International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 12, Issue 3, March 2021, pp.410-420 Article ID: IJARET_12_03_038
Available online at http://iaeme.com/Home/issue/IJARET?Volume=12&Issue=3
ISSN Print: 0976-6480 and ISSN Online: 0976-6499
DOI: 10.34218/IJARET.12.3.2021.038

IMPLEMENTATION OF A BIMODAL BIOMETRIC ACCESS CONTROL SYSTEM FOR DATA CENTER

Kennedy Okokpujie, Sarah Alex, Olusola Abayomi-Alli, Abubakar John, Anthony Adoghe and I. P. Okokpujie

Department of Electrical and Information Engineering
Covenant University, Nigeria

ABSTRACT

The use of biometrics has become one of the only sure ways to provide secure access control to rooms where vital asset are stored, such as data centers where valuable information are stored. This paper aim at designing and implementing a bimodal biometric access control system for data center using fingerprint and Iris trait of the same person, it is called bimodal biometric system. The system was implemented by integrating hardware components such as PIC18F452 microcontroller, fingerprint and iris sensors and so no with the software programs as such C language and MYSQL interface. On testing, it is found to improve the security and reliability in the access control systems management of the data center.

Key words: Biometrics, Fingerprint, Iris, Access control, Data Center, Security, and Information.

Cite this Article: Kennedy Okokpujie, Sarah Alex, Olusola Abayomi-Alli, Abubakar John, Anthony Adoghe and I. P. Okokpujie, Implementation of a Bimodal Biometric Access Control System for Data Center, *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 12(3), 2021, pp. 410-420.
http://iaeme.com/Home/issue/IJARET?Volume=12&Issue=3

1. INTRODUCTION

Biometric system can be described as the automated estimation of biological, physiological or behavioral qualities of individuals for verification and identification with high consideration in different areas of application such as medicine, access control, security, and so no [1]. A verification system confirms an individual by looking at the captured biometric trait with the dataset biometric format pre-stored features in the system (1:1). While an identification framework recognizes a person by searching the whole template database to obtain a match (1:N). It conducts many comparisons to ascertain the identity of the person. Any human physiological and behavioral characteristic can be utilized as a biometric identifier to recognize an individual as long as it fulfils these necessities: universality, uniqueness, permanence and

collectability. However, the current studies have shown that biometric data are sensitive data in countries like the European Union (EU), and such data should keep subject to the right of privacy preservation [2].

A data center is a facility that integrates an organization's collective Information Technology (IT) operations and equipment for the dedications of storing, processing, and disseminating data and applications. The data center of an organization is the home of sensitive information which houses the company's critical data such as sensitive customer information, essential company strategies and plans, and so no. These sensitive data are to be kept from unauthorized individuals; therefore, there is a need for a secured measure that is not only safe but allows proper identification of individual access to such information [21].

Unfixed reactive dye and/or hydrolyzed dye, along with alkali used for fixation, may also pose an environmental hazard because the hydrolyzed dye will pass in the effluent thereby increasing the pollution load. Certain reactive dyes, like mono- and di-chlorotriazine, or flourotriazine type of reactive dyes may cause the passage of organo-halogen in the discharge effluent, which may by-pass the permissible discharge limit fixed by certain countries.

The use of biometrics has become one of the safest ways to provide secure access to rooms, bank vaults, museums and other sensitive places, which are used to house data or information. Several methods have been used to enhance the performance of biometric data by previous researchers, such as the use of encryption, fuzzy, and other machine learning methods [3][4]. Therefore, biometric technology evolution can be described as a method involves the use of an individual's unique physical characteristics such as fingerprint, face, palm prints, iris, signature verification, speech recognition, iris, etc. for storing sensitive information and valuables. The motivation of this study is based on the difficulty in storing information without invaders gaining access to such information; therefore, incorporation two biometric traits is expected to improve safety and access control. The aim of this study is to design a bimodal biometric door using fingerprints and iris as a security measure [5].

2. LITERATURE REVIEW

2.1 The Fingerprint Identification System

The fingerprint is the most widely applied biometric traits due to its robustness against spoofing attack as finger-veins are embedded inside a finger and need to be captured by an infrared sensor [1].

