**DEVELOPMENT OF AN AUTOMATED ACCESS CONTROL SECURITY SYSTEM USING BIOMETRIC TECHNOLOGY**

**CHAPTER ONE**

**INTRODUCTION**

# 1.1 Preamble

Authentication security is the process of protecting a system by determining whether a person or object is, in fact, who or what it claims to be. In security systems, authorization—the process of allowing someone access to system objects based on their identification—is different from authentication. Authentication does not reveal the individual's access permissions; it merely confirms that the individual is who they say they are. Although they often occur together, authentication logically comes before authorisation. Often, the two terms are used interchangeably. Actually, these are two different processes (Jiang, Ma2, Li and Yang, 2018; More, 2018; Rousse, 2019).

The security industry uses three types of authentication: something you are familiar with, like your mother's maiden name, a PIN, or a password; A card key, smart card, or token (such a Secure ID card) are examples of things you possess; biometrics are examples of things you are.   
The process of verifying a user's identity through distinctive physical characteristics or measurements is known as biometric authentication. The Greek words bio, which means life, and metric, which means measurement, are the roots of the word biometrics. The study of individuals' distinct physical and behavioural traits via measurement and statistical analysis is known as biometrics.

Rouse (2019) and Jung, Kang, Lee, and Won (2020) state that the technology is typically utilised for access control and identification, as well as for identifying individuals under surveillance. The fundamental idea behind biometric authentication is that each person may be accurately identified by their innate behavioural or physical traits. Physiological or behavioural traits serve as the foundation for the two primary forms of biometric identification (Vallabhu and Satyanarayana, 2019). Physiological identifiers that are associated with the makeup of the person being validated include fingerprints, finger geometry (the size and positioning of fingers), facial recognition, iris recognition, vein recognition, retina scanning, DNA matching, and voice recognition.

Security with biometric authentication improves efficacy and efficiency as well as the ability to store and analyse large volumes of data. Additionally, it enhances the capacity for intelligence and investigation, as well as the speedy access to criminal histories and other relevant information (Tistarelli and Nixon, 2019; Lazaroff, 2024; Khan, 2016; BBC, n.d; ArcAspicio, 2019). The proposed project's objectives are to provide a safe fingerprint-based registration system for consideration and to examine the function and difficulties of biometric authentication security in Nigerian law enforcement.

# 1.2 Problem Statement

The majority of facial-based registration systems currently in use are based on Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), which are time-consuming for individual authentication and lack strong discrimination ability due to the large dimensions of the resulting features of such techniques (Dihong, Zhifeng, Dahua, Jianzhuang, and Xiaoou, 2018). In various fields, dimensionality reduction is used to lessen the curse of dimensionality and other unfavourable aspects of high-dimensional spaces (Babatunde, Olabiyisi, Omidiora, and Ganiyu, 2018). In order to solve the aforementioned problems, this project will create a robust fingerprint-based registration system based on the Local Binary Pattern.

**1.3 Aim and Objectives**

The aim of this research work is to develop an Automated Biometric Based Access Control

Security System for a Restricted Environment. The specific objectives of this research are to:

i perform critical review on the existing systems with a view to identify problems associated with them and to determine suitable algorithm for proposed system.

ii. design a computationally-efficient, Local Binary Pattern feature extraction technique. iii. implement the developed improved LBP feature extraction technique for facial recognition.

iv. evaluate the performance of the LBP feature extraction technique over HOG PCA and LDA using recognition time, recognition accuracy, False Accept Rate (FAR) and False Reject Rate (FRR) as performance evaluation metrics.

# 1.4 Significance of the Study

By utilising the many advantages that come with integrating a robust biometric-based security system, the study aims to improve the effectiveness and efficiency of security agents in carrying out their duties. These benefits include increased speed, efficiency, and effectiveness in conducting investigations, building necessary databases, networks, and information sharing systems, creating criminal profiles, and a variety of other tasks.

# 1.5 Scope of the Study

The goal of the research is to create a reliable biometric-based access control system for restricted environments.

# 1.6 Definition of Relevant Terms

Biometrics: It refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked.

Convict: declared to be guilty of a criminal offence by the verdict of a jury.

Crime: An action which constitutes a serious offence against an individual or the state and is punishable by law.

Criminal: a person who has committed a crime Suspect: a person who has committed a crime Victim: A person harmed, injured, or killed as a result of a crime, accident. Suspect: Believe to be guilty of a crime or offence, without certain proof

Witness: A person giving sworn testimony to a court of law or the police.

Secret Police: A police force that operates in secrecy

Law Enforcement Agency: An agency responsible for insuring obedience to the laws

Posse Comitatus: A temporary police force

Police Officer: a member of a police force

Police Station: the office or headquarters of a local police force

Police Dog: A dog trained to work with policemen (in tracking criminals, drugs etc)

SARS: Special Anti- Robbery Squad

INTERPOL: International Police

DNA: Deoxyribonucleic acid [Deoxyribo (D) nucleic (N) acid (A)]

USB: Universal Serial Bus

PC: Personal computer

VNTR: Variable number tandem repeat

2D barcode: 2-dimension barcode

Posse Comitatus: A temporary police force

ID: Identification

DMV: Department of Motor Vehicles

N.P.F: Nigeria Police Force

C.I.D: Criminal Investigation Department

C.I.B: Criminal Investigation Bureau

S.I.B: State Investigation Bureau

S.F.U: Special Fraud Unit

I.G.P: Inspector General of Police

C.C.R: Central Criminal Registry

2i/c: Second In charge

E.O.D: Explosive Ordinance Department

# CHAPTER TWO

# LITERATURE REVIEW

## 2.1 Review of Literatures

### 2.1.1 Biometrics

The Greek terms bio, which means life, and metric, which means measurement, are the roots of the word biometrics. The study of individuals' distinct physical and behavioural traits via measurement and statistical analysis is known as biometrics. Rouse (2019) claims that the technology is typically utilised for access control, identification, and identifying individuals under surveillance. Traditionally, ID cards and passwords have been used to limit access to protected systems, but these methods are unstable and easily compromised. Biometric systems have been built using fingerprints, face features, voice, hand geometry, handwriting, the retina, and the iris (Sanderson, Aliye, and Paliwal, 2021). Faking a biometric is difficult, if not impossible, as biometrics cannot be borrowed, stolen, or forgotten.

**2.1.2 Biometric Authentication**

The process of verifying a user's identity through distinctive physical characteristics or measurements is known as biometric authentication (Jung, Kang, Lee, and Won, 2019). The fundamental idea behind biometric authentication is that each person may be accurately identified by their innate behavioural or physical traits. The two primary types of biometric identification systems rely on physiological or behavioural characteristics (Mudholkar, Shende, and Sarode, 2020; Vallabhu and Satyanarayana, 2019). Physiological identifiers that are associated with the makeup of the person being validated include fingerprints, finger geometry (the size and positioning of fingers), facial recognition, iris recognition, vein recognition, retina scanning, DNA matching, and voice recognition.

### 2.1.3 Computerized Biometric Systems

The process of verifying a user's identity through distinctive physical characteristics or measurements is known as biometric authentication (Jung, Kang, Lee, and Won, 2019). The fundamental idea behind biometric authentication is that each person may be accurately identified by their innate behavioural or physical traits. The two primary types of biometric identification systems rely on physiological or behavioural characteristics (Mudholkar, Shende, and Sarode, 2019; Vallabhu and Satyanarayana, 2020). Physiological identifiers that are associated with the makeup of the person being validated include fingerprints, finger geometry (the size and positioning of fingers), facial recognition, iris recognition, vein recognition, retina scanning, DNA matching, and voice recognition.

### 2.1.4 Electronic Authentication and Identification

Adopting a robust fingerprint-based registration system in police makes it much simpler to identify a specific individual, claim Jain et al. (2019). To find a culprit and keep the crime under control while upholding law and order, the police can use a number of tactics. A person can now be electronically identified using almost any type of electronic communication (Burr, Dodson, Newton, Perlner, Polk, Gupta, and Nabbus, 2021). Among the various electronic identification techniques are a person's driver's license number, passport number, bank account number, phone number, mobile number, national identity card number, and digital signature. Security officials can quickly identify a person as a means of ensuring the safety of society because these information sources offer comprehensive details about every individual.

### 2.1.5 Fingerprint Recognition

Patterns on the tip of a finger are studied by Mudholkar, Shende, and Sarode (2022), Matyá and Ha (2021), and Krishneswari and Arumugam (2020) (Biometric data Recognition). Various methods are frequently employed for fingerprint authentication, verification, and identification. Some employ straight pattern matching devices, some employ techniques a little more specialised, including moiréfringe patterns and ultrasonics, while others use procedures akin to the traditional police method of comparing minutiae. Additionally, certain verification and authentication systems can tell when a real finger is supplied, while others cannot.

