PASSPORT IDENTIFICATION AND VERIFICATION THROUGH FINGERPRINT

Dr.Rakesh Kumar Giri

Assistant Professor,
Saisha Institutions, Chennai, India

Abstract: The primary goal of this work is to investigate and construct a fingerprint-based passport identification and verification system based on microcontroller matching, which is often utilized in fingerprint approaches. The method consists of deleting fingerprint feature elements from the fingerprint sensor unit and then comparing fingerprints based on how many times the two fingerprints in question have been linked. When they do, the passports' validity for individual verification is confirmed. It's a wonderful method for selecting and positively identifying a specific person. We can use technology to improve security in every location.

***Index Terms* - Fingerprint Recognition, Biometric Authentication, Cryptography Authentication.**

I. INTRODUCTION

Due to their being more durable, dependable, and secure than other devices today, fingerprint sensors are generally selected.

These present, businesses and individuals are embracing these technologies, As automobile theft is a major concern for customers these days, we are proposing bio matrices (Fingerprint) based authentication here for automobile safety. In this concept, no users can be enrolled in a household to accessing the lockers.

FINGERPRINT RECOGNITION

The earliest biometric approach that has been effectively applied in many industries is fingerprint-based authentication. People's fingerprints are recognised to be distinct and unchangeable. A fingerprint is composed of several peaks and furrows on the finger's surfaces. The arrangement of grooves and furrows in addition to the minute points on a fingerprint can help identify its individuality. Local texture features known as local features appear at ridge bifurcations or ridge endings.

VERIFICATION VS IDENTIFICATION

In essence, a biometric system is a pattern recognizing system that establishes a person's private identity by confirming the veracity of a certain physical or behavioural trait. The method used to identify a person is a crucial consideration in the design of afunctional system. A biometric technology can be an identity system or a verification method, according to the situation.

Verification and identification are the two methods used to establish an user's character. Verification entails validating or rejecting a person's stated identification. To identify someone, one must first determine their identity (Who am I?). Every one of these strategies has unique difficulties that could possibly be better resolved by a specific biometric technology.

Most persons you transact businesses with in daily life confirm your identification. You make a claim about who you are, and you support it up with evidence. There is no requirement to present an identification when speaking to colleagues and relations. However, folks who know you well recognize by recognising your face or understanding your voice.

The current approach uses outdated technologies for lockers and has a number of flaws, like the fact that if a key is lost, anyonewith access to it can open the locker.

If a locker's system isn't used for a long time or is exposed to humidity and dust, it will corrode and become stuck, making it impossible to open. This issue is solved by technological advances, which increases the locker's level of safety for the user.

Due to the possibility of keys being lost, stole, or forgotten, outdated technology cannot guarantee a person's locker protection.

To resolve this issue, our system offers a certain fix and quick.

I. STEPS OF FINGERPRINT RECOGNITION

FINGERPRINT FEATURE EXTRACTION

The left loop, sequential pattern, arched, concentric circle, and raised arch ridges designs make up the individual's fingerprint. These patterns are generally categorised using the decades-old Henry method. Approximately 2/3 of all fingerprints have loops, about 1/3 whorls, and maybe 5–10% arches. Although these categorization are useful in several extensive forensic purposes, biometric identification usually employs them. Right loop may be seen in this fingerprint.

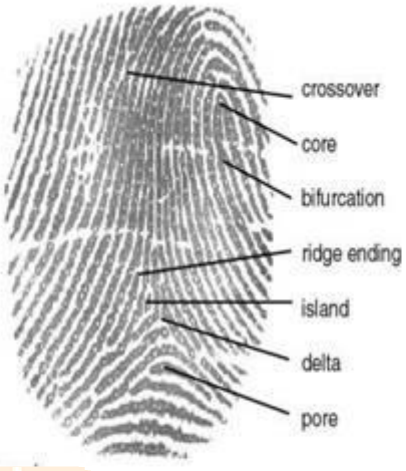

Figure 1: Features in Fingerprint

FINGERPRINT IMAGE ENHANCEMENT

Automatically and dependably extracting details from the captured fingerprint is a crucial step in automated fingerprint identification. Furthermore, a local feature extraction system's effectiveness is highly dependent on the calibre of the input fingerprint photos. It is crucial to include a fingerprint improvement technique in the local feature extraction component in order toguarantee that the functionality of an automatic fingerprint identification/verification systems will be reliable with regards to the quality of the fingerprint.