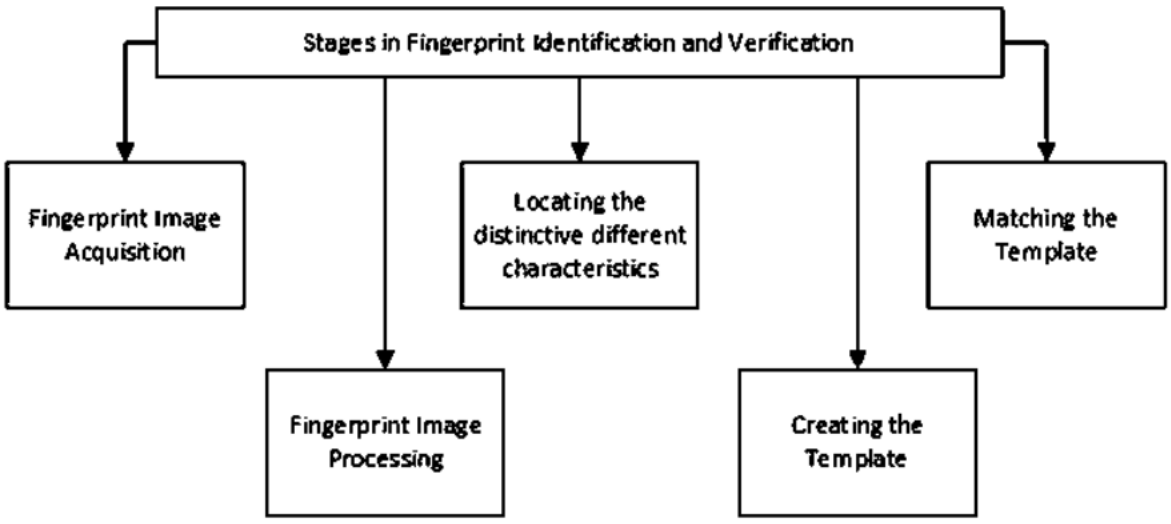

Figure 1. Stages in Fingerprint Identification and Verification

The fingerprint is the production of a fingerprint epidermis, delivered when a finger is squeezed against a smooth surface. The most apparent characteristic for a fingerprint is an example of interleaved edges and valleys. Fingerprints are made of a progression of ridges and furrows on the surface of the finger. The Fingerprints have a center around which designs like whirls, loops, or arches are bent to guarantee that each print is unique. Minutiae and patterns are essential in the examination of fingerprints since no two fingers have been shown to have identical fingerprints. Figure 1 shows the stages of fingerprint identification and verification.

2.2 The Iris Recognition System

Iris recognition is the process of recognizing a person by examining the irregular pattern of the iris [7]. The Iris Recognition Technology combines pattern recognition, computer vision, optics and statistical inference. However, the colour and structure of an iris are usually linked genetically, unlike the pattern details. Therefore an individual's irises are unique and structurally distinctive, which makes it suitable for biometric identification [8] [9].

2.3 Review of Related Works

[10] Proposed fingerprint identification security systems using Minutiae Matching Algorithm and the Gabor filter bank. The study describes the importance of minutiae pattern in analyzing fingerprints since no two fingers are identical. The fingerprint sensor takes a Mathematical image, which is combined with a fingerprint enhancement algorithm to remove noise and preserve the structure of the ridge and valleys on the finger to ensure that the quality of the system will not be affected by differences or variations in the fingerprint images. [11] Proposed a human identification technique using images of the iris and wavelet transform. The study aims to display a better approach for perceiving humans from images of the iris of the eyes under functional conditions with the end goal of recognizing diverse iris by using zero-crossing representations. These representations are then stored in the database of the system and referred to as models [12].

[13] Highlighted the issues of usability and acceptability of biometric security systems with the focus on existing challenges with the conventional biometric system. The study shows that certain factors increase biometric system usability such as small, cheap sensor, convenient, easy, and accessible and able to give a more reliable result. The study concluded that aside from the physical issues, it is important for users to have a fundamental understanding of this system. [14] Presented a biometric recognition: sensor characteristic and image. This study stated the importance of personal recognition and recommended that for better security, there is a need to interface the digital identity of a person to his body qualities. The paper also discusses the challenges faced with fingerprint scanner designs as the inability of dry or wet fingers in making good contact with sensor surface, electrostatic.