Compared to other biometric features, fingerprint devices come in a wider range. Fingerprint scanners are becoming increasingly widely used for user authentication as the device's price drops. This verification method works best with internal systems when users will be adequately informed and trained and the system will operate in a controlled setting. Since fingerprint verification is the sole biometric verification option that most workstations come with for application access, it has grown incredibly popular. The reason for this is believed to be its small size, low cost, and simplicity of integration with fingerprint authentication devices (Chaos Computer Club, 2018; van der Putte and Keuning, 2020).



Figure 2.1: Fingerprint types (Lazaroff, 2024)

### 2.1.6 Concept of a Robust Fingerprint Based Registration System

We now have a better grasp of the cosmos thanks to technological advancements, which has allowed us to create a wide range of more complex systems and technology. Conversely, every technological development entails the possibility of misuse and hidden risks for its users. In the modern world, theft of private data and information is a serious concern. Users take every precaution to safeguard their data

One technique that users frequently employ to ensure security is the use of identification cards and highly encrypted passwords (Kumari, Chaudhry, Wu, Li, Farash and Khan, 2015; Sadqi, Asimi and Asimi, 2018; Yang, Ma and Jiang, 2022; Ferguson, Schneier and Kohno, 2022; Chiasson, Forget, Biddle and van Oorschot, 2018; Mannan and van Oorschot, 2018).

**2.1.7 Advantages of Robust Fingerprint Based Registration System**

The uniqueness that comes with uniqueness identification is one of the most significant benefits of using biometric technology. This has encouraged many security-conscious people to use biometric security technologies in their daily lives. According to Tistarelli (2019), it is practically impossible for two people to have the same biometric system identity because biometric technology is so distinctive in terms of identification. Additionally, because biometric identity is exclusive to each person's physical body, users are less likely to divulge their login information to other parties—a behaviour that is known to be linked to security breaches.

This makes it extremely difficult to make duplicate copies of a biometric feature that is necessary to access other users' data and rights. Consequently, it becomes extremely difficult to obtain unauthorised access using biometric impersonation (Tistarelli, 2019). The majority of authenticating systems are also immune to social engineering attacks, and since biometric factors require users to be physically present, they can also be used to stop dishonest employees from claiming that someone else used their login credentials to access the system while they were away.

Furthermore, because of its ease of use and comfort, the biometric technology-based identifying function for individuals cannot be forgotten, lost, or stolen, which makes it highly popular among its users. The majority of biometric security systems are inexpensive to buy and easy to set up, despite the fact that some are sophisticated and costly (Tistarelli, 2019). Last but not least, a robust fingerprint-based registration system also helps to improve data integrity, reduce redundancies and inconsistencies, ensure user-defined rules to ensure data integrity, facilitate data sharing across multiple applications, have an intelligent backup that runs automatically, and authorise data access.

**2.1.8 Iris Recognition**

Its distinctive features—ridges, freckles, rings, and furrows—as well as its intricate pattern have drawn a lot of interest in the Recognition System in recent years. We estimate that the likelihood of discovering two people with similar iris patterns is almost zero, making iris recognition-based automated individual identity authentication frameworks the most reliable of all biometric techniques. Iris recognition technology is therefore emerging as a key biometric choice for person identification and managing networked access to software.

The delicate, spherical iris is an internal organ that is fixed inside the eye. Figure 2.2 shows the structure of the iris. Iris scans look at features including freckles, furrows, and rings in the pigmented tissue around the pupil, which provides more than 200 sites for comparison. Compared to a retinal scan, the scans can be done from a greater distance using a regular video camera. According to Jain, P. Flynn, A.A. Ross, and A.K. (2015), it can be used with glasses or contact lenses and can provide a measurement that is sufficiently accurate.

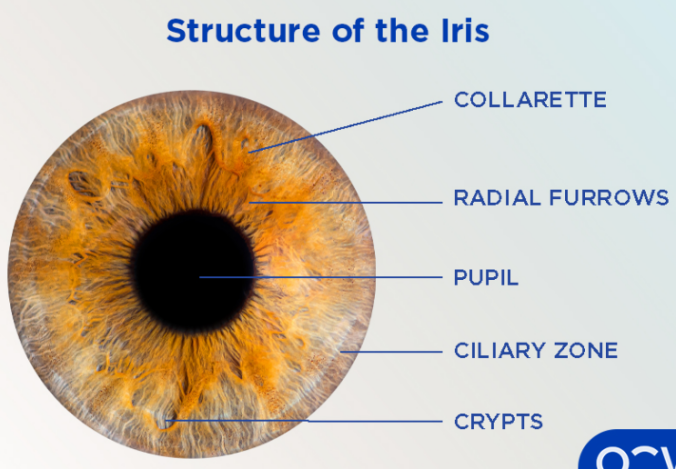


Fig. 2.2: Structure of the Iris: Jain, (2015)

The delicate, spherical iris is an internal organ that is fixed inside the eye. Figure 2.2 shows the structure of the iris. Iris scans look at features including freckles, furrows, and rings in the pigmented tissue around the pupil, which provides more than 200 sites for comparison. Compared to a retinal scan, the scans can be done from a greater distance using a regular video camera. According to Jain, P. Flynn, A.A. Ross, and A.K. (2019), it can be used with glasses or contact lenses and can provide a measurement that is sufficiently accurate.

The round iris is therefore perfectly situated. Following that, the iris recognition system decides which areas of the iris image can be used to extract and analyse features. According to Jain, A.K., P. Flynn, and A.A. Ross (2019), this means eliminating any deep shadows and regions concealed by the eyelids. Iris recognition software looks for a random pattern in a person's iris. The majority of commercial iris recognition systems use patented techniques developed by Ahonen T. and Pietikäinen M. (2017). The outside borders of the pupil and iris are determined by the algorithms.

In order to do a statistical comparison between a template and an image provided by a user who needs to confirm or identify anything, this region is transformed into bit patterns.   
Here is a summary of the algorithm as presented by Ahonen T. and Pietikäinen M. (2017). The conversion of a camera-captured iris image into an Iris Code, a bit stream that resembles a bar code, is illustrated in Figure 2.3.

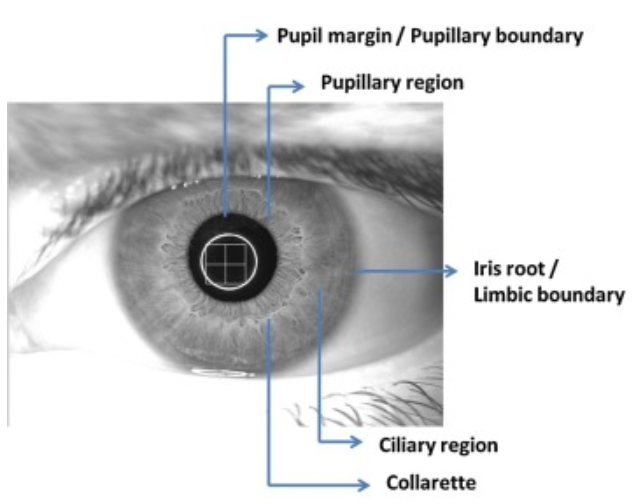


Figure 2.3: An Iris pattern: Ahonen, (2007)

The Iris Code is constructed using data from a set of Gabor wavelets. Specialised filter banks known as wavelets are used to extract information from signals at various scales and locations. The filters enhance resolution in both the frequency and spatial domains. Eight circular bands that have been altered to meet the iris and pupil boundaries are used to create the Iris Code, as shown in Figure 2.11. This operation generates Iris Codes, which are then compared to previously generated Iris Codes. The number of sites where the two Iris Codes diverge is known as the Hamming distance (HD). When two Iris Codes are exactly the same, the HD is zero; when two Iris Codes are completely discordant, the HD is one. A 50% difference in the codes is indicated by the average HD for various irises, which is approximately 0.5. For two distinct photos taken from the same iris, the HD varies between approximately 0.05 and 0.1; this variance includes both video noise and variations in the user's eye location in relation to imaging optics. An HD threshold of 0.32 may typically effectively separate authentic users from fraudsters. Numerous techniques have been put forth for iris recognition. A method for personal verification based on iris recognition is described by T. Ahonen and M. Pietikäinen (2017).

# 1. General Structure of Iris

Figure 2.4 displays a general stream of iris recognition algorithms. Using specialised equipment with an integrated megapixel camera is the first stage in taking the picture. Following the isolation of the image's eye region, sophisticated image processing techniques are used to segment the iris's internal and external edges. After identifying and separating the iris in the isolated eye image, mathematical techniques are used to encode it, producing a code that includes the distinctive iris quality. Nevertheless, no two photographs taken in various settings and at different times will be identical, and the procedure will identify whether or not the iris is that person's.

