ISSN: 2641-6336
DOI: 10.33552/ABBA.2019.03.000560
Annals of
Biostatistics & Biometric Applications
Iris Publishers

Research Article

Securing E-Library System with Bimodal Biometric Technique

Afolabi AO*, Falohun AS and Adedeji OT

Department of Computer Science and Technology Ladoke Akintola University of Technology, Ogbomoso, Nigeria

***Corresponding author:** Afolabi AO, Department of Computer Science and Technology Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

Received Date: September 24, 2019
Published Date: September 27, 2019

Abstract

The project focuses on securing e-library system with dual biometric features viz: face recognition and fingerprint identification techniques. The results obtained from the research support the set of objectives. The findings indicate that a real time fingerprint and face based authentication security system can be achieved. For the fact that it involves the use of human and biological characteristics, thus some false rejections were recorded during the performance of the system, this occurs mostly in the section of face recognition. This is as a result of the conditions under which the face images were acquired (that is, image background, lightening, distance of face from camera, etc.). The function of the system is based on the ability to match a required fingerprint and face within the database in order to authenticate the user of the facility and therefore grant or refuse access to the electronic library and this was achieved as reported in the paper.

Introduction

Biometrics is used to describe the use of physiological or behavioral characteristics to verify an individual's identity [1]. Physiological biometrics is a physical measurement of how an action takes place, such as a signature. In order for a measurement to qualify as biometrics, the certain requirements must be met [2003]. Some of the assumptions on which biometrics concepts is based are:

- **Universality:** Each person should have a biometric characteristic.
- **Distinctiveness:** The characteristics must be distinct among persons and no two should be alike.
- **Permanence:** The characteristics must remain invariant over a period of time
- **Collectability:** The characteristics can be measured quantitatively and easy to collect
- **Performance:** In term of a biometric system, the performance should be practical in its accuracy, speed and resources requirement.
- **Acceptability:** It is the extent to which intended users will accept the system.
- **Circumvention:** Refers to how well the system can detect attacks that are fraudulent.

Authentication is described as the process of determining the identity of a communicating party [1. With all biometric measurements and corresponding requirements, there are two methods of authentication: identification and verification. If the method chosen is identification, it authenticates its users from the biometric characteristic alone without the use of smart cards, usernames or ID numbers. The biometric template is compared to all records within the database and a closest match score is returned. The closest match within the allowed threshold is deemed the individual and authenticated.

A biometric system is essentially a pattern recognition system that makes personal identification possible. It does so by establishing the authenticity of specific biological or behavioral characteristics of the user, that is, the person who is being identified. Logically, a biometric system may be divided into two distinct units/modules: an enrollment module and an identification module.

The enrollment module equips the system to identify a given person. During enrollment, a biometric sensor scans the characteristics of the user to acquire a digital representation of the characteristics, such as a digital of a person's face. A computer program known as a feature extractor then processes the digital representation to generate a more compact representation called a template. With a facial image, the template of features may include the size and relative position of the eyes, nose and mouth. The template for each user is stored in the system's database or recorded on a smart card, which is a small plastic card containing a microchip that can store personal data. If the template is recorded on a smart card, the card is issued to the user. To be identified as the true user, the card holder must match the characteristic record on the card. In the development of the enrollment process, it must first follow a determined enrollment policy due to the fact that very private information will be supplied to the organization that will in turn be required to protect it (Belle, R.M., 2004) [2].

Biometric Performance

Biometric systems are susceptible to the following kinds of errors:

- **False Rejection Rate (FRR):** The probability that the system will reject a valid biometric credential [FDIC (2004)]. This would be an issue when a legitimate individual is denied access because the biometric authentication systems are primarily an additional level of security versus a sole method of authentication for organization.
- **False Acceptance Rate (FAR):** This is the probability that the system will accept a false biometric credential as legitimate [FDIC. (2004)], this would be an issue of an individual requesting access to his or her account, but instead given access to another person's account base.
- **Speed:** This is the rate at which the identification is made. The time it takes for the system to run.
- **Accuracy:** This is the measure of how error free the system is.
- **Cost:** This involves the amount that is expended on the design and implementation of the system.

