A REVIEW ON FINGERPRINT ORIENTED LOCK AND UNLOCK IDENTIFICATION SYSTEM

Venkappanavara Basavaraja¹ Dept. of Studies in Computer Science and Research Davangere University Davangere, India v.basavaraja@gmail.com

Abstract— For both personal and commercial protection, security has always been a major concern, and numerous solutions are available to address the problem. Since people are more concerned about the security of their belongings in the real world, such as jewelry, cash, important documents, etc., safe deposit lockers are the safest place to store the valuables. Users can now operate high security systems using electronic identity alternatives and evolving further. The RFID (Radio-Frequency Identification) or password-based lock mechanisms can be broken when the RFID card or passwords are shared or stolen, hence it is necessitating the use of a biometric-based secure system in facilities with shared access. Security breaches occur even when RFID cards or passwords are used. Identification with biometric credentials or fingerprint recognition can help to overcome such problems. For the purpose of granting access to a facility that is utilized by the numerous users, fingerprints of the authorized users are registered and checked. Additionally, a user may be unenrolled from the system and a new user may be added. This fixes the issues of forgetting your personal locker's combination and not understanding how the numbers should be fed. As a nutshell concept the user's fingerprint will essentially serve as their locker key in this setup.

Keywords— Fingerprint, biometric, RFID

I. INTRODUCTION

This study talks about review of existing biometric fingerprint authentication system for locking and unlocking devices. Authentication by fingerprints has been practiced for several entries. Fingerprints were mostly employed during this time to identify criminals. Fingerprint authentication is a good biometric because of the numerous features of fingerprints, such as high reliability and security.

Since the invention of fingerprint technology more than 100 years ago, much has changed. Compared to the sleek, modern livescan fingerprint readers that were first released in 1988, which had few issues, there are currently cheap, tiny sensors on the market. We have learned more about individuality, the information contained in fingerprints, and effective methods of processing this information during the past few decades thanks to research into and practical use of fingerprint matching and indexing. Automatic fingerprint algorithms are now practical for daily usage in a wide range of applications thanks to decreasingly expensive processing power, less expensive fingerprint sensors, and the demand for security, efficiency, and simplicity.

Chandrakant Naikodi²

Dept. of Studies in Computer Science and Research Davangere University Davangere, India chandrakant.naikodi@yahoo.in

Designing a fully automatic and trustworthy fingerprint individualization system still presents a number of difficulties, particularly when fingerprint scans are of poor quality. Despite substantial advancements, the design of automated systems still falls short of the sophisticated decision-making of choices are made to match certain fingerprints, especially latent prints, by a skilled fingerprint expert. However, automatic fingerprint matching systems show great potential for the creation of efficient, quick, consistent, and dependable solutions in a variety of established and upcoming applications.

Research on automatic fingerprint identification has been focused on simulating a human fingerprint expert's performance without having access to the numerous underlying, information-rich traits an expert can identify through visual inspection. The lack of advanced modelling and image-processing techniques that can reliably and consistently extract detailed features in the face of noise is mostly to blame for the lack of such a large range of useful features in automatic systems. The design of automatic fingerprint identification systems may not be best based on the human, intuition-based manual fingerprint recognition method. There may be a need to investigate radically alternative features rich in discriminatory information, reliable fingerprint matching techniques, and more creative, automatable ways to combine fingerprint matching with classification.

Since fingerprints are fairly ubiquitous and almost everyone has them, and also almost anyone can utilize this technique. Another advantage of fingerprints is their uniqueness. Even the identical person's fingers have unique fingerprints. The process of recognizing fingerprints is typically quick, efficient, and most importantly accurate. Recording fingerprints is straightforward. Generally speaking, using fingerprints to identify someone is a trusted, easy, and accepted technique.

A modified Automated Fingerprinting Identification System (AFIS) is the foundation of a biometric fingerprint lock. Based on their geometric characteristics, fingerprints are categorized by AFIS systems or systems that are comparable to AFIS. dividing up fingerprints

The benefit of many categories is that they can speed up fingerprint matching. You could search a subset of them (only the ones in the same category) rather than all of the known fingerprints if you could categorize all fingerprints into a number of groups. Studies have led to the development of algorithms that classify fingerprints into 5 or 6 groups with an accuracy rate of 90%. To categorize fingerprints into additional categories while maintaining a better level of accuracy, though, is thought to be difficult. Generally speaking, there are different forms of fingerprints: arch, tented arch, left loop, right loop, whorl, and twin-loop.