3. DESIGN METHODOLOGY

This section gives a detailed description of the proposed system design methodology and the steps taken to design the biometric implemented door. This project involves the uses access control in a secure data center facility using a regulated biometric door. This model is centered on two distinct biometric traits to gain access to the data center. The project design consists of hardware design, software design, and the choice of iris and fingerprint serves as a means to ensure additional security and reliability of the system.

3.1 Methods

The circuit diagram in Figure 2 consists of the following components: 20MHz Oscillator, 33pf capacitor, PIC18F452 microcontroller, LCD, Keypad, Motor driver, Fingerprint scanner, Iris

scanner (Irishield), 12V Battery, Power switch, Electrolytic capacitors, Variable Resistor, DC Motor, 4066 Bilateral Analog switch. The microcontroller used in this project is depicted in Figure 3, which is a PIC18F452 that possesses an enabling program C environment.

The PIC18F452 Microcontroller has a total of 5 ports where each port is 1byte (8bits) hence each port has eight (8) pins of microcontroller except for port E with three (3) pins. Also, the PIC18F452 has four inbuilt timers, which also serve as counters for setting count or in setting delays.

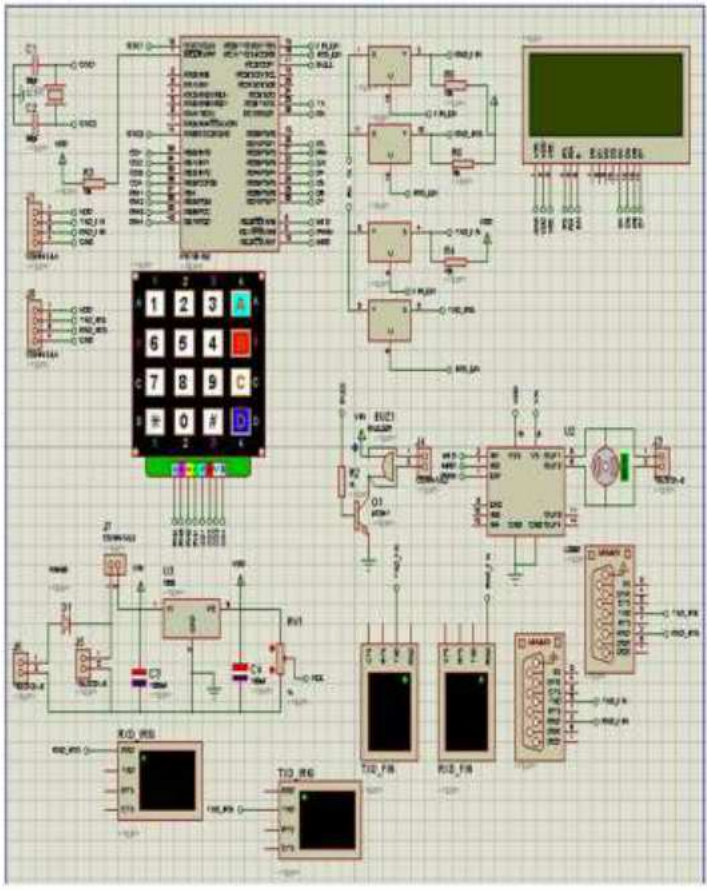

Figure 2 Schematic Circuit diagram of the system

3.1.1 The Fingerprint Sensor

The proposed system utilizes an SM360 fingerprint scanner which consists of an optical fingerprint sensor, high-performance DSP Processor and flashes with compelling features. Some of these features include fingerprint enrollment, image processing, extraction of the minutiae, template storage, and the verification of the fingerprint under the host command, which can be a personal computer. The SM360 fingerprint scanner was used to acquire individual fingerprint image for enrollment and authentication in ascertaining user's identity. The fingerprint sensor has a self-adaptive modification mechanism that is used to improve the quality of both dry and wet fingers.