System Design and Implementation

The security system based on fingerprint identification and facial recognition design is basically a security system involving a personal computer running a control program which has the capability of indentifying fingerprints and faces. The function of the system is based on the ability to match a required fingerprint and face within the database and therefore grant or refuse access to the restricted area as the case may be [3].

Security systems usually consists of devices, component functioning together to perform the function of protection, safety, detection of crime, protection of information, environment and much more. The introduction of a control system has helped in restricting access to a secured environment, creating more diversification in security world and gradually eliminating of human effort.

Design architecture

A dual biometric featured e-learning security system comprising of both facial recognition and fingerprint identification capabilities is one that grants access to the registered user if both the face and fingerprint supplied matches the one in the database. This system is designed so as to fit this stated purpose i:e to serve as a security to a e-learning system.

Facial recognition

Face recognition systems have been widely researched in computer vision and lots of algorithms can be used according to their superior performances using optimized and controlled environments and white faces. The system has been developed to match such successful performances using black faces. The algorithm used for the face recognition is PCA (Principal Component Analysis).

Principal component analysis (Pca): It is a type of image recognition system. It represents pictures of faces into its eigenface components. Principal component analysis reduces the dimensionality of the data while retaining as much as possible the variation present in the original dataset. The steps involved in identifying images through eigenspace projection are:

- Creation of eigenspace
- Project training images
- Identify test images

A facial recognition device is one that views an image or video of a person and compares it to one that is in the database. It does this by comparing structure, shape and proportions of the face; distance between the eyes, nose, mouth and jaw; upper outlines of the eye sockets; the sides of the mouth; location of the nose and eyes; and the area surrounding the check bones.

Fingerprint identification: Fingerprint scanning essentially provides an identification of a person based on the acquisition and recognition of those unique patterns and ridges in a fingerprint. Likewise, the fingerprint reader is the device that generates the input data which is going to be basis on which the security system is going to grant access or not. It creates a pattern in identify a user. The actual fingerprint identification process will change slightly between products and systems. The basis of identification, however, is nearly the same. Standard systems are comprised of a sensor for scanning a fingerprint and a processor which stores the fingerprint database and software which compares and matches the fingerprint to the predefined database. A SecuGen thumbprint reader is used for this project research. It is shown below Figure 1.

Figure 1: Secu Gen Thumbprint Reader.

Fingerprint analysis

The analysis of the fingerprint is explained in the following steps.

Conversion of fingerprint into grey scale: The colored images in the database were read and converted into the grayscale images with pixels between 0 and 255. These images were converted into grayscale because most fingerprint identification algorithms use matrix in their analysis [4].

Performing of fast Fourier transform on the image: We divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$$F(u,v)=\sum_{X=0}^{M-1}\sum_{Y=0}^{N-1} f(x,y)\times\exp\left\{-j2\pi\times\left(\frac{ux}{M}+\frac{uy}{N}\right)\right\} \quad (1)$$

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs(F(u,v)) = |F(u,v)|.

The enhanced image after FFT has the improvements to connect some falsely broken points on ridges and to remove some spurious connections between ridges.

Find the ridges and breaking point furrows: The ridges and breaking point furrows are the unique part of the thumbprint which makes identification easy. They are important parts for comparison of fingerprints, i:e, if the ridges and breaking point furrows of a user does not match that which is in the database, access to the system will be denied.

Extraction of minutiae: Minutiae, the discontinuities that interrupt the otherwise smooth flow ridges, are the basis for the most fingerprint authentication. Minutiae are mainly ridging endings, the point at which ridge stops and bifurcations, the point at which one ridge divides into two. Other types of minutiae exists including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporary divergent ridges), ponds or lakes (empty space between two temporary divergent ridges), spurs (a bridge notch protruding from a ridge), (small ridges joining together adjacent ridges), and crossovers (two ridges which cross each other) (Figure 2).

