

Chief Editor

Dr. A. Singaraj, M.A., M.Phil., Ph.D.

Editor

Mrs.M.Josephin Immaculate Ruba

EDITORIAL ADVISORS

1. Prof. Dr.Said I.Shalaby, MD,Ph.D.
Professor & Vice President
Tropical Medicine,
Hepatology & Gastroenterology, NRC,
Academy of Scientific Research and Technology,
Cairo, Egypt.
2. Dr. Mussie T. Tessema,
Associate Professor,
Department of Business Administration,
Winona State University, MN,
United States of America,
3. Dr. Mengsteab Tesfayohannes,
Associate Professor,
Department of Management,
Sigmund Weis School of Business,
Susquehanna University,
Selinsgrove, PENN,
United States of America,
4. Dr. Ahmed Sebihi
Associate Professor
Islamic Culture and Social Sciences (ICSS),
Department of General Education (DGE),
Gulf Medical University (GMU),
UAE.
5. Dr. Anne Maduka,
Assistant Professor,
Department of Economics,
Anambra State University,
Igbariam Campus,
Nigeria.
6. Dr. D.K. Awasthi, M.Sc., Ph.D.
Associate Professor
Department of Chemistry,
Sri J.N.P.G. College,
Charbagh, Lucknow,
Uttar Pradesh. India
7. Dr. Tirtharaj Bhoi, M.A, Ph.D,
Assistant Professor,
School of Social Science,
University of Jammu,
Jammu, Jammu & Kashmir, India.
8. Dr. Pradeep Kumar Choudhury,
Assistant Professor,
Institute for Studies in Industrial Development,
An ICSSR Research Institute,
New Delhi- 110070, India.
9. Dr. Gyanendra Awasthi, M.Sc., Ph.D., NET
Associate Professor & HOD
Department of Biochemistry,
Dolphin (PG) Institute of Biomedical & Natural
Sciences,
Dehradun, Uttarakhand, India.
10. Dr. C. Satapathy,
Director,
Amity Humanity Foundation,
Amity Business School, Bhubaneswar,
Orissa, India.



ISSN (Online): 2455-7838

SJIF Impact Factor : 6.260

ISI I.F. Value : 1.241

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed
International Online Journal

Volume: 4, Issue:8, August 2019

Indexed By:



Published By
EPRA Publishing

CC License





BIOMETRIC ATTENDANCE WITH DATA LOGGER

Kasipati Arsavelli¹

Raghu Engineering College, Visakhapatnam, A.P, India

Dr. G.V. Sridhar²

Raghu Engineering College, Visakhapatnam, A.P, India

ABSTRACT

This paper describes the biometric, fingerprint time and attendance recording system. The Aim of this paper focuses Time and attendance recording system of students in educational institute. Truly it is an electronic attendance monitoring system which reduces the risk of fake attendance recording. It also reduces the problems like keeping the paper attendance record, damage of paper record or loss of paper attendance record. It will record the attendance of subject teacher and students for a particular class and subject. The objective of this paper is very simple to go for paperless attendance recording system and to save papers, save environment i.e. go Green. In this paper provides the design method of portable fingerprint based student attendance system using Serial Communication. The system includes terminal fingerprint acquisition module and attendance module. It can realize automatically such functions as information acquisition of fingerprint, processing, wireless-transmission, fingerprint matching and making an attendance report. After taking the attendance, this system sends the attendance of every student to their parent's mobile through UART. Attendance system facilitates access to the attendance of a particular student in a particular class. This system eliminates the need for stationary materials and personnel for the keeping of records.

I. INTRODUCTION

BIOMETRICS refers to the automatic identification of a person based on his physiological / behavioral characteristics. This method of identification is preferred for various reasons; the person to be identified is required to be physically present at the point of identification; identification based on biometric techniques obviates the need to remember a password or carry a token.

A biometric is a unique, measurable characteristic or trait for automatically recognizing or verifying the identity of a human being. Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information and property.

With the increased use of computers or vehicles of information technology, it is necessary to restrict access to sensitive or personal data. By replacing PINs, biometric techniques can

potentially prevent unauthorized access to fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric systems of identification are enjoying a renewed interest.

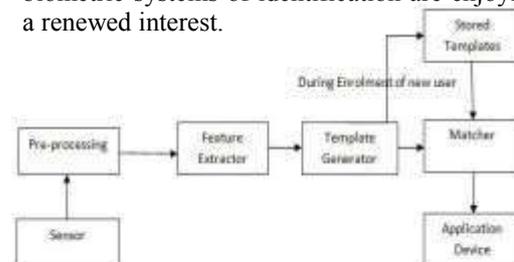


Figure 1: Basic block diagram of biometrics system

Biometrics encompasses both physiological and behavioral characteristics. A physiological characteristic are related to the shape of a body. A relatively stable physical feature such as fingerprint, hand geometry, iris pattern or facial features. These factors are basically unalterable without trauma to the individual. Behavioral tracts, on the other hand, are related to the behavior of a person. The most common trait used in identification is a person's signature. Other behaviors used include a person's keyboard typing, gait and speech patterns. Most of the behavioral characteristics change over time.

