International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 10 – No.5, February 2016 – www.ijais.org

An Access Control System using Bimodal Biometrics

A.S. Falohun
Dept. of Computer Sc. & Eng.
Ladoke Akintola Univ. of Tech
Ogbomoso, Nigeria

O.D. Fenwa
Dept. of Computer Sc. & Eng.
Ladoke Akintola Univ. of Tech
Ogbomoso, Nigeria.

A.O. Oke
Dept. of Computer Sc. & Eng.
Ladoke Akintola Univ. of Tech
Ogbomoso, Nigeria.

ABSTRACT
In today's society, advances in technology have made life easier by providing us with higher levels of knowledge through the invention of different devices. However, each technological innovation harbours the potential of hidden threats to its users. One major threat is theft of private or personal data, information and properties. As digital data become more prevalent, users try to secure their information with highly encrypted passwords and ID cards. However, the misuse and theft of these security measures are also on the rise, taking advantage of security flaws in ID cards result in cards being duplicated or counterfeited and being misused. This increasing battle with cyber security has led to the birth of biometric security systems.

In this work, iris and fingerprint samples were acquired using the iris camera and Secugen pattern extracting sensor respectively. The pre-processing of the acquired images were done, after which templates were generated and stored. Verification of the acquired images was done and voting fusion techniques was used to fuse the information presented by individual modalities. A door prototype was constructed with electric circuit design and an iris and fingerprint recognition software development using MatLab. was interfaced with the door prototype.

The developed system was tested widely with the pre-enrolled subjects as well as freshly introduced subjects. The red light indicator showed the hardware and software connection and door lock .With template match, the door opens (green light indicator comes on accompanied with the buzzer), and with non-match, the door is not opened (red light remains and the buzzer is off).

General Terms
Security, Pattern Recognition, Image Processing

Keywords
Fourier-Mellin Transform, Bimodal, Multimodal, Verification, Authentication

1. INTRODUCTION
Biometrics is defined as the unique (personal) physical/logical characteristics or traits of human body. [8]. These characteristics and traits are used to identify each human. Any detail of the human body which differs from one human to other will be used as unique biometric data to serve as that person's unique identification (ID), such as: retinal, iris, fingerprint, palm print and DNA. Biometric systems will collect and store this data in order to use it for verifying personal identity. The combination of biometric data systems and biometrics recognition/ identification technologies creates the biometric security systems. The biometric security system is a lock and capture mechanism to control access to specific data. In order to access the biometric security system, individuals will need to provide their unique characteristics or traits which will be matched to a database in the system. If there is a match, the locking system will provide access to the data for the user. The locking and capturing system will activate and record information of users who accessed the data. The relationship between the biometric and biometric security system is also known as the lock and key system. The biometrics security system is the lock and biometrics is the key to open that lock [9].

There are seven basic criteria for biometric security system as illustrated in figure 1: uniqueness, universality, permanence, collectability, performance, acceptability and circumvention [16]. As mentioned above, uniqueness is considered as the priority one requirement for biometric data. It will indicate how differently and uniquely the biometric system will be able to recognize each user among groups of users. For instance, the DNA of each person is unique and it is impossible to replicate. Universality is the secondary criteria for the biometric security. This means that everyone in the world has one biometric trait or the other. Thirdly, a permanence parameter is required for every single characteristic or trait which is recorded in the database of the system and needs to be constant for a certain period of time. This parameter is not affected by the age of the user. Following the permanence parameter is the collectability. The collectability parameter requires the collection of each characteristic and trait by the system in order to verify their identification. Then, performance is the next parameter for the system which outlines how well the security system works. The accuracy and robustness are main factors for the biometric security system. These factors will decide the performance of the biometric security system. The acceptability parameter will choose fields in which biometric technologies are acceptable. Finally, circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process. DNA is believed to be the most difficult characteristic to fail in the verification process. [12].

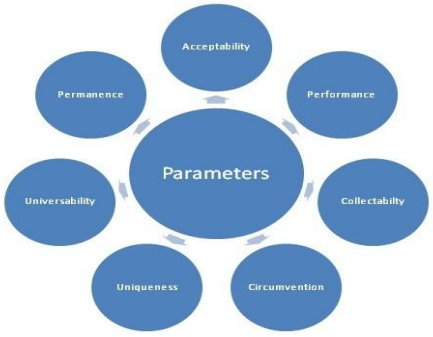

Figure 1.1 Parameters of Biometric

The general biometric system has data acquisition, preprocessing, feature extraction, matching sections. The function of data acquisition section is to collect the number of sample of biometrics in different conditions and store it as a database. In preprocessing section the images are normalized by colour conversion, cropping and resizing.