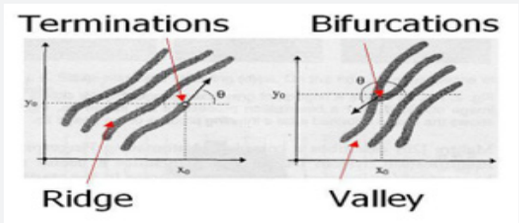

Figure 2

Calculation of euclidean distance: The Euclidean Distance Algorithm is required in the analysis of the biometric application system to calculate the distance between each pixel (dots per inch) of trained images. If this distance is greater than the threshold, the image will not match.

Matching: This is when the comparing of images occurs. The images are compared with that of the user saved in the database. If the captured image matches that in the database, access is granted. If the image does not match that in the database, access is denied [5].

Application program

The application is designed to accept data from the thumbprint reader which server as the input to the application. Aside the fact that this segment is accepting input data from the thumbprint it does some other things such as:

- Fingerprint identification: This is where the images given to the application are compared with the images in the database of the application. This is to ensure such a user is an authorized user in this environment.
- It creates the database so as to add or remove user's fingerprint as the case may be.
- This application program also controls the security in order to access.

Also, in the case of the face recognition the webcam is used to capture the images that were used in this project.

Image analysis: The face images used for this project work were taken within Ladoke Akintola University of Technology, Ogbomomso. Face images of some individuals were taken with a webcam and all the images in JPEG format. Each individual has four images. The size of each image was originally 180pixel by 180pixel. The images were grouped into two classes namely: training class which consists of four per individual and testing class which consists of two images per individual.

Grayscale conversion: The colored images in the database were read and converted into the grayscale images with pixels between 0 and 255. These images were converted into grayscale because most face recognition algorithms use matrix in their analysis.

Image resizes and matrix format: The grayscale images were resized by the program so as to extract the features such as eyes,

nose, and mouth regions in each image with reference to the center of each face image in the database and appropriately represent it in matrix format and stored in a vector of size N.

Conversion into vector form: The steps used in the conversion of vector form are:

- **Centre data:** Each of the training images was centered by subtracting the mean image from each of the training images. The mean image is a column vector such that each entry is the mean of all corresponding pixels of the training images.
- **Create data matrix:** The training images were combined into a data matrix of size N by P once the training images were centered. (P is the number of training images and each column is a single image).
- **Create covariance matrix:** To create a covariance matrix, the data matrix's transpose is multiplied by the data matrix.

Calculate the eigenvalue and eigenvector: The eigenvalues and the corresponding eigenvectors were converted for the covariance matrix. The data matrix was multiplied by the eigenvectors and the eigenvectors were divided by their norms [6].

Software environment

The real time-based security using fingerprint and face consist of subsystem namely the thumbprint reader, interfacing control system, webcam, and the control program written in MATLAB 2010. The developed control program application which operation depends on the sensing of the matched fingerprint and face with the database template direct and control the operation of the interfacing control which enables the access to be granted or to be denied.

Biometric library automation

This interface consists of two important options boxes which are: "sign in" and "sign up" options.

Sign in: This key enables registered user to gain access to the library system. The user supplies his/her necessary information (matric number and name). The facial image and fingerprint of the user is obtained, and access is granted if they match those in the database.

Sign up: This interface enables new user to register into the system. The new user supplies his/her name, matric number, and allows the system to capture his/her facial image and fingerprint. All this information are saved into the database Figure 3.

Figure 3: Biometric library automation interface.

Registration interface

The user supplies matric number and name in the column provided. The matric number serves as a unique identity for each registered user. After supplying the required information, the "proceed" icon is pressed 'proceed' key which enables him/her to use other keys like on webcam, snap, load fingerprint, save and exit.

