *Combining multiple biometrics*, J Daugman . http://www.cl.cam.ac.uk/users/jgd1000/combine/

[Jain et al. ()] 'Combining multiple matchers for a high security fingerprint verification system'. A K Jain , S Prabhakar , S Chen . *Pattern Recognition Letters* 1999. 20 p. .

[Hu et al. ()] 'Combining Spatial and Temporal Information for Gait Based Gender Classification'. M Hu , Y Wang , Z Zhang , Y Wang . *Proceedings of IEEE/IAPR Int. Conf. Pattern Recog*, (IEEE/IAPR Int. Conf. Pattern Recog) 2010. p. .

[Rajanna et al. ()] 'Comparative Study on Feature Extraction for Fingerprint Classification and Performance Improvements Using Rank-Level Fusion'. U Rajanna , E Ali , B A George . *Pattern Anal Application*, 2009. Springer-Verlag London.

[Zhang and Wang ()] *Core-Based Structure Matching Algorithm of Fingerprint Verification*, W Zhang , Y Wang . 2002. IEEE.

[Koo and Kot ()] 'Curvature-Based Singular Points Detection'. W M Koo , A Kot . *Proceedings of 3 rd International Conference on Audio and Video-Based Biometric Person Authentication*, Lecture Notes in Computer Science (3 rd International Conference on Audio and Video-Based Biometric Person Authentication) 2001. 2 p. .

[Iwasokun ()] *Development of a hybrid platform for the pattern recognition and matching of thumbprints*, G B Iwasokun . 2012. Akure, Nigeria. Department of Computer Science, Federal University of Technology (PhD Thesis)

[Liang et al. ()] *Distorted Fingerprint Indexing Using Minutia Detail and Delaunay Triangle*, X Liang , T Asano , A Bishnu . http://www.jaist.ac.jp/jinzai/Paper18/ISVD2006.pdf,Accessed25/08/2013 2007.

[Betch (2014)] 'DNA Fingerprint in Human Health and Society'. D Betch . http://archive.ndsj.org/classes/evashenk/bio2/assignments/DNA/ *Biotechnology Information Series* 19/11/2014. (DNA Fingerprinting Human Health Society)

[Mihir ()] *DSP Implementation of a Fingerprintsbased Biometric Authentication System*, M Mihir . 2004. New Zealand. p. . De partment of Electrical & Computer Engineering, University of Auckland (Part 4 Final Project Report)

[Deny and Sudhararajan ()] 'Efficient Methods of Multimodal Biometric Security System-Fingerprint Authentication, Speech and Face Recognition'. J Deny , M Sudhararajan . `www.researchpublish.com` *International Journal of Electrical and Electronics* 2011. 2 (2) p. .

[Marcialis and Roli ()] 'Experimental Results on Fusion of Multiple Fingerprint Matchers'. G L Marcialis , F Roli . *Proceedings of 4 th Int'l Conf. on Audio and Videobased Biometric Person Authentication (AVBPA)*, (4 th Int'l Conf. on Audio and Videobased Biometric Person Authentication (AVBPA)Guildford, UK) 2003. p. .

[Marcialis and Roli ()] 'Experimental Results on Fusion of Multiple Fingerprint Matchers'. G L Marcialis , F Roli . *Proceedings of 4 th Int'l Conf. on Audio and Videobased Biometric Person Authentication (AVBPA)*, (4 th Int'l Conf. on Audio and Videobased Biometric Person Authentication (AVBPA)Guildford, UK) 2003. p. .

[Bigun et al. ()] 'Expert Conciliation for Multimodal Person Authentication Systems Using Bayesian Statistics'. E Bigun , J Bigun , B Duc , S Fischer . *Proceedings of First International Conference on AVBPA*, (First International Conference on AVBPACrans-Montana, Switzerland) 1997. p. .

[Toh et al. ()] 'Exploiting Global and Local Decisions for Multimodal Biometrics Verification'. K A Toh , X Jiang , W Y Yau . *IEEE Transactions on Signal Processing* 2004. 52 p. .