Some of physical biometrics is

- Fingerprint - analyzing fingertip patterns.
- Facial Recognition- measuring shape of the hand.
- Hand Geometry- measuring the shape of the hand.
- Iris recognition- analyzing features of colored ring of the eye.
- Some of behavioral biometrics is
- Speaker Recognition- analyzing vocal behavior.
- Signature Recognition - analyze the physical activity of signing.
- GestureRecognition - analyzing the motions of body.

In this project I have used Fingerprint Biometrics.

In section I paper introduction then after in section II finger print biometrics were discussed followed by Experimental methodology in section III, then in section IV Results were displayed and in section V the paper was concluded.

II. FINGER PRINT BIOMETRICS

Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high. Fingerprinting is probably the best-known biometric- method of identification used for 100 years. There are a few variants of image capture technology available for such commercially oriented fingerprint sensor, including optical, silicon, ultrasound, thermal and hybrid.

Among all the biometric techniques, fingerprint-based Identification is the oldest method that has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger as shown in the fig 3.1.1. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as minutiae points. Minutiae points are the local ridge characteristics that occur either at a ridge ending or a ridge bifurcation. A ridge ending is defined as the point where the ridge ends abruptly and the ridge bifurcation is the point where the ridge splits into two or more branches.

When a user places their finger on the terminals scanner the image is electronically read,

analyzed, and compared with a previously recorded image of the same finger which has been stored in the database. The imaging process is based on digital holography, using an electro-optical scanner about the size of a thumbprint. The scanner reads three-dimensional data from the finger such as skin undulations, and ridges and valleys, to create a unique pattern that is composed into a template file. An algorithm is developed to classify fingerprints into five classes, namely, whorl, right loop, arch and tented arch as shown in figure 2.2. Critical points in a fingerprint, called core and delta are marked on one of the fingers as shown in figure 3 (c). The core is the inner point, normally in the middle of the print, around which swirls, loops, or arches center. It is frequently characterized by a ridge ending and several acutely curved ridges.

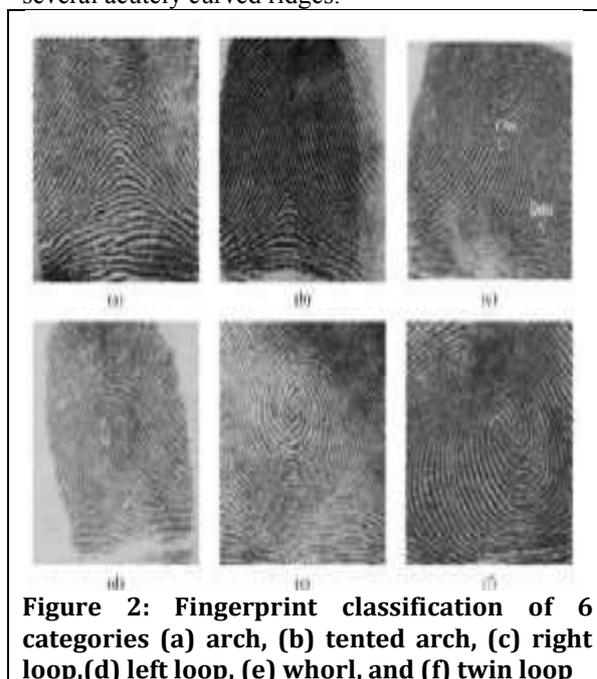


Figure 2: Fingerprint classification of 6 categories (a) arch, (b) tented arch, (c) right loop,(d) left loop, (e) whorl, and (f) twin loop

Deltas are the points, normally at the lower left and right hand of the fingerprint, around which a triangular series of ridges center. The algorithm separates the number of ridges present in four directions (0 degree, 45 degree, 90 degree and 135 degree) by filtering the central part of a fingerprint with a bank of Gabor filters. This information is quantized to generate a finger code which is used for classification. To avoid fake-finger attacks, some systems employ so-called live detection technology, which takes advantage of the sweat activity of human bodies. High-magnification lenses and special illumination technologies capture the finger's perspiration and pronounce the finger dead or alive.

It has advantages of Fingerprint recognition equipment is relatively low-priced compared to other biometric system. Fingerprints are unique to each finger of each individual and the ridge arrangement remains permanent during one's lifetime and drawbacks of some people have damaged or

eliminated fingerprints and Vulnerable to noise and distortion brought on by dirt and twists.

