**ADEKUNLE AJASIN UNIVERSITY**

**DEPARTMENT OF COMPUTER SCIENCE**

**A MULTIMODAL BIOMETRIC RECOGNITION SYSTEM**

**USING FACE AND FINGERPRINT**

**NAME: ADEFUWA OLUWAPONMILE HUSSEIN**

**MATRIC NO: 160404013**

**SUPERVISOR**

**DR. ARANUWA, F.O**

**CHAPTER ONE**

**INTRODUCTION**

* 1. **BACKGROUND TO THE STUDY**

By definition, biometrics has been described as the science and technology of recognizing an individual based on his or her physiological or behavoural traits (Akhtar and Affrarid, 2011). Stanley, Jeberson, and Klinsega (2009) described biometrics as the most secured and convenient authentication tool that cannot be stolen, forgotten, borrowed or forged. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known) and consequently that they belong to a group with certain rights (or to a group to be denied certain privileges). It relies on the presumption that individuals are physically and behaviorally distinctive in a number of ways. Biometric systems are used increasingly to recognize individuals and regulate access to physical spaces, information, services, and to other rights or benefits, including the ability to cross international borders. Biometrics is a rapidly developing branch of information technology. There are several advantages of biometric technologies compared to traditional identification methods. This include adequate measures against increasing security risks in modern world, and prevention in the access of an unauthorized identity (Delac and Mislavgrgic, 2014).

Biometric traits are classified into physiological and behavioral traits. Examples of physiological traits include fingerprints, face, eye retina, facial patterns, and hand measurements. Examples of behavioraltraits include writing signatures, gaits, and typing patterns. Voice recognition is considered a combination of both physical and behavioraltraits. (Reid et al, 2013). This work considered two basic biometric physiological biometrics traits i.e face and fingerprint.

The intent of this work is to combine two biometric traits, specifically face and fingerprint Ridge based and Eigen face features are going to be combined for a parallel execution respectively. The aim is to reduce acceptance and rejection errors in the unimodal biometric system.

Experimental studies have shown that Unimodal biometric systems had little challenges. Hence the need for multimodal biometric system to overcome the challenges. (Rubiyah, 2010). According to Mane and Jadhav (2009) noisy data, intraclass variation, interclass similarities, non-universality and spoof which usually leads to poor performance of the system. Some of the limitations imposed by unimodal biometrics can be overcome by including multiple source of information for establishing identity of person. Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a single verification or identification system (Shyam, 2011). They address the problem of non- universality, since multiple traits ensure sufficient population coverage. Multimodal biometrics also address the problem of spoofing as it concern with multiple traits or modalities, it would be very difficult for an imposter to spoof or attack multiple traits of genuine user simultaneously. Multimodal biometric system has the potential to be widely adopted in a very broad range of applications: banking security such as ATM security, check cashing and credit card transactions, information system security like access to databases via login privileges. Generally biometrics operates in two phases i.e. Enrollment phase and authentication phase which are described as follows:

1. Enrollment phase: - In enrollment phase, biometric traits of a user are captured and these are stored in the system database as a template for that user and which is further used for authentication phase.
2. Authentication phase: - In authentication phase, once again traits of a user captured and system uses this to either identify or verify a person. Identification is one to many matching which involves comparing captured data with templates corresponding to all users in database while verification is one to one matching which involves comparing captured data with template of claimed identity only.

**1.2 STATEMENT OF PROBLEM**

Studies have shown that biometric with single traits has this tendency to faced with challenges such as noisy data, intraclass variation, interclass similarities, spoofing etc, which recedes the efficiency of the system . Combining multiple traits have been suggested as possible solution, but integrating the evidences has been an issue that attract research attention.

**1.3 AIM AND OBJECTIVES**

The aim of this work is to develop a multi modal biometric system using face recognition and finger print and model a fusion strategy that will combine the evidences effectively.

Specific objectives are:

1. To develop a system that can enroll and verify an individual using both face and finger print traits.
2. To acquire data from the two traits and implement the proposed system.
3. To model a fusion strategy to combine the evidences from the two traits
4. Evaluate the performance of the system.
   1. **RESEARCH METHODOLOGY**

To achieve the objective of this work, the following method shall be considered.

1. Conduct a review of related works the domain.
2. Acquiring data for the trait from selected population.
3. Develop a system prototype to test the proposed system.
4. Evaluate the performance of the system.
   1. **CONTRIBUTION TO KNOWLEDGE**

At the completion of this work, the research work will profer solution to challenges imposed by unimodal biometric system and improve the efficiency of the biometric system.

* 1. **DEFINITION OF TERMS**

**Recognition:** widely use term is identification.

**Response Time:** the amount of time in which a biometric system analyzes a sample and returns with a decision.

**Multimodal:** Multimodal biometricsystems work on accepting information from two or more biometricinputs.

**Finger Ridge:** In the biometric process of finger scanning, a ridge is a curved line in a finger image.

**Biometric:** A physical trait or pattern which is unique to every individual. It often used to Verifying and authenticate a person’s identity who is enrolled into a system. Biometric patterns can be anything from fingerprints, iris scans, facial recognition or even voice recognition.

**Biometric Application**: the implementation of any system that involves biometric data.

**Biometric data**: A sample taken from individual which is unique to their own person. Common biometric data are: fingerprint, voice and iris scans, palm vein patterns and even facial patterns.

**Capture:** the process of collecting biometric data from the end user or enrollee. Most biometric data are “captured” by use of an image scanner in cases of fingerprints, palm vein patterns or a camera to collect facial and iris scans.

**Face Recognition**: facial features are analyzed and gathered as biometric data.

**Eigen Face:** a method that represents the human face as a linear deviation from an average or mean face.

**Enrolment**: Gathering and processing of biometric data with the intent of storing them into a database.

**Extraction**: The moment a biometric sample is converted into data after which it compared to a biometric template

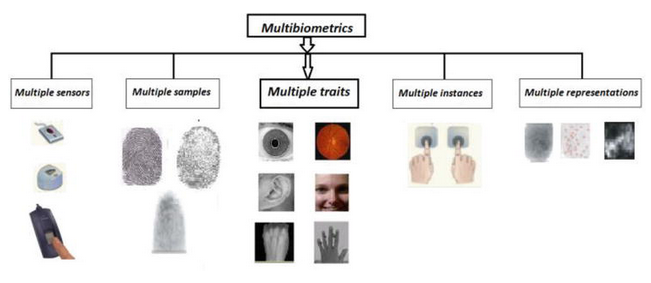
**CHAPTER TWO**

**LITERATURE REVIEW**

**2.1 MULTIMODAL BIOMETRIC**

Multimodal biometrics refers to the use of a combination of two or more biometric modalities in an identification system. For instance, a system that combines face and fingerprint recognition can be considered as a multimodal biometric system. Multimodal biometrics provides supplementary information among different modalities in order to increase the recognition performance in terms of accuracy and reliability to overcome the drawbacks of a single biometric system. (Ahmed, 2014)

The multi-biometric system can be (a) a multi-sensor system that allows obtaining data from various sensors using one biometric feature, (b) a system with multiple algorithms processing a single biometric feature, (c) a system consolidating multiple occurrences of the same body trait, (d) a system using multiple templates of the same biometric method obtained with the help of a single sensor, and (e) a multimodal system combining information about the biometric features of the individual to establish his identity

****

**FIGURE 2.1 SAMPLE OF A MULTIMODAL SYSTEM**

Multimodal biometric system certainly offers considerable improvements in reliability, accuracy and reduce error rate with reasonably overall performance in many applications over the unimodal biometric system. The new paradigm has become an underpinning of highly secured identification and personal verification solutions, more importantly in the wake of heightened concern about security challenges in our world today. However, the issue of efficient and effective integration of the evidences obtained from different traits and its computational complexity remains an overt concept that attracts research attention. Several different fusion techniques such as rule based, statistical methods and machine learning algorithms have been proposed for biometric information fusion at different levels such as, feature level, match score level, and decision level. (Aranuwa, 2016) In addition, since each biometric approach provides a certain confidence about the identity being established, a decision fusion scheme which exploits all the information at the output of each module can be used to make a more reliable decision.