[Chang et al. ()] 'Face recognition using 2D and 3D facial data'. K I Chang , K W Bowyer , P J Flynn . *Proceedings of Workshop on Multimodal User Authentication*, (Workshop on Multimodal User AuthenticationSanta Barbara, CA) 2003. p. .

[Li ()] *Face Recognition: Methods and Practice*, S Z Li . 2012. India. Center for Biometrics and Security Research (CBSR) & National Lab of Pattern Recognition (NLPR) Institute of Automation, Chinese Academy of Sciences: ICB Tutorial Delhi

[Ahmad ()] 'Feature Extraction and Information Fusion in Face and Palmprint Multimodal Biometrics'. M I Ahmad . *A PhD Thesis Submitted to the Faculty of Science*, 2013. Agriculture and Engineering, Newcastle University

[Jain et al. ()] 'Filterbank-Based Fingerprint Matching'. A K Jain , S Prabhakar , L Hong , S Pankanti . *IEEE Transaction on Image Processing* 2000. 9 (5) p. .

[Karu and Jain ()] 'Fingerprint classification'. K Karu , A Jain . *Pattern Recognition* 1996. 18 (3) p. .

[Jain and Pankanti ()] *Fingerprint Classification and Matching*, A Jain , S Pankanti . `http://www.research.ibm.com/ecvg/pubs/sharat-handbook.pdf` 2004. 2004.

[Wang and Zhang ()] 'Fingerprint Classification by Directional Fields'. S Wang , W Zhang . `http://aya.technion.ac.il/projects/2005winter/Fingerprint1.pdf.Accessed13/08/2012` *Proceedings of the Fourth IEEE International Conference on Multi-modal Interfaces*, (the Fourth IEEE International Conference on Multi-modal Interfaces) 1995.

[Hong and Jain ()] 'Fingerprint Enhancement'. L Hong , A Jain . *Automatic Fingerprint Recognition Systems, N. Ratha and R. Bolle*, (New York) 2004. Springer-Verlag.

[Jamieson et al. ()] 'Fingerprint Identification: An Aid to the Authentication Process'. R Jamieson , G Stephen , S Kuma . *Information Systems Audit and Control Association* 2005. 1.

[Raymond ()] *Fingerprint image enhancement and minutiae extraction*, T Raymond . 2003. 16/05/2009. Submitted to School of Computer Science and Software Engineering, University of Western Australia (Postgraduate Thesis)

[Iwasokun et al. ()] 'Fingerprint Image Enhancement: Segmentation to Thinning'. G B Iwasokun , O C Akinyokun , B K Alese , O Olabode . *International Journal of Advanced Computer Science and Applications (IJACSA)* 2012. 3 (1) p. .

[Jain et al. ()] *Fingerprint Matching*, A K Jain , F Jianjiang , N Karthik . 2011. IEEE Computer Society. p. .

[Khazaei and Mohades ()] 'Fingerprint Matching and Classification using an Onion Layer algorithm of Computational Geometry'. H Khazaei , A Mohades . *International Journal of Mathematics and Computers in Simulation* 2007. 1 (1) .

[Nandakumar ()] 'Fingerprint Matching Based On Minutiae Phase Spectrum'. K Nandakumar . *Proceedings of ICB2012*, (ICB2012) 2012.

[Kawagoe and Tojo ()] 'Fingerprint Pattern Classification'. M Kawagoe , A Tojo . *Journal of Pattern Recognition* 1984. 17 (3) p. .

[Mali and Bhattacharya] 'Fingerprint Recognition Using Global and Local Structures'. K Mali , S Bhattacharya . *International Journal on Computer Science and Engineering (IJCSE)* 3 (1) .

[Tha and Tam ()] 'Fingerprint Recognition Using Standardized Fingerprint Model'. L H Tha , H N Tam . *IJCSI International Journal of Computer Science Issues* 2010. 7 (7) .

[Bo et al. ()] 'Fingerprint Singular Point Detection Algorithm by Poincaré Index'. J Bo , H P Tang , M L Xu . *WSEAS Transactions on Systems* 2008. 7 (12) .

[Yount ()] *Forensic Science: From Fibres to Thumbprints*, L Yount . 2007. Chelsea House Publisher.