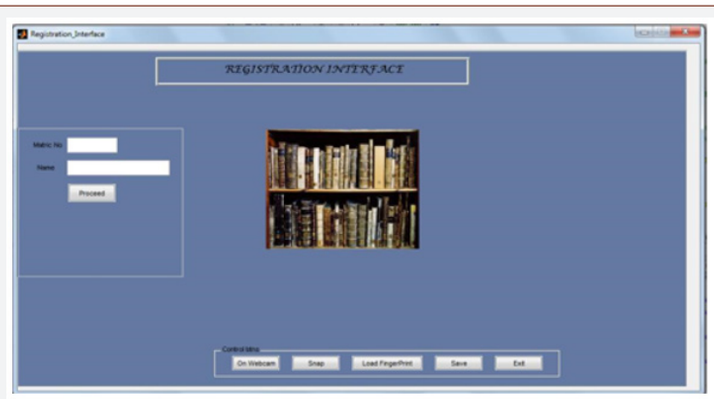

Figure 4: Registration Interfaces.

The webcam is switch on to enable the user to snap his/her picture and later load the fingerprints that have been saved into the fingerprints database and finally save the user's information into the database Figure 4 and Figure 5.

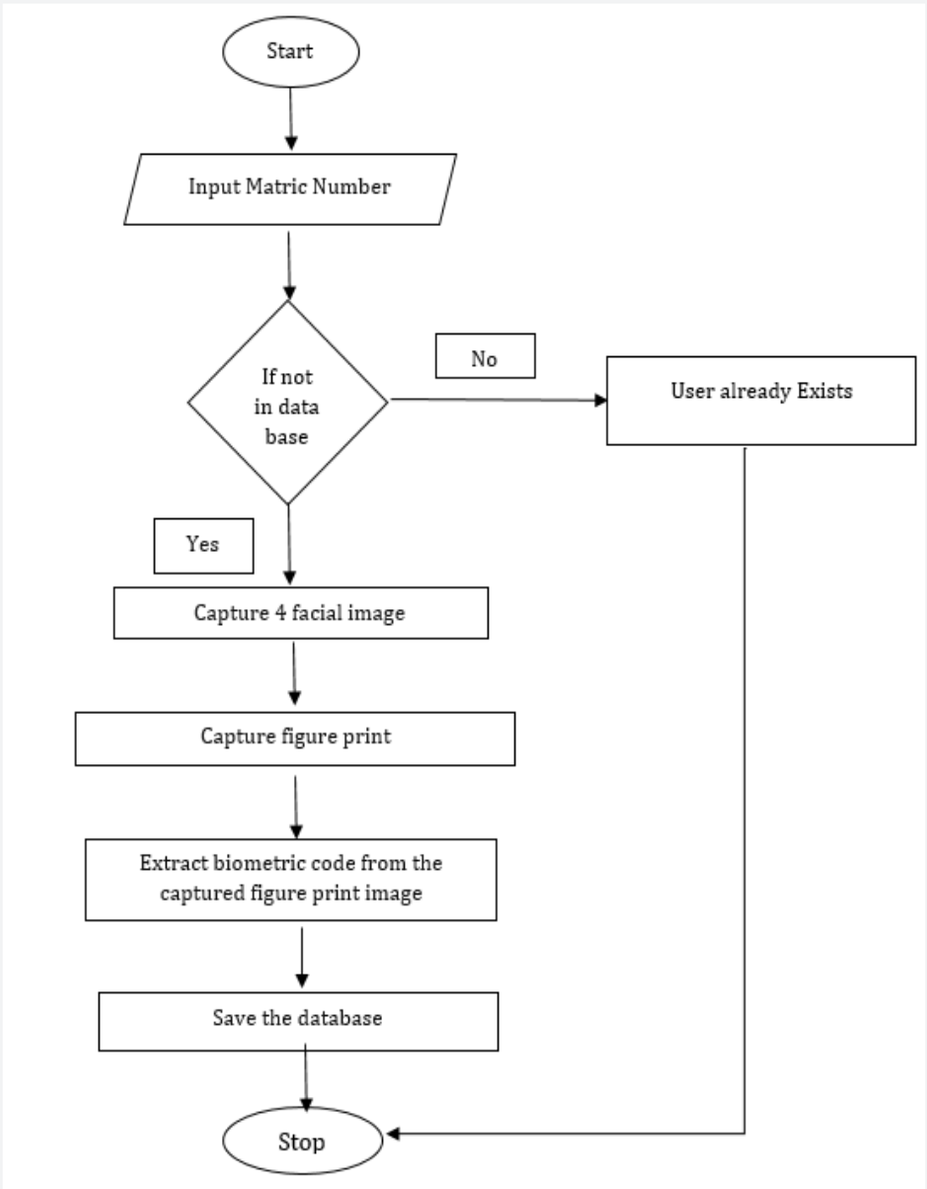

Figure 5

Fingerprint and face database

The fingerprint and face database work differently. The fingerprint database is where the fingerprints taken during the course of registration by new users are been stored while the face database is where the images taken while registering for new users are been stored and the images and fingerprints are retrieved from the two databases when necessary.

Authentication

This is the process by which the registered user information is matched with those in the database, if it corresponds, that is, the Euclidean distance of the face image and fingerprint is less than the threshold value, the user is granted access into the library, else, access is denied.

Authentication interface: The interface provides a platform for the registered user to gain access into the library system. The matric number of the user is supplied, after which "On Webcam" button is pressed to start the computer webcam. An image appears on the screen of the computer, the "snap" button is pressed to capture the displayed image. The fingerprint image is then loaded from the fingerprint database by clicking on the "load fingerprint" button. The interface will display the facial image and fingerprint image, then, the "authentication" button is pressed. This will compare the images acquired from the user to those in the database, if they match correctly with those in the database, access is granted, else, access id denied and the message box "will you like to register" is displayed Figure 6.

