BIOMETRIC EXAMHALL AUTHENTICATION

Rajesh N B[1], Subhiksha R[2], Oormila T S[3]

[1]Assistant Professor, Electrical and Electronics Engineering Velammal College of Engineering and Technology Viraganoor, Madurai, Tamil Nadu.

[2, 3]Student, Electrical and Electronics Engineering Velammal College of Engineering and Technology Viraganoor, Madurai, Tamil Nadu.

---***---

Abstract*-Impersonation in exam halls is increasing day by day. This is due to careless and time-consuming traditional candidate checking and authentication system in exam halls. This project is designed to reduce impersonation in exam hall by verifying biometric features of the candidate. Our system consists of fingerprint scanner connected to arduino and iris and palm vein data stored in mat lab database. The system is designed to pass only users by verifying their fingerprint, iris and palm vein and block non verified users. The fingerprint system was designed to scan the fingerprint and ID number which were properly saved into the database of the system and confirm the eligibility of candidate for examination. Automated iris recognition is provided for the verification and identification of people as iris is highly distinctive to an individual. The first image acquisition is processed and concerned with localizing the iris from a captured image. Then it is matched with candidate data base entries. Also, the contactless palm vein authentication technology used here captures an infrared ray image of the user's palm and the sensor can capture the palm image regardless of the position and movement of the palm. The matlab program then matches the translated vein pattern with the recorded pattern, while taking a pattern matching method to determine the position and orientation of the palm. If the details are authorized, the microcontroller now sends a signal to a motor driver. The motor driver now operates a motor to open a gate. It ensures only authorized users are allowed to enter the examination section and unauthorized users are not allowed to enter without any human intervention.*

Key Words: **Matlab, impersonation, iris, palm vein technology, Arduino.**

1. INTRODUCTION

Recognition of person based on biometric feature is an emerging phenomenon in our society. In the exam hall, authentication has always been a major challenge and verification of the authentic candidate is not an easy task and it consumes a lot of time and process. Traditional systems to verify a person's identity are based on knowledge (secret code) or possession (ID card), however codes can be forgotten or overheard and ID cards can be lost or stolen giving impostors the possibility to pass the identity test. The use of features inseparable form of person's body significantly decreases the possibility of fraud. Biometrics acts as a source for identifying a human being. This is used for authentication and identification purposes. In order to overcome the limitations of unimodal biometric system multimodal biometrics came into existence. It combines two or more biometric data recognition results such as a combination of a subject's fingerprint, palm and iris that increases the reliability of personal identification system that discriminates the approved and the fraudulent. Besides improving the accuracy, Multi-biometric systems are being progressively establish in many large-scale biometric applications because they have several advantages such as lower error rates and larger population coverage compared to uni-biometric systems. In this paper multimodal fusion of iris and palm vein images along with fingerprint sensor is proposed. Fingerprint based authentication is one of the beneficial biometric technique and are easily accessible, recognition requires minimal efforts on the part of the users, it does not capture information other than strictly necessary. Automated iris detection is yet another option for human identification and non-invasive verification. Interestingly, the spatial patterns of the human iris are highly distinctive to an individual. Among these, touch less palm vein authentication technology is integrated because of its high precision that comparing the vascular pattern under the skin, which are unique to each individual. The system is designed to pass only candidates validate by their biometric verification and block non-validate users.

2. RELATED WORK

The application of biometric technology related to impersonation has been used by Federal Bureau of Investigation (FBI) in the 1960s. According to research on biometric methods has gained renewed attention in recent years brought on by an increase in security concern. A more secured and accurate biometric based model is needed for implementation. Systems like sensing the fingerprints, iris, face and palm of the candidate who logged in for the exam has been separately done by the researchers. These things are the unique features of all humans and hence can detect the unauthenticated candidate easily. Some of such devices used in biometric system are

2.1. FINGER PRINT (PAD):

The presentation attack detection system acquires fingerprint image of a person within short wave infrared (SWIR) spectrum to determine the security that any person could eventually fabricate or using gummy finger or face mask to impersonate someone else. To tackle it, analysis of the bona-fide properties below the skin within SWIR spectrum is needed to be performed.