[Buyssens and Revenu (2013)] *Fusion Levels of Visible and Infrared Modalities for Face Recognition*, P Buyssens , M Revenu . `Avaialble:www.researchgate.net` Accessed19/06/ 2013. Caen, France. GREYC Laboratory -CNRS UMR 6072 ENSICAEN, University of Caen

[Ben-Yacoub et al. ()] 'Fusion of Face and Speech Data for Person Identity Verification'. S Ben-Yacoub , Y Abdeljaoued , E Mayoraz . *IEEE Transactions on Neural Networks* 1999. 10 p. .

[Wang et al. ()] 'Fusion of static and dynamic body biometrics for gait recognition'. L Wang , H Ning , T Tan , W Hu . *IEEE Transactions on Circuits and Systems for Video Technology*, 2004. p. .

[Dawson ()] 'Gait Recognition'. M R Dawson . 14/03/ 2013. `http://rageuniversity.org/DISGUISETECH/files/Gait%20Recognition%20REPORT.PDF` *Technology & Medicine London* 2002. Master of Engineering Thesis submitted to the Department of Computing, Imperial College of Science

[Boulgouris and Chi ()] 'Gait recognition using radon transform and linear discriminant analysis'. N V Boulgouris , Z X Chi . *IEEE Trans. Image Process* 2007. 16 (3) p. .

[Boreki and Zimmer ()] 'Hand geometry: a new approach for feature extraction'. G Boreki , A Zimmer . *Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies*, (the Fourth IEEE Workshop on Automatic Identification Advanced Technologies) 2005. p. .

[Daugman ()] 'How iris recognition works'. J Daugman . *IEEE Transactions on Circuits and Systems for Video Technology*, 2004. 14 p. .

[Nanavati et al. ()] 'Identifying Verification in a Networked World'. S Nanavati , M Thieme , R Nanavati . *Biometrics* 2002. John Wiley & Sons, Inc. p. .

[Pellerin ()] 'Increasing Accuracy in Multimodal Biometric Systems'. K Pellerin . *GIAC Security Essentials Certification (GSEC)* 2004.

[Ross and Jain ()] 'Information fusion in biometrics'. A Ross , A K Jain . *Pattern Recognition Letters* 2003. 24 p. .

[Hong and Jain ()] 'Integrating Faces and Fingerprints for Personal Identification'. L Hong , A K Jain . 23/02/2014. *IEEE Transactions on PAMI* 1998. 20 p. .

[Kuncheva et al. ()] 'Is independence good for combining classifiers?'. L I Kuncheva , C J Whitaker , C A Shipp , R P W Duin . *Proceedings of Int'Conf. on Pattern Recognition (ICPR)*, (Int'Conf. on Pattern Recognition (ICPR)Barcelona, Spain) 2000. 2 p. .

[Shekhar et al. ()] 'Joint Sparse Representation for Robust Multimodal Biometrics Recognition'. S Shekhar , V M Patel , M N Nasrabadi , R Chellappa . *IEEE Transactions on Pattern Analysis and Machine Intelligence* 2013.

[Snelick et al. ()] 'Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems'. R Snelick , U Uludag , A Mink , M Indova , A Jain . *IEEE Transactions on Pattern Analysis and Machine Intelli-gence*, 2005. 27 p. .

[Humbe et al. ()] 'Mathematical Morphology Approach for Genuine Fingerprint Feature Extraction'. V Humbe , S S Gornale , K Ramesh , V Kale . *International Journal of Computer Science and Security* 2007. 1 (2) .

[Xu et al. ()] 'Methods of Combining Multiple Classifiers and their Applications to Handwriting Recognition'. L Xu , A Krzyzak , C Suen . *IEEE Transactions on Systems, Man and Cybernetics* 1992. 22 (3) p. .

[Karray et al. (2013)] *Multi Modal Biometric Systems: A State of the Art Surve*, F Karray , J A Saleh , M N Arab , M Alemzadeh . 13/05/2013.

[Soltane and Bakhti ()] 'Multi-Modal Biometric Authentications: Concept Issues and Applications Strategies'. M Soltane , M Bakhti . *International Journal of Advanced Science and Technology* 2012. 48.