This fingerprint scanner has a single USB supply voltage of (5.0V, ±5%) and a supply current of (<100mA, 120mA, <0.5mA) for scanning, idle and suspended mode respectively. The key advantages of SM360 scanner are its low cost, ease of use, compatible with USB 1.0, 1.1, and 2.0

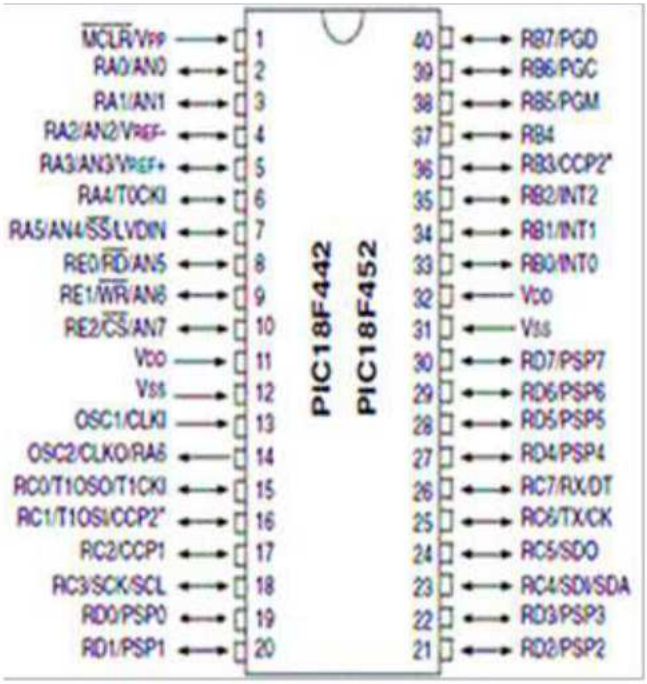

Figure 3 The PIC18F452 Microcontroller

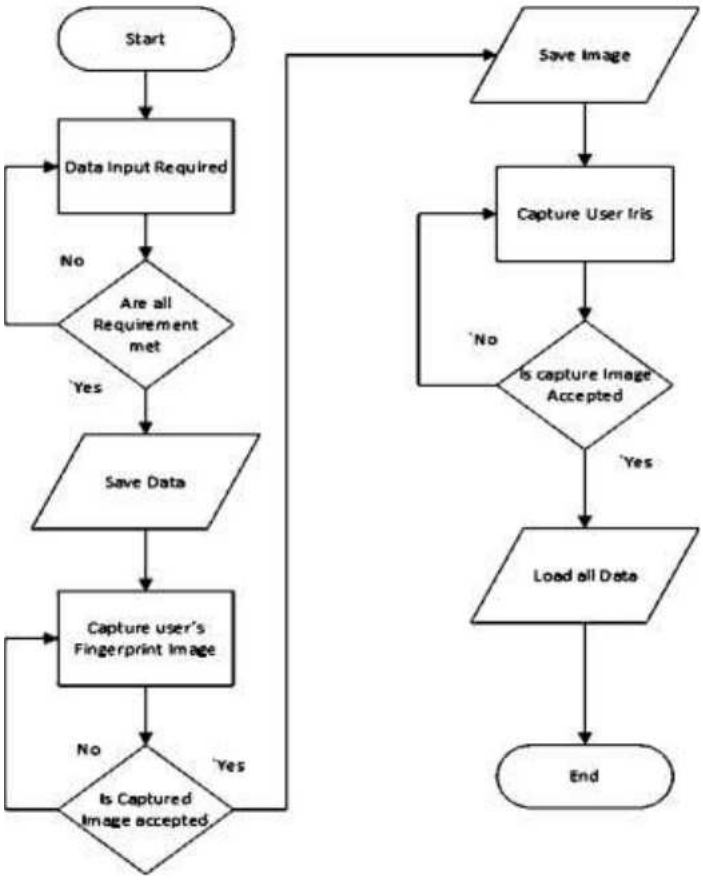

Figure 4 The Enrolment Flowchart

3.1.2 The Iris Scanner

The iris scanner used in this project was Irishield-UART MO2120 which is an auto-capture Iris Scanner with key functionalities for board capturing of the iris image, template generation,

verification and identification of an individual. It features superior iris matching and iris quality assessment algorithms to provide right quality image and also avoid false-positive while maximizing true-positive identification rates. The Irishield MO2120 supports various operating systems ranging from windows, Linux. The benefits of Irishield is the ability to secure data and communication and end to end biometric solution; it is portable, lightweight and utilizes low power consumption [18].

3.1.3 The LCD Display

For feedback on the operations of the model, an alphanumeric 20x4 Light Emitting Diode (LCD) is applied. It, however, offers an option of a 4bit wide bus to reduce the pin-count required to interface with a microcontroller. In total, seven (7) pins are used to interface the LCD to the microcontroller [20].