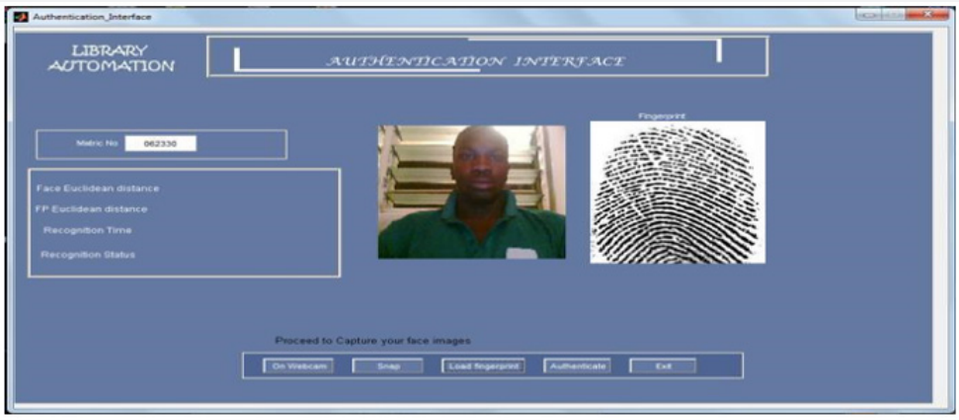

Figure 6: Authentication Interface.

The main program

Since the security system designed using fingerprint identification and facial recognition is meant to be a real time process, the software module are designed to automatically perform operations and it is always running as expected unless it is halted by an administrator or when maintenance is to be done on it or its database of image is to be updated to allow for addition or removal of some fingerprints that has or should have access to restricted area. The main program is written with MATLAB 2010 [7].

Result and Discussion

Computer and operating system characteristics

The application is designed with MATLAB which is mostly used for engineering works that involves calculations. Consequently, the system can run perfectly on Microsoft windows (2000, xp, vista or window 7) with 32 bits and at least Pentium III class processor of 800MHZ and 64MB physical memory. The minimum free space capacity on the hard disc should not be less than 60MB and a super VGA or any other higher resolution monitor with a keyboard and a mouse.

Result

The prototype of the dual biometric security system was tested with about 10 individuals. There was success in enrolling some of the extracted fingerprint and face in the database. The recognition software correctly identified all test images used with it and reported whether a match existed in the database or not. At instance where there is a match, it can be deduced that the said finger or face was found in the data base.

