Biometric Authentication System

Mr. Ramveer Singh Yadav[1] Vikash Tirkey[2] Jyoti[3] Ashish Kumar[4] Bharti Saini[5]
[1]Guide
[1,2,3,4,5]BBDIT,Ghaziabad, India

Abstract— This paper is to develop biometric fingerprint Based Examination Validation systems that help in the removal of examination enactment. People sitting for examinations for others who collect the result at the end. With the implementation of biometric fingerprint, this will be removed as fingerprint identification will also be employed during collection of results and certificates. This target can be mainly breakdown into image pre-processing, feature extraction and feature match. For each sub-task, some classical and up-to-date methods in books are analysed. Based on the research, an integrated solution for fingerprint recognition is developed for affirmation.

General Terms: Authorization, Authentication, Design, Elimination

Key words: Malpractices, Impersonation, Biometric

I. Introduction

Authorization has always been a big challenge in all types of examinations. Verification of the authentic candidate is not straight forward task, and also it takes a lot of time and process. This led to the design of Fingerprint biometric based examination authorization system that is designed to allow only candidate verified by their fingerprint scan and block non verified candidates.

On the era of 19th century, formal written examinations became common in universities, schools, and other educational institutions. Examinations were also increasingly employed for the selection of recruits to the government service, and the professions, and to designation in industry and to begin. Over the years, standard testing has been the most common method, yet the validity and credibility of the expanded range of contemporary assessment techniques have been called into question.

II. Significance of the Study

With the rising rate of exam malpractices in the educational examination sectors, the Universities management have to infuse a tight security means to make sure that these practices of exam impersonators stops. The practices of these examination impersonators have seen the educational sector suffer some serious form fraud ranging from registered student, to examination supervisor. So it best for the educational system to set up new planning and some certain security means to stop this aspect of fraud in the educational system.

III. Biometric Authentication System

This system uses a fingerprint scanning system, this will help to make sure that only registered candidate during registration with their finger prints are allowed into the examination room. The system would provide in the area of prohibiting any practices of corruption in the educational system among students, and student to teachers. Hard work would be appreciated as every registered student knows he/she is going to write the exam by him or herself. The impersonation which has been destroying the educational system there by encouraging laziness among students would be removed and standard of student educational performance would be appreciated. This system was designed by using Protuse and C Programming Language, embedded C and also all necessary method of data collection reachable to make sure the system meet up to acceptable norms has been put into consideration.

IV. Analysis

Although it was not an easy task, to prove that the biometric authentication system is working according to how the real systems work. This was proved by carry out the project in simulation but its working according to the way it is intended to work. By simulating this project one will see the display on the Liquid Crystal Display(LCD), the system writing the name of the project “Biometric Fingerprint Authorization ”, few seconds later it will display the following message: “PLACE YOUR FINGER” this is just to tell the candidate to be authorizes to place her/his finger on the fingerprint scanner for it to be able to scan his/her fingerprints, after that if the student is authorized then the following message will be displayed: “ENTER YOUR PASSWORD”, this is a password that every registered student got during registration process.

V. Objective of Biometric Authentication System

- To make a system that is able of tracking impersonators in the examination system using the methods of finger print biometrics.
- To decrease the rate of fraud in the educational system and appraise the rate of self-confidence on students.
- To show the possibility of computer technology in the fulfilment of human needs and also implement strict security measures that makes sure unregistered candidate do not write exams for other registered candidates.

VI. The Structure of Biometric Authentication System

A Biometric Authentication system has the following components-

A. *Fingerprint Scanner*

This is a fingerprint scanner device with TTL UART interface for straight connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. Which can save the finger print data in the device and can be configured in 1:1 or 1: N mode for recognizing the candidate? The Fingerprint module can directly interface along with 3v3 or 5v Microcontroller. A level converter (MAX232) is necessary for interfacing with PC serial port.

Optical fingerprint sensor imaging involves capturing a digital picture of the print using visible light. This type of sensor is essence, a well-designed digital camera. The top layer of the sensor device, where the finger is placed, is called the touch surface. Below this layer is a light-emitting phosphor layer which illumines the surface of the finger. The light reflected from the finger goes through the phosphor layer to an array of solid state pixels which records visual pictures of the fingerprint.