3.2 Software Design Specification

The embedded platform is programmed using program C language, and MYSQL was used for storing the biometric traits and was programmed using PHP. The GNU compiler was used in addition to an Eclipse Integrated Development Environment (IDE). The necessary plugin used was a CDT (c/CPP Development Tool) which utilize a complete functional C based on the Eclipse.

3.3 The Operational Principle of the System

The operation of the system involves two stages: the biometric enrollment stage and the identification or authentication stage. The model is designed to pattern a predefined sequence of steps logically, and it consists of five stages. However, there are five states involved in the operation of the system.

Idle state: At this state, the system is idle; that is not operational. The idle state is also known as the initial state of the system at startup; it can be changed from this state to another and back

Request state: At this state, a user presses the enter key on the keypad, and the fingerprint module is a startup where the fingerprint of the user is requested for, after which the iris sensor is a startup, and the users' iris scan is requested. In the event, only the fingerprint is read; without the iris for scanning the system returns to an idle state.

Biometric Registered state: This state occurs only once where the authorized personnel fingerprint and iris are scanned and stored in the database.

Biometric Authentication state: At this state, a user presses the enter key on the keypad, and the fingerprint module is a startup where the fingerprint of the user is requested for, after which the iris sensor is a startup, and the users' iris scan is requested. In the event, only the fingerprint is read; without the iris for scanning the system returns to an idle state.

Authenticated state: When the individual has been authenticated, access is granted, and the data center access control is opened.

3.3.1 The Enrollment Stage

Prior to an individual being identified or verified by the iris sensor and the fingerprint sensor, the enrolment process must first be completed. The objective of the enrollment process is to create a profile for the user, as shown in Figure 4. The enrollment process involves the following two steps, which are: Data input and print storage.

3.3.2 The Verification Stage

The flow diagram for the identification system is shown in Figure 5. This section gave the general implementation of the project, the testing of the system and analysis of results obtained.

System Testing: The system was tested at different stages of the design to determine if any errors. Both the software and hardware needed to be checked if it is performing its specified purpose to avoid waste of effort, time and cost.

Unit testing: Each program module is being tested independently. It is carried out to execute each statement at least once.

Integration Testing: Testing the program in combination with each other and the access control system itself.

Functional Testing: This type of test was carried out to check and ensure that the system was working according to its specified requirements.

Finger 6 shows the code use in programming the microcontroller interface. While Figure 7 shows the access control prototypes and Figure 8 shows the access control prototype's LCD.