Fingerprint Module GT-511C3 the module does all the heavy work of reading, identifying, and storing the fingerprint data. It can be issued several commands for all the functionalities. The module can store up to 200 different fingerprints recognition. For working the fingerprint must be registered by sending appropriate commands. On successful execution of the command it sends acknowledgement for success and Error code otherwise. The database of the prints can even be downloaded from the unit and distributed to other modules. The raw images of the fingerprints can also be retrieved from the module.

The design includes the following:

- Microcontroller (TM4C123GH6PMI)
- SD Card
- Fingerprint Scanner
- Real Time Clock
- TFT Display
- Serial Terminal
- Power Supply

III. EXPERIMENTAL METHODOLOGY

To enroll the fingerprint the finger is to be pressed to the module thrice. All the three times it creates a template for the finger that was put on the optical sensor, added to that, the third time it also merges the three templates to create the final template. On successful enrolling the device sends a unique ID pertaining to the finger enrolled. This ID can be saved and later used for verification of the finger.

Enrolling Procedure:

- 1) Enroll Start (ID); // Issue command to start enrolling over the ID as parameter.
- 2) Capture Finger; // Take snapshot of the finger.
- 3) Enroll1; // Create template of the 1st Image.
- 4) Remove and press finger again;
- 5) Capture Finger;
- 6) Enroll2; // Create template of the 2nd Image.
- 7) Remove and press finger again;
- 8) Capture Finger;
- 9) Enroll3; // Create template of the 3rd image and merge all 3 templates

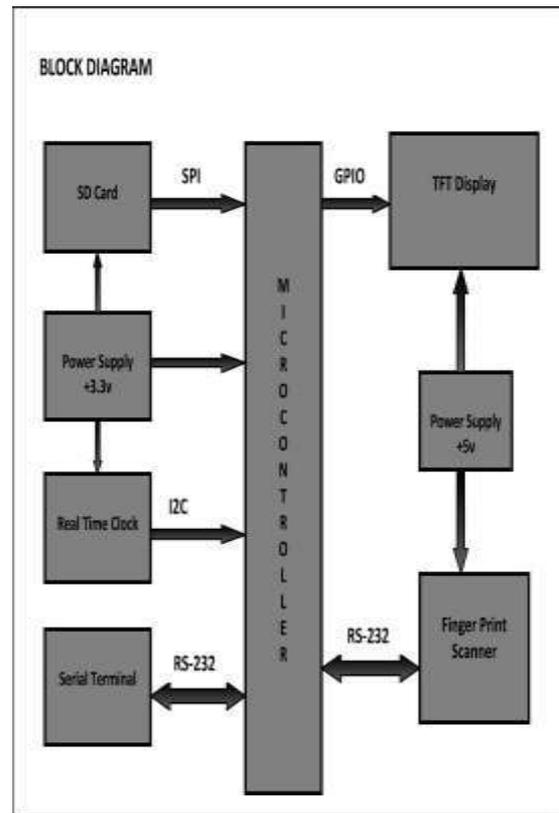


Figure 3: Block diagram of Fingerprint Attendance system

Verifying Procedure:

- Capture Finger
- Identify1_N
- If(ID < 200) ◊ Verified ID
- Else Invalid Finger

NOTE: · During enrolling, we have to press longer time the fingerprint module· during marking attendance, we have to press it only once.

IV. RESULTS

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 to whatever needs protecting, from a door, to your car to... Blood Banks:

When it comes to giving blood; identity is pretty important. In the past donors were issued with blue cards containing all the information required. More and more these days that crucial data is being stored digitally – with donors using fingerprint or iris recognition to access their vital details.

- Consumer/Residential Biometrics
- Financial
- Fingerprint & Biometric Locks

- Healthcare Biometrics
- Justice/Law Enforcement
- Logical Access Control

To ensure that the 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

In order to be useful, biometrics must be stored in a database. Alice's voice biometric works only if you recognize her voice; it won't help if she is a stranger. You can verify a signature only if you recognize it. To solve this problem, banks keep signature cards. Alice signs her name on a card when she opens the account, and the bank can verify Alice's signature against the stored signature check was signed by Alice.

One area where biometrics can provide substantial help is in guarding against attempts to establish fraudulent multiple identities or prevent identity fraud. By searching through the stored references, individuals who appear to have previously enrolled using a different identity can be highlighted for further investigation. It is very difficult to perform this type of check without the use of biometrics. On the other hand, some biometrics are easy to steal. Imagine a remote system that uses face recognition as a biometric. In order to gain authorization, take a Polaroid picture of yourself and mail it in. We'll compare the picture with the one we have in file.