[Yadav et al. ()] 'Multimodal Biometric Authentication System: Challenges and Solutions'. S S Yadav , J K Gothwal , R Singh . *Global Journal of Computer Science and Technology* 2011. 11 (16) .

[Eshwarappa and Latte] 'Multimodal Biometric Person Authentication using Speech'. M N Eshwarappa , M V Latte . *IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Artificial Intelligence* (Signature and Handwriting Features)

[Meraoumia et al. ()] 'Multimodal Biometric Person Recognition System based on Iris and Palmprint Using Correlation Filter Classifier'. A Meraoumia , S Chitroub , A Bouridane . *ICCIT* 2012.

[Kim et al. ()] 'Multimodal Biometric System Based on the Recognition of Face and Both Irises'. Y G Kim , K Y Shin , E C Lee , K R Park . *International Journal of Advanced Robotic Systems* 2012. 9 (65) .

[Abdolahi et al. ()] 'Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic'. M Abdolahi , M Mohamadi , M Jafari . *International Journal of Soft Computing and Engineering* 2013. 2 (6) .

[Kazi et al. ()] 'Multimodal Biometric System Using Face and Signature: A Score Level Fusion Approach'. M M Kazi , Y S Rode , S B Dabhade , N N H Al-Dawla , A V Mane , R R Manza , K V Kale . `http://www.bioinfo.in/contents.php?id=33` *Advances in Computational Research*, 2012. 4 p. .

[Kaur et al. ()] 'Multimodal Biometric System Using Speech and Signature Modalities'. M Kaur , A Girdhar , M Kaur . *International Journal of Computer Applications* 2013. 5 (12) .

[Sasidhar et al. ()] 'Multimodal Biometric Systems -Study to Improve Accuracy and Performance'. K Sasidhar , V L Kakulapati , K K Ramakrishna & K , Rao . *International Journal of Computer Science & Engineering Survey (IJCSES)* 2010. 1 (2) .

[Ribaric et al. ()] 'Multimodal Biometric User Identification System for Network Based Applications'. S Ribaric , D Ribaric , N Pavesic . *IEEE Proceeding of Vision, Image and Signal Processing*, 2003. 150 p. .

[Lupu and Lupu (2007)] 'Multimodal Biometrics for Access Control in an Intelligent Car'. C Lupu , V Lupu . *3 rd International Symposium on Computational. Intelligence and Intelligent Informatics -ISCIII*, (Agadir, Morocco) 2007. March 28-30, 2007.

[Zhang et al. ()] 'Multimodal Biometrics Using Geometry Preserving Projections'. T Zhang , X Li , J Tao , Yang . *Pattern Recognition* 2008. 41 p. .

[Khatoon and Ghose ()] 'Multimodal Biometrics: A Review'. N Khatoon , M Ghose . *International Journal of Computer Science and Information Technology & Security* 2013. 3 (3) .

[Ross and Jain ()] 'Multimodal Biometrics: An Overview'. A Ross , A K Jain . *Proceedings of 12th European Signal Processing Conference (EUSIPCO)*, (12th European Signal Processing Conference (EUSIPCO)Vienna, Austria) 2004. p. .

[Lam and Suen ()] 'Optimal Combination of Pattern Classifiers'. L Lam , C Y Suen . *Pattern Recognition Letters* 1995. 16 (9) p. .

[Palm Print Recognition] `http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/palm-print-recognition.pdf.Accessed23/02/2014` *Palm Print Recognition*,

[Chandran and Rajesh ()] 'Performanance Analysis of Multimodal Biometric System Authentication'. G C Chandran , R S Rajesh . *IJCSNS-International Journal of Computer Science and Network Security* 2009. 9 (3) .

[Fathima et al. ()] 'Person Authentication System with Quality Analysis of Multimodal Biometrics'. A A Fathima , S Vasuhi , T M Treesa , N T Naresh-Babu , V Vaidehi . *WSEAS Transactions on Information Science and Applications* 2013. 10 (6) .

[Brunelli and Falavigna ()] 'Person identification using multiple cues'. R Brunelli , D Falavigna . *IEEE Transactions on PAMI* 1995. 12.