FINGERPRINT MATCHING

The matching of various size (unauthorised) feature patterns presents challenges for fingerprint identification based on features. Nuances cannot fully describe the local ridge formations. In order to collect more local information and provide a fixed length code for the fingerprint, researchers are attempting a different method of representing fingerprints. The work of computing the Euclidean distance between the two values will therefore, ideally, become fairly straightforward after the matching.

We are creating algorithms that are more accurate in real time and more resistant to distortion in fingerprint images. For a given False Accept Rate, a professional fingerprint-based identification system needs an extremely low False Reject Rate (FAR) (FAR). Any one strategy is exceedingly tough to use to accomplish this. We are looking on ways to combine data from various matching approaches to improve the model accuracy level. The sensor, the data acquisition, and the fluctuation in system effectiveness over time are all crucial in a genuine application. In order to assess the system's effectiveness over time, we are also field evaluating system with a small group of users.

Figure 2: Sample of Fingerprint

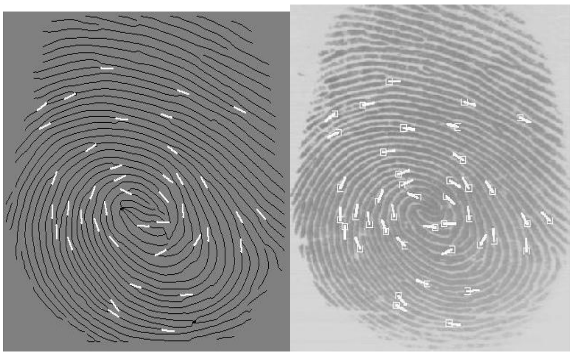

Figure 3: Features in Fingerprint

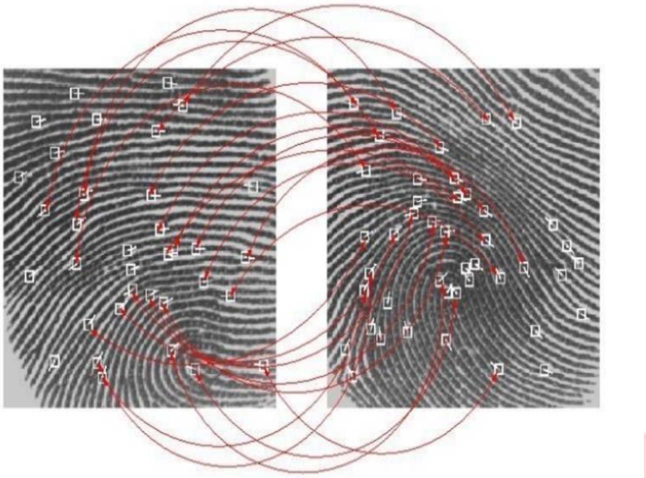

Figure 4: Finger print Matching

FINGERPRINT CLASSIFICATION

A technique known as fingerprint categorization places a fingerprint into one of the many pre-specified categories that have already been developed in the research and can act as an indexing system. The categorization of fingerprints can be thought of as a rough matching of the fingerprints. An input fingerprint is first evaluated to one of the pre-specified categories at a coarse level before being examined to the portion of the dataset that only contains that type of fingerprinting at a refined scale.

II. PROPOSED METHODOLOGY

Figure 5 shows the block diagram of proposed fingerprint-based passport identification and verification system. It includes microcontroller, Fingerprint sensor, keypad, LCD.