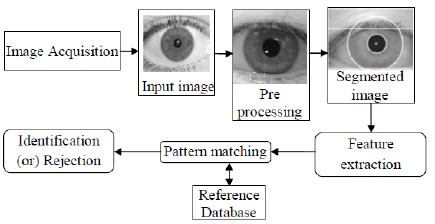


Fig. 2.4: General flow of iris recognition: Ahonen, (2019)

# 2. Iris Recognition Using Hough Transform

T. Ahonen and M. Pietikäinen (2017) developed a reliable iris localization algorithm. They used a robust technique based on the Hough transform and image gray level insights to first constrain the coarse site of the iris in the eye image. They also used a solid system that included a bivalued adaptive-threshold based on Histogram bisection and image gray level statistics; third, they reused the Hough collector, which was created for coarse iris region confinement, as well as image gray level statistics, to robustly localize the limbic limit. Finally, they use an approach based on the radial gradient-maxima and the Fourier series to regularize these limits. The procedure's execution was found to be satisfactory when compared to other modern procedures. T. Ahonen and M. Pietikäinen (2019) established a pupil site method based on the OTSU strategy and the Hough transform. To begin, it found a half quart using the gray summing operator to ensure the likely territory for finding the pupil's focal point, and then it chose one channel from R, G, and B using the distribution of histograms of three channels independently to reduce computing complexity. At that time, the OTSU approach ensured an automatic threshold value and obtained the binary image. Finally, to fit the pupil edge in the binary image, it used the Hough transform in a specific location. Their algorithm reaches a precision of 100 percent. It also ensured the stability of the environment.

# 3. Iris Recognition using Feature Extraction

Hao Li and Xi Fu (2018) suggested a new key points-centered feature extraction framework for iris detection in the presence of variable image quality. Their argument was based on the effective fusion of SIFT's three data sources at the matching score level. To distinguish specific important locations, three detectors were used: Harris-Laplace, Hessian-Laplace, and Fast Hessian. After obtaining the three sources, they were depicted in terms of SIFT properties. The suggested fusion rule calculates weights, which represent the degree of reliability that each individual source must contribute in order to determine more discriminative matching scores. The intended feature extraction stage, which is arduous, is a downside of this strategy. Neil Yager and Adnan Amin (2018) used a multi resolution analysis in iris template to project energy-centered features. It was based on the triplet half-band filter bank that was recommended (THFB). The iris template was divided into six equispaced sub-templates, each of which was subjected to two levels of deterioration using THFB, with the exception of the second. As a result, energy features were derived from each sub template's decayed coefficients. A comparison was made using already available features such as the Gabor transform, the CDF 9/7 filter bank, and the Fourier transform. The proposed scheme outperformed the competition in terms of FAR, GAR, and AUC. In time-frequency and spatial domains, Neil Yager and Adnan Amin (2018) proposed a reliable iris identification approach based on a new scale, shift on top of rotation invariant feature extraction strategy. To be sure, a 2-level nonsubsampled contourlet change (NSCT) was applied to the standardized iris pictures, along with a gray level co-occurrence matrix with three distinct orientations, and NSCT frequency sub-bands were processed on the spatial image. Furthermore, the influence of the occluded part was reduced by using an iris localization technique with four regions of interest selection. To reduce the influence of unusual values in the feature vector, the extracted feature set was processed and normalized. Then, using a two-phase technique that included a filtering phase and wrapper-based selection, notable features focused at iris recognition were chosen. Finally, a support vector machine was used to characterize the chosen feature set (SVM).

Finally, LOOCV was used to assess the suggested strategy's accuracy. The average accuracies on CASIA that were obtained

**4. Segmentation methods on iris recognition**

Only properly segmented images suitable for advancing to the latter step of iris identification require segmentation. T. Ojala, M. Pietikainen, and T. Maenpaa (2020) investigated the performance of several segmentation strategies in order to improve overall iris recognition accuracy.

# 5. Machine Learning approach on iris recognition

## T. Ojala, M. Pietikainen, and T. Maenpaa (2020) proposed a method for computing iris differences based on Computer Vision and Machine Learning. The computation of the displayed work retains the piece's primary originality.

## 2.1.9 Facial recognition

Facial recognition is a major scientific topic that cuts across many industries and disciplines. Face recognition is a fundamental human habit that is vital for good communications and interactions among people, in addition to having several practical uses such as bankcard identification, access control, Mug shots searching, security monitoring, and surveillance systems. Despite the fact that face recognition systems have been around for decades, there are numerous active research projects on the subject. The topic can be broken down into three sections. M.O. Oladele, E.O. Omidiora, and O.A. Afolabi (2018);

1. Detection
2. Recognition
3. Detection & Recognition

# 1. Face detection

The initial step in a face recognition system is face detection. The detection can produce two results: a location of the entire face region and a location of the face region with facial features (i.e. eyes, mouth, eyebrow, nose etc.). Because most algorithms combine approaches for detecting faces to boost accuracy, detection methods in the literature are difficult to categorize precisely. Rafael C. et al. divide detection into two categories: knowledge-based methods and image-based methods (2018). The detecting methods are shown in Figure 2.5.

Facial Features, Skin Color, and Template Matching are all used in knowledge-based approaches. To recognize human faces, facial features are employed to find eyes, mouths, noses, and other facial features. Skin color is distinct and distinct from other colors, and its properties do not vary with changes in position or occlusion. Color schemes such as RGB (Red-Green-Blue), YCbCr (Luminance-Blue Difference Chroma-Red Difference Chroma), HSV (Hue-Saturation-Value), YUV (Luminance-Blue Luminance Difference-Red Luminance Difference), and statistical models are used to model skin color. Faces have a distinct pattern that allows them to be distinguished from other things, therefore a template can be created to scan and detect faces. Facial features are crucial information for human faces, and they can be used to create standard images. Many face feature detection techniques are available in the literature, according to Rafael C. et al (2018).

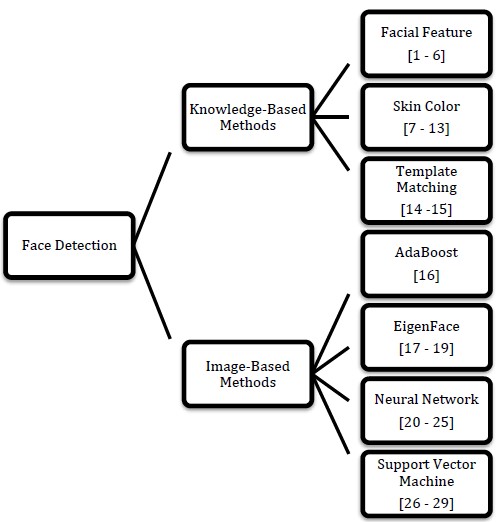


Fig. 2.5 Methods for Face Detection: Rafael C. et. al (2019).

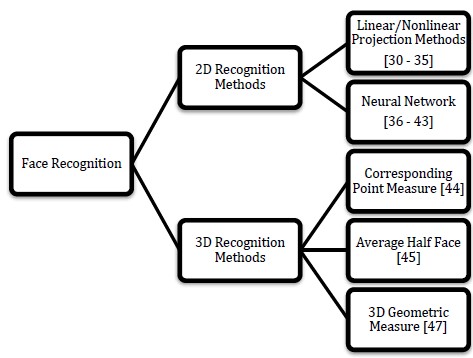
Rafael C. et al. (2019) extract a skin-like region with YCbCr color space and detect edges in the skin-like region to detect faces and facial features. Then, on the bordered region, Principal Component Analysis (PCA) is used to find eyeballs. Finally, Mouth is discovered using geometrical data. Another method uses the Normalized RGB color space to extract a skin-like region, and the face is then confirmed via template matching. Color snakes are applied to confirmed face picture segment skin regions in YCbCr color space to discover eyes, eyebrows, and mouths, and faces are verified with Linear Support Vector Machine (SVM). The information of Cb and Cr difference is used to find the ultimate verification of the face, eyes, and mouth

The pattern of the human face provides important information concerning human face detection. Window scanning or a divided region can be used to apply template matching. Scanning is done with a small window, such as a 20x20 or 30x30 pixel frame. This method scans the entire original image and then reduces the image size using some iteration that is sufficient for re-scanning. It's crucial to reduce the size in order to find the large or medium-sized faces. To locate faces, however, this necessitates a significant amount of processing time. Because it just examines the matching of segmented parts, template matching in a segmented region takes substantially less time to compute than scanning. Template matching has a wide range of applications in the literature. Instead of using a full-face template, Maltoni D., et al. (2018) use a half-face template. This strategy reduces the amount of time it takes to compute. This half-face can also be applied to different facial positions. Another method use abstract templates that are not image-like but instead consist of a set of parameters (i.e., size, shape, color, and position). The YCbCr color space is used to separate skin-like regions. The segmented region is then given abstract eye and eye pair templates. The first template locates the eye region, whereas the second template locates each individual eye. The direction of the eyes is likewise determined by the second template. The face candidate region is then verified using the Texture template.