	A	B	C
1	SNO	Student	Time
2	1	Ramesh	9:22:22
3	2	Suresh	9:24:22
4	3	Kasi	9:22:26
5	4	Raghu	9:25:30
6	5	Teja	9:26:40
7	6	Mahesh	9:27:35
8	7	Blessy	9:28:25
9	8	Amrutha	9:29:30
10	9	Srinivas	9:31:10
11	10	Raju	9:22:32

Figure 4: Output of registered entry

V. CONCLUSION

Biometric is an emerging area with many opportunities for growth. Biometrics is widely being used because of its user friendliness, flexibility in specifying required security level and long term stability. The technology will continue to improve and challenges such as interoperability solved through standardization. This will lead to increase in the market adoption rate and the technology will proliferate. Possibly in the near future, you will not have to remember PINs and passwords and keys in your bags or pockets will be things of the past. In this paper, I have presented a fingerprint-based attendance management system. The proposed system will make way for perfect management of students and staff attendance and produce more accuracy. Fingerprint recognition is universally applied and is very relevant in an institute. This system can be implemented in academic institutes for better results regarding the management of attendance. This system will save time and reduce the amount of work of the administration. The future of biometrics holds great promise for law enforcement applications, as well for private industry uses. Biometrics' future will include e-commerce applications for extra security on the checkout page, and biometrics will guard against unauthorized access to cars and cell phones. In the future, biometric technology will further develop 3-D infrared facial recognition access control, real-time facial recognition passive surveillance, and visitor management authentication systems. Already A4Vision, a provider of 3D facial scanning and identification software uses specialized algorithms to

interpret the traditional 2D camera image and transfer it into a 3D representation of a registered face. This makes it almost impossible to deceive the biometric system with still photos or other images. Strengthening existing biometric innovations for future growth all of these security innovations will make biometric technology more accurate and make its usage more widespread.

Biometric”, IEEE 2014 international conference on information and communication Technology

VI. REFERENCES

1. MurizahKassim, HasbullahMazlan, NorlizaZaini, Muhammad KhidhirSalleh “Web-based Student Attendance System using RFID Technology” 2012 IEEE.
2. B. Rasagna, Prof. C. Rajendra “SSCM: A Smart System for College Maintenance” *International Journal of Advanced Research in Computer Engineering & Technology*, May 2012.
3. LI Jian-po, ZHU Xu-ning, LI Xue, ZHANG Zhi-ming “Wireless Fingerprint Attendance System Based on ZigBee Technology” 2010 IEEE.
4. O. Shoewu, O.A. Idorwu “Development of Attendance Management System using Biometrics” *The Pacific Journal of Science and Technology*, May 2012.
5. “How does a fingerprint sensor work” Online Available:
http://wiki.answers.com/Q/How_does_a_fingerprint_sensor_work [Accessed: Sept. 15, 2013].
6. “What is GSM?” Online Available:
http://www.tutorialspoint.com/gsm/gsm_overview.htm [Accessed: Sept. 17, 2013].
7. L. Rajasekar, S. Vivek “Wireless Fingerprint Attendance System using ZigBee Technology” *International Journal of Power Control Signal and Computation (IJPCSC)*, Vol3. No1. Jan-Mar 2012.
8. ZatinSinghal, Rajneesh Kumar Gujral “Anytime Anywhere- Remote Monitoring of Attendance System based on RFID using GSM Network” *International Journal of Computer Applications*, February 2012.
9. Mohamed Basheer K P , Raghu C V , “Fingerprint Attendance System for classroom Needs”, *India Conference(INDICON), Annual IEEE 2012*.
10. M A MeorSaid,M H Misran, M A Othman, M M Ismail, H A Sulaiman,ASalleh, N Yusop, “Biometric Attendance”, 2014 *International Symposium on Technology Management and Emerging (ISTMET 2014)*.
11. LI Jian-po, ZHU XU-ning , LI Xue, ZHANG Zhi-ming, Ji Sheng SUI ,“Wireless fingerprint attendance system based on Zigbee Technology”, *IEEE 2010 2nd international workshop on intelligent systems and applications*.
12. Amir Nizam Ansari, ArundatiNavada, SanchitAgarwal, SiddharthPatil, BakvantiSonkamble, “Automation of Attendance system using RFID ,Biometrics, GSM modem with.. Net framework”, *IEEE 2011 International conference on multimedia technology*.
13. Zhang Yongqiang ,LIUJi, “The design of wireless fingerprint Attendance system”, *IEEE 2006 International conference on communication Technology*.
14. NurIzzatiZainal, KhairulAzamisidek, Teddy suryaGunawan, HasmahMansor Mira Kartiwi, “Design and development of portable classroom attendance system based on Arduino and fingerprint