The features are extracted from normalized image in feature extraction section by using spatial domine, transformation domine or combination of both. The final results obtained from extracted features are checked for matching using the distance formulas like Euclidian Distance (ED), Hamming Distance, Chi-square, Linear Discriminant Analysis, Support Vector Machine, Neural Networks etc., The biometric systems are very much essential in applications like Home Security, Airport Checking, Voting machine, Entry to high security zone like parliament House, ATM, Laptop, public places like shopping mall etc. [14]

In this work, we present a bimodal biometric system using iris and finger print whose features and performance were tested under various conditions. Bimodal biometrics systems utilizes dual physiological or behavioral characteristics for enrollment, verification and identification**.**

2. LITERATURE REVIEW

2.1 Biometrics

The need for a reliable security measure brought about the use of anatomical characteristics in identification, verification and access control. [6] defined biometric as the use of physiological or behavioural characteristics to recognize or verify the claimed identity of an individual, [17] claimed that biometrics technology make use of physiological or behavioural characteristics to identify individuals. [2] explained the term biometrics as a science involving the statistical analysis of biological characteristics. [13] viewed biometrics as both characteristics and process. As a characteristics, it is a measurable biological (anatomical and physiological) and behavioural characteristics that can be used in automated recognition and as a process, it encompasses automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioural characteristics. Though, each biometrics technology has its merits and shortcoming.

2.2 A Typical Biometric System.

Figure 2 illustrates biometric system as a pattern recognition system that recognizes a person based on feature vectors derived from a specified physiological and behavioural characteristic that the person possesses. [10]

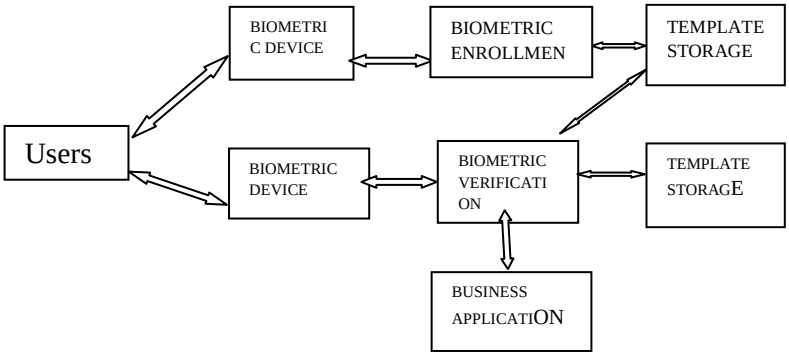

Figure 2 Biometric System Process (Wikipedia; [10])

2.3 Fusion Techniques

Fusion Technique is an integrated scheme required to fuse the information presented by individual modalities. [10] Some of fusion techniques are as follows:

2.3.1 Sum Rule

The sum rule method of integration takes the weighted average of the individual score values. This strategy is applied to all possible combinations of two or more biometrics module. Equal weights are assigned to each modality, as the bias of each matcher is not available. [15].

2.3.2 Voting Techniques

Voting techniques are classical empirical techniques where the global decision rule is obtained simply by fusing the hard decisions made by two biometrics modules. A hard decision is a score that only returns either a 0 or a 1. This technique accepts the identity claimed by the person under investigation if at least *k*-out-of-2 modules decide that the person is genuine. When $k = 1$, this is called the *OR* rule. The identity claimed is accepted if at least one of the two experts decides that the person under investigation is genuine. While $k = 2$, this is called the *AND* rule. The identity claimed is accepted only if both the experts decide that the person under test is genuine. [15]

2.3.3 Multilayer Perceptron (MLP)

An MLP is a neural classifier that separates the training data of the several classes by implementing a separation surface, which can have any arbitrary flexible shape. The flexibility of the separating surface is determined by the complexity of the architecture. In this paper, an MLP with two neurons on the input layer (two scores coming from two module biometrics), three neurons on the hidden layer and one neuron (two classes) on the output layer, sigmoidal activation functions for all neurons and the Back propagation training algorithm is adopted. Using sigmoidal activation functions, the value of the output neuron lies in the interval [0, 1], and the optimal decision threshold is fixed at 0.5. ([15]

2.4 Review of Related Works

[5] developed a biometrically-controlled door system using iris alone (unimodal trait) but [1] of the Michigan State University brought up a multimodal biometric system using Fingerprint, Face and Speech and observed that the identity established with the three is more reliable (stronger) than with each of the traits.