The performance of face detection algorithms is evaluated, although each approach uses either its own library photos or images from a face detection database. As a result, comparing the performance of the algorithms is difficult, and the best algorithm cannot be determined.

The recognition part of a face recognition system is the other half. Both 2D and 3D picture data can be used for recognition; each has advantages and disadvantages. 2D picture data is easier to collect and less expensive than 3D image data. 2D images, on the other hand, are sensitive to light fluctuations, whereas 3D images are not. The surface of the face can be easily modelled using 3D photographs, but 2D images lack depth data. Face recognition algorithms are also run on the libraries of faces. Because these libraries use standard face images, the face recognition system should be able to deal with this issue. Figure 2.6 depicts the approaches for facial recognition. Face recognition is a pattern recognition problem, hence to compare the faces, a training/learning method should be utilized. Linear/Nonlinear Projection techniques and Neural Networks are utilized for 2D recognition. PCA, Linear Projection, and Nonlinear Projection are examples of linear/nonlinear projection algorithms.

To recognize Pratt, W.K. (2021)., cosine similarity measures and the nearest neighbor classification rule are employed after feature extraction, Another method for determining the input vector is to use facial distance. PCA is used to reduce the number of dimensions, while NN is used to classify them.



*Figure 2.6: Methods for Face Recognition:* Pratt, W.K.(2021)

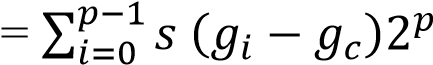
## 2.1.10 Local Binary Pattern (LBP)

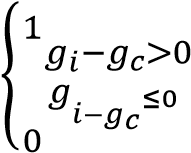
LBP has the advantage of being able to describe its local texture character quickly. The LBP operator's most essential quality is its resistance to variations in light (Ojala, Pietikäinen, and Mäenpaa, 2020). It's also simple to use in real-time applications from a computational standpoint. Designers of LBP operators must contend with three major concerns. The first problem is figuring out how to characterize diverse local texture patterns and then extracting them. Figure 2.4 depicts the LBP method for face recognition as a flowchart.

The second difficulty is how to select the critical subset of these local patterns to represent textures, because not all of them are equally important to texture analysis The final problem is figuring out how to combine these local patterns into a useful texture descriptor. The original LBP method (Ahonen and Pietikäinen, 2019) is a grayscale irrelevant texture analysis algorithm with strong discriminating. LBP gives a unified description of a texture patch that includes both statistical and structural properties, making it more powerful for texture analysis.

LBP is a gray-scale texture operator that describes the local image texture's spatial structure. A pattern number is calculated by comparing the value of a center pixel in the image with the values of its neighbors. With the neighborhood set P and a circle of radius R, and the difference between the central pixel “gc” and its neighborhood {g0, g1,…,gp-1}, the value of LBP

operator can be obtained as (Ojala*et al*., 2020):

LBP *P,R* 2.1

s = 

2.2

The original LBP labels the pixels of an image by thresholding the local area, neighborhood of each pixel with the center value and considering the result as a binary number.

**2.1.11 Fast Fourier Transform and Gabor Filters:**

Gualberto used Fast Fourier Transform and Gabor Filters to conduct fingerprint and facial identification in this work (2019). It's utilized to improve and reconstruct the fingerprint image's information, as well as to extract two sorts of minutiae: ending points and bifurcations. Finally, the fingerprint recognition is performed using the derived features.

**2.1.12 Fusion and Context Switching Frameworks:**

To match two latent fingerprints, the Fusion and Context Switching framework concept is used in a forensic science application. Unlike matching latent with inked or live fingerprints, proper analysis and attention are given in this idea.

**2.1.13 Segmentation Algorithm:**

## The result of fingerprint analysis and recognition is determined by segmentation, which is one of the earliest and most important pre-processing procedures for any fingerprint verification. Various segmentation algorithms were utilized.

**2.1.14 Gauss Filtering**

Distortions are generally drawn into the fingerprint image during the collection process for a variety of reasons, including dust inhalation and spots on the sensor surface (Jun et al. 2020).

As a result, the Gaussian filter is employed to reduce the effect and improve the image quality. The following is the two-dimensional Gaussian function:Where x is the distance from the origin in the horizontal axis and y is the distance from the origin in the vertical axis.

## 2.2 Related Works

For decades, fingerprint technology has been extensively researched. A great deal of effort has gone into resolving the issue in various conditions, including lighting, position, and shape. Burt and Perrett (2018) first used a cartoon method to exaggerate age in order to imitate the effect of fingerprint pictures. The mean patterns of various ages are calculated and combined with the test pattern to create a new pattern. The shape of the synthesized pattern is a combination of the mean and test patterns. However, only when the shape difference between the probe and the nearest pattern in the gallery is tiny did the cartoon method boost recognition rate. Most of the time, the technique is complicated and requires a large dataset to work effectively.

Modeling fingerprint verification as a two-class classification was done by Moghaddam, Wahid, and Pentland (2018). For the intra-personal and extra-personal pattern classification, the authors adopted a Bayesian framework. A 3D pattern modeling technique was also devised, which automatically produces some missing images in various age groups. It learned shaped patterns in separated 3D space and texture from a 2D database using PCA coefficients.

Young and Niels (2020) investigated how the face changes with age. Many fingerprint sections were rearranged, and then snakelet was used to calculate some ratios between them and remove wrinkles. The study found that as a person grows from a kid to an adult, his skull undergoes significant modifications, with wrinkles being the most noticeable alteration as he gets older.

This claim only works in theory and has never been tested against cutting-edge technology.

The method is said to be accurate, although it takes a long time.

A method for mimicking aging effects on fingerprint pictures was developed by Lanitis et al. (2020). A combined form intensity model was utilized to depict thumb printing on a database of age progressive patterns of individuals under 30 years of age. The authors used the PCA coefficients retrieved from the model parameters to model aging as a quadratic function. It was reported on the results of tests such as calculating an individual's age from a finger image and simulating aging effects on thumb images.

On a similar dataset, the model evaluated the performance of three fingerprint classifiers: the first was based on a quadratic function of the model parameters, the second on the distribution of model parameters, and the third on supervised and unsupervised neural networks trained on the model parameters. Using a quadratic function of the model parameters for the classifiers, the model produced the most efficient output. The structure, however, is not practicable in practice for usage by various thumbprinting recognition systems. The leave-one-out and generalization mistakes of ensembles of kernel machines, such as SVMs, were explored by Elisseeff, Evgeniou, and Pontil (2018). It was revealed that the best SVM and the best ensembles had roughly the same test performance; when the parameters of the machines are properly tuned, merging SVMs does not result in better performance than a single SVM. Ensembles of kernel machines, on the other hand, are more stable learning algorithms than a single kernel machine; bagging, in other words, improves the stability of unstable learning machines. When only a limited collection of features is presented to SVM, it performs exceptionally well. The dimensionality curse was ignored, resulting in erroneous recognition results with a large time complexity overhead. A more meaningful result can be produced by optimizing SVM, which is one of the goals of this study.

**CHAPTER THREE**

# METHODOLOGY

## 3.1 Research Approach

For the biometric authentication system, the Local Binary Pattern was employed to create an improved feature extraction approach known as the LBP feature extraction technique. Particle Swarm Optimization (PSO), an effective feature selection approach suitable for fingerprint patterns (Shinde and Gunjal, 2012), was used to manage the curse of dimensionality of the pool of initially-generated features using LBP in order to produce an optimal feature subset for detection. The final classification was done using a Support Vector Machine (SVM). This research comprises five (5) development phases:

i. Acquisition of test pattern from individuals.

ii. Pre-processing of the fingerprint pattern.

iii. Development of a LBP features extraction technique.

iv. Evaluation of the developed LBP feature extraction technique against LDA and PCA using false acceptance rate, false rejection rate, recognition accuracy and recognition time as performance evaluation metrics.

v. Recognition of fingerprint patters using the SVM classification system.

The complete framework for the developed facial/fingerprint recognition system is presented in Figure 3.1.