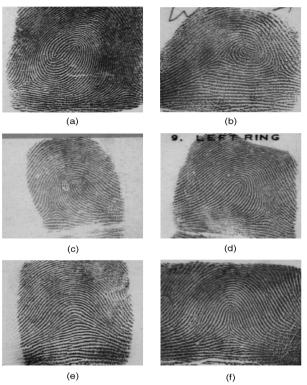


Figure 1:[1] Major fingerprint classes. Twin loop images are labelled as whorl in the NIST-4 database. (a) Twin loop (W), (b) Whorl (W), (c) Right loop (R), (d) Left loop (L), (e) Arch (A), (f) Tented arch (T).

Fingerprint Classification

Unique fingerprints exist. Each person's epidermis develops in a distinct pattern. As a result, three general categories for fingerprints exist: loops, whorls, and arches.

2.1 Loops

It makes up 60–65% of the world's population. The print features one or more ridges that come from a single side curve, and depart from that same side.

2.2 Whorls

Around the world, between 30 and 35 percent of people have whorls on their fingers. Type lines and two deltas are present in all whorl patterns. There are four primary types: plain, double loop, centre pocket.

2.2.1 Simple Whorls

A hypothetical line from one delta to the other must touch a whorl ridge, and they all have at least one ridge that forms a full circuit.

2.2.2 Central Pocket Whorls

A hypothetical line connecting one delta to the next cannot touch a whorl ridge, and they all have at least one ridge that forms a full circuit.

2.2.3 Double loop

In this, two loops are combined to form a whorl.

2.3 Arches

Rarely does this pattern appear. It makes up 5% of the total population. Arch ridges typically enter the print from one side and exit the other. Plain arches and tented arches are two different forms.

2.3.1 Simple archways

They feature a design that resembles waves

2.3.2 Tented arches

They depict a pointed spike in the arch's middle.

As a result, different types of prints are processed by an individual. Each person has a set of distinctive fingerprints that are unmatched worldwide. Even the twins have unique prints of their own. A novel notion is taken into consideration in relation to this classification and property. Let's first examine the operation of the fingerprint recognition technology.

II. LITERATURE REVIEW

In this paper [2] the authors determine how the fingerprint sensor operates. The two fundamental components of fingerprint processing are enrolment and verification. Every user must place their finger twice during the enrolment process for fingerprints. In order for the system to process, create, and store the finger's pattern, it must first verify the photographs of the finger. When a user places their finger on an optical sensor, the system creates a pattern of the finger and compares it to template fingers in the finger library. The system will examine the exits finger with respect to a specific pattern that is selected within the module. The scanning system will similarly search for the whole finger records for the finger matching for 1: N matching. The scanning system will return to the appropriate result in either case of success or crash. When the finger is positioned, the image of the finger is taken, resized, and improved. When the image is matched with an image in the database, a dialogue box stating that the image is matched appears. The same thing happens when the image is mismatched—a dialogue box appears.

In the paper [3] finding for system improvement, an assessment of the Fingerprint Recognition System (FRS) is provided. For a better understanding of the system, the fundamental phases of the FRS are presented along with various matching approaches & identification keys. To explain why fingerprint is chosen over other biometric approaches, analysis of various biometric systems and FRS strengths are covered. To understand the task clearly, challenges are created in this discipline, and applications are defined to solve the task effectively. The researcher is given a range of options in this area.

Approval by paper [4] while using a locker key for banking has lately been suggested, there are certain drawbacks that need to be considered. It can provide the wrong individual access to the account. Therefore, they are integrating a biometric-based security system in this. This system will be the ideal banking system because it is affordable and secure. Correct and quick user verification is offered for biometric and GSM security. Biometrics cannot be forgotten, making them impossible for both users and adversaries to fabricate and reject. Everybody may be identified by their fingerprint. Someone was trying to unlock his locker, he learned. By utilizing fingerprint biometrics as the authentication mechanism, the system has successfully solved some of the drawbacks of the current technologies.

In this research paper [5] a methodical design process for a microcontroller-based system that secures user transactions and provides security for the locker system and considerably more for the use of a finger-print scanner for passport verification. In all three modes, the results obtained when providing security are very reliable. By using finger print biometrics as the authentication technology, the system has successfully solved some of the drawbacks of the current methods.