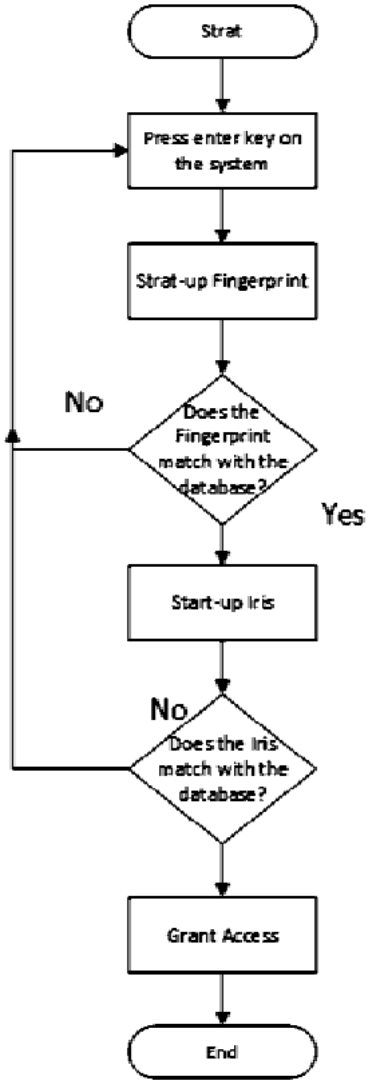

Figure 5 The Identification Flowchart

```
    for (;;){
        HandleSerial();
        CDC_Device_USBTask(&VirtualSerial_CDC_Interface);
        HID_Device_USBTask(&Digitizer_HID_Interface);
        USB_USBTask();
    }
}

/** Configures the board hardware and chip peripherals for the demo's functionality. */
void SetupHardware(void){
    int ret;

    /* Disable watchdog if enabled by bootloader/fuses */
    MCUSR &= ~(1 << WDRF);
    wdt_disable();

    /* Disable clock division */
    clock_prescale_set(clock_div_1);

    /* Backlight comes on early to suppress the full on blink. */
    BL_on(0);

    /* Set up USB */
    USB_Init();

    ret = EEPROM_Init();
    if(ret)
        dev_err("EEPROM error: %x\n", ret);

    ret = LCD_Init();
    if(ret)
        dev_err("LCD error: %x\n", ret);

    _delay_ms(100);

    ret = Digitizer_Init();
    if(ret)
        dev_err("Digitizer error: %x\n", ret);

    DDRC  |= PIN_PD;  // Powerdown
    PORTC |= PIN_PD;  // High for normal operation
    DDRB  |= PIN_PDO; // Powerdown outputs
    PORTB |= PIN_PDO; // High for normal operation

    /* Now we can turn on BL */
    BL_on(128);

    /* Init the LEDs now to show that the hardware init has gone ok */
    LEDs_Init();
```

Figure 6 Interfacing the Microcontroller

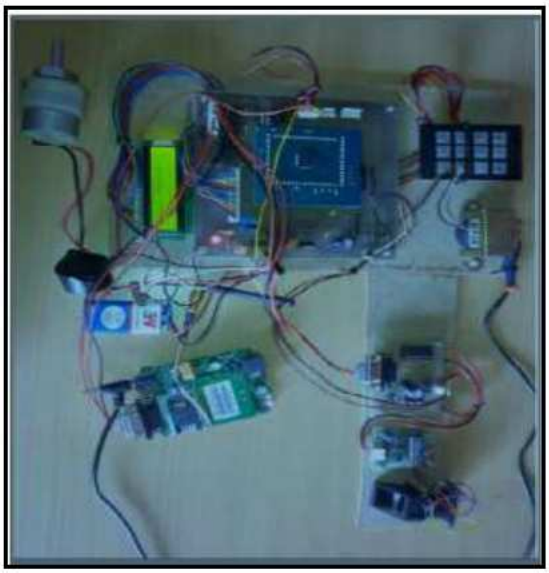

Figure 7 Access Control Prototype

Figure 8 Access Control Prototype's LCD

4. RESULTS AND DISCUSSION

When power is supplied to the system, it first displays on the LCD, as shown in Figure 8. The LCD shows the prompt to scan the fingerprint and iris. The LCD is connected to the 4x4 Matrix keypad and acts as an input and output device respectively, while the keypad is an input device.

The input of the keypad is connected to the integrated circuit, while the output of the LCD is connected to the Integrated Circuit as shown in Figure 8. The opening of the door sends back EMF to the system causing it to restart continually and was rectified using a high capacitor at that point to feed the back EMF to that capacitor which discharge when the door is closing. The fingerprints are being stored in an IC with relatively large memory. In a conventional system, a database would have to be created to store prints and iris samples obtained from the sensors.

For the data acquisition, Figure 9 shows a sample of ten fingerprints extracted by the SM630 fingerprint sensor during the enrolment process. These fingerprints are converted into a series of digits and letters that are then stored in the database, in this case, the integrated circuit. There are two different modes for the target image being captured by the iris scanner. The classical still image indicates the iris image has decent quality while the distant video frame indicates that the image was captured on the move at a distance. Hence, while matching the iris would read an error if the image stored in the database is classical still image and during verification, a distance video frame image is scanned and vice versa. Finger 10 and Figure 11 show the matching Iris process and Iris image storage respectively.

Figure 9 Samples of Fingerprint

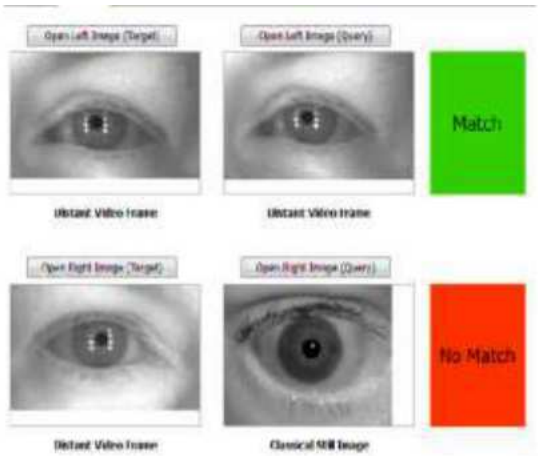

Figure 10 Matching Irises

Figure 11 Iris Image Storage

5. CONCLUSION

In conclusion, a bimodal biometric access control system for data centers has been designed and implementation using fingerprint and Iris as the traits. On testing the system, it was found to have met it purpose of access restrictions to non-authorized persons. While the persons whose trait match the traits on the biometric database of the system where granted accesses. The work has hereby-improved security to securing of information center that are very vital to all organizations.