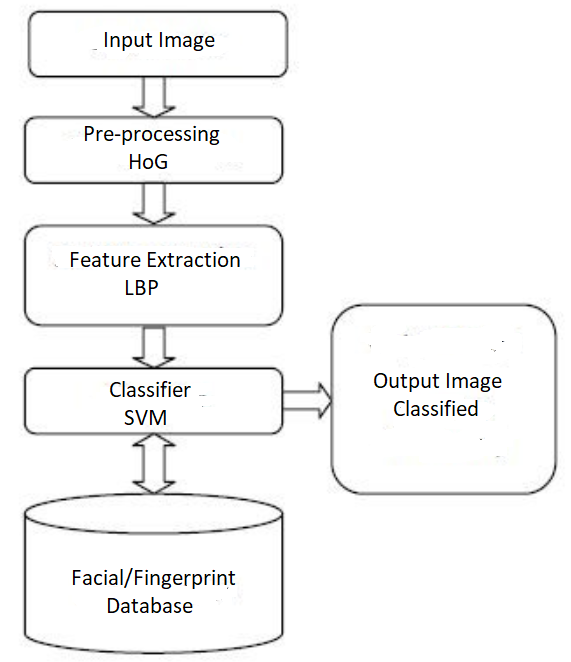


Figure 3.1: Framework of the Developed System

The block diagram of the Biometric Identification System (BIS) is clearly referred in a figure 3.2 given below. It consists of three components which are shown with the help of a flowchart to identify facial image (Hao et al. 2016)

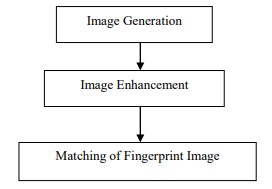


Fig. 3.2: Flowchart to identify facial image

Each of the component mentioned in the flowchart are described as follows:

**3.2 Image Generation:**

Figure 3.3 shows the basic components comprising a typical general-purpose system used for digital image processing.

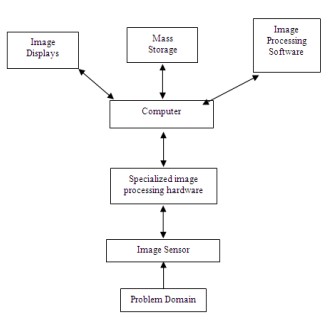


Fig. 3.3: Generation of an Image

The image sensor acquires digital images in relation to the issue domain. The first is a physical gadget that detects the object's radiated energy (Maltoni et al. 2013). The second, known as a Digitizer, is a device that converts the physical sensing equipment's output into digits. The digitizer and gear that performs other primitive functions make up specialized image processing hardware. A computer is an image processing system that can range in size from a personal computer to a supercomputer. Image processing software is made up of specialized modules that execute certain tasks. In image processing applications, mass storage is a necessary (Jahne 2017). If an image with a resolution of 1024x1024 pixels and an intensity of 8 bits per pixel is not compressed, it will take up one megabyte (MB) of storage space. Color TV monitors are the most common image displays in use. The outputs of image and graphics display cards, which are an intrinsic part of the computer system, drive monitors. Rafael (Rafael, 2017)

**3.3 Image Enhancement:**

### Image enhancing techniques are divided into two groups, which are addressed in this section.

### 3.3.1 Spatial Domain Methods

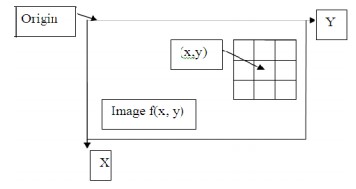
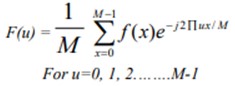
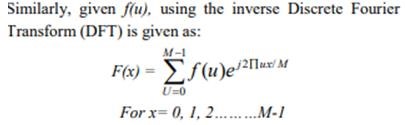
The aggregation of pixels that make up an image is referred to as the spatial domain. Procedures that work directly on these pixels are known as spatial domain approaches. The phrase g(x, y) = T [f (x, y)] can be used to represent it. Where f (x, y) denotes the input image, g (x, y) is the processed image, and T denotes an operator of f defined over a region of x, y. (x, y). 

Fig. 3.4: A 3\* 3 neighborhood about a point (x,y) in an image

### 3.3.2 Frequency Domain

The Fourier transform of a discrete function of one variable, f(x), x=0, 1, 2….M-1, is given by the equation:

 3.1

 3.2

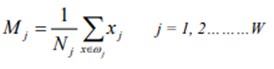
The 1/M multiplier in front of the Fourier transform is placed in front of inverse instead. In order to compute f(u), we start by substituting u=0 in the exponential term and then summing for all values of x. We repeat this process for all M values of u in order to obtain the complete Fourier Transform.

## 3.4 Matching of Fingerprint Image

Recognition techniques based on matching represent each class by a prototype pattern vector. An unknown pattern is assigned to the class to which it is closest in terms of a predefined metric. The simplest approach is the minimum-distance classifier, which as its name implies, computes the distance between the unknown and each of the prototype vectors.

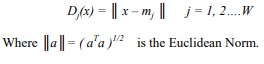
### 3.4.1 Minimum Distance Classifier

Suppose that we define the prototype of each pattern class to be the mean vector of the patterns of that class:

 3.3



Here, W is the number of pattern classes. One way to determine the class membership of an unknown pattern vector x is to assign it to the class of its closest prototype. Using the Euclidean distance to determine closeness reduces the problem to computing the distance measures:

 3.4

## 3.4.2 Image Acquisition

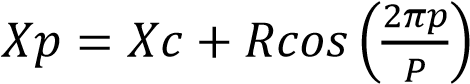
## The performance of the developed local binary pattern feature extraction technique was evaluated using a series of photos from various participants in this study. This dataset is difficult to work with because the photos are of varying ages (Ramanathan and Chellappa, 2006).

## 3.4.3 Pre-Processing of the thumb printing Images

## Image preprocessing aids in the removal of extraneous data that would otherwise be extracted as features, as well as reducing the amount of effort required during dimensionality reduction (Oladele, Omidiora and Afolabi, 2016). Appendices C and D show how the contrast and geometrical size of the fingerprint images were standardized at this step. To avoid image distortion, all images were shrunk to the same size.

## 3.4.4 The Developed LBP Feature Extraction Technique

LBP was utilized to extract local features for identification in the developed LBP approach. The LBP values were then divided into 42 equal-sized horizontal and vertical blocks using the converted image. Each block's histogram of uniform local binary patterns was obtained. Local binary patterns represent textures of a tiny local area, and histograms of uniform local binary patterns of the blocks tend to capture the local textural aspects of distinct regions of a face. With the coordinates of the center pixel of an image *I*(*x,y*) defined as (xc, yc), then the coordinates of his P neighbors (xp, yp) on the edge of the circle with radius R can be calculated with the cosine rule:

 3.5

The algorithm is as follows:

Input: Training and Test Image set

i.Initialize temp = 0 ii.FOR each image I in the training image set iii.Initialize the pattern histogram, H = 0 iv.FOR each center pixel tc εI

v.Compute the pattern label of tc, LBP using Equation 3.5 vi.Increase the corresponding bin by 1.

vii.END FOR viii.Find the highest LBP feature for each face image ix. Apply particle swarm optimization for feature subset selection

Intermediate Output: Reduced LBP features of face image

In the same vein, the GWT was implemented as a process depicted in the algorithm as follows:

Input: Training and Test Image set

1. Convolve Image *I* (*x, y*) using Gabor wavelets to extract local features at these feature points
2. Calculate the mean deviation, μmn, of the Gabor wavelet coefficients for each point
3. Calculate the standard deviation, 𝜎*mn,* of the Gabor wavelet coefficients for each pointConstruct Gabor feature vector using μmn and 𝜎*mn.*

v. Apply particle swarm optimization for feature subset selection

Intermediate Output: Reduced GWT features of face image

Repeat for all features

For each feature in LBP, choose a corresponding feature in GWT

Take average of each matching features in LBP and GWT Apply sum rule fusion strategy End Repeat

**3.5 Evaluation of the Developed LBP Feature Extraction Technique**

The performance evaluation metrics that were used to evaluate the developed feature extraction technique are:

### 3.5.1 False Accept Rate (FAR)

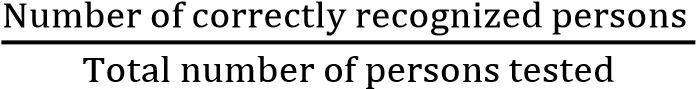
This is the probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percentage of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people. In the case of single-attempt scenario the False Acceptance Rate (FAR) can be computed as: FAR = (1 - FTE)2 · (1 - FTA) · FMR

### 3.5.2 False Reject Rate (FRR)

This is the probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percentage of valid inputs being rejected. In the case of single-attempt scenario the False Rejection Rate (FRR) can be computed as: FRR = FTE + (1 - FTE) · FTA + (1 - FTE) · (1 - FTA) · FNMR

### 3.5.3 Recognition Accuracy

This is the main measurement to describe the accuracy of a recognition system. It represents the number of faces that are correctly recognized from the total number of faces tested (Jeremiah *et*

*al.*, 2012). Recognition Accuracy =  x 100%3.6

# 3.5.4 Recognition Time

This represents the time required to process and recognize all faces in the testing set.