Testing the system can get the desired results. The code for this project [6] is implemented by referring to many papers. First, go over the recently proposed banking using locker keys. Despite being safe, there are certain drawbacks. It can provide the wrong individual access to the account. Therefore, they are integrating a biometric-based security system in this. This system will be the ideal banking system because it is affordable and secure. Correct and quick user verification is offered through biometric and GSM security. due to biometric. They are impossible to misplace and are challenging for users to reject. Everybody may be identified by their fingerprint. Someone was trying to unlock his locker, he learned. By utilizing fingerprint biometrics as the authentication mechanism, the system has successfully solved some of the drawbacks of the current technologies.

The primary goal of this project [7] is to use a microcontroller to build and construct a fingerprint-based bank locker system. This project will use embedded systems and biometrics, two distinct technologies, to give bank lockers complete security and to facilitate work. The microcontroller-based system was designed utilizing a step-by-step process to secure user transactions, provide security for the locker system, and even more for the passport verification using a finger-print scanner. In all three modalities, the security result was attained with a high degree of dependability. By using finger print biometrics as the authentication technology, the system has successfully solved some of the drawbacks of the current methods.

In the project [8] "Intelligent door locking system" initiative is a step towards resolving passwords or card entry access problems by limiting access for unauthorized people. By creating a lock that stores the fingerprints of one or more authorized users, unauthorized access is prevented. The user's fingerprint is scanned and verified for authentication if he or she wants to get entrance. If the fingerprints match, the door will automatically open; if not, the system will stay locked until it receives authentication at that same moment. This feature increases the system's effectiveness. Consequently, the biometric finger print technology offers a solid answer to the problem of home safety. The shortcomings of existing systems are overcome by the design of our suggested system. The proposed system places a high value on user usability, making it more comfortable to use than any other systems now in use. Additionally, it was created using open-source hardware, which reduced the cost.

This paper [9] outlines a cutting-edge security system created for door locking. Our identities cannot be stolen, only our keys. Additionally, it is quite difficult to bypass a fingerprint sensor door lock, so the system ensures strong security. Because there is no chance of forgetting passwords or losing keys, a fingerprint sensor door lock is undoubtedly the most practical choice at this time. Future applications for this security system include face recognition thanks to artificial intelligence capabilities can be included to make the identification procedure easier. In addition to temperature sensors, the system can also be equipped with fire sensors, iris scanners, and other security measures.

Various articles that employed biometrics as a locking system are explained in this document [10]. Their primary goal was to create a locker with no security issues; thus, they developed a biometric-based locker that uses a fingerprint verification technique. In this article, they looked at a few studies that dealt with this project. They introduced biometric-based lockers with a high level of security in our paper. Nobody who is not authorized will be able to access the locker. Their system uses fingerprints as verification method because it is impossible to duplicate a fingerprint. This device is inexpensive and simple to operate. This system can be installed anywhere where a high level of security is required. One of the most crucial aspects of this project is its low cost, the safe and dependable locker.

In this paper [11] the fingerprint door lock security system is so well-liked as a method of access control for a number of important reasons. The fingerprint door lock security system is one of the few examples of a security improvement that also boosts convenience. Traditionally, upgrading to more secure technologies comes with a compromise in terms of comfort. The best of both worlds is present. The preferred option for access control is gradually evolving to be fingerprint door lock security systems. Its superior military-grade security, improved usability, and lower costs make it the clear alternative over conventional access controls. In order to improve security and accuracy, multimodal biometrics are now being used. Fingerprints, face, iris, palm, and DNA-based recognition are some of the most well-known methods. Multimodal biometric systems typically require two biometric credentials, such as a face and fingerprints, rather than one, for identification. They can get around common problems with mono-modal systems.

Designing, building and testing a biometric fingerprint locking system to regulate access to a group of lockers was the goal of

this capstone project [12]. This technique makes using lockers simpler and provides a practical replacement for conventional locks. The creation of an easy-to-use system with no obstacles or questions was the project's most crucial goal. Furthermore, it was critical to have a high recognition rate and a low false positive rate in order to prevent people from being "accidentally" given access to other people's lockers. The project was built around a fingerprint scanner that was managed by a microcontroller to address this issue. The system's brain was the microcontroller. In order to make the system more user-friendly, it sends commands to the fingerprint scanner, interprets data that is returned, and manages an LCD display. The background information necessary to understand a fingerprint identification system, a thorough explanation of the design requirements, design alternatives and the rationale behind component selection, the preliminary proposed design, and the design of the final prototype are all included in this report.