REFERENCES

[1] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. IEEE security & privacy, 99(2), 33-42.

[2] Gomez-Barrero, M., Rathgeb, C., Li, G., Ramachandra, R., Galbally, J., & Busch, C. (2018). Multi-biometric template protection based on bloom filters. Information Fusion, 42, 37-50.

[3] Sarier, N. D. (2018). Multimodal biometric Identity Based Encryption. Future Generation Computer Systems, 80, 112-125.

[4] Meenakshi, V. S., & Padmavathi, G. (2010). Security analysis of password hardened multimodal biometric fuzzy vault with combined feature points extracted from fingerprint, iris and retina for high security applications. Procedia Computer Science, 2, 195-206.

[5] K. O. Okokpujie, M. Odusami, E. Noma-Osaghae, O. Abayomi-Alli, and E. Oluwawemimo, "A BIMODAL BIOMETRIC BANK VAULT ACCESS CONTROL SYSTEM," International Journal of Mechanical Engineering and Technology (IJMET), vol. 9, pp. 596-607, 2018..

[6] Berry, J., & Stoney, D. A. (2001). The history and development of fingerprinting. Advances in fingerprint Technology, 2, 13-52.

[7] K. O. Okokpujie, E. Noma-Osaghae, O. J. Okesola, S. N. John, and O. Robert, "Design and implementation of a student attendance system using iris biometric recognition," in 2017 International Conference on Computational Science and Computational Intelligence (CSCI), 2017, pp. 563-567.

[8] K. Okokpujie, E. Noma-Osaghae, O. Okesola, O. Omoruyi, C. Okereke, S. John, et al., "Fingerprint Biometric Authentication Based Point of Sale Terminal," in International Conference on Information Science and Applications, 2018, pp. 229-237.

[9] K. Okokpujie, E. Noma-Osaghae, O. Okesola, O. Omoruyi, C. Okereke, S. John, et al., "Integration of Iris Biometrics in Automated Teller Machines for Enhanced User Authentication," in International Conference on Information Science and Applications, 2018, pp. 219-228.

[10] Lourde, M., & Khosla, D. (2010). Fingerprint Identification in Biometric Security Systems. International Journal of Computer and Electrical Engineering, 2(5), 852.

[11] Boles, W. W., & Boashash, B. (1998). A human identification technique using images of the iris and wavelet transform. IEEE transactions on signal processing, 46(4), 1185-1188.

[12] Kak, N., Gupta, R., & Mahajan, S. (2010). Iris Recognition System. (IJACSA) International Journal of Advanced Computer Science and Applications. 1(1), 34-40.

[13] Patrick, A. S. (2004). Usability and acceptability of biometric security systems. In Financial Cryptography (p. 105).

[14] Prabhakar, S., Ivanisov, A., & Jain, A. (2011). Biometric recognition: Sensor characteristics and image quality. IEEE Instrumentation & Measurement Magazine, 14(3).

[15] Ziauddin, S., & Dailey, M. N. (2010). Robust iris verification for key management. Pattern Recognition Letters, 31(9), 926-935.

[16] Liu, E., Liang, J., Pang, L., Xie, M., & Tian, J. (2010). Minutiae and modified biocode fusion for fingerprint-based key generation. Journal of Network and Computer Applications, 33(3), 221-235.

[17] Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods. In Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium (pp. 184-193). IEEE.

[18] Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2007). Handbook of biometrics. Springer Science & Business Media.

[19] Subban, R., & Mankame, D. P. (2013). A study of biometric approach using fingerprint recognition. Lecture notes on software engineering, 1(2), 209

[20] Nasrin, A. Vidya, A. and Rani, H. (2016). Fingerprint Security Systems for banks. International Research Journal of Engineering and Technology (IRJET). 3(4), 1907-1911.

[21] Benson, T., Akella, A., & Maltz, D. A. (2010, November). Network traffic characteristics of data centers in the wild. In Proceedings of the 10th ACM SIGCOMM conference on Internet measurement (pp. 267-280)