The flowchart of the proposed system processes is depicted in figure 3.5

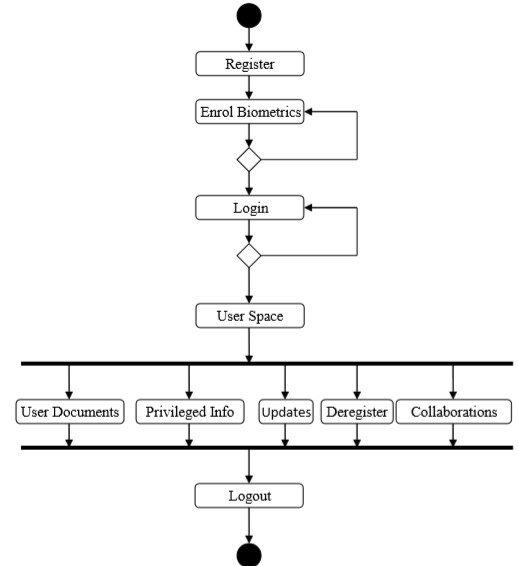


Fig. 3.5: The flowchart of the proposed system

**CHAPTER FOUR**

**RESULTS AND DISCUSSION**

**4.1 Results**

The implementation of a biometric based access control security system using the developed Local Binary Pattern (LBP) feature extraction techniques is presented in this chapter.

Face images of varying subjects were used for test and train data. All the algorithms were implemented on Windows 7 Ultimate 32-bit operating system, AMD Athlon (tm) X2 Dual Core QL-66 central processing unit with a speed of 2.2GHZ, 2GB random access memory and 320GB hard disk drive.

**4.1.1 Simulation Results**

This phase of the project shows the screen short of how the system works, due to its menu driven capabilities.

W**elcome page:** Once the program is loaded, the welcome page is displayed, after few seconds (say 10sec) as shown in figure 4.1

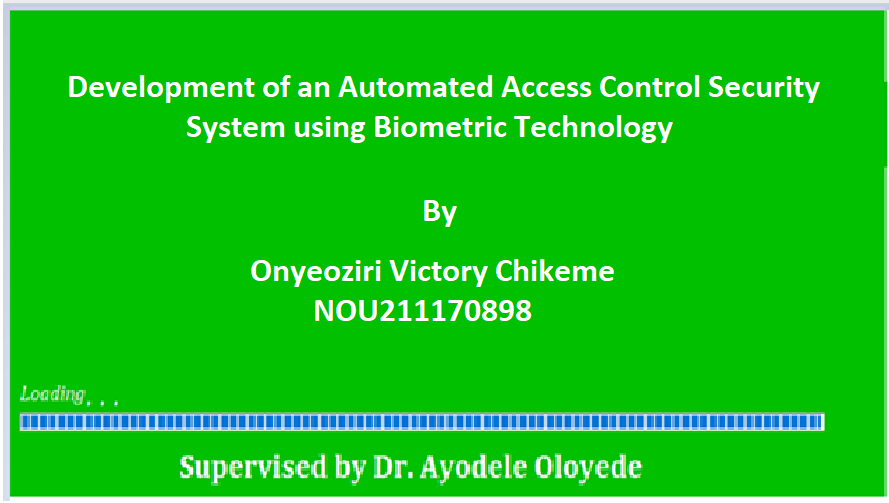


Fig. 4.1: The Screen Splash

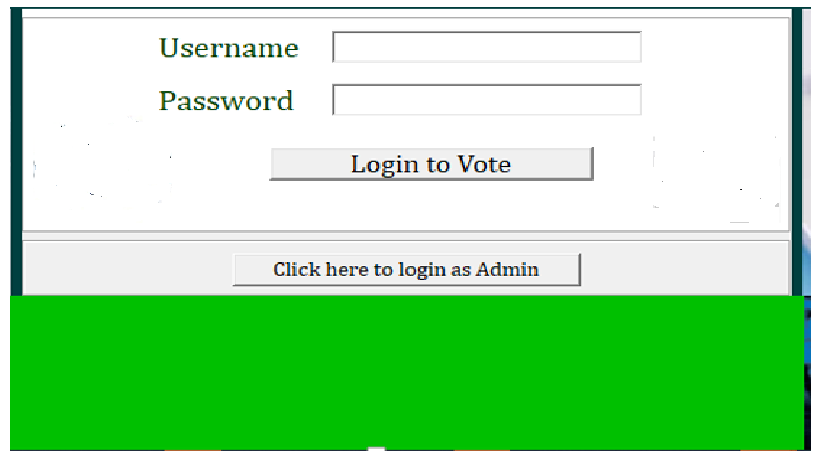


Fig.4.2: Home / Login Page

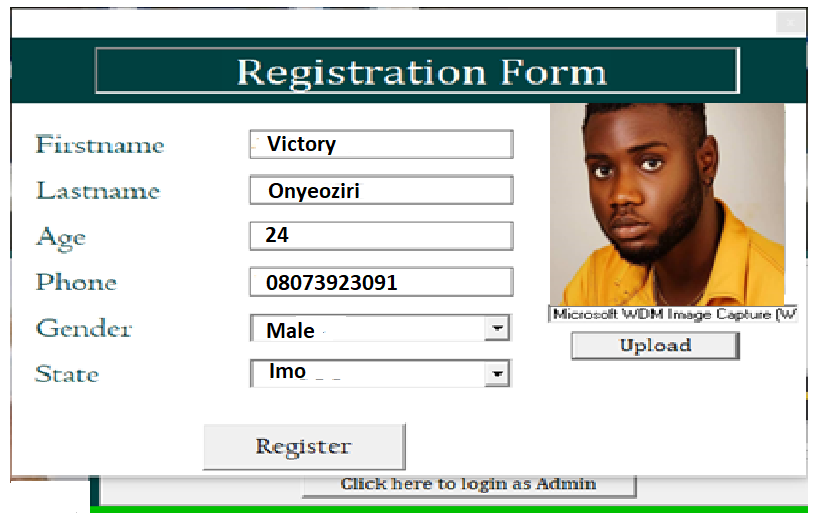
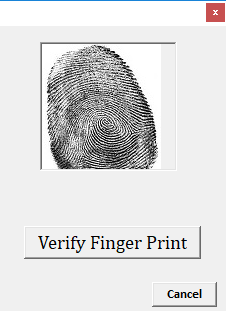


Fig. 4.3: Registration Page



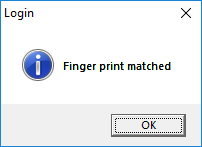


Fig. 4.4: Verification Page

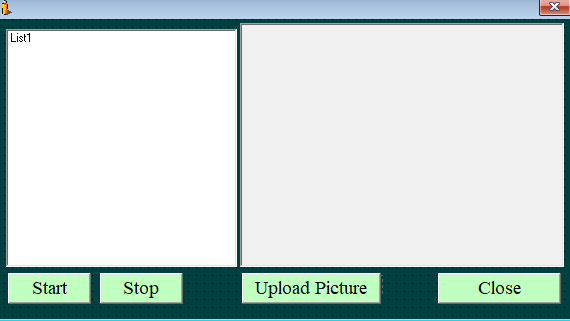


Fig 4.5: Upload Picture Section Page

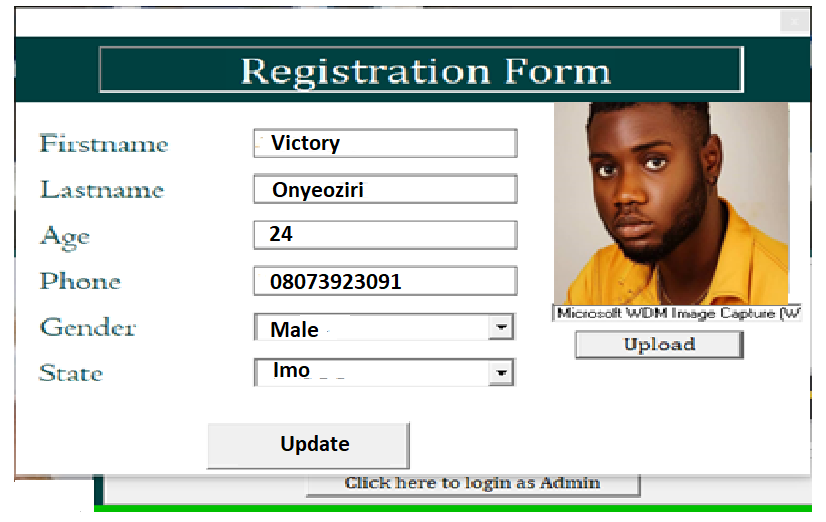


Fig. 4.6: Information Editing Page

**4.2 Result Analysis**

The results of the biometric based access control security system simulation shows that the use of LBP feature extraction technique outperforms PCA, and LDA in terms of FAR, FRR, Recognition accuracy and Response Time

**CHAPTER FIVE**

**SUMMARY, CONCLUSION AND RECOMMENDATION**

**5.1 SUMMARY**

Biometric recognition--the automated recognition of individuals based on their behavioural and biological characteristic--is promoted as a way to help identify terrorists, provide better control of access to physical facilities and financial accounts, and increase the efficiency of access to services and their utilization. Biometric recognition has been applied to identification of criminals, patient tracking in medical informatics, and the personalization of social services, among other things. In spite of substantial effort, however, there remain unresolved questions about the effectiveness and management of systems for biometric recognition, as well as the appropriateness and societal impact of their use. Moreover, the general public has been exposed to biometrics largely as high-technology gadgets in spy thrillers or as fear-instilling instruments of state or corporate surveillance in speculative fiction.