In the paper [13] the fingerprint recognition software permits the enrolment of legitimate users' fingerprints in a database as samples of stored images of the bmp, tiff, jpg, jpeg, and gif image types files. Therefore, before any user may unlock or start the car, his or her fingerprint image is compared to the fingerprints in this database; users for whom the database contains no matches are prevented from using the system. The person must be physically present for the biometric approach to work. Therefore, compared to conventional techniques of personal recognition, biometric recognition systems offer higher security and ease.

The primary objective of this project [14] is to develop and put into use a fingerprint-based bank locker security system. This can be set up at banks, workplaces, and residences. only in this system. The authenticated individual retrieves the money or documents from the lockers. A fingerprint is employed in this security method. First-time users of this system must enroll using their name, password, and mobile number. If the user's name and password are identical, the person's finger will be detected and stored with their ID. whether there are matches to the ID.

Therefore, Bluetooth app security and biometric security have greater advantages than other systems. A log of the check-ins and check-outs made possible by this system each user along with the fundamental data. With real-time security passwords that are user created, we can boost bank locker security quickly and save time by using this E-Smart card, which can check personal information in 3 seconds. The project's ATMEGA-328 IC and AVR Microcontroller are both controlled by embedded C programmes created with Arduino software. The AVR Microcontroller can be reprogrammed, thus in the future the system can be improve it for more security concerns relating to jewelry stores, the RBI, the aerospace industry, the military, hospitals, etc. The AVR Microcontroller can be reprogrammed to increase the number of applications in future.

In the paper [15] proposed the fingerprint lock device's layout and operation can be altered to suit the situation. This method of locking doors is more expensive than having to have lock structures within the normal market. Their fingerprint lock device has a very high level of accuracy and is similarly simple to comprehend fingerprints, allowing seamless integration with clients and offering reliable security. They intend to create a device that should be inexpensive for both large and small businesses while keeping setup costs in mind. With careful research and development, the design may be improved, and the gadget could gain new features and millions more users. Therefore, if this lock can be used to mislead numerous departments, they don't want to spend that much money on just one lock. It may be possible to create a printer storage device that does not require a laptop, but it will need components that are bigger than the ones we used. A complete machine should be installed inside the door panel or another area of the door to maintain proper safety. The battery device can also be created using or fuelled by sunlight. One of this system's key benefits is its flexibility.

The reduction of data loss is main goal of this study's [16]. Fast detection takes less time, and accuracy is improved. Security is a major concern in our daily lives, and digital locks have evolved into a crucial component of these security systems. A number of security measures can be used to secure Our Bike. In this article, they proposed to build a biometric security system based on fingerprints to start a car engine by attaching a fingerprint sensor module to a Grow Board. Since fingerprints can be used to identify any individual and are challenging to duplicate, they are one of the safest keys for locking or unlocking any device. All of the security problems with the current system are resolved by thier suggested solution, which also offers excellent security and efficiency. This is a great/ideal choice to prevent the hassle of a stolen/lost key or an unauthorised admission. Since fingerprinting has a high level of identification accuracy, it is a great solution to these problems. Our palms and soles have friction ridges, which are flow-like patterns of ridges. The friction ridge pattern on each finger is unique and constant. As a result, everyone's fingerprints serve as a unique form of identification. The results of suggested project are summarised as it offers more security and quicker detection than current systems. Both the setup process and user access are straightforward. Less data is lost and less time is used with this module. This study explores the use of inexpensive scanners and other parts to secure bicycles.

In this article [17] a safe biometric measurement that guarantees data confidentiality is fingerprinting. The suggested device provides a high level of security by acting as a means of safely delivering and receiving data to applications and websites. Systems for fingerprint-based authentication guarantee dependability, precision, and clarity. Although there is commercially available fingerprinting equipment, adopting a portable, lightweight device will enable this technology get to places where it is less well recognized. Additionally, fingerprinting is a security solution that is anticipated to be widely employed in the future because its benefits exceed its drawbacks. The purpose of this work [18] was to thoroughly compare the fingerprint classification performance of various CNN architectures and to give recommendations for the best network for categorizing fingerprints from various databases and in accordance with various well-established taxonomies (i.e., four-, five-, and eight-class classification). According to the average performance across the various classification kinds the main conclusions from their experiment are as follows:

On the NIST database, AlexNet and ResNet outperformed GoogLeNet to achieve equivalent performance in the fourand five-class classifications; AlexNet performed significantly better in the eight-class classification; and all of the CNNbased architectures under investigation displayed comparable performance for high-quality images (such as those in the PolyU database).