**2.2 FACE RECOGNITION**

A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. Face recognition systems are usually applied and preferred for people and security cameras in metropolitan life. These systems can be used for crime prevention, video surveillance, person verification, and similar security activities. (Cahit, 2012). There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within database (Kriby, 2010). Face recognition system is a complex image-processing problem in real world applications with complex effects of illumination, occlusion, and imaging condition on the live images. It is a combination of face detection and recognition techniques in image analyzes. Detection application is used to find position of the faces in a given image. Recognition algorithm is used to classify given images with known structured properties, which are used commonly in most of the computer vision applications. Recognition applications use standard images, and detection algorithms detect the faces and extract face images which include eyes, eyebrows, nose, and mouth. That makes the algorithm more complicated than single detection or recognition algorithm. (Abdulkadir, 2012)

Facial recognition includes five steps to complete their process.

Step1: ACQUIRING THE IMAGE OF AN INDIVIDUALS FACE; 2 WAYS TO AQUIRE IMAGE:

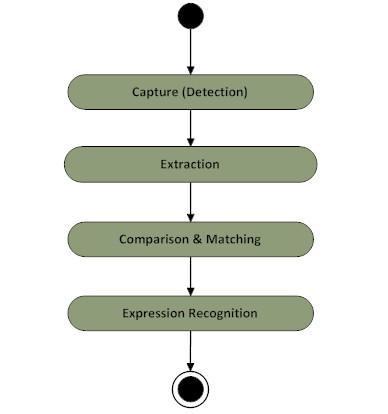
1. Digitally scan an existing photograph;
2. Acquire a live picture of a subject.

Step2: LOCATE FACE IN THE IMAGE CAPTURED: software is used to locate the faces in the image that has been obtained.

Step3: FEATURE EXTRACTION IN FACE: software measures face according to is peaks and valleys; focuses on the inner area of the face identified as the “golden triangle”, valleys are used to create a face print with their nodal points.

Step4: COMPARISON: the face print created by the software is compared to all face prints the system has stored in its database.

Step5: MATCHING: software decides whether or not any comparisons from step 4 are close enough to declare a possible match.



**FIGURE 2.2 DEPICT TYPICAL FACE RECOGNITION ARCHITECTURE**

Facial recognition utilizes distinctive features of the face including the upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and eyes to perform verification and identification. Most technologies are fairly resistant to modest changes in haircut as they do not exploit areas of the face located near the hairline. When used in identification mode, facial recognition technology generally returns candidate lists of close matches as opposed to returning a single definitive match. (Zdene, 2001)

* 1. **FACE RECOGNITION ALGORITHMS**

Throughout the past few decades there have been many face recognition algorithms proposed and implemented. Some of the common methods described are presented below;

* + 1. **PRINCIPAL COMPONENT ANALYSIS (PCA)**

In high-dimensional data, this method is designed to model linear variation. Its goal is to find a set of mutually orthogonal basis functions that capture the directions of maximum variance in the data and for which the coefficients are pairwise decorrelated. For linearly embedded manifolds, PCA is guaranteed to discover the dimensionality of the manifold and produces a compact representation. PCA is used to describe face images in terms of a set of basic functions, or “Eigen faces”. Eigen faces was introduced early on as powerful use of principal components analysis (PCA) to solve problems in face recognition and detection. PCA is an unsupervised technique, so the method does not rely on class information. (Jonatan et al., 2005).

* + 1. **MULTILINEAR PRINCIPAL COMPONENTS ANALYSIS (MPCA)**

One extension of PCA is that of applying PCA to tensors or multi linear arrays which results in a method known as multilinear principal components analysis (MPCA). Since a face image is most naturally a multilinear array, meaning that there are two dimensions describing the location of each pixel in a face image, the idea is to determine a multi linear projection for the image, instead of forming a one- dimensional (1D) vector from the face image and finding a linear projection for the vector. It is thought that the multilinear projection will better capture the correlation between neighborhood pixels that is otherwise lost in forming a 1D vector from the Image (Lu et al., 2008).

* + 1. **LINEAR DISCRIMINANT ANALYSIS (LDA)**

Fisher faces is the direct use of (Fisher) linear discriminant analysis (LDA) to face recognition. LDA searches for the projection axes on which the data points of different classes are far from each other while requiring data points of the same class to be close to each other. Unlike PCA which encodes information in an orthogonal linear space, LDA encodes discriminating information in a linearly separable space using bases that are not necessarily orthogonal. It is generally believed that algorithms based on LDA are superior to those based on PCA. However, other work such as showed that, when the training data set is small, PCA can outperform LDA, and also that PCA is less sensitive to different training data sets(Cai et al.,2005).

* + 1. **INDEPENEDENT COMPONENT ANALYSIS (ICA)**

ICA is a generalization of PCA in that it tries to identify high-order statistical relationships between pixels to form a better set of basis vectors, where the pixels are treated as random variables and the face images as outcomes. In a similar fashion to PCA and LDA, once the new basis vectors are found, the training and test data are projected into the subspace and a method such as NN is used for classification. The code for ICA was provided by the authors for use in face recognition research (Rahman et al., 2012)

* + 1. **EDGE BASE**

Face detection based on edges was introduced by (Sakai et al,. 1969). This work was based on analyzing line drawings of the faces from photographs, aiming to locate facial features. It is a very important area in the field of Computer Vision. Edges are responsible for defining the boundaries between regions in an image, which helps with segmentation and recognition of object. They are almost successful in showing where the shadows fall in an image or any other distinct change in the intensity of an image. (Reema, 2013)

**2.3.6 LOCAL BINARY PATTERN HISTOGRAM (LBPH)**

(LBP) is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number. It was first described in 1994 (LBP) and has since been found to be a powerful feature for texture classification. It has further been determined that when LBP is combined with histograms of oriented gradients (HOG) descriptor, it improves the detection performance considerably on some datasets. Using the LBP combined with histograms we can represent the face images with a simple data vector. (Nikhil, 2018). It is designed to be a texture analysis for the gray-scale image. To detect faces in an RBG (colored) photo, we have to convert the image into a grayscale image at first. In this work, the researcher has chosen to use this algorithm.