**5.2 CONCLUSION**

In this work, a local feature extraction technique which can be used to identify a person through its fingerprint was demonstrated to be real. This mentioned method concludes that the fingerprint is fast and accurate for more reliable and secure system. The methodology of the biometric identification system is represented with the help of diagrams and flow charts which can be used to enhance the quality of the image as well as to verify the identity of a person. Future research work can be carried out to improve the quality of the image by improving the image enhancement technique and develop a better matching technique.

**5.3 RECOMMENDATION**

Although traditional biometrics testing tends to focus on the match performance for a test data set, experience from many domains suggests that process and quality control should be analyzed for the complete system life cycle. Methods used successfully for the study and improvement of systems in other fields such as manufacturing and medicine (for example, controlled observation and experimentation on operational

**REFERENCES**

Ahonen T. and Pietikäinen M. (2017): “Soft histograms for local binary patterns”, Finnish Signal

Ali H.A., Hind R.M. and Raghad S.A. (2012): Gabor wavelet Transform in Image Compression,

Journal of Kufa for Mathematics and Computer 1(6), pp.107-113.

Baxes, G.A... Digital Image Processing: Principles and Applications, John Wiley & Sons, NY[2014].

Bazen .A.M., and S.H. Gerez, "Segmentation of Fingerprint Images", Proc. Workshop on Circuits Systems and Signal Processing (ProRISC200l), pp.276-280, Nov, 2010.

Castleman, K.R. Digital Image Processing, 2nd ed., Prentice Hall, Upper Saddle River, NJ.

Dario Maio and Davide Maltoni, A structural approach to fingerprint classification. In 13th International Conference on Pattern Recognition, 1996.

Dougherty, E.R.(Ed.); Random Processes for image and signal processing, IEEE Press, NY [2010].

Duda, R.O., Hart, P.E., and Stork, D.G. Pattern Classification, 2nd ed., John Wiley & Sons, NY [2011].

Francis Galton, Finger Prints; Macmillan & Co., London, New York, 1892.

Gonzalez, R.C and Woods, R.E... Digital Image Processing, Addison-Wesley, Reading, MA [2012].

Gualberto Aguilar, Gabriel Sanchez & Mariko Nakano, “Fingerprint Recognition”, IEEE, Second International Conference on Internet Monitoring & Protection, 2017.

Gualberto Aguilar, Gabriel Sanchez, “Fingerprint Recognition” IEEE, 2013.

Hao Li, Xi Fu, Proficient in Visual C++ and Algorithms Implement of Fingerprint Pattern Recognition System; Posts and Telecom Press, Bei Jing, 2016.

Jahne, B. Digital Image Processing: Concepts, Algorithms, and Scientific Applications, Springer-Verlag, NY [2017].

Jain .A.K., P. Flynn, & A.A Ross; Handbook of Biometrics; Springer, Secaucus, NJ, USA, 2014.

Joao De Barros, Biometric history, August, 2015.

Jun Ma, Xiaojun Jing, Yuanyuan zhang, “Simple effective fingerprint segmentation algorithm for low quality images”, IEEE 2010.

Lim, J.S. Two-Dimensional Signal and Image Processing, Prentice Hall, Upper Saddle River, NJ [1990].

Maltoni D., D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition”,Springer-Verlag, June, 2013.

Neil Yager and Adnan Amin; Fingerprint verification based on minutiae features: A review Pattern Analysis and Application, 7:94-113, February 2014.

Ojala T., Pietikainen M. and Maenpaa T. (2012): “Multiresolution Gray-Scale and Rotation

Invariant Texture Classification with Local Binary Patterns”, IEEE Transaction on Pattern

Analysis and Machine Intelligence, 24 (7): pp. 971–987.

Oladele M.O., Omidiora E.O. and Afolabi O.A. (2016): “A face-based age estimation system usingback propagation neural network technique”, British Journal of Mathematics & Computer Science, 13(5): pp.1-9.)

Petrou, M. and Bosdogianni, P... Image Processing: The Fundamentals, John Wiley & Sons, UK [1999].

Pratt, W.K. Digital Image Processing, 2nd ed., Wiley-Interscience, NY [1991].

Pratt, W.K. Digital Image Processing, 3rd ed., John Wiley & Sons, NY [2011].

Processing Symposium, Oulu, Finland.pp.107-117.

Rafael C. Gonzalez, Richard E. Woods. “Digital Image Processing”; Pearson [2017].

Shila Samantaray, “A DoG based approach for fingerprint Image Enhancement”, Ph.D Thesis, Department of Computer Science and Engineering, NIT Rourkela [2011].

**APPENDIX A**

Private Sub cmdBack\_Click()

Unload Me

frmLogin.Show

End Sub

Private Sub cmdNext\_Click()

' Validating the fields

If txtUserID = "" Or txtFname = "" Or txtLname = "" Or txtPhone = "" Or txtEmail = "" Or txtDob = "" Or cmbState = "" Or cmbState = "Enter your State" Or txtPassword = "" Or cmbGender = "" Or cmbGender = "Gender" Or txtImg = "" Then

MsgBox "Empty Field(s)! Ensure all the fields are filled. ", vbOKOnly + vbInformation, "Empty field(s)"

Else

' save picture

Dim PixIdAs Integer

Randomize

PixId = Int(Rnd \* 12345) + Int(Rnd \* 4444)

If Dir(App.Path& "\myPic", vbDirectory) = "" Then MkDir (App.Path& "\myPic")

Set Me.imgPix.Picture = hDCToPicture(GetDC(modWebCam.hHwnd), 0, 0, 149, 157)

SavePictureimgPix.Picture, App.Path& "\myPic\" &Format(Date, "dd\_MM\_yyyy") &PixId& ".jpg"

txtImg = App.Path& "\myPic\" & Format(Date, "dd\_MM\_yyyy") &PixId& ".jpg"

'post to submit form

frmSubmit.lblUserID = txtUserID

frmSubmit.lblFname = txtFname

frmSubmit.lblLname = txtLname

frmSubmit.lblPhone = txtPhone

frmSubmit.lblEmail = txtEmail

frmSubmit.lblDob = txtDob

frmSubmit.lblGender = cmbGender

frmSubmit.lblLga = cmbState

frmSubmit.txtImg = txtImg

frmSubmit.lblPassword = txtPassword

Me.Hide

frmBiometrics.Show

End If

End Sub

Private Sub cmdUpload\_Click()

Dim PixIdAs Integer

Randomize

PixId = Int(Rnd \* 12345) + Int(Rnd \* 8888)

' lblSaleId.Caption = PixId

' StartWebCam Capture

If Me.List1.ListCount = 0 Then Exit Sub

If List1.ListIndex = -1 Then Exit Sub

modWebCam.OpenPreviewWindow List1.ListIndex, Me.Picture1

txtImg = App.Path& "\myPic\" & Format(Date, "dd\_MM\_yyyy") &PixId& ".jpg"

End Sub

Private Sub cmgGenerate\_Click()

Randomize

txtUserID = "PO" &Int(Rnd \* 1234567) + Int(Rnd \* 4444567) & "Rgg"

End Sub

Private Sub Form\_Load()

'Generate random number for ID

Num = 5

Num1 = 4

Randomize

RandomNumbers (Num1)

lblUserID = Format(Now(), "YYYY") + Letters & Numbers

modWebCam.LoadDeviceList Me.List1

'State

cmbState.AddItem "Abia"

cmbState.AddItem "Adamawa"

cmbState.AddItem "AkwaIbom"

cmbState.AddItem "Anambra"

cmbState.AddItem "Bauchi"

cmbState.AddItem "Bayelsa"

cmbState.AddItem "Benue"

cmbState.AddItem "Borno"

cmbState.AddItem "Cross River"

cmbState.AddItem "Delta"

cmbState.AddItem "Edo"

cmbState.AddItem "Enugu"

cmbState.AddItem "Ekiti"

cmbState.AddItem "Gombe"

cmbState.AddItem "Imo"

cmbState.AddItem "Jigawa"

cmbState.AddItem "Kaduna"

cmbState.AddItem "Kano"

cmbState.AddItem "Kastina"

cmbState.AddItem "Kebbi"

cmbState.AddItem "Kwara"

cmbState.AddItem "Lagos"

cmbState.AddItem "Nasarawa"

cmbState.AddItem "Niger"

cmbState.AddItem "Ondo"

cmbState.AddItem "Ogun"

cmbState.AddItem "Osun"

cmbState.AddItem "Oyo"

cmbState.AddItem "Plateau"

cmbState.AddItem "Rivers"

cmbState.AddItem "Sokoto"

cmbState.AddItem "Taraba"

cmbState.AddItem "Yobe"

cmbState.AddItem "Zamfara"

cmbState.AddItem "F.C.T"