Recognition time: The recognition time is the time it takes from the time the "enter" key is pressed to the time access is granted (after the facial image and fingerprint have been supplied). This time depends a lot on the system's configuration. A system with higher configuration (like a dual core processor, 4gig Ram and a large available disk space) will have a lower recognition time, while a system with a little less configuration (like a single core processor, 1gig Ram and little available disk space) will have a higher recognition time. The following recognition time are gathered to compute the average recognition time:

5.7654sec,4.5379sec,5.9782sec,6.2351sec

The average recognition time is the mean value for the above recognition times:

$$\frac{5.7654 + 4.5379 + 5.9782 + 6.2351}{4}$$

This gives the mean recognition time to be 5.6292 seconds.

Euclidean distance: The fingerprint Euclidean distance is high if a false fingerprint is supplied into the system. This will result in denied access to the system (Figure 7,8).

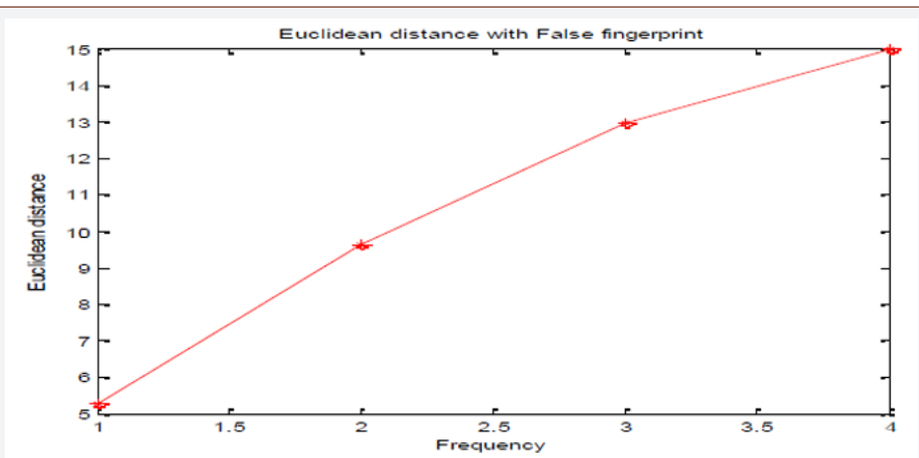

Figure 7: Graph of Euclidean distance against frequency for false fingerprint.

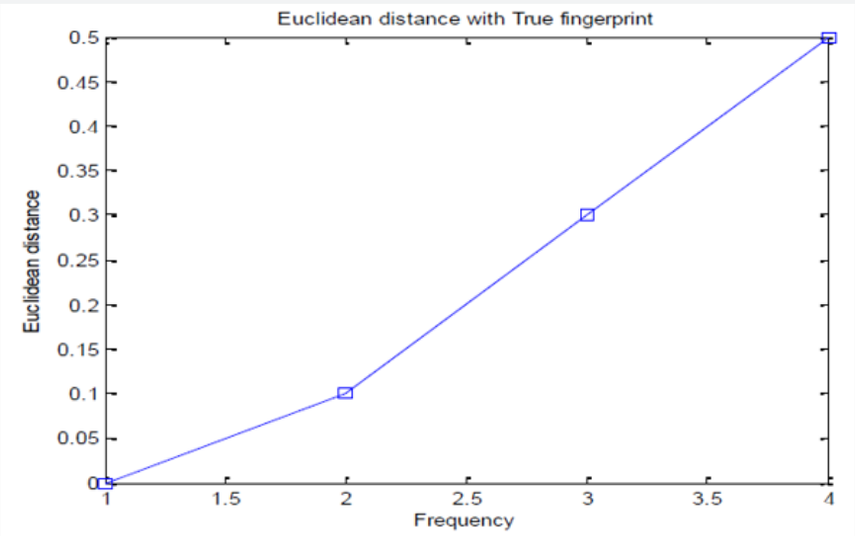

Figure 8: Graph of Euclidean distance against frequency for true fingerprint.