2.2. FINGERPRINT SENSOR WITH PIC18F4520:

The system operates by having each student's finger is scanned while the system cross check the fingerprint database that was captured during registration to verify if the scanned fingerprint is valid. This proposed system has matching tendency of 25% of the threshold value set of the operation.

2.3. CONVOLUTION NEURAL NETWORK:

A bi-modular biometric acknowledgment framework is recommended to rank-based combination calculation Bio Maximum Inverse Rank (BMIR) for recognizing IITD iris databases and CASIA datasets for palm print and unique mark are utilized for investigation with existing multi modular frameworks. Iris recognition components are more harmful and cause discomfort to human as they have to keep their eyes close to the illumination of the machine for accurate scanning.

2.4. RASPBERRYPI:

Raspberry Pi's blend with the cloud has contributed to a trend-setting period. Internet-of-things (IoT), or machine-to-machine (M2 M) or machine-to-human (M2H) communication. The biometric characteristics are transmitted to a remote location via an unsecured path, updated AES-256 is applied to ensure a safe transmission.

2.5. PALMVEIN SCANNER:

Palm vein authentication has a high level of authentication accuracy due to the uniqueness and complexity of vein pattern also it is difficult to forge. The system is contactless & hygienic for use in public areas. This scanner offers high cost and the information should always be encrypted. The images made during the control shouldn't be saved.

3. METHODOLOGY

3.1. BIOMETRIC EXAM HALL AUTHENTICATION USING ARDUINO:

This project is to develop biometric based exam hall authentication systems that assist in the elimination of examination impersonation. Our system consists of a fingerprint sensor connected to arduino microcontroller circuit. In registration mode, the system allows to register up to 120 users and save their identity with respective id number. In addition to that our project includes automatic iris recognition and palm vein technology. The biomedical literature indicates that irises are as distinct as retinal blood vessel signatures or patterns. Therefore prior to performing iris pattern matching, it is important to localize that portion of the acquired image that corresponds to the iris. The knowledge about the veins is difficult to replicate because the veins are internal to the human body. At last the fingerprint, iris and palm image is fused to a single image and determine the characteristics value for the three. After obtaining the values the matlab checks out whether the values are same. If same, it will display output as authenticated otherwise it displays unauthenticated. Also, another check-in is there to enter the hall that is the fingerprint sensor connected to arduino. It will check the candidate's fingerprint with their respective ID and motor will open the door if the candidate is authenticated otherwise buzzer will sounds on.

The component for this system comprises of hardware and software. They are as follows:

3.2. HARDWARE REQUIREMENTS

3.2.1. POWER SUPPLY:

The 9-volt battery is a popular battery size that was developed for early transistor radios, consisting mainly of alkaline batteries made of six individual 1.5 V LR61 cells in a wrapper.

3.2.2. DC MOTOR:

A DC motor is one of a class of rotary electric motors which converts electrical direct current into mechanical energy. The most common forms depend on magnetic-field forces. Here, the arduino output is fed into a motor, which in turn drives and then opens and closes the door.

3.2.3. ARDUINO:

The Arduino Uno variant of the Arduino family is the most growing. The Arduino Uno is an ATmega328-based micro controller board with 14 digital input / output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB link, a power jack, an ICSP header, and a reset button. The Arduino Uno is great choice for beginners. It contains everything you need to support the micro controller; simply attach it to a device with a USB cable, or power it to get going with an AC-to-DC adapter or battery.

3.2.4. FINGERPRINTSENSOR:

The basic function of fingerprint scanner is to get an image of a person's fingerprint and find a match for this print in the database. The capacitance scanner is better, because the images are more reliable and precise.

3.2.5. RELAY:

It is a relay style single pole double throw (SPDT) with 5 pins in a box type cube and rated to operate at 5VDC.Load Current Max.: 7Amps 250V AC or 12Amps 24V DC. Coil Resistance: 65-75 Ohms. The following block diagram represents the hardware components:

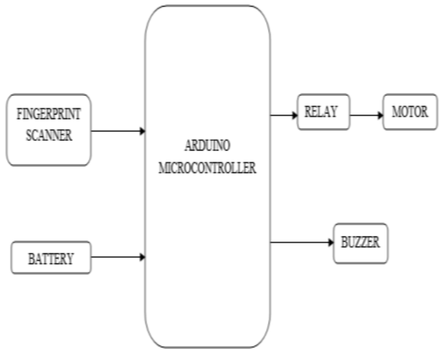


Fig: 3.2.5.1. Hardware development

3.3. SOFTWARE REQUIREMENTS

3.3.1. ARDUINO IDE:

Arduino is an open-source company of hardware and software computers. The development boards are known as Arduino Modules, which are open-source prototyping platforms. The simplified microcontroller board comes in a variety of development board packages. The most common programming approach is to use the Arduino IDE, which utilizes the C programming language. It gives you access to a massive Arduino Library. Once it's been opened, it opens into a blank sketch where we can start programming immediately. First, we should configure the board and port settings to allow us to upload code. Connect Arduino board to the PC via USB cable.

3.3.2. MATLAB:

MATLAB® is a high-performance language for technical computing. It integrates computation, visualization, and programming into an easy-to-use environment where familiar mathematical notation expresses problems and solutions. MATLAB is an interactive system whose basic element of data is an array which needs no dimensioning. This allows you to solve many technical computing problems in a fraction of the time it would take to write a program in a scalar non-interactive language like C or FORTRAN, particularly those with matrix and vector formulations.

The following is the block diagram about the software requirements of the system:

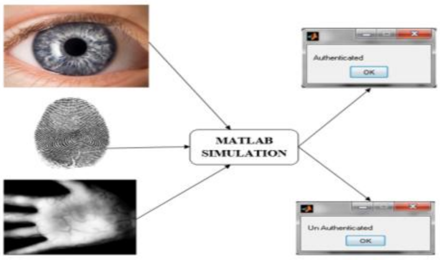


Fig: 3.3.2.1. Software development

4. PROPOSED SYSTEM

Biometric based exam hall authentication system helps to eliminate the unauthenticated candidate in the exam hall with the help of fingerprint sensor and matlab simulation with the database registered before. The overall system can be viewed in three stages. They are,

4.1. PRIMARY UNIT:

4.1.1. SENSING:

The first unit is sensing unit. Here we use fingerprint sensor connected to arduino microcontroller circuit. It will check the candidate fingerprint with their respective I'd which was registered before.

4.1.2. IMAGE ACQUISTION:

In this step, the images of palm-vein, fingerprint and iris are acquired by the matlab simulation. The images are converted to the round off size of 256*256.

4.2. PROCESSING UNIT:

It is the technique in which the input data is obtained as image by the arduino in hardware session and as matrix form in mablab process. In arduino adafruit fingerprint library is used.

This step consists of

4.2.1. ENROLLMENT PROCESS:

To register a fingerprint, the enroll(id) is called in arduino program. The ID passed is passed to link the scanned fingerprint also each fingerprint has an unique ID number. If the scanner is able to read the fingerprint, it will ask to remove and then replace the same finger on the scanner. This happens because granting access of the matching fingerprint.

4.2.2. GRAY SCALE CONVERSION:

The image is converted to gray scale because OpenCV functions tend to work on the gray scale image representing vectors, matrices, images and linear algebra functions in matlab. Grayscale images are also called monochromatic, denoting the absence of any chromatic variation. The resize level of the image is converted to gray scale image and then to matrix. From the matrix it checks the contrast, correlation, entropy, homogeneity and energy levels of the three images. These characteristics are essential to describe the quality of the image.

4.2.3. SUPPLEMENTARY PROCESS:

The gray scale images are subjected to fusion process in matlab. Multimodal biometrics can be accomplished by fusion of two or more images, in which the resulting fused image is secured more. Fusion at feature extraction level generates a homogeneous template for fingerprint, iris and palm vein features. The feature extraction of three biometric traits fused using feature level fusion and encrypted using RSA and stored in a database for desired authentication and verification. The newly captured biometric traits of the individual are compared against the stored data is used to determine the user identity.

4.3. FINAL UNIT:

The last step is to detect the matching of the fingerprint which is sensed by the sensor at present with the respective Id's by the arduino. Also the final encrypted information is then stored in the database and decrypted image is matched with the current query in matlab simulation. The verification module for the current query template to identify an individual for authorization.

Biometric exam hall authentication technique implements the flow of sequential process in matlab.

