A

Project Report

On

***“Fingerprint based Exam Hall Authentication System”***

Submitted

to

**School of Applied Sciences**



by

**(16CSEG112)**

|  |  |  |
| --- | --- | --- |
| S. No. | Name | Roll No |
| 1 | Kriti Shahi | 1610991466 |
| 2 | Lokesh | 1610991482 |
| 3 | Malkeet Kaur | 1610991492 |
| 4 | Mannat Kaur | 1610991501 |

Under the supervision

Of

(Ms Garima Turan)

**ACKNOWLEDGEMENT**

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them.

We are highly indebted to Chitkara University for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

We would like to express our gratitude towards our parents and our IP project guide Ms. Garima Turan for their kind co-operation and encouragement which help us in completion of this project.

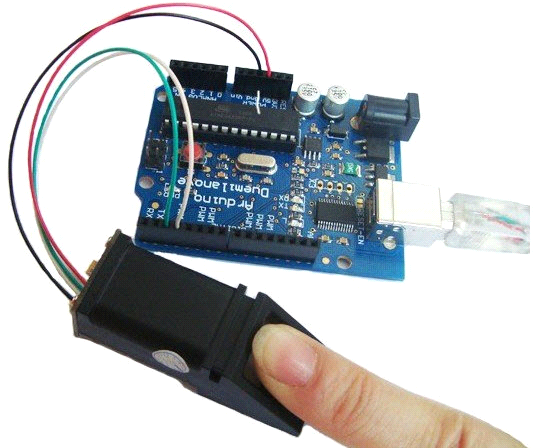
Our thanks and appreciations also goes to our mentor in developing the project and people who have willingly helped me out with their abilities.

**ABSTRACT**

Biometrics as a branch of industry, science and technology exists since about 20 years. Its size is about 1 billion Euros. Problems and questions related with automatic people recognition are attracting more and more scientists and technicians. Although many devices already exist or are being proposed, it is certain that biometrics is still in the early stages of its history.

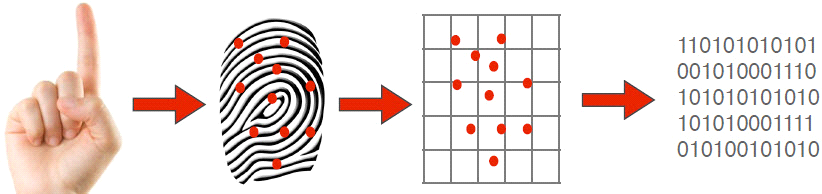
The main aim of FINGER PRINT BASED SECURITY SYSTEM project is to develop a security lock system based on fingerprint scanning. In this project we are using microcontroller for opening and closing lock so that only authorized person will access the security lock.

Finger print comparison is one of the tough task, mainly comparing latent finger prints like palm, foot prints will be most difficult part in finger print science.



**INTRODUCTION**

In today‘s regular life there are many problems of common companies and other security for home application and there are also important applications of automatic control in many applications, so we dedicate this project to this common man and other industries. Nowadays accurate personal identification is becoming more and more important. Currently fingerprint recognition is the most widely used technique for personal identification. Fingerprints are made up of locally parallel ridges with singular points, and they constitute a unique permanent universal pattern. These sensors exploit different techniques to acquire the image (pressure, electrical field, temperature…) and require a static (matrix sensor) or mobile finger position (sweeping mode sensor). In this project the fingerprint sensor sense the thumb impression of the corresponding person and that image will be compared with registered image, if the both images are unique, then the finger print device activates particular task like access control to a secured area, identification of the employee etc.



Fingerprint image is scanned by the fingerprint device. If the scanned image matches with the registered image then Microcontroller sends the authorized persons Id to the computer when the person enter and leave the examination hall.

The system is designed to pass only users verified by their fingerprint scan and block non-verified users. In the examination hall we are use the fingerprint verification system for verified the authorized user or not. If authorized user then it allow to the examination hall. Otherwise cannot be allowed.

It can store up to 265 finger prints on its own memory. It can be controlled through its serial port. You can add a fingerprint, Delete a fingerprint and identify the fingerprint. To add a fingerprint, just show the finger on the module and press the ADD key. Now the microcontroller will send the ADD command to the module and the module will add it into the memory. To delete the finger follow the same as above. To identify the finger, press the Identify button and if the finger matches then the Relay is complemented. Also the fingerprint ID is displayed over the LCD display.

**DEFINITION**

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity

**METHODOLOGY**

Fingerprint based examination hall authentication system consists of a fingerprint scanner connected to Arduino Uno R3. The **Arduino Uno R3** is a microcontroller board based on the ATmega328 ([datasheet](http://www.atmel.com/dyn/resources/prod_documents/doc8161.pdf)). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button

Functions of microcontroller

1. Reading various digital input signals from fingerprint sensor
2. Sending this data to LCD so that the person operating this project should understand the

status.

1. Sending the data to the computer using serial port. This data consist of the status of

valid or invalid access.

In registration mode, the system allows to register users and save their identity with respective id numbers in the system memory. After storage the person needs to first scan his finger on the scanner. The microcontroller now checks the persons fingerprint validity and displays the required message on the LCD display.