**2.4 FINGERPRINT RECOGNITION**

Fingerprint recognition is one of the most mature biometric technologies and is suitable for a large number of recognition applications. Live scan fingerprint scanners can easily capture high quality fingerprint images. The matching stage uses the position and orientation of minutia features. As a result, the reliability of feature extraction is crucial in the performance of fingerprint matching.

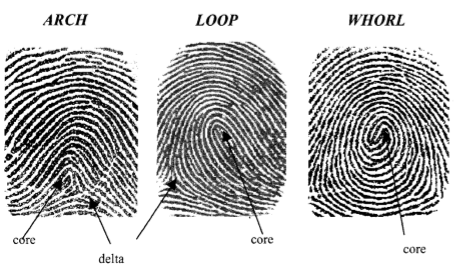
**2.4.1 MATCHING IN FINGERPRINT**

Matching can be classified into two categories: verification and identification. It is the comparison of a claimant fingerprint against an enrollee fingerprint, where the intention is that the claimant fingerprint matches the enrollee fingerprint. For verification process, a person initially enrolls his or her fingerprint into the verification system. A representation of that fingerprint is stored in some compressed format along with the person's name or other identity. Subsequently, each access is authenticated by the person identifying him or herself, then applying the fingerprint to the system such that the identity can be verified. Verification is also termed, one-to-one matching. Identification is the traditional domain of criminal fingerprint matching. A fingerprint of unknown ownership is matched against a database of known fingerprints to associate while identification is termed as, one-to many matchings. There is an informal third type of matching that is termed one-to-few matching. This is for the practical application where a fingerprint system is used by "a few" users, such as by family members to enter their house.

**2.4.2 FINGERPRINT FEATURE**

The lines that flow in various patterns across fingerprints are called ridges and the spaces between ridges are valleys. It is these ridges that are compared between one fingerprint and another when matching. Fingerprints are commonly matched by one (or both) of two approaches. The more microscopic of the approaches is called minutia matching. The two minutia types are ridge ending and bifurcation.

A bifurcation is a feature where a ridge splits from a single path to two paths at a Y-junction. For matching purposes, a minutia is attributed with features. These are type, location (x, y), and direction (and some approaches use additional features).



**FIGURE 2.3 FINGERPRINT PATTERNS: ARCH, LOOP, AND WHORL. FINGERPRINT LANDMARKS ARE ALSO SHOWN: CORE AND DELTA.**

**2.4.3 FINGERPRINT IMAGE PROCESSING AND VERIFICATION**

Today, image processing techniques are developed for automatic biometric systems by applying machine learning and deep learning techniques. Image scaling, image filtering and other morphological techniques are used to remove unwanted noise.

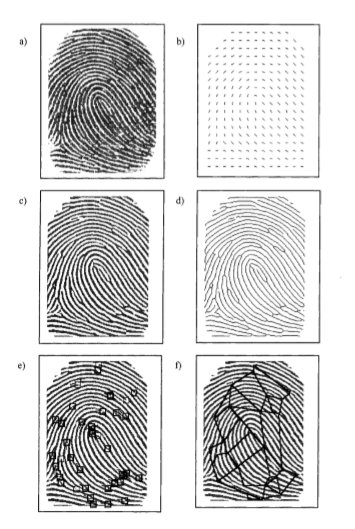
Binarizing image, thinning image and image enhancement techniques are used to get the perfect pattern of an image.

**2.4.4 IMAGE SPECIFICATIONS**

Depending upon the fingerprint capture device, the image can have a range of specifications. Commonly, the pixels are 8-bit values, and this yields an intensity range from 0 to 255. The image resolution is the number of pixels per unit length, and this ranges from 250 dots per inch (100 dots per centimeter) to 625 dots per inch (250 dots per centimeter), with 500 dots per inch (200 dots per centimeter) being a common standard. The image area is from 0.5 inches square (1.27 centimeter) to 1.25 inches (3.175 centimeter), with 1 inch (2.54 centimeter) being the standard.

**2.4.5 FEATURE EXTRACTION IN FINGER PRINT**

After a fingerprint image as been captured, the next step is the extraction of features from the images. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window. The most commonly employed method of minutiae extraction is the Crossing Number concept. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight neighborhoods. Using the properties of the CN, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point.. For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation.



**FIGURE 2.4 SEQUENCE OF FINGERPRINT PROCESSING STEP**

**a) Original, b) Orientation, c)Binarized, d)Thinned, e)Minutiae, f)Minutia graph**

Feature attributes are determined for each valid minutia found. These consist of: ridge ending or bifurcation type, the (x,y) location, and the direction of the ending or bifurcation. Although minutia type is usually determined and stored, many fingerprint matching systems do not use this information because discrimination of one from the other is often difficult. The result of the feature extraction stage is what is called a minutia template. This is a list of minutiae with accompanying attribute values. An approximate range on the number of minutiae found at this stage is from 10 to 100. If each minutia is stored with type (1 bit), location (9 bits each for x and y), and direction (8 bits), then each will require 27 bits — say 4 bytes - and the template will require up to 400 bytes. It is not uncommon to see template lengths of 1024 bytes.

At the verification stage, the template from the claimant fingerprint is compared against that of the enrollee fingerprint. This is done usually by comparing neighborhoods of nearby minutiae for similarity. A single neighborhood may consist of three or more nearby minutiae. Each of these is located at a certain distance and relative orientation from each other. Furthermore, each minutia has its own attributes of type (if it is used) and minutia direction, which are also compared. If comparison indicates only small differences between the neighborhood in the enrollee fingerprint and that in the claimant fingerprint, then these neighborhoods are said to match. This is done exhaustively for all combinations of neighborhoods and if enough similarities are found, then the fingerprints are said to match.

**2.5 FINGERPRINT MATCHING ALGORITHM**

**2.5.1 CORRELATION-BASED FINGERPRINT MATCHING**

The correlation based ﬁngerprint matching algorithms are the older matching algorithm. Correlation between images ﬁngerprint considers similarity measure of the fundamental features. As a result of the inevitable differences of two ﬁngerprint impressions (rotation, displacement), a simple superposition of the images do not resolve the ﬁngerprint matching problem. In order to deal with some of the problems of the minutiae-based approach, that has brought up this approach. Instead of only using the minutiae locations, this method directly uses the gray-level information from the ﬁngerprint image, since a gray-level ﬁngerprint image contains much richer, more discriminatory, information than only the minutiae locations. Those locations only characterize a small part of the local ridge-valley structures. The correlation-based ﬁngerprint veriﬁcation system is inspired by Roddy (1999). It ﬁrst selects characteristic templates in the primary ﬁngerprint. Then, template matching is used to ﬁnd the positions in the secondary ﬁngerprint at which the templates match best. Finally, the template positions in both ﬁngerprints are compared in order to make the decision whether the prints match.