This study could be further improved by taking into account other data-augmentation approaches that make use of histogram-based operations and other geometric changes (such as cropping, rotation, and stretching). As an added bonus, Generative Adversarial Network (GAN)-based for classification and detection tasks, data augmentation could be examined in terms of both picture improvement and geometrical modifications. The creation of adversarial examples-which involves making minor adjustments to the source photos that are close to the decision boundaries discovered by a classifier-may have an impact on Deep Learning-based authentication and fingerprint recognition systems.

In order to effectively identify the corpse in deaths and conduct criminal investigations, this paper [19] has covered the fundamentals and requirements of fingerprinting. Their presentation of its cutting-edge fingerprint algorithms for classification, matching, feature extraction, identification, and fingerprint spoof detection is just the beginning. Additionally, they have been highlighted fingerprint applications for the future and showed them in our daily lives.

The characteristics of pressed fingerprints, such as the types, centers, and directions of the centers, as well as the uppercenters, lower-centers, left-triangles, right-triangles, minutiae, and its direction, can be automatically retrieved by CAFIS (Cogent's Automated Fingerprint and Palm Print Identification System).

This paper [20] researches the AFIS based on CAFIS. However, due to the pressed fingerprints' poor quality, the algorithm is unable to extract these features precisely. CAFIS can categorize depending on the quality of the pressed fingerprints, rectification work is then done by fingerprint technicians. The device can automatically extract features from fingerprints collected at the crime scene. But the effect of extracting them usually has little impact. Currently, doing this work without a specialist is not advised. How to pretreat fingerprints of poor quality and how to extract their features are the main areas of future study for CAIFS.

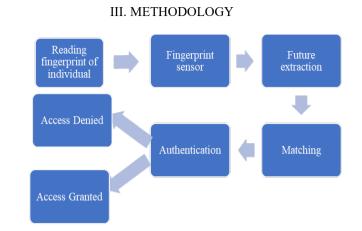


Fig. 2 Fingerprint authentication system

There are five main steps in this system [21]. These are the verification methods used to confirm that a user is legitimate. A fingerprint verification system's key component is:

- a) Fingerprint sensing: A fingerprint scanner collects a person's fingerprint to create a raw digital representation.
- **b) Pre-processing:** The input fingerprint is improved and modified to make feature extraction easier.
- c) Feature extraction: After further processing, the fingerprint is used to create feature vectors, which have distinct properties.
- d) Matching: The input fingerprint's feature vector is matched to one or more fingerprint templates that have already been created.
- e) Authentication: The system unlocks itself to start offering the service when the fingerprints match and the user authenticates themselves as a legitimate user.

Benefits of the fingerprint lock and unlock system

- a. Quicker than traditional locks. It takes less time to scan your fingerprint as a credential than it does to input a passcode or use a regular key.
- b. Better protected than other types of locks. Physical keys are susceptible to theft or copying, which can compromise security. Physical keys are easier to duplicate than fingerprint credentials.
- c. More trustworthy than keys and key fobs. Traditional keys are costly to replace and can be lost. But everyone has a set of fingerprints as identification! So, if you use a fingerprint lock, you won't need to worry about replacing your keys.
- d. Less expensive compared to other biometric locks. The cost of locks that use different biometric identification methods, such as voice or iris scanning, is higher.

IV. CONCLUSION

According to the literature survey conducted on various papers, it is clear that, most of physical files use traditional method to secure them and it needs more robust approach so that the files can be kept safely. Fingerprint is proven secured approach to authenticate any system and this paper proposes to use fingerprint technique to lock and unlock the physical files. The future plans to keep physical files even more secure can be made possible by updating the file with multiple fingerprint technique around the file altering system to the owner.