While storing the entry in database, scanner takes an image of these patterns and stores in its own memory. Then while performing search operation, it again takes pattern of fingerprint of that user who needs to gain access. This pattern is compared with all patterns previously stored in memory. In short it performs a task which is related to Digital image processing. It performs various iterations and executes matching algorithms and if it finds exact match then it gives out fingerprint ID number otherwise it gives out error signal.

**LITERATURE SURVEY**

1. Qijun Zhao proposed an adaptive pore model for fingerprint pore extraction. Sweat pores have been recently employed for automated fingerprint recognition, in which the pores are usually extracted by using a computationally expensive skeletonization method or a unitary scale isotropic pore model.

To accurately and robustly extract pores, they propose an adaptive anisotropic pore model, whose parameters are adjusted adaptively according to the fingerprint ridge direction and period. The fingerprint image is partitioned into blocks and a local pore model is determined for each block. With the local pore model, a matched filter is used to extract the pores within each block. Experiments on a high resolution (1200dpi) fingerprint dataset are performed and the results demonstrate that the proposed pore model and pore extraction method can locate pores more accurately and robustly in comparison with other state-of- the-art pore extractors.

2. Moheb R. proposed an approach to image extraction and accurate skin detection from web pages. As part of the proposed system, using Band Object control, they build a Tool bar named “Filter Tool Bar (FTB)” by modifying the Pavel Zolnikov implementation. In the proposed system, they introduce three new methods for extracting images from the web pages (after loading the web page by using the proposed FTB, before loading the web page physically from the local host, and before loading the web page from any server). These methods overcome the drawback of the regular expressions method for extracting images suggested by Ilan Assayag. The second part of the proposed system is concerned with the detection of the skin color regions of the extracted images. So, they studied two famous skin color detection techniques. The first technique is based on the RGB color space and the second technique is based on YUV and YIQ color spaces. They modified the second technique to overcome the failure of detecting complex images background by using the saturation parameter to obtain an accurate skin detection results. The performance evaluation of the efficiency of the proposed system in extracting images before and after loading the web page from local host or any server in terms of the number of extracted images is presented. Finally, the results of comparing the two skin detection techniques in terms of the number of pixels detected are presented.

**FUTURE SCOPE**

1. ***Authentication***

It is reasonable to expect, that in a relatively short time, all personal documents will contain some form of biometric data. Moreover, in time, we could expect that all such documents will no longer be needed, because, in every instance where this type of authentication would be necessary, biometric readers will be connected to the location via network. This would allow a comparison with stored data to be used in lieu of documentation.

1. ***Access and attendance control***

In the relatively near future, biometrics will certainly gain increased acceptance in all kinds of access and attendance control applications. We can expect to see biometrics used for these applications in homes, offices, computers, machines, devices, etc. There will be no need to carry keys, identity cards, personal documents, etc. Furthermore, this implementation of biometrics will add to the overall security solution: precluding the possibility of theft or unauthorized use of equipment/technologies. Biometric devices will offer new quality to security solutions, but not necessarily new market opportunities or potential.

1. ***Travel control***

For a variety of reasons, there is an increasing requirement to have people traveling via planes, ferries, and even trains to be individually registered, with interim checks at multiple locations. Today these requirements are being driven mostly by security concerns, visa regulations and other such reasons. And, because the amount of people traveling is already large and predicted to increase at significant rates, all organizations involved in the management and control of mass transportation industries are very interested in the rationalization and automation of necessary procedures. This is especially the case in International Civil Aviation Organization. The pressure caused by the growing number of passengers is surely one of the largest reasons for the introduction of biometric passports, visas and other controls/documents.

1. ***Financial and other transactions requiring authorization***. In applications having to do with money it is already apparent, that money in physical form (bank notes and coins) is being replaced more and more by virtual forms of financial transactions – digital transactions via data base entry. Today this happens in form of credit or bank cards, pocket electronic money, etc. Spreading of biometric authentication in the economic sector (i.e. banking and trade) will decrease the need for physical objects, such as cards – since virtual money can be directly connected to a person (or to the legal person). This will result in a significant change both in the behavior of people, but also in the abilities that governmental organizations will have in their surveillance of money movements (financial transactions).
2. ***Remote voting (authorization)***

Perhaps the most important change in the society will result from the creation of an entirely new market for biometric devices that I call remote authorization. The merging of existing and future networking developments with biometric solutions will allow people to have the opportunity to authorize a wide range of transactions (e.g. voting, purchasing, accessing, decision-making authorizations, etc.) via the network, from remote locations. No longer will they be required to personally present at a given location in order to authenticate a specific action. Indeed, this is a capability that is partially possible today.