[Kumar et al. ()] 'Personal verification using palmprint and hand geometry biometric'. A Kumar , D C M Wong , H C Shen , A K Jain . *Proc. of 4th Int'l Conf. on Audio and Video-based Biometric Person Authentication (AVBPA)*, (of 4th Int'l Conf. on Audio and Video-based Biometric Person Authentication (AVBPA)Guildford, UK) 2003. p. .

[Kounoudes et al. ()] 'POLYBIO: Multimodal Biometric Data Acquisition Platform and Security System'. A Kounoudes , N Tsapatsoulis , Z Theodosiou , M Milis . Lecture Notes In Computer Science 2008. 5372 p. .

[Vatsa et al. ()] *Quality Induced Fingerprint Identification Using Extended Feature Set*, M Vatsa , R Singh , A Noore , S K Singh . 2008. IEEE.

[Kumar and Imran ()] 'Research Avenues in Multimodal Biometrics'. G H Kumar , M Imran . *IJCA Special Issue on"Recent Trends in Image Processing and Pattern Recognition*, 2010. (RTIPPR)

[Mane and Judhav] 'Review of Multimodal Biometrics: Applications, Challenges and Research Areas'. V M Mane , D V Judhav . *International Journal of Biometric and Bioinformatics* 3 (3) .

[Vélez et al. ()] 'Robust off-line signature verification using compression networks and positional cuttings'. J F Vélez , Á Sánchez , A B Moreno . *Proceedings of the 2003 IEEE Workshop on Neural Networks for Signal Processing*, (the 2003 IEEE Workshop on Neural Networks for Signal Processing) 2003. p. .

[Jain et al. ()] *Score Normalization in Multimodal Biometric Systems*, A Jain , K Nandakumar , A Ross . 2005. 38.

[Devi ()] 'Secure Crypto Multimodal Biometric System for the Privacy Protection of User Identification'. M Devi . *International Journal of Innovative Research in Computer and Communication Engineering* 2014. 2.

[Dieckmann et al. ()] 'Sesam: A biometric Person Identification System Using Sensor Fusion'. U Dieckmann , P Plankensteiner , T Wagner . *Pattern Recognition Letters* 1997. 18 (9) p. .

[Weng et al. ()] 'Singular Points Detection Based on Multi-Resolution in Fingerprint Images'. D Weng , Y Yilong , Y Dong . *Journal of Neuro-Computing* 2011. 74 p. .

[Gafurov et al. ()] 'Spoof attacks on gait authentication system'. D Gafurov , E Snekkenes , P Bours . *IEEE Transactions on Information Forensics and Security* 2007. 2 (3) p. .

[Yun ()] 'The '123' of Biometric Technology'. Y W Yun . *Synthesis Journal* 2002. p. .

[Lupu ()] 'The Annals of The ?tefan cel Mare University of Suceava. Fascicle of The Faculty of'. C Lupu . *Economics and Public Administration* 2010. 10. (Car Access Using Multimodal Biometrics)

[Wambaugh ()] *The Blooding*, J Wambaugh . 1989. William Morrow, N.Y..

[Daugman ()] 'The importance of being random: statistical principles of iris recognition'. J Daugman . *Pattern Recognition* 2003. 36 (2) p. .

[Zuev and Ivanon ()] 'The Voting as a way to increase the decision reliability'. Y Zuev , S Ivanon . *Foundations of Information/ Decision Fusion with Applications to Engineering Problems*, (Washington D.C., USA) 1996. p. .

[Sara et al. ()] *User interface design of the interactive fingerprint recognition (INFIR) System*, N Sara , D Sergie , V Gregory . http://www.researchgate.net/profile/Sara_Nasser2/zpublication/221199370_User_Interface_Design_of_the_Interactive_Fingerprint_Recognition_(INFIR)_System/links/0fcfd509c0e72c9b2c000000.pdf.Accessed12/11/2013 2004.

[Voice Recognition and Speech Recognition (VRSR) Software and Vendors Guide] *Voice Recognition and Speech Recognition (VRSR) Software and Vendors Guide*, http://www.voice-commands.com/51 (Biometric identification)

[Levine et al. ()] *Whittle's Gait Analysis*, D F Levine , J Richards , M Whittle . 2012. Elsevier Health Sciences.