REFERENCES

- K. Karu and A.K. Jain, "Fingerprint Classification", Pattern Recognition, Vol. 29, No. 3, pp.389-404, 1996.
- [2] Chenna Nithin and Dr.Fairooz, "Implementation on Banking System Using Fingerprint Module", Vol 13, Issue 04, APRIL / 2022 ISSN NO: 0377-9254.
- [3] Munish Kumar and Priyanka, "Fingerprint Recognition System: Issues and Challenges" International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887 Volume 6 Issue II, February 2018.
- [4] Atar Nasrin, Awatade Vidya, Hegadkar Rani, Bansude Vijaysinh, " Fingerprint Based Security System for Banks" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 04 | Apr-2016 p-ISSN: 2395-0072.
- [5] A. Aditya Shankar, P.R.K. Sastry, A. L.Vishnu Ram, A.Vamsidhar, "Finger Print Based Door Locking System" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 3 March 2015, Page No. 10810-10814.
- [6] Shreya Dilip Nagraj., Poonam Dejappa Pujari., Sayali Laldas Tungar., Prof: A.A.Hatkar, "Bio-Metric Based Private Locker System with GSM Technology" IJARIIE-ISSN(O)-2395-4396, Vol-4 Issue-2 2018.
- [7] Pavithra.B.C, Myna.B.C, Kavyashree.M, "Fingerprint Based Bank Locker System Using Microcontroller" Proceedings of IRF International Conference, 05th April-2014, Pondicherry, India, ISBN: 978-93-82702-71-9
- [8] Kanak Chopra and Garvit Jain, "Door Opening System based on Fingerprint Scanning" International Journal of Engineering Research & Management Technology, March- 2015 Volume 2, Issue-2, ISSN: 2348-4039.
- [9] Arkajyoti Poddar, Somrup Roy, Subhasish Raha, Kusal Thakur, Tamojit Dasgupta, Dr Saikat Maity, "Fingerprint Door Lock System with Temperature Sensor", IOCER 2020, IOP Publishing, Journal of Physics: Conference, 1797(2021) 012052 doi:10.1088/1742-6596/1797/1/012052.
- [10] Hemant Kumar, Pradeep Kumar Gupta, Divyanshu Kapoor, Gautam Rana, 1Govind Varshney, "BIOMETRIC BASED LOCKER USING FINGERPRINT", International Journal of Scientific Research and Management Studies (IJSRMS), Volume 3 Issue 10, pg: 339-344, ISSN: 2349-3771
- [11] Dilshad Mahjabeen and Moshiur Rahman Tarafder, "Unique Authentication for Door Lock system through Bio Scanning-Finger Print Security System", Global Scientific Journals. GSJ: Volume 9, Issue 10, October 2021 ISSN 2320-9186
- [12] Nathaniel Clark, "A Biometric Fingerprint Scanner with a Locking Mechanism"2011). Honors, Theses.959. https://digitalworks.union.edu/theses/959.
- [13] Ajinkya Kawale, "Fingerprint based locking system", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 899 ISSN 2229-5518
- [14] Pooja K M, Chandrakala K G, Nikhitha M A, Anushree P N, "Finger Print Based Bank Locker Security System", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org NCESC - 2018 Conference Proceedings.
- [15] Shubham Rahinj, Sarika Lohar, Tanaj Tamboli, Prof. Sushma Bhosale, "Fingerprint Based Door Lock System", Journal of Emerging Technologies and Innovative Research (JETIR), © 2022 JETIR May 2022, Volume 9, Issue 5, www.jetir.org (ISSN-2349-5162)
- [16] Nitish Kaushik and Gaurav Kumar, "Advance Security of Bike Using A Locking System with Fingerprint Scanner Key", © 2022 IJCRT Volume 10, Issue 12 December 2022 | ISSN: 2320-2882
- [17] Varun Saxena, Darshan Hiremath, Kaustav Sen, Aditya Deshpande. "Security Using Detachable Fingerprint Scanner", International Journal of Scientific & Engineering Research, Volume 5, Issue 11, November-2014 ISSN 2229-5518.
- [18] Carmelo Militello 1, Leonardo Rundo 2, Salvatore Vitabile 3 and Vincenzo Conti 4, "Fingerprint Classification Based on Deep Learning Approaches: Experimental Findings and Comparisons", Symmetry 2021, 13, 750. https://doi.org/10.3390/sym13050750

- [19] Khin Nandar, Win, Kenli Li, Jianguo Chen, Philippe Fournier Viger ^c, Keqin Li, "Fingerprint classification and identification algorithms for criminal investigation: A survey", Future Generation Computer Systems Volume 110, September 2020, Pages 758-771
- [20] Rui Zhang and Jianwei Wang, "Cogent automatic fingerprint identification system research", Journal of Chemical and Pharmaceutical Research, 2014, 6(7):442-448, ISSN: 0975-7384.
- [21] Anil K. Jain, IEEE, Salil Prabhakar, and Lin Hong, "A Multichannel Approach to Fingerprint Classification", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 21, NO. 4, APRIL 1999.