International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (online): 2347-5552, Volume-11, Issue-3, May 2023
https://doi.org/10.55524/ijircst.2023.11.3.22
Article ID IJIRD-1260, Pages 110-113
www.ijircst.org

An Improved Quality Enhancement Fingerprint Analysis

Suresh Dara[1], Sri Kavya[2], A. Naga Varalakshmi Devi[3], B. Krishna Priya[4], R. Indira Priyadarsini[5], and I. Triveni[6]

[1,2,3,4,5,6]Department of Computer Science & Engineering, PACE Institute of Technology and Sciences, Ongole, Andhra Pradesh, India

Correspondence should be addressed to Suresh Dara; darasuresh@live.in

ABSTRACT- The use of fingerprint authentication as a biometric technique for secure authentication and access control has gained significant traction in recent years. This article presents an overview of the technology used for fingerprint identification, its history, as well as the fundamental components that make up a fingerprint recognition system. We also go through the many approaches to fingerprint identification techniques and algorithms, such as the minutiae-based approach, the ridge feature-based approach, and the pattern recognition-based approach. All of these are utilized in the process of authenticating fingerprints. In addition, we emphasize the limitations of fingerprint authentication as well as the security risks that are linked with it, as well as alternative methods to overcome these constraints.

KEYWORDS- Finger Print, Authentication, Biometric Techniques, Minutiae Based Approach.

I. INTRODUCTION

An example of a biometric technology that can be used for secure authentication and access control is fingerprint authentication. It is determined by the distinctive ridges and furrows that are found on the top surface of the fingertips. The usage of fingerprint authentication is gaining more and more favor as a result of its high level of accuracy, reliability, and speed. In this article, we will present an overview of the technology used for fingerprint identification, as well as its history and the fundamental components that make up a fingerprint recognition system. In addition to this, we look at the various approaches to fingerprint recognition as well as the algorithms that are utilized for fingerprint authentication. In addition, we emphasize the limitations of fingerprint authentication as well as the security risks that are linked with it, as well as alternative methods to overcome these constraints [1].

The use of a person's fingerprints as a method of identification dates back millennia. At the tail end of the 19th century, fingerprints began to be utilized more frequently for the purpose of identification. Sir Francis Galton was the first person to demonstrate that each individual's fingerprint is distinct and that fingerprints may be used for identification. At the beginning of the 20th century, fingerprint identification started to be utilized more frequently in law enforcement. By the middle of the 20th century, automated fingerprint recognition systems had been established [2].

II. LITERATURE SURVEY

In the framework of this work, the automatic recognition of fingerprints in electronic identity documents serves as the backdrop. We investigate how the accuracy of recognition changes when a digital change is made to a fingerprint picture that was previously utilized for enrollment. Both unintentionally (for example, by the device used for acquisition or printing) and purposely (for example, by humans modifying photographs to look more beautiful), alterations can be made in a digital image. Our research demonstrates that the most advanced algorithms are resilient enough to handle certain modifications; however, other types of deterioration can have a major impact on accuracy, necessitating the use of appropriate detection methods. This calls for the use of appropriate detection mechanisms [1].

The use of biometric technology as a tried-and-true strategy for implementing foolproof identification and access management is becoming increasingly common. In order to authenticate and verify the identification of an