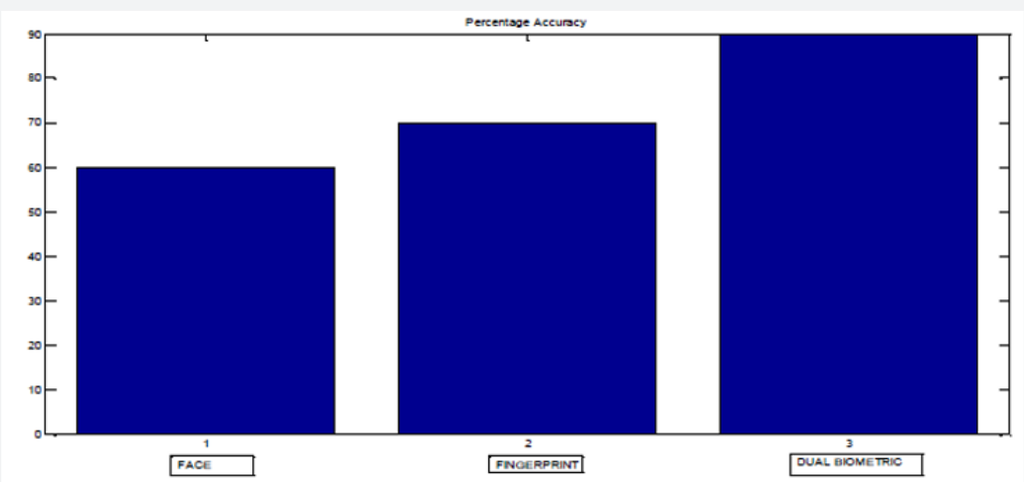

Figure 9

The fingerprint Euclidean distance is low if a true fingerprint is supplied into the system. This will result in granted access to the system (Figure 9).

Discussion

The results obtained from the research work support the set of objectives. The findings indicate that a real time fingerprint and face based authentication security system can be achieved. Although consideration such as the improper functionality of the recognition system as a result of wear and tear of the components, configuration of the system, corrupt recognition software could put a question mark on the proposed robustness and efficiency of the system.

A useful suggestion for minimizing the occurrence of such problems is the adoption of a preventive maintenance culture carried out periodically to ensure the system is always in an optimal working condition.

From the point of view of image quality, the best fingers to use on a fingerprint reader are the index finger, the middle finger and the ring finger. Thumb and the little finger are not recommended because of their area. Some thumbs are too big for the fingerprint reader's area and could result in getting two images with totally different regions. The little finger is very small; this could cause the fingerprint recognition software to extract only a few fingerprint features.

Conclusion

The dualisation of a fingerprint and face recognition based security has brought about a comprehensive blending of the ability of fingerprint and face recognition knowledge into security system which can be implemented in various environments or arena where high security is required. Importantly, there is none or minimal human effort being utilizes both the minutiae and ridge flow information available in the fingerprint and face. From the results obtained from the research work, it can be deduced that the use of biometric security systems offer a much better and foolproof means of restricting the access to an environment by an unauthorized user.

Acknowledgement

None.

Conflict of Interest

No conflict of interest.

References

1. Bolle RM, Ratha NK, Connel JH (2004) "biometrics break-ins and band aids", pattern Recognition Letters.
2. Anil K Jain, Lin HB (2000) "On-line fingerprint verification", pp. 302-314
3. Cappelli R (2003) "Handbook of Fingerprint Recognition". Chapter synthetic fingerprint generation. Springer, New York, USA.
4. Cappelli R, Ferrara M, Maltoni D (2006) "The Quality of Fingerprint Scanners and Its Impact on the Accuracy of Fingerprint Recognition Algorithms". In Processing of Multimedia Content Representation, Classification and Security (MRCS2006), pp. 10-16.
5. Sukthanker G (1999) "Face Recognition: A critical look at Biologically-Inspired Approaches" 2: 45-48.
6. Tang Homan, Sunny (2001) "Face Recognltion Review" Term paper: Department Computer Science and Engineering, Chinese University of Hong Kong, Shatin.
7. Valetin D, Abdi H, O Toole AJ, Cottrell GW (1994) "Connectionist models of Face Processing: A survey", Pattern recognition, 27(9): 1209-1230.