[11] presented a paper that used multimodal biometrics in order to identify or verify a person that wants to start the engine of a car. First of all, a fingerprint sensor was posted on the car's door, one on the steering wheel, a camera for iris recognition on the car's main mirror, and finally a microphone for voice recognition. There were two possibilities: if the person is identified as the car owner or a known user, then he/she can take control over the car; if it's an intruder, the car can announce the security service or the police using a complex GPRS system.

The industry also is not left out as MorphoTrak, an IT based Industry provides finished products and services in both unimode and multimodes for more than 450 government agencies in over 100 countries and is consistently ranked #1 by NIST for enrollment and matching accuracy (www.morpho.com/USA.) used in Biometric Sensors and Detectors, Facial Recognition, Fingerprint Readers, Iris Scanners & Recognition, Smart Cards, Border Control / Airports, Consumer / Residential Biometrics, Justice / Law Enforcement, Logical Access Control, Mobile Biometrics. Other Uses of Biometrics, Physical Access Control, Time and Attendance, Hand Readers & Finger Scanners, Middleware/Software, Vein Recognition. [7]

3. METHODOLOGY

3.1 Iris

3.1.1 Iris Acquisition

Iris images used were capture using a sizeable iris camera with Megapixel 7.0.

Black Faces Iris: Iris images captured within our immediate environment were also used to test the performance of the system.

Figure 3 Black iris images

3.1.2 Segmentation

Two-level segmentation technique combining Circular Hough Transform and Daugman's Integro-Differential Operator was used due to the low contrast in the nature of the black eye´s irises used (Nigerian eyes). Its parameters are the center coordinates xc and yc, and the radius r, which are able to define any circle according to the equation

$$x_c^2 + y_c^2 - r^2 = 0 \quad (1)$$

It also detect eyelids, approximating the upper and lower eyelids with parabolic arcs, which are represented as

$$\left(-\left(x-h_j\right)\sin\theta_j + \left(y-kj\right)\cos\theta_j\right)^2 = a_j\left(\left(x-h_j\right)\cos\theta_j + \left(y-kj\right)\sin\theta_j\right) \quad (2)$$

Where a_j controls the curvature, (h_j, k_j) is the peak of the parabola and Ø is the angle of rotation relative to the x-axis.

And because inner and outer iris boundaries are not concentric like the pupil, integrodifferential operator was performed around the pupil canter and the iris radius in order to find the iris canter according to equation 3.

$$max_{(r,x_0,y_0)} |G_\sigma(r) * \partial \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \ | \quad (3)$$

Where I(x, y) is the eye image, r is the radius to search for, Gσ (r) is a Gaussian smoothing function, and s is the contour of the circle given by r, x_0, y_0. The operator searches for the circular path where there is maximum change in pixel values, by varying the radius and centre x and y position of the circular contour.

3.1.3 Feature Extraction

A feature extraction based on Enhanced Inverse Analytical Fourier-Mellin Transforms was used to extract the isolated iris texture. [4]

3.1.4 Feature Matching

The Hamming distance gives a measure of how many bits are the same between two bit patterns [3]. Using the Hamming distance of two bit patterns, a decision can be made as to whether the two patterns were generated from different irises or from the same one. In comparing the bit patterns X and Y, the Hamming distance, HD, is defined as the sum of disagreeing bits (sum of the exclusive-OR between X and Y) over N, the total number of bits in the bit pattern.

3.2 Finger Print

3.2.1 Acquisition of finger print image using pattern extracting sensor

Acquisition was done by the use of Secugen Fingerprint pattern-extracting device.