**2.5.2 MINUTAE BASED FINGERPRINT ALGORITHM**

Fingerprint matching algorithms based on minutiae are the most used and the best known technique. In most countries, minutiae are accepted as legal proof of identity. Each minutiae can be described by multiple attributes, the most common are: its location, orientation, type, the ﬁngerprint image quality of the minutia neighbor-hood, among others. One important step in the minutiae matching process is the alignment of two ﬁngerprint. To obtain a correct alignment of two ﬁngerprints, the displacement (in x and y) and rotation (orientation) are needed. Also, to compensate other geometrical transformation like scale (when the ﬁngerprints images have different resolutions) or other possible distortion tolerances if the ﬁngerprints are affected by severe distortions is important. The ﬁngerprint alignment step has a large computational cost. To avoid the problems caused by the alignment of minutiae and to better deal with local distortions, some authors perform the minutiae matching locally. Very few authors have tried to performed global ﬁngerprint matching without the alignment step. Local matching provides simplicity, low computational complexity, and high tolerance. (Maltoni, 2009). The aim of most minutiae-based algorithms is to compare full ﬁngerprint impressions. To provide an accurate result, these algorithms require a certain number of minutiae. When the ﬁngerprint image have very few usable minutiae (low quality or a small ﬁngerprint area), the performance of these algorithms is very poor (many false positives).

**2.5.3 RIDGE-BASED ALGORITHM**

To minimize the false positives and obtain better alignments due to the absence of a considerable number of minutiae, the use of ﬁngerprints ridge pattern features has been increased. This is an important area, especially in the case of latent prints. For example, level 3 features are frequently used by latent print examiners to assist in identiﬁcation and the idea of ridges in sequence which is recommended by SWGFAST (2005) is used too. Ridge pattern features can be used to increase the accuracy of the ﬁngerprint matching algorithms. Hence, another line of ﬁngerprint matching algorithms may be called ridge feature-based ﬁngerprint matching. In this approach, other ﬁngerprint distinguishing features in replace or addition to minutiae are sought.

To improve the accuracy and robustness of the ﬁngerprint matching algorithm, the ridge pattern features are used with minutiae, not instead of them. It is well known that several techniques of this type use the minutiae in the pre-alignment step or to deﬁne the anchor points.

**2.6 MULTIMODAL BIOMETRIC SYSTEM**

In designing a multimodal biometric system, a number of issues need to be considered: (i) what is the main purpose of utilizing multiple biometrics? (ii) what is the operational mode? (iii) which biometrics should be integrated? and (iv) how many biometrics are sufficient? Since the applicable population and system robustness depend mainly on the characteristics of the selected biometrics, the main problem in designing a multimodal biometric system is the integration of individual biometrics to improve the performance in making a personal identification. Typically, performance refers to (i) accuracy and (ii) speed. System accuracy indicates how reliable and confident a biometric system is in differentiating between a genuine individual and an impostor. System speed refers to the time taken by a biometric system in making a personal identification. By properly incorporating those biometrics that are relatively fast, the overall speed of a biometric system can be improved.

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

1. **Robustness:** It is important to consider how robust the system is to fraud and impersonation. Such fraud can occur at the enrolment stage as well as at the verification stage. Using more than one biometric modality can help combat fraud and increase robustness. Also the system should be robust to small variations of the users’ biometrics over time. For this, an adaptive system that gradually modifies the stored templates may be used.
2. **Acceptability**: The technology must be socially acceptable and easy to use during both the enrolment and comparison phases. The users would not accept a system that may threaten their privacy and confidentiality or that might appear to treat them as potential suspects and criminals.
3. **Speed and Storage Requirements:** The time required to enroll, verify or identify a person is of critical importance to the acceptability and applicability of the system. Ideally, the acceptable verification time should be of the order of one second or faster. The storage requirement for the templates is also an important issue, especially if the templates are to be stored in magnetic stripe or smart cards.
4. **Integration:** The hardware platform on which the system is to be implemented is a key concern. The software, hardware and networking requirements should ideally be compatible with existing systems, allowing the biometric system to be integrated to the existing infrastructure. The system cost should be reasonable and the maintenance costs should be understood.
5. **Legal issues:** This also have to be considered in relation to biometric systems, since there are concerns over potential intrusions into private lives by using biometric systems. Legal issues must be considered for any potential application and appropriate measures must be taken. A clear public stance on the issue of privacy in relation to biometric technologies is required to ensure broad public acceptance.

**2.7 MULTIPLE BIOMETRIC INTEGRATION**

Integration of multiple biometrics for a verification system may be performed in the following scenario: (i) integration of multiple snapshots of single biometrics, for example, a number of fingerprint images of the same finger in fingerprint verification and (ii) integration of a number of different biometrics. In this sense, multimodal biometrics is a conventional decision fusion problem to combine evidence provided by each biometrics to improve the overall decision accuracy.

**2.8 RELATED WORK**

**1. AUTHORS: Elisardo et al, (2009)**

**TOPIC:** Multimodal Biometrics-based Student Attendance Measurement in Learning Management Systems

**AIM:** The aim of this project is to develop a system that will monitor how much time a student spend on a computer.

**METHOD:** The methodology adopted here was the combination of face recognition and voice recognition. The techniques used for the finger was Minutae feature and the Voice adopted the Gaussian Mixture Model-Universal Background Model (GMM-UBM) system where both UBM and user models are 256 mixtures GMMs.

**OBSERVATION AND CONCLUSION:** This paper has presented a multimodal system for control access and student attendance measurement system in LMS environments. The control access is based on multimodal fusion of face and voice. The student attendance measurement system is mainly based on face tracking and face veriﬁcation. Collaborative authentication has been incorporated in the system in order to avoid long periods of time without reliable information about the identity of the tracked faces

**2. AUTHORS:** Sanjekar and Patil (2013)

**TOPIC:** An Overview Of Multimodal Biometrics

**AIM:** The aim of this work is to solve the problem associated to unimodal biometric system by introducing multimodal system.

**METHOD:** Matching Score Level Fusion and decision level fusion techniques was adopted in this paper.

**OBSERVATION AND CONCLUSION:** In this paper, it was observed that multimodal biometrics is frontier to the unimodal biometrics as it overcomes the problems related with unimodal biometrics like noisy data, interclass similarities, intra class variation, non-universality and spoofing. There are many multimodal biometric systems in existence for authentication of a person but still selection of appropriate modals, choice of optimal fusion level and redundancy in the extracted features are some challenges in designing multimodal biometric system that needs to be solve.

**3. AUTHORS: Ross, Nandakumar and Jain (2006)**

**TOPIC:** Handbook of Multibiometric

**AIM:** This work was intended to provide an overview of the state of the art in multi biometrics and technology

**METHOD:** The multi-set canonical correlation analysis is used to fuse multiple feature sets. The feature based on MCCA achieves the recognition performance, with EER = 2.3900e-04

**OBSERVATION AND CONCLUSION:** The work introduces multi-biometric systems, and demonstrates the noteworthy advantages of these systems over their unimodal counterparts. In addition, this book describes in detail the various scenarios that are possible when fusing biometric evidence from multiple information sources.

**4. AUTHORS:** Bokade and Sapkal (2012)

**TOPIC:** Feature level fusion of palm and face for secure recognition

**AIM:** This paper proposes an authentication for a multimodal biometric system identification using two traits i.e., face and palmprint at feature extraction level

**METHOD:** The PCA is used to extract features of palm and face images. Fusion technique concatenated the feature vectors of the face and palm modalities into one fused vector, and feature selection is performed.