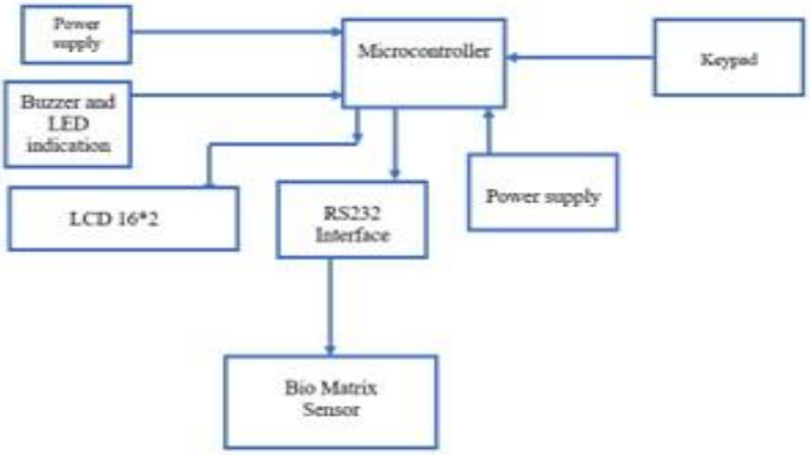

Figure 5: Block diagram of Proposed Fingerprint based passport identification and verification System

3.1 COMPONENT DESCRIPTION

Processor ARM 7: The ARM7 is part of the Advanced RISC Machines (ARM) family of general purpose 32-bit microprocessors, which offer very low power consumption and price for high performance devices. The architecture is based on

Reduced Instruction Set Computer (RISC) principles, and the instruction set and related decode mechanism are much simpler in comparison with micro programmed Complex Instruction Set Computers. This results in a high instruction throughput and impressive real-time interrupt response from a small and cost-effective chip.

Power Supply: For our all IC we require 5V D.C. supply which can be generated by step down transformer, full wave bridge rectifier, filter condenser & voltage regulator IC7805.

12V supply for relay is generated separately using the same procedure as above.

Keypad: Key pad is a set of feather touch keys used for entering the database setting the authentication and providing some functions for the officials and users to gain access to the machine whenever it is required to. These are function keys to perform specific function such as Enter, clear, reset, read, etc.

Biometrics Sensor: It is sensor which senses each person's bio matrix structure of each human being's thumb structure, as here only thumb imprints are being considered, or in other cases palm structures. As each human has its own unique structure of prints on its palm, has unique identity, and unique resistance based on it, that what it is analyzed in this sensor and corresponding electrical signal are generated which are decoded and stored in the memory.

RS232 interface: As there is signal level difference between PC and microcontroller so to match this level shifter IC RS232 isused to interface between two logic levels.

Buzzer: It is a audio indication to the user about the problem in accessing his account or some problems encountered at the timeof authentication and problem of the machine.

Buffer Driver: This stage provides the needed isolation from the main driver stage as well as current boost of the microcontroller signal.