**ADVANTAGES**

Biometric authentications systems are very desireable because of the following advantages. The most obvious advantage is that biometric data can’t get lost, stolen, duplicated or forgotten like keys or access cards. They also can’t be forgotten, compromised, shared, observed or guessed like passwords, secret codes or PINs. People also don’t have to change the data used for authentication every three months like we sometimes have to do with passwords. Therefore authentication systems using biometric data are more convenient to use. The most important advantage is that biometric authentication systems can increase the security of the system, if the accuracy is high, the hardware used can’t be cheated easily and if it is used together with other authentication methods. In addition to that biometric authentication systems reduce costs because it is possible to eliminate overheads resulting from password management. The reason for this is that people can’t forget their passwords anymore and so the queries at help desks become less. Besides reducing the mentioned overhead this also saves money because there are no more costs for distributing new passwords in a secure way.

The main reason for applying biometric solutions is security. This perspective is supported by politicians, spreading the message that biometric technologies can help in the fight against terrorism, help locate criminals, etc. This is not fundamentally wrong. Indeed, if automatic devices for identity recognition were more prevalent in locations such as airports, police stations and other areas that are sensitive or involve high concentrations of public activity, they would surely make the life of criminals and terrorists much more difficult. However, there are many reasons to believe that biometrics will change the life of people in near future mostly because its use will be much more convenient than other techniques in use today for individual identity authentication. This is already apparent today, especially in connection with applications such as physical and logical access control, transportation, and also in the financial industry.

**APPLICATIONS**

Biometric technology can be used for a great number of applications. Chances are, if security is involved, biometrics can help make operations, transactions and everyday life both safer and more convenient.

***Biometric Security***

As connectivity continues to spread across the globe, it is clear that old security methods are simply not strong enough to protect what’s most important. Thankfully, biometric technology is more accessible than ever before, ready to bring enhanced security and greater convenience

***Border Control and Airport Biometrics***

A key area of application for biometric technology is at the border. Anyone who’s traveled by air can tell you security checkpoints border crossings are some of the most frustrating places to have to move through. Thankfully, biometric technology is helping automate the process.

***Consumer and Residential Biometrics***

Recent innovations in mobility and connectivity have created a demand for biometrics in the homes and pockets of consumers. Smartphones with fingerprint sensors, apps that allow for facial and voice recognition, mobile wallets: these are the increasingly popular ways that consumers around the world are finding biometric in their lives.

***Financial Biometrics***

It can’t be overstated how much biometrics can benefit financial transactions. With recent implementations of mobile and online payments protected by biometrics it’s clear that the security and convenience are welcomed by the consumer when it comes to buying goods.

***Fingerprint Biometric Locks***

Biometric physical access control solutions are stronger authentication methods than keys, key cards and PINs for a simple reason: they’re what you are, not what you have. While a key can be lost or stolen by anyone.

***Biometrics in Healthcare***

Biometrics bring security and convenience wherever they’re deployed, but in some instances they also bring increased organization in the field of healthcare, this is particularly true. Doctors need access to health records which are the most valuable personal documents and they need to be accurate.

***Justice and Law Enforcement***

Biometric technology and law enforcement have a very long history, and many very important identity management innovations have sprouted from this beneficial relationship. Today, law enforcement biometrics are truly multimodal; fingerprint, face and voice recognition all play their own unique role in enhancing public safety and tracking down wanted persons.

Logical Access Control Biometrics Logical access control is a major area of application for biometric technology. When we say, “It’s time to kill the password,” this is the tech we’re talking about.

***Mobile Biometrics***

They incorporate either one or many biometric modalities for authentication or identification purposes, and take advantage of smartphones, tablets, other types of handhelds, wearable technology, and Internet of Things…

[***Other***](http://findbiometrics.com/applications/other-biometric-applications/)

As cyber threats continue to escalate and connectivity begins to proliferate all facets of life around the globe other biometric applications that are not listed in our showcase section rise to meet the demand. The following vendors and organizations are a perfect place to look for those in need of biometric technology outside the…

[***Physical Access Control***](http://findbiometrics.com/applications/physical-access-control/)

Biometric physical access control solutions are stronger authentication methods than keys, key cards and PINs for a simple reason: they’re what you are, not what you have. While a key can be lost or stolen and used by another person where as physical access is limited to a particular person.

**CONCLUSION**

Fingerprint is the cheapest, fastest, most convenient and most reliable way to identify someone. Fingerprint authentication has many advantages over traditional systems such as passwords. The greatest strength of Fingerprint recognition is its greatest liability. Today, fingerprint recognition technology is used for security purposes, to restrict access or to protect computers. As fingerprint recognition technology develops, it is expected that more affordable and more portable fingerprint recognition devices will become available, and finger-print recognition will be considered a safe and convenient personal identification system. Eventually, fingerprint recognition will be used to secure the safety and reliability of a variety of businesses in the industrial sector including the personal devices and financial industry.

Further development of biometric technologies will significantly change the world. These technologies can be surely not only used for making the life easier, but also for more perfect invigilation.

**REFERENCES**

1. <http://findbiometrics.com/applications/>
2. <http://webcache.googleusercontent.com/search?q=cache:http://nevonprojects.com/fingerprintbased-exam-hall-authentication-project/&gws_rd=cr&ei=oz24WPvpG4qD8gX0w4HoBQ>
3. <https://www.optel.eu/uploads/PDF%20ENG/future%20of%20biometrics.pdf>