3.2.2 Pre-processing of the finger print image

The quality of the obtained raw images was low because the images are blurred and noisy due to variations in environmental conditions, skin conditions, and acquisition devices. A set of tasks were applied to improve the clarity of the print pattern structure and localize the prints grid such as:

Image Enhancement: This is the first stage in improving the quality of the acquired print pattern, it includes the following steps;

(i) **Image Preparation**: The input image is converted to be 8-bit gray image. Then, it is converted to the negative which make the ROI as bright region.

(ii) **Brightness Stretching & Normalization**: A simple linear type of contrast stretching is applied to enhance the visual **appearance** of the image details. The dynamic range of pixels values is adjusted to be. This process is done using the following equation;

$$N(x,y) = \frac{N_{max} - N_{min}}{O_{max} - O_{min}}(O(x,y) - O_{min}) + N_{min} \quad (4)$$

(iii) **De-Noising & Integration**: Despite the image is blurred, a simple mean smoothing filter is used to reduce the noise and to integrate the white ROI. Mean filter can lead to good result, when applying it in a specific way. The size of the applied mean filter is 7x7, and is applied four times to obtain an acceptable result, denoted $I_s()$

3.2.3 Post- Processing

This involves **cleaning the gaps and pores; Binarization; Thinning. Then Feature Extraction** was done and **Template Matching.**

3.2.4 Voting fusion Technique

Voting techniques are classical empirical techniques where the global decision rule is obtained simply by fusing the hard decisions made by the two biometrics modules. A hard decision is a score that only returns either a 0 or a 1. This technique accepts the identity claimed by the person under investigation if at least *k*-out-of-2 modules decide that the person is genuine. Here, $k = 2$, called the *AND* rule was used. The identity claimed is accepted only if both the iris and fingerprint extracts belong to the individual.

3.2.5 System Software

When images of iris and finger print are captured, the images are loaded into the system software, the images are then processed by the system software. The system software was written in MatLab. codes.

3.3 Control Unit

The control unit consist majorly of a microcomputer IC (PIC16F84A), which serves as the intermediary between the software and the door to be controlled.(Figure 4) When the iris and finger print are scanned and analyzed, on verification, the authorization is sent to the microcontroller, through a serial protocol. The microcontroller will actuate the door unit. The lock will be opened. The microcontroller's speed is controlled by the crystal oscillator attached to it, the frequency of the crystal oscillator is divided by four and that gives the speed of the microcontroller.

$$\text{No of Instructions/sec} = \frac{crystal\ oscillator\ value}{Dividing\ factor} \quad (5)$$

Where the dividing factor for PIC = 4

$$\text{No of instructions/sec} = \frac{20000000}{4} = 5000000MHz$$

3.4 Access Control System (Door Unit)

The door unit is made up of an electromagnetic door lock; this door lock utilizes little electric signal to switch over from open to close and vice versa. When authentication is sent from the system software to the control unit, the control unit will energize the actuator which unlocks the door lock. The Algorithm is as follows:

1. Start
   a) Enrol Iris Template
   b) Enrol Fingerprint Template
2. Match Templates
3. If ´´ Match Found `` then go to 5 else go to 2
4. Template Fusion
5. Unlock Door
6. Stop.

4. IMPLEMENTATION

The Pseudocode above illustrates the flow direction of the bimodal biometric as regarding access control system: Biometric traits are acquired (Start), and these traits were extracted and stored in the database of the system (enrolment), i.e., the iris and the fingerprint images. The verification of individual users compares the newly generated iris and finger print templates with the reference or pre-enrolled templates at the matching stage. If a match is found it proceeds to fuse the iris and finger print templates as a single entity and the door is unlock but otherwise, access is denied and a loop returns the user back to the starting stage.