III. EXPERIMENTAL SETUP AND RESULT

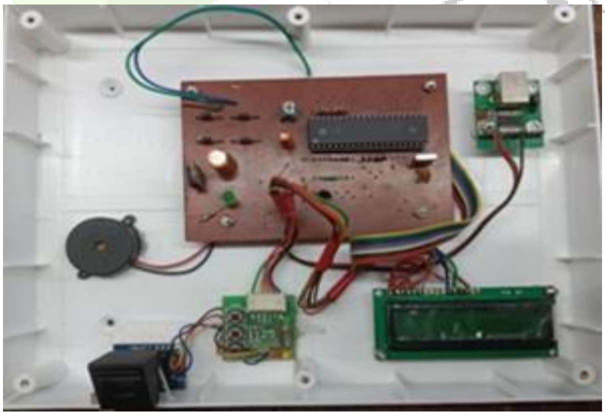

Figure 6: Experimental Setup of Proposed Model

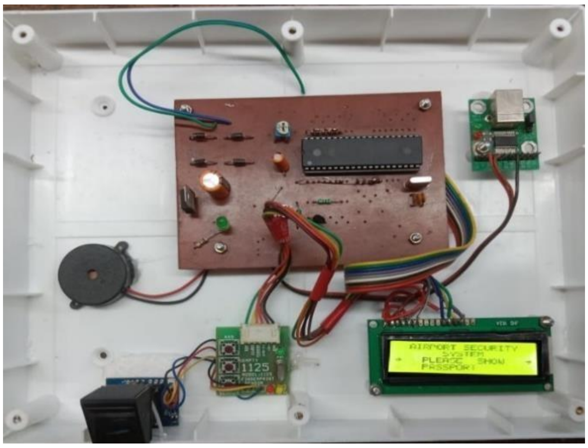

Figure 7: Requisition of User

IV.CONCLUSION AND FUTURE SCOPE

This paper gives clear idea about the passport identification and verification system based on fingerprint recognition which is much more beneficial for the airports and universities. It also reduces the burden of documentation as well as it reduces the time consumption. We analyzed the major current and potential uses of microcontroller in identifying documents and the most important feature of this study is security, this will make the system centralized. The security of the system can be further increased by adding more biometric information such as palm scan, iris scan, digital signature and other active authentication inthe passport identification and verification system.

For the future enhanced following point to considered.

1. OTP option or pin can be provided if biometric fail to work.
2. Face recognition can be used for better security purpose.
3. All data can be clouded/ stored in data base for verification.
4. Eye scan technology can also be added to increasebiometric identification for advance security.

REFERENCES

[1]V.Ravali, P.Bhavani,D.Sampath Kumar,"Passport verification system using RFID", JRTIR, Vol. 5, No.9, 2018.

[2] J. Prashant Shende, Pranoti mude, Sanket Lichade,"Design and implementation of secure electronic passport system ", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, No.11, 2015.

[3]Bhagya Wimalasiri & Neera Jeyamohan " An E-passport system with multistage authentication: A case study of the security of Sri Lanka's E-passport",Global Journal of Computer Science and Technology", Vol. 18, No. 2, 2018.

[4] Ahmed Raad Al-Sudani, Wanlei Zhou Bo Liu, Ahmed Almansoori, Mengmeng Yang, "Detecting unauthorized RFID tag carrier for secure access control to a smart building", International Journal of Applied Engineering Research, Vol.13, No. 1,2018.

[5] Ramshida.V.P.,"Dynamic traffic control system using RFID and GSM",Journal of network communications and emerging technologies, Vol.8, No.2, 2018.

[6] Kanchan Warke, Attar Sultana Mahamad, Gardare Swati.S, Gaikwad Snehal Sunil, Nichal Bhagyshri Sudhir,"Smart ration card system using RFID and embedded system", Vol. 4 No.3, 2018.

[7] Arulogun O.T.,Olatunbosun.A,Fakolujo.O.A, Olaniyi.O.M," RFID based students attendance management system",
International Journal of Scientific & Engineering Research, Vol. 4, No. 2, 2013

[8] Vishal Yuvraj Mulmule, Prof. C. S. Patil, "Study of Biometric Authentication Techniques and Its Application", International Journal of Advanced Innovative Technology in Engineering, 2022, 7(5), PP 10-15

[9] Robert Cockell and Basel Halak, "On the Design and Analysis of a Biometric Authentication System Using Keystroke Dynamics", Cryptography 2017, 4, 12; doi:10.3390/cryptography4020012

[10]Dakhil, I. and Ibrahim, A. (2018) Design and Implementation of Fingerprint Identification System Based on KNN Neural Network. Journal of Computer and Communications, 6, 1-18. doi:

10.4236/jcc.2018.63001.

[11] Dennis Mugambi Kaburu, Julianne Sansa-Otim, Kajumba Mayanja, Drake Patrick Mirembe, Tony Bulega, "A usability based approach to designing continuous user biometric authentication system", Quality and User Experience (2018) 3:8 https://doi.org/10.1007/s41233-018-0021-1.