They are as follows

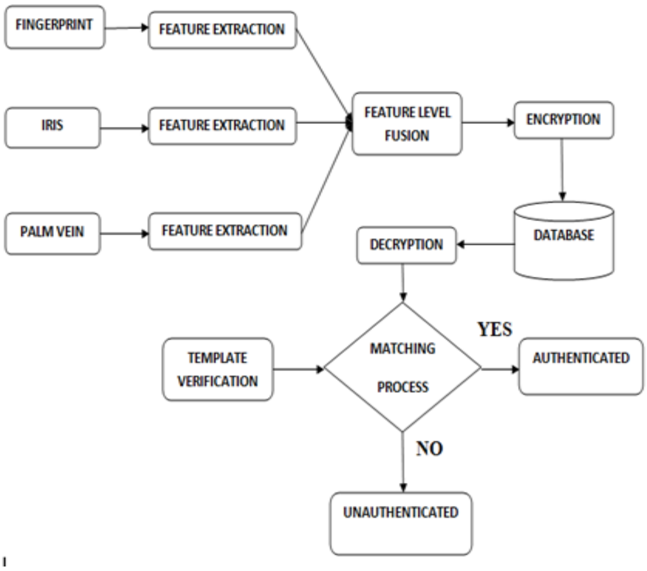


Fig- 4.3.1. Block diagram of the matlab processing

5. EXPERIMENTAL RESULTS

The figure shows the final prototype of BIOMETRIC EXAMHALL AUTHENTICATION system. It consists of Arduino placed on board with fingerprint sensor placed along with motor, relay and buzzer. It is cost effective and beneficial.

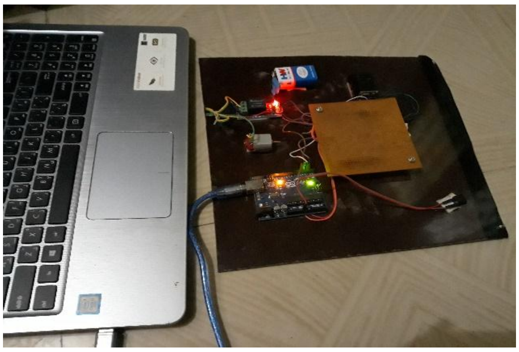
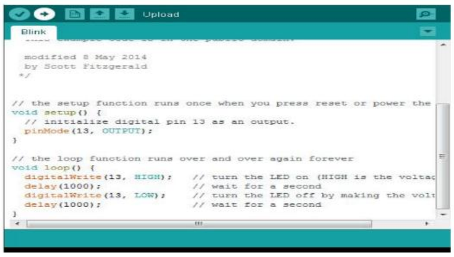


Fig: 5.1. Prototype model

5.1. CODE COMPILATION



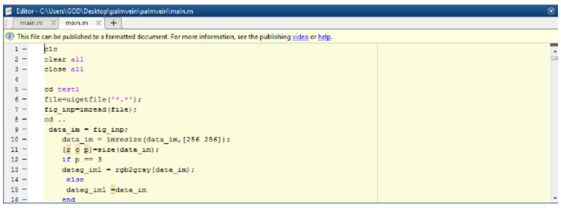
```
  modified 8 May 2014
  by Scott Fitzgerald
 */


// the setup function runs once when you press reset or power the
void setup() {
  // initialize digital pin 13 as an output.
  pinMode(13, OUTPUT);
}

// the loop function runs over and over again forever
void loop() {
  digitalWrite(13, HIGH);   // turn the LED on (HIGH is the voltag
  delay(1000);              // wait for a second
  digitalWrite(13, LOW);    // turn the LED off by making the volt
  delay(1000);              // wait for a second
}
```

Fig -5.1.1. Code compilation

The code compilation is done using Arduino 1.8.8-Windows compiler and output is converted into microcontroller readable language and fused into microcontroller.

5.2. SIMULATION

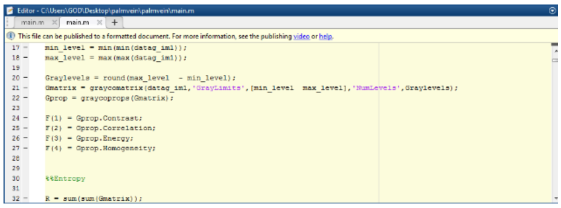
The simulation is made to run using Matlab software.