Fig. : Fingerprint scanner

B. Microcontroller (ATmega328)

The selection of this type of microcontroller is induce by the number of ports and internal memory that the component possess, enough ports to connect all of the components of the project and the enough memory for buffering and store fingerprints scan samples for simulation purposes.

- High Performance, Low Power AVR 8-Bit Microcontroller
- Flash Program Memory: 32 Kbytes
- EEPROM Data Memory: 1 Kbytes
- SRAM Data Memory: 2 Kbytes
- I/O Pins: 23
- Timers: Two 8-bit / One 16-bit
- A/D Converter: 10-bit Six Channel
- PWM: Six Channels

Fig. : Microcontroller (ATmega328)

VII. OPERATION

This system need controlled direct current power supply to power the components and the power need to be controlled because, this components need stabilized state power supply and at the defined limit. When the system is powered on the bright green light is displayed on the screen display to show that the system is switched on, the few seconds later, the following message is displayed on the screen display: (“Fingerprint Biometric Authentication”) the name of the system, then one seconds later it will display for the user to put the finger on the scanner for the fingerprint scan to be recorded for authorization. The distinguishing is done by the microcontroller, distinguishing the recently recorded with the one in the database stored after registration step, if there is a match found then the system will ask for a password and if the password is right then the microcontroller will send commands to the motor drive to open the door to the examination hall. If there is no match found between the fingerprints then the system will shows that access has denied, candidate not registered, it will never ask for password.

To conclude the operation, this system contain a fingerprint scanner connected to a microcontroller. The person needs to first scan his finger on the scanner. The microcontroller now checks the candidate fingerprint validity. If the fingerprint is authorized the microcontroller now sends a commands to a motor driver. The motor driver now runs to open a gate. This makes sure only authenticated candidate are allowed to enter the examination hall and unauthorized candidate are disallowed to enter.

VIII. RESULT

By using this Biometric Authentication System the design and implementation of identity authentication system based on Fingerprint Identification is designed, and finally, the problem at hand, which is candidates impersonation and corruption is tertian Education will be bring to an end and to show that anything can be grabbed using computer technology in this growing Information Technology and communication world . Prototyping phase of this project has been gained, with the following devices: Microcontroller , LCD display device (LM016L), regulated DC power supply, Keypad-phone, Virtual Terminal, X1 Crystal clocking, Variable Resistor, and Capacitors.

Controlled direct current power supply is used for alive the devices on the system and it has to be controlled to avoid too much power to damage the device and to be too low for it to be inadequate for the devices operation. Microcontroller, this is the main part of the whole system, it is there to provide the connection between devices, control the functions of every device connected on this system, it has timing equipment that must be synchronised with the crystal timing device to make sure accurate operation of the system. Keyboard, this device is used as a input device used by the candidate when they are putting down their password during authentication process. Screen display is used as the output device of the complete system because, every message that the system required to pass the information to the candidate, is display on system screen, starting from displaying the name of the system (Biometric Authentication System), asking the user to put their fingers (Place your finger), screening the results of the authentication (Enter the password or Access denied candidate not registered) and the final display if the user’s password is correct (Access granted). Variable resistor, this is to give brightness to the screen display. Crystal timing, this has the simple task, which is to provide timing to the system, clocking which is synchronised with the clock timer of the microcontroller. Virtual Port is used as input device as well to input the candidate number of the candidate when the system ask the candidate to place their finger, because there is no fingerprint scanned data on the system, so this device is used in the simulation phase.

IX. Conclusions

In this proposal a Biometric Fingerprint Model for Examination impersonation and Biometric Access is a better option for the use of ID card in verifying candidate identity. Experience has shown the loop holes of Identity cards in uniquely identifying individual candidate in the face of complicated Forgery technology. The originality in the use of fingerprint makes it a trust worthy access control technique. The fact that a candidate no longer needs to carry identification cards and other documents for identification explain the ease of use.

The Biometric Authentication system using fingerprints. The implemented minutiae extraction is much more precise and faster than our previous feature-extraction. In our proposed system precisely verifies the fingerprint is validated candidate or not. If valid candidate then it allow attending the exam else disallowed. In this experimental result shows the proposed method is good enough for all the authorization based application and also it reliable.

References

[1] www.scribd.com
[2] S.Chand & Co.Ltd"Microcntroller 8051 advanced" by Ramcharan Krishna.
[3] ATMEL 89S52 Data Sheets.
[4] T. M. e. al, Japan: Yokohama National University, 2002.