End Sub

Private Sub cmdBack\_Click()

Me.Hide

frmBiometrics.Show

End Sub

Private Sub cmdSubmit\_Click()

Call Connect

Dim r1 As New Adodb.Recordset

r1.Open "select \* from RegistrationTable", con1, 3, 2

With r1

.AddNew

r1!UserID = lblUserID.Caption

r1!Fname = lblFname

r1!Lname = lblLname

r1!Phone = lblPhone

r1!Email = lblEmail

r1!DOB = lblDob

r1!Sex = lblGender

r1!LGA = lblLga

r1!Photo = txtImg

r1!BiotempID = frmBiometrics.txtPic

r1!PassWord = lblPassword

r1.Update

MsgBox "Registration Successful", vbInformation, "Register"

lblUserID = ""

lblFname = ""

lblLname = ""

lblPhone = ""

lblEmail = ""

lblDob = ""

lblGender = ""

lblLga = ""

txtImg = ""

frmRegistration.txtLname = ""

frmRegistration.txtFname = ""

frmRegistration.txtPhone = ""

frmRegistration.cmbGender = "Gender"

frmRegistration.txtDob = ""

frmRegistration.txtEmail = ""

frmRegistration.cmbState = "Enter your State"

frmRegistration.txtImg = ""

frmRegistration.txtPassword = ""

frmBiometrics.txtPic = ""

Unload Me

frmLogin.Show

End With

'End With

'End If

End Sub

Private Sub txtImg\_Change()

imgPix.Picture = LoadPicture(txtImg.text)

End Sub

Private Sub cmdBack\_Click()

Me.Hide

frmRegistration.Show

End Sub

Private Sub cmdBiometrics\_Click()

cdlPicture.ShowOpen

txtPic.text = cdlPicture.FileName

imgPix.Picture = LoadPicture(txtPic.text)

End Sub

Private Sub cmdNext\_Click()

Me.Hide

frmSubmit.Show

End Sub

Private Sub txtPic\_Change()

imgPix.Picture = LoadPicture(txtPic.text)

End Sub

Private Sub cmdFlogn\_Click()

Call Connect

Dim r1 As New Adodb.Recordset

r1.Open "select \* from AdminTable", con1, 3, 2

r1.MoveFirst

r1.Find ("User ='" &txtFuser& "'")

If r1.EOF Then

MsgBox "No user with such username!. Please enter your correct username.",vbOKOnly, "Login"

txtFuser.SetFocus

txtFuser.text = ""

Else

If (Trim(r1. Fields.Item("password").Value)) = Trim(txtFpass.text) Then

Unload Me

mdiHome.Show

mdiHome.lblAdmin = "Admin"

Else

MsgBox "No password like that exists!",vbOKOnly, " login"

txtFuser.SetFocus

txtFuser.text = ""

txtFpass.text = ""

End If

End If

fraAdmin.Visible = False

End Sub

Private Sub cmdLogin\_Click()

Dim getUserID, getFname, getLname, getGender, getPhone, getEmail, getDOB, getLGA, getImg, getBiotempID, getPassword As String

If txtUser.text = "" Or txtPassword.text = "" Then

MsgBox "Field(s) is empty!Please fill all the field", vbOKOnly + vbInformation, "Login"

Else

Call Connect

Dim r1 As New Adodb.Recordset

r1.Open "select \* from RegistrationTable", con1, 3, 2

r1.MoveFirst

r1.Find ("UserID ='" &txtUser& "'")

If r1.EOF Then

MsgBox "No user with such username!. Please enter your correct username.",vbOKOnly, "Login"

txtUser.SetFocus

txtUser.text = ""

Else

If (Trim(r1.Fields.Item("Password").Value)) = Trim(txtPassword.text) Then

getUserID = r1!UserID

getFname = r1!Fname

getLname = r1!Lname

getGender = r1!Sex

getPhone = r1!Phone

getEmail = r1!Email

getDOB = r1!DOB

getLGA = r1!LGA

getImg = r1!Photo

getBiotempID = r1!BiotempID

getPassword = r1!PassWord

frmView.lblUserID = getUserID

frmUpdate.lblUserID = getUserID

frmUpdate.lblBio = getBiotempID

frmUpdate.lblPass = getPassword

txtUser.text = ""

txtPassword.text = ""

' Exit Sub

frmVerify.txtImg = getBiotempID

Unload Me

frmVerify.Show

Else

MsgBox "No password like that exists!",vbOKOnly, " login"

txtUser.SetFocus

txtUser.text = ""

txtPassword.text = ""

End If

End If

End If

End Sub

Private Sub lblAdmin\_Click()

fraAdmin.Visible = True

End Sub

Private Sub lblRegister\_Click()

Unload Me

frmRegistration.Show

End Sub

Option Explicit

Private Type BITMAP

bmType As Long

bmWidth As Long

bmHeight As Long

bmWidthBytes As Long

bmPlanes As Integer

bmBitsPixel As Integer

bmBits As Long

End Type

Private Declare Function GetObject Lib "gdi32" Alias "GetObjectA" (ByValhObject As Long, ByValnCount As Long, lpObject As Any) As Long

Private Declare Function GetBitmapBits Lib "gdi32" (ByValhBitmap As Long, ByValdwCount As Long, lpBits As Any) As Long

Private Declare Function SetBitmapBits Lib "gdi32" (ByValhBitmap As Long, ByValdwCount As Long, lpBits As Any) As Long

Dim tmp As String

Private Sub cmdCancel\_Click()

'tmp = ""

' tmp = OpenDialog(Me)

'If tmp<> "" Then Text2 = tmp: Picture2.Picture = LoadPicture(Text2)

Unload Me

frmLogin.Show

End Sub

Private Sub cmdFingerPrint\_Click()

tmp = ""

tmp = OpenDialog(Me)

If tmp<> "" Then Text2 = tmp: Picture2.Picture = LoadPicture(Text2)

cmdFingerPrint.Visible = False

cmdVerify.Visible = True

End Sub

Private Sub cmdVerify\_Click()

Picture1.AutoSize = True

Picture2.AutoSize = True

' Picture1.Picture = LoadPicture(Text1)

' Picture2.Picture = LoadPicture(Text2)

' Picture2.Picture = LoadPicture("C:\Temp\test2.bmp")

MsgBoxfComparePic(Picture1, Picture2), vbInformation, "Login"

cmdFingerPrint.Visible = True

cmdVerify.Visible = False

End Sub

Public Function fComparePic(Pic As PictureBox, pic2 As PictureBox) As Boolean

Dim PicBits() As Byte, PicInfo As BITMAP

Dim PicBits2() As Byte, PicInfo2 As BITMAP

Dim i As Long, BytesPerLine As Long

GetObjectPic.Image, Len(PicInfo), PicInfo

GetObject pic2.Image, Len(PicInfo2), PicInfo2

If PicInfo.bmWidth<> PicInfo2.bmWidth Then

fComparePic = False

MsgBox "Finger print does not match", vbInformation, "Login"

Exit Function

End If

If PicInfo.bmHeight<> PicInfo2.bmHeight Then

fComparePic = False

MsgBox "Finger print does not match", vbInformation, "Login"

Exit Function

End If

'reallocate storage space

BytesPerLine = (PicInfo.bmWidth \* 3 + 3) And&HFFFFFFFC

ReDimPicBits(1 To BytesPerLine \* PicInfo.bmHeight \* 3) As Byte

BytesPerLine = (PicInfo2.bmWidth \* 3 + 3) And&HFFFFFFFC

ReDimPicBits2(1 To BytesPerLine \* PicInfo2.bmHeight \* 3) As Byte

GetBitmapBitsPic.Image, UBound(PicBits), PicBits(1)

GetBitmapBits pic2.Image, UBound(PicBits2), PicBits2(1)

For i = 1 To UBound(PicBits)

If PicBits(i) <> PicBits2(i) Then

fComparePic = False

MsgBox "Finger print does not match", vbInformation, "Login"

Exit Function

End If

Next i

fComparePic = True

MsgBox "Finger print matched", vbInformation, "Login"

Unload Me

mdiHome.Show

End Function

Private Sub txtImg\_Change()

Picture1.Picture = LoadPicture(txtImg.text)

End Sub