This file can be published to a formatted document. For more information, see the publishing video or help.

```
clc
clear all
close all

cd test1
file=uigetfile('*.*');
fig_inp=imread(file);
cd ..
 data_im = fig_inp;
    data_im = imresize(data_im,[256 256]);
    [r c p]=size(data_im);
    if p == 3
    datag_im1 = rgb2gray(data_im);
     else
     datag_im1 =data_im
    end
```

Fig: 5.2.1. Gray image conversion



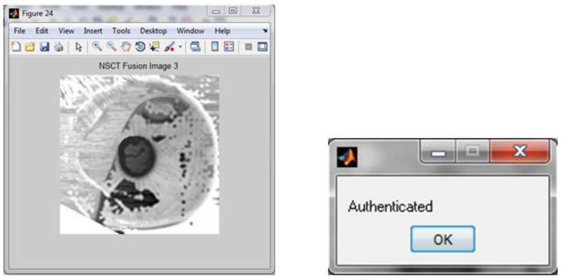
This file can be published to a formatted document. For more information, see the publishing video or help.

```
min_level = min(min(datag_im1));
max_level = max(max(datag_im1));

Graylevels = round(max_level  - min_level);
Gmatrix = graycomatrix(datag_im1,'GrayLimits',[min_level  max_level],'NumLevels',Graylevels);
Gprop = graycoprops(Gmatrix);

F(1) = Gprop.Contrast;
F(2) = Gprop.Correlation;
F(3) = Gprop.Energy;
F(4) = Gprop.Homogeneity;


%%Entropy

R = sum(sum(Gmatrix));
```

Fig: 5.2.2. Gray scale matrix

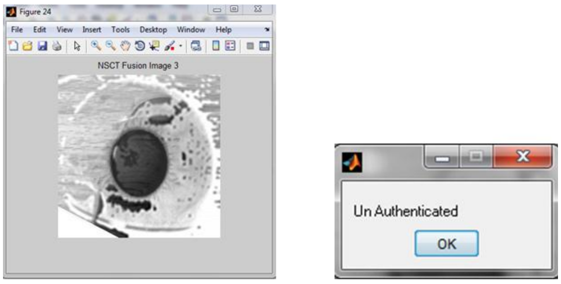
AUTHENTICATION OF IRIS

The extracted iris image is compared with image stored in database and result is shown if it is authenticated or not authenticated.



Authenticated

Fig: 5.2.3. Fusion image of authenticated

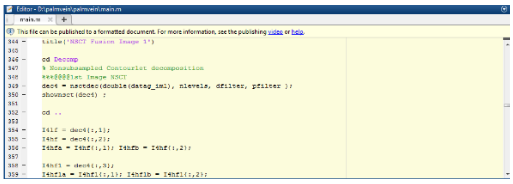


Un Authenticated

Fig: 5.2.4. Fusion image of unauthenticated

5.3. FUSION PROCESS:

The iris and palmvein database are fused together into single image through fusion.



This file can be published to a formatted document. For more information, see the publishing video or help.

```
title('NSCT Fusion Image 1')

cd Decomp
% Nonsubsampled Contourlet decomposition
%%%@@@@1st Image NSCT
dec4 = nsctdec(double(datag_im1), nlevels, dfilter, pfilter );
shownsct(dec4) ;

cd ..

I4lf = dec4{:,1};
I4hf = dec4{:,2};
I4hfa = I4hf{:,1}; I4hfb = I4hf{:,2};

I4hf1 = dec4{:,3};
I4hf1a = I4hf1{:,1}; I4hf1b = I4hf1{:,2};
```

Fig: 5.3.1 Fusion process using matlab

6. FUTURE SCOPE

However, there are some limitations in the proposed solution which can be addressed in the future implementations. Hence, the following features are recommended to be incorporated in the future versions.

- Integration of all these scanner units and making it as a kit fixed at doorstep of all exam halls.
- complexity of design can be reduced and made compact.
- Fusing information extracted from the red, green and blue components of an image might produce a better fused feature vectors which contains richer information than that in gray scale image.