**OBSERVATION AND CONCLUSION:** This paper has presented a feature level fusion system of face and palmprint traits using a simple fusion algorithm. Since feature set contains relevant and richer information about the captured biometric evidence, fusion at feature level is expected to provide more accurate results as compared to other fusion methods. The GAR using palm images only is found to be 81.48%. The GAR using face images is found to be 88.88%. The fusion results indicate substantial increase in GAR as compared to GAR obtained using only palm and only face modality and gives overall accuracy more than 95%.

**5. AUTHORS:** Shubhangi D C et al (2012)

**TOPIC:** Artificial Multi-Biometric Approaches to Face and Fingerprint Biometrics

**AIM:** Their work aim in the development of a multi-biometric with the combination of both face and iris. Which would recognize the face first and then the iris in sequence. The trained ANN groups the input pixels into the different clusters which provide the results.

**METHOD:** This paper presents an efficient Face and Fingerprint recognition algorithm combining ridge based matching for the finger and Eigen Face approach for the face.

**OBSERVATION AND CONCLUSION:** Artificial Neural Network (ANN) is implemented. Feature extraction using principle component analysis and recognition using the feed forward back propagation neural network was used.

**CHAPTER THREE**

**RESEARCH METHODOLOGY**

This chapter covers the development processes to achieve the aim of this work. It also covers the system architecture, the algorithm to be used for both recognition techniques and the fusion techniques.

**3.1 SYSTEM ARCHITECTURE**

Figure 3.1 shows the system architecture for the proposed system

Face Acquisition

Fingerprint Acquisition

Decision Threshold

Fusion Information

Feature Extraction and Matching

Feature Extraction and Matching

LBPH Algorithm

(Confidence Value)

Minutae Based Algorithm

(Confidence value)

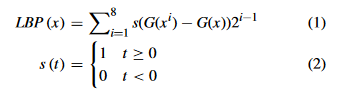
We are concentrated our implementation on LBPH algorithm and Minutiae Based Algorithm for face and fingerprint recognition respectively.

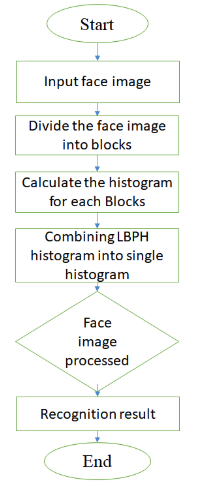
* 1. **SYSTEM ARCHITECTURE COMPONENT ANALYSIS**

**3.2.1 FACE AND FINGERPRINT ACQUISITION:** A persons would be captured by using an HP Laptop default camera and a fingerprint recognition device (Digital Persona) would be used to capture the finger. The faces are saved in the system directory with a unique name and the details of the faces where stored in a database for matching references and the fingerprint template would be saved in bytes in the system database.

* + 1. **FEATURE EXTRACTION IN FACE AND FINGERPRINT**
    2. **FEATURE EXTRACTION IN FACE**

For feature extraction in faces. This involves cropping out the needed face from a person full face and we would be using the LBPH algorithm by OpenCv for the process. It is a simple solution for the face recognition problem, which can be recognizing both the front face and side face. LBP is a simple and efficient text description operator which labels the pixels of an image by thresholds the neighborhood of each pixel and which produce the result as a binary number. Then the LBP combined with histogram. We can represent the face images with a simple data vector.

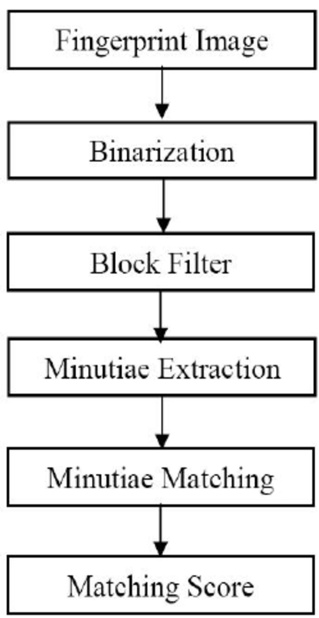




**FIGURE 3.3 LBPH EXTRACTION MODEL**

**3.2.4 FINGERPRINT FEATURE EXTRACTION**

On the other hand feature extraction stage in fingerprint, this uses the minutiae extraction algorithm. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window. The most commonly employed method of minutiae extraction is the Crossing Number concept. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight neighborhoods. An approximate range on the number of minutiae found at this stage is from 10 to 100. If each minutia is stored with type (1 bit), location (9 bits each for x and y), and direction (8 bits), then each will require 27 bits that is 4 bytes and the template will require up to 400 bytes. It is not uncommon to see template lengths of 1024 bytes. This minutae extraction values are saved into templates and stored in the system database. Using the properties of the CN, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point. For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation.

****

**FIGURE 3.4 MINUTIAE EXTRACTION MODEL**

**3.2.5 FUSION AND MATCHING:** The fusion techniques to be used here is summation rule.

A simple summation rule is the most popular combination scheme for combining score values from multiple systems. The scores from different systems is however required to be standardized. The standardization is learned from development dataset by estimating distributions score values from each system. The scores are then translated and scaled to have zero mean and unit variance. The simple sum rule adds the scores of each classifier to calculate the fused score. This can be expressed in the equation stated below:

* + 1. **FACE AND FINGERPRINT RECOGNITION:** For Recognition, a new face and fingerprint is matched with the previously stored faces and finger in the data base for a 1:N matching approach.

**3.3 SYSTEM IMPLEMENTATION**

The system would be developed using Java programming language and MYSQL to create the database. The IDE (Integrated Development Environment) to be used for development is Netbeans and the Database Management System is XAMMP Server.

**CHAPTER FOUR**

**IMPLEMENTATION AND ANALYSIS**.

**4.1 IMPLEMENTATION**

The multimodal system were implemented on Netbeans IDE 8.2 and coded as a Java swing Application. Various pro-programmed libraries were referenced and used for basic Java Swing interface function which include JTextField, JButton, JLabel etc. Other Face recognition libraries where also used like OpenCv, Haar classifier, lbd classifier and for the fingerprints library, the researcher used digital persona UareU4500 library.

**4.1.1 LOGIN SCREEN:** In other to gain access to this system, the admin has the power to login to the system.

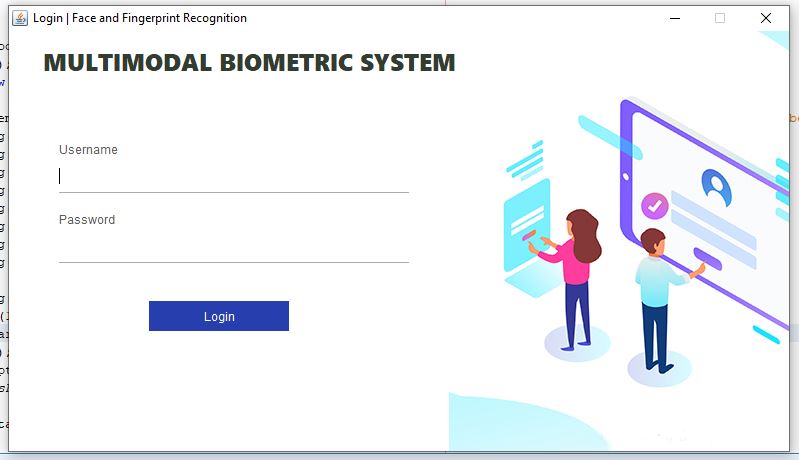


Figure 4.1 Login Screen

**4.1.2 MAIN MENU SCREEN**

This main menu holds all the navigation to both the fingerprint recognition screen and face recognition screen.