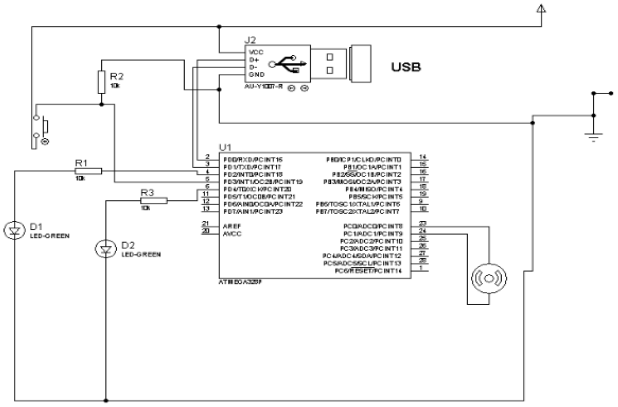

Figure 4. Circuit Diagram of the access system

As seen from the circuit diagram above, three resistors are used to oppose the flow of electricity in the circuit. They are used to limit the current in the circuit and they are also used as a potential divider to achieve a specific value of voltage across a terminal. Also LED diodes used are semiconductor devices consisting of a P-N junction formed either in germanium or silicon crystal. The P and N regions are referred to as anode and cathode respectively. The PIC used belongs to the mid-range family of the PIC microcontroller devices.

The program memory contains 1k words, which translates to 1024 instructions, since each 14-bit program memory word is the same width as each device instruction. The data memory (RAM) contains 68 bytes. Data EEPROM is 64 bytes. There are also 13 I/O pins that are user-configured on a pin-to-pin basis. The buzzer buzzes when the door is opened and the USB is used to connect the prototype to the computer system.

After the assemblage the USB cable was connected to the circuit for communication between the circuit and computer that will authorize the opening and closing of the door. Plate 1 shows the circuit assemblage before the USB was connected to it.

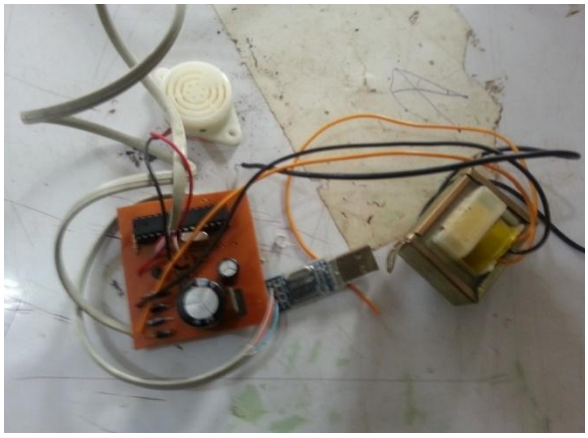

Plate 1. Circuit Assembly on Printed Circuit Board (PCB)

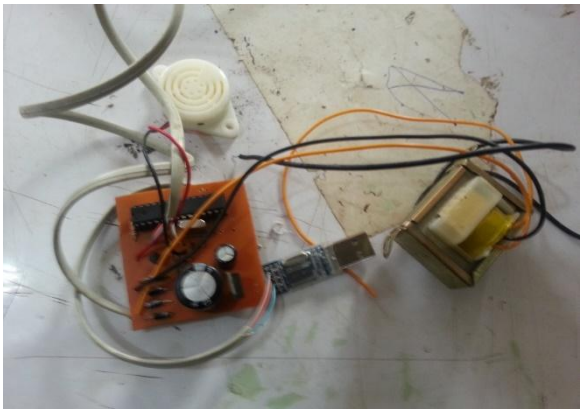

Plate 2. Picture of the programmer hardware used for the programming

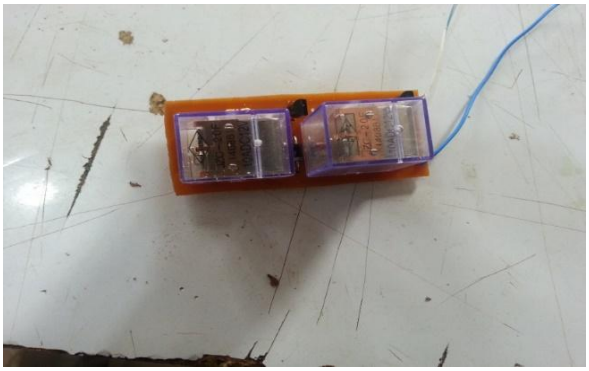

Plate 3. Programmer Hardware

4.1 Casing

After the hardware part of the system has been successfully assembled as shown in plates 2 and 3, the system was cased in a white plastic box of dimension 2cm × 4cm× 4cm. as seen in plate 4. Holes were made on the casing in order to allow passage of wires into the box; to connect the indicators and the lock to the circuit inside the case.

Plate 4. Casing for the hardware

4.2 The Door Model

Since this project is access based system, there arose a need to design a mode of a door system, and to make the system easily movable the size of the door model must be considered.