7. CONCLUSION

The advent of fast-growing technologies is making users have hi

gh-security systems with options for electronic identification. The identification based on biometric or fingerprint authentication is the efficient and reliable solution for stringent protection. Microcontroller-based review hall authentication device based on fingerprint. This system is more accurate and faster than previous feature-extraction Iris technology is expanding in real time applications of security measures since it is stable, secure and authentic. Authentication of the palm vein is one of the most accurate of authentications. This paper represents the authentication system for contactless palm veins that takes the design of the blood vessels as a personal identification. By verifying all these parameters, if user is valid then allows attending the exam else not allowed.

8. REFERENCES

[1]. Ruben Tolosana, Marta Gomez-Barrero, Christoph Busch, Javier Ortega-Garcia, Fellow, "**Biometric Presentation Attack Detection: Beyond the Visible Spectrum**", IEEE Transactions on Information Forensics and Security, 10.11.19/TIFS.2019.2934867 (**Main Paper**).

[2].J. Galbally, S. Marcel, and J. Fierrez, "**Biometric antispoofing methods: A survey in face recognition**," IEEE Access, vol. 2, pp. 1530–1552, 2014.

[3].R.Tolosana, R. Vera-Rodriguez et al., s"**Exploring recurrent neural networks for on-line handwritten signature biometrics**," IEEE Access, pp.1– 11, 2018.

[4].A.Rattani, W.Scheirer, and A. Ross, "**Open set fingerprint spoof detection across novel fabrication materials**," IEEE Trans. on Information Forensics and Security, vol. 10, no. 11, pp. 2447–2460, 2015.

[5]. D. Menotti, G. Chiachia et al., "**Deep representations for iris, face, and fingerprint spoofing detection**," IEEE Trans. on Information Forensics and Security, vol. 10, no. 4, pp. 864–879, 2015.

[6].A. Toosi, A. Bottino, S. Cumani, P. Negri, and P. L. Sottile, "**Feature fusion for fingerprint liveness detection: a comparative study**," IEEE Access, vol. 5, pp. 23 695–23 709, 2017.

[7].F. Nicolo and N. A. Schmid, "**Long range cross-spectral face recognition: matching SWIR against visible light images**," IEEE Trans. on Information Forensics and Security, vol. 7, no. 6, pp. 1717–1726, 2012.

[8].A. Rattani and A. Ross, "**Automatic adaptation of fingerprint liveness detector to new spoof materials**," in Proc. IEEE International Joint Conference on Biometrics, 2014, pp. 1–8.

[9].Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, and C. V. Jawahar, "**Blind Authentication: A Secure Crypto-Biometric Verification Protocol**," IEEE Transactions on Information forensics and security, vol. 5, no. 2, June 2010, pp.225-268.

[10].Ajay Kumar, Vivek Kanhangad, and David Zhang, "**A New Framework for Adaptive Multimodal Biometrics Management**," IEEE Transactions on Information forensics and security, vol. 5, no. 1, March 2010p, p. 92-102.

[11].Abhishek Nagar, Karthik Nandakumar, Anil K. Jain, and Dekun Hu, "**Multibiometric Cryptosystems Based on Feature-Level Fusion,**" IEEE Transactions on Information forensics and security, vol. 7, no. 1, February 2012, pp. 255–268.

[12].Koen Simoens, Julien Bringer, Herve Chabanne, and Stefaan Seys, " **A Framework for Analyzing Template Security and Privacy in Biometric Authentication Systems**," IEEE Transactions on Information forensics and security, vol. 7, no. 109 – 116 2, April 2012, pp. 833-841.

[13].Q. Zhang, Y. Yin, D. Zhan and J. Peng, "**A Novel Serial Multimodal Biometrics Framework Based on Semisupervised Learning Techniques**," in IEEE Trans. on Info. Forensic and Sec., vol. 9, no. 10, pp. 1681-1694, Oct. 2014.

[14]. B. E. Manjunathswamy, J. Thriveni, and K. R. Venugopal, "**Bimodal biometric verification mechanism using fingerprint and face images(BBVMFF)**," in Proc. IEEE 10th Int. Conf. Ind. Inf. Syst. (ICIIS), pp. 372-377, 2015.

[15].Y. Lin, E. Y. Du, Z. Zhou, and N. L. Thomas, "**An efficient parallel approach for Sclera vein recognition**," IEEE Trans. Inf. Forensics Security, vol. 9, no. 2, pp. 147–157, Feb. 2014.