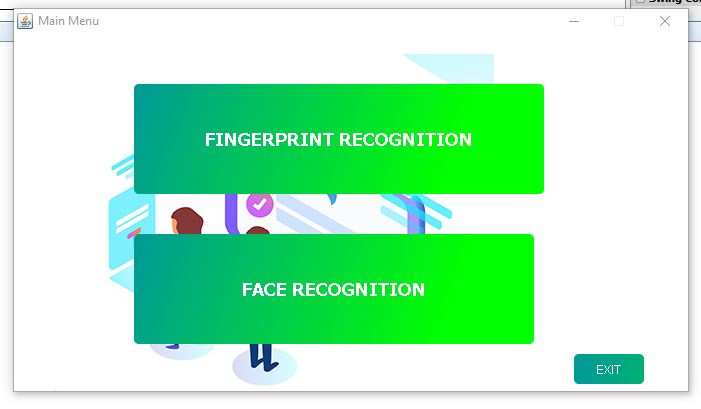
****

Figure 4.2 Main window

**4.1.3 FINGERPRINT ENROLLMENT FORM:** In this section. Faces are detected from an individual, as well as the user details can be captured and saved in the system database

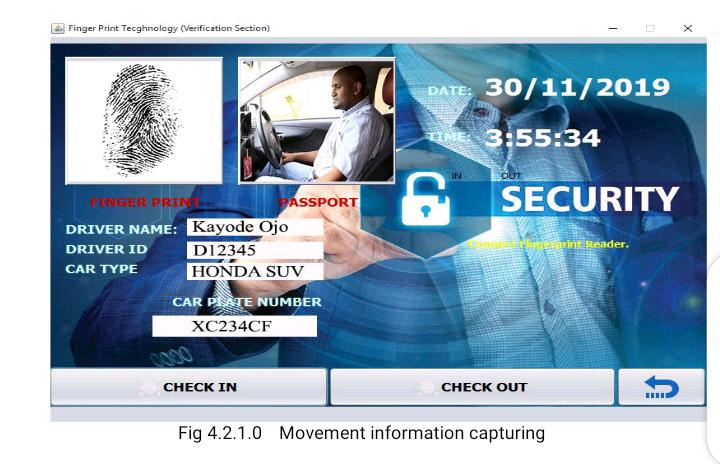
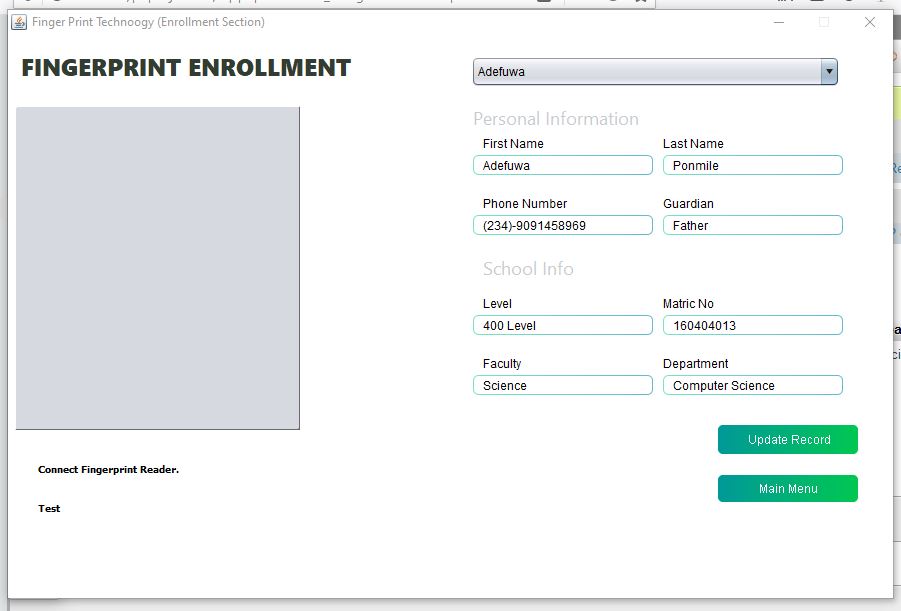
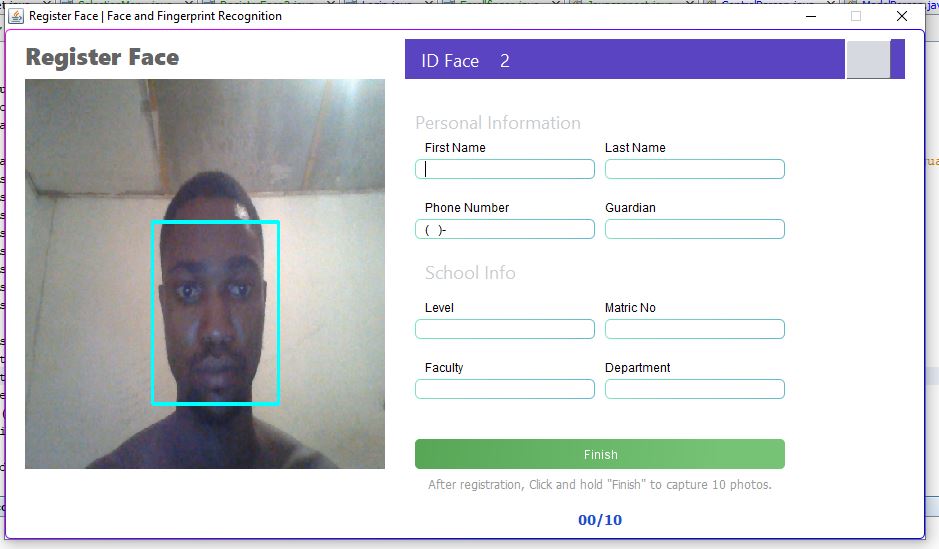
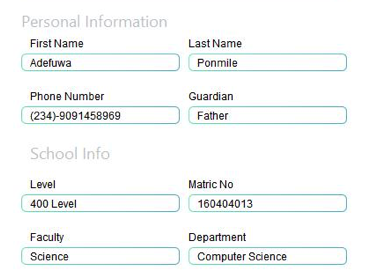
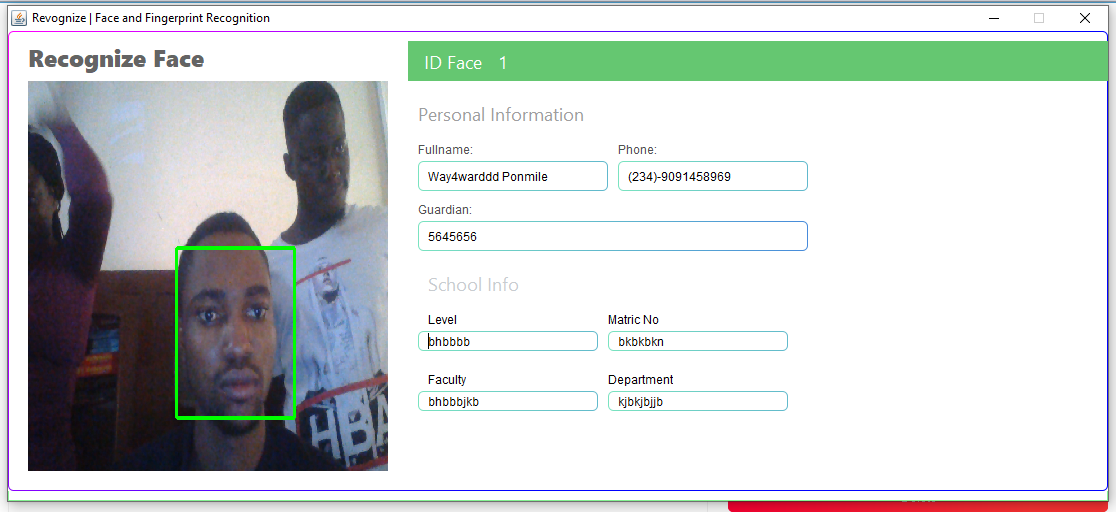


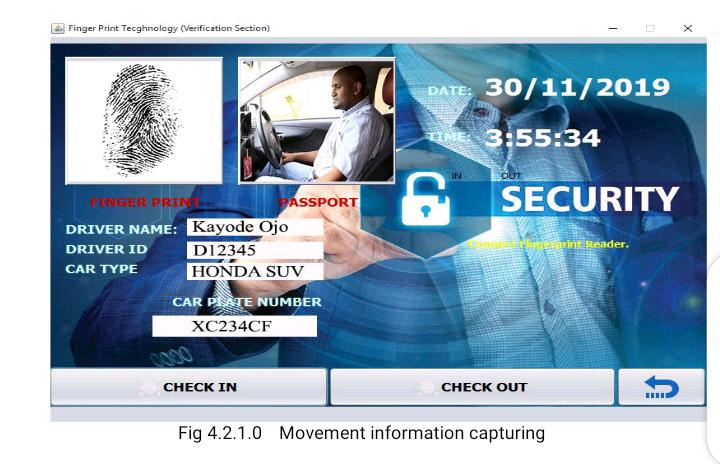
Figure 4.3 Enrollment Screen For Finger

**4.1.4 FACE RECOGNITION ENROLLMENT FORM:** In this section, we can capture the finger of a new user and update it with the data of the same individual whose face has been captured.

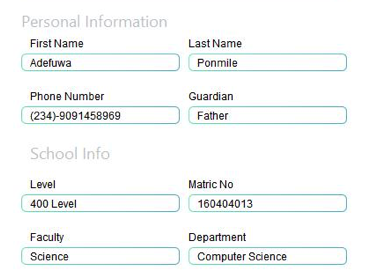
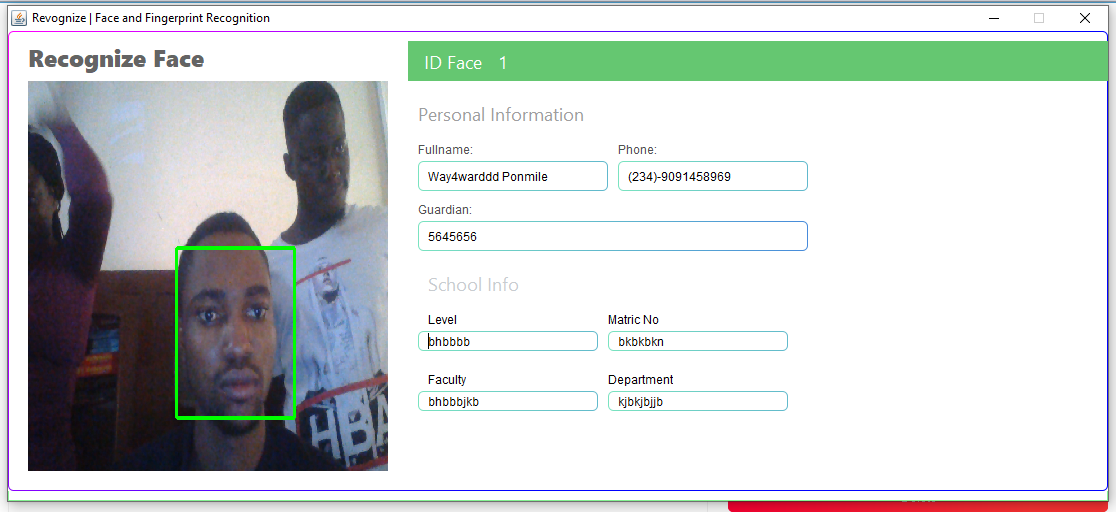
****

**4.1.5 DATA VERIFICATION SECTION (FACE RECOGNITION AND FINGER PRINT):** Once a face has been captured. The person data would be retrieved. In this section, if a face is detected and the face is recognized, the data of the face that was previously stored would be retrieved from the database of the system. In cases where the face is not easily identify, user can as well retrieve his/her data with the fingerprint of the user.





**Figure 4.4 Recognition Screen for Faces**



**Figure 4.5 Recognition Screen for fingerprint**

**4.2 FACE AND FINGERPRINT RECOGNITION PROCESS**

**4.2.1 FACE RECOGNITION**

The next step after locating a face inside of an image is the recognition of it. The recognition is the process of identifying a face inside of a set of previously learned faces. Local Binary Patterns Histograms (LBPH) is used. The process start by capturing the displayed colored image sequence but analyze only the de-saturated grayscale image. After this each section will be weighted with a grayscale value, representing the dissimilarity to the neighbor sections. The black sections indicate a value of 0.0 and the white sections are weighted with a value of 4.0. After this dissimilarity analysis the weighted sections represent a shape and texture pattern that can be compared to the existing samples of a person.

**4.2.2 FINGER PRINT RECOGNITION**

For the fingerprint recognition, a live scan fingerprint scanners (UareU4500 Digital Persona) was used to easily capture high quality fingerprint images. The matching stage uses the position and orientation of minutia features. As a result, the reliability of feature extraction is crucial in the performance of fingerprint matching. When a new finger is placed on the fingerprint device. The system extract the features of the new finger and compares it with the new template finger saved in the system database.

**4.3 PROTOTYPE TESTING**

Each candidate faces and fingerprint were compared with every member in the population set without repetition. The process was automated by ensuring that every query faces is selected from the population and matched against each and every faces in the entire population in the database. This process was able to uniquely match faces belonging to the same individual. In this research, the experiment was conducted be executing each algorithm against a database of sampled finger print and obtaining values of similarity scores (accuracy) and time taken from the query and the trained faces. The outputs were then analyzed.

An extract of the sample results are given in the Table 1

Table 1 - Sample Matching Results Using Lbph Face Recognizer Algorithm and Minutae fingerprint algorithm

|  |  |  |  |
| --- | --- | --- | --- |
| S/N | Face Confidence Value | Finger Accuracy Value | Fusion |
| 1 | 35.337 | 49.9358 | 85.27275 |
| 2 | 50.361 | 37.0898 | 87.45084 |
| 3 | 51.83 | 53.6393 | 105.4693 |
| 4 | 33.872 | 30.5571 | 64.42913 |
| 5 | 63.629 | 36.5301 | 100.1591 |
| 6 | 46.093 | 51.9381 | 98.03106 |
| 7 | 38.602 | 36.2624 | 74.8644 |
| 8 | 35.843 | 35.6299 | 71.47286 |
| 9 | 55.063 | 31.5853 | 86.64828 |
| 10 | 54.019 | 47.7652 | 101.7842 |
| 11 | 64.223 | 36.5419 | 100.7649 |
| 12 | 53.454 | 41.2099 | 94.66393 |
| 13 | 36.098 | 53.6569 | 89.75491 |
| 14 | 49.74 | 51.8152 | 101.5552 |
| 15 | 46.705 | 32.1583 | 78.86327 |
| 16 | 68.123 | 57.6319 | 125.7549 |
| 17 | 51.365 | 55.2 | 106.565 |
| 18 | 60.89 | 39.9813 | 100.8713 |
| 19 | 46.471 | 53.7519 | 100.2229 |
| 20 | 34.905 | 49.6341 | 84.53907 |
| 21 | 33.66 | 56.9482 | 90.60824 |

**4.4 METRICS FOR THE PERFORMANCE ANALYSIS**

The metrics for the analysis was based on the threshold decision value. The confidence value was used to determine the accuracy of the face recognizer and the accuracy of the fingerprint would be used to determine its performance. The accuracy of the captured faces and finger is measured by the threshold value (100) which is calculated using the formula;

The threshold value is determined by the summation of both accuracy. The lower the number in the range of 100 which is the threshold value, the more accurate it is.

**CHAPTER FIVE**

**SUMMARY, CONCLUSION AND RECOMMENDATION**

**5.1 SUMMARY**

In this research we were able to implement and analyze effectively a biometric multimodal system using both face and fingerprint. LBPH Algorithm for face recognition and Minutiae Extraction Algorithm was used. In this research, we also developed and implemented a prototype for face recognition matching to identify duplicate records using a sample of 50 candidates. The experiment was executed in a controlled environment using the necessary libraries. The prototype developed was able to extract and convert faces captured using hp default camera and UareU400 fingerprint device. Multimodal biometric technology indeed offers considerable improvements in reliability with reasonably overall performance in many applications over unimodal biometric system.

**5.2 CONCLUSION**

Multimodal biometric system certainly offers considerable improvements in reliability, accuracy and reduce error rate with reasonably overall performance in many applications over the unimodal biometric system. The new paradigm has become an underpinning of highly secured identification and personal verification solutions, more importantly in the wake of heightened concern about security challenges in our world today. However, the issue of efficient and effective integration of the evidences obtained from different traits and its computational complexity remains an overt concept that attracts research attention.

**5.3 RECOMMENDATION**

I would recommend the use of multimodal biometric techniques for some authentication processes. In as much as it has been testing and its accuracy has been confirmed.

**REFERENCES**

Ahmed (2014) Finger multibiometric cryptosystems: Fusion strategy and template security Journal of Electronic Imaging 23(2), 023001 (Mar-April)

A. Ahmed, J. Guo, F. Ali, F. Deeba and A. Ahmed, "LBPH based improved face recognition at low resolution," 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD), Chengdu, 2018, pp. 144-147.doi: 10.1109/ICAIBD.2018.8396183

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

A.R. Roddy and J.D. Stosz, “Fingerprint feature processing techniques and poroscopy,” in Intelligent Biometric Techniques in Fingerprint and Face Recognition, L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, and S. Tsutsui, Eds., pp. 37–105. CRC Press, 1999

Bigun et al (1997), "Expert conciliation for multi modal person authentication systems by Bayesian statistics," In Proceedings 1 Int. Conf. On Audio Video-Based Personal Authentication, pp. 327-334, Crans-Montana, Switzerland, 1997.

Brunelli et al (1993), "Face recognition: Features versus templates," IEEE Trans, on Pattern Analysis and Machine Intelligence, Vol, 15, No. 10, pp. 1042-1052, 1993.

Cahit and Abdulkadir (2012) Design of face recognition system

D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. Handbook of ﬁngerprint recognition. Second Edition, Springer, 2009.

Dieckmann et al (1997) "SESAM: A biometric person identification system using sensor fusion," Pattern Recognition Letters, Vol. 18, No. 9, pp. 827-833.

Espinosa Duro , V. “Minutiae Detection Algorithm for Fingerprint Recognition”, Polytechnic University of Catalonia, Electronic and Automatic Department, IEEE 2001, pp. 264-266.

Gumbel et al (2008), Statistics of Extremes, Columbia University Press, New York.

Gayatri et al (2012) Feature Level Fusion of Palm and Face for Secure Recognition

Kittler et al (1997), "Combining evidence in multimodal personal identity recognition systems," In Proceedings 1^^ International Conference On Audio Video-Based Personal Authentication, pp. 327-344, Crans-Montana, Switzerland

Long et al(2012) Multimodal Biometric Person Authentication Using Fingerprint, Face Features. In: Anthony P., Ishizuka M., Lukose D. (eds) PRICAI 2012: Trends in Artificial Intelligence. PRICAI 2012. Lecture Notes in Computer Science, vol 7458. Springer, Berlin, Heidelberg

J. Clark and A. Yuille Data Fusion for Sensory Information Processing Systems, Kluwer Academic Publishers, Boston, 1990.

Dr. Aranuwa (2014) Multiple biometric systems: design approach and application Scenario

Dr. Aranuwa (2016) Multilevel decision threshold authentication mechanism for efficient Multimodal Biometric Systems

Reema ajmera, Namrata Saxena ―Face Detection in Digital Images Using Color Spaces and Edge Detection Techniques‖ International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013.

Ryszard (2002) Multimodal Biometrics for Person Authentication

**Ross et al** (2006) Handbook of Multibiometrics

Solberg et al (1996), "A Markov random field model for classification of multisource satellite imagery," IEEE Trans. Geoscience and Remote Sensing, Vol. 34, No. l,pp. 100-113.

Samayita et al (2011) Fingerprint Identification

Shyam Sunder Yadav, Jitendra Kumar Gothwal , Prof. (Dr.) Ram Sing (2011) Multimodal Biometric Authentication System :Challenges and Solutions

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

SWGFAST. Swgfast, memo to mike mccabe (nist) regarding ansi/nist itl 1-2000, Nov. 2005.

Y. Wang, T. Tan, and A. K. Jain, "Combining Face and Iris Biometrics for Identity Verification," Proceedings of the Fourth International Conference on Audio and Video-Based Biometric Person Authentication, (AVBPA), pp. 805-813, 2003.