The mode of the system was made with an aluminum and transparent glass. This was made in form of a safe and a show glass. To the door was attached the status light indicator that indicates if the door is locked (red) or unlocked (green).

Plate 5. Model of The System's Door

4.3 Software Design

The following software was used in the design of the interface:

- Matlab
- Serial-to –USB Driver

The program was written using the Matlab IDE (Integrated Development Environment). The software was design to be able to enroll iris template and finger print template that has been trained with the software and identify to give authorization for opening the door. Figure 5 shows the software interface for the system.

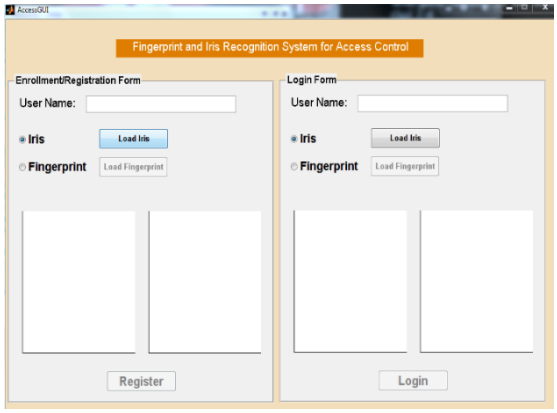

Figure 5 Software Interface

4.4 Discussion

The proposed system has been tested with a number of iris and fingerprint templates and is found to be working fine with the hardware connected to it. The figures below show the working interface of the system.

4.4.1 Registration Interface

This interface presents the registration platform for iris and fingerprint templates. At this point, the iris and finger print template is browsed for and registered with a unique user name. The registered templates are processed and saved in the database (Figures 6 and 7).

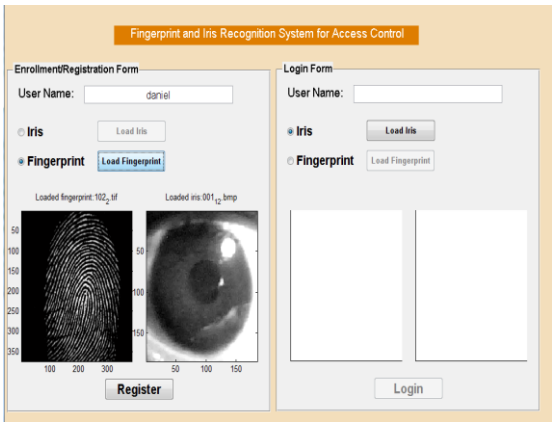

Figure 6 Registration Interface

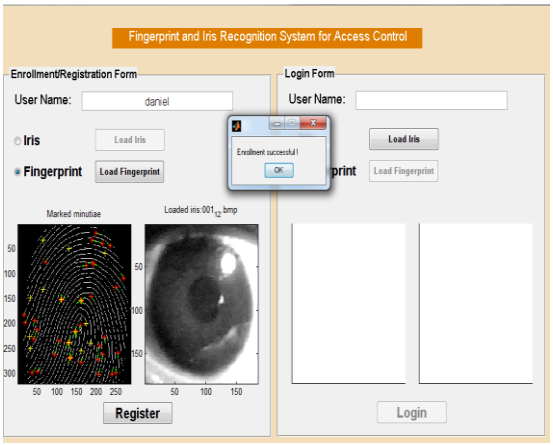

Figure 7 Registration interface showing successful enrolment

4.4.2 Authentication Interface

This interface compares the already registered iris and fingerprint templates with the captured templates. Figure 8 shows a matched template. At this point the door is unlocked granting access but in a situation where there is difference in templates an error message "no match templates: access denied" is flagged (Figure 8) and the door remain locked.

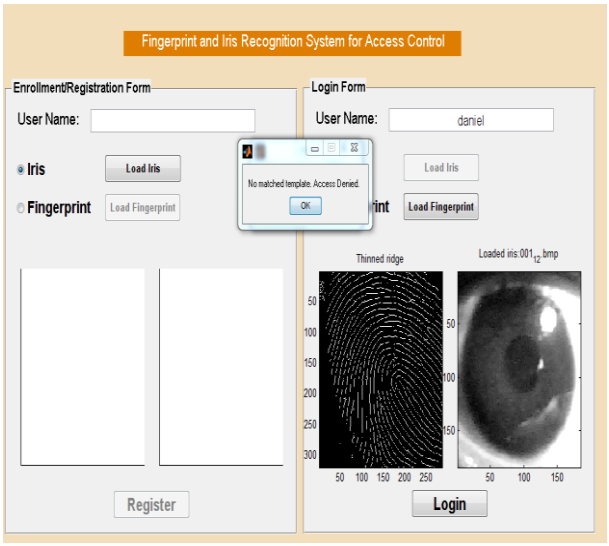

Figure 8 Authentication interface showing access denied

5. CONCLUSION

A biometrically controlled door system using Iris and fingerprint templates has been successfully designed and constructed. The hardware was successfully designed, constructed and a computer program that enabled the door's operation via an electric circuit was also developed. This will provide a more secured and foolproof access control system. The work also emphasizes the uniqueness of bimodal biometrics in performance over the unimodal counterparts.

6. RECOMMENDATION

Future work can look into fusion techniques that will enhance template matching accuracy and speed.

7. REFERENCES

[1] Anil J., Lin H., & Yatin K. "Multimodal Biometric System using Fingerprint, Face and Speech." Michigan State University MSU-CPS-98. 32. ps.

[2] Babak Ganji 2005. Civil–Military Relations, State Strategies and Presidential Elections in Iran, Camberley: Conflict Studies Research Centre, Defence Academy of the United Kingdom. 42. Ibid., pp. 75–76.

[3] Daugman J. 1993 "High Confidence Visual Recognition of persons by a test of Statistical independence". IEEE Transactions on Pattern Analysis and Machine Intelligence, 1148 – 1161.

[4] Falohun, A.S. 2012 "Development of a Feature Extraction Method for Iris Recognition using Enhanced Inverse Analytical Fourier-Mellin Transform". Unpublished Ph.D. Thesis. April 2012.

[5] Falohun, A.S., Omidiora, E.O., Fakolujo, O.A., Afolabi, O.A., Oke, A.O., Ajala, F.A. 2012. "Development of a Biometrically-Controlled Door System (Using Iris), with

power Backup." American Journal of Scientific and Industrial Research., vol 3, No 4, pp 203-207.

[6] Gray Ross 2001 "Biometrics and Technologies and Economic Indications", International Conference on image and graphics 12-18, Ohio, USA.

[7] http://findbiometrics.com/solutions/multimodal-biometrics/. 2014 Find biometrics retrieved on 14 january 2016.

[8] Jain A.K, Ross A, Prabhakar S 2004;"An introduction to biometric recognition", GVIP Journal 14(1): 4 – 20

[9] Jain A.K, Ross A, Pankanti S. 2006 "Biometrics: a tool for information security", Keesing Journal 1(2): 125 – 143

[10] Kresimir D. and Mislav. G. 2004. "A survey of biometric recognition methods."*Proceedings of the 46th International Symposium Electronic in Marine (ELMAR).* pp: 16-18.

[11] Lupu C and Lupu V. 2007 Car Access Using Multimodal Biometrics 'Computational *Computer Intelligence and Intelligent Informatics.368-377.*

[12] Maestre, Sandra Sean Nichols 2009. "DNA Biometrics",

[13] NSTC subcommittee 2006. "Biometric Overview", *www. Biometricscatalog.org/NSTCSubcommitee*

[14] Ramachandra A. C., Abhilash S. K., Raja K. B., Venugopal K. R., Patnaik L. M. 2012. Feature Level Fusion Based Bimodal Biometric Using Transformation Domine Techniques IOSR Journal of Computer Engineering (IOSRJCE) Vol 3, Issue 3 (July-Aug. 2012), PP 39-46

[15] Samad and Hussain. 2006 "Introduction to Fusion Techniques", Rome Air development center, RACDC-TR-81-161 final technical report.

[16] Schuckers Michael E. 2001 "Some Statistical Aspects of Biometric Identification Device Performance" Some Statistical Aspects of Biometric Identification Device Performance ***Submitted to Stats Magazine*** Department of Statistics West Virginia University.

[17] Xie Mei 2006. "Iris Recognition Techniques" Journal on Electronic Science and Technology of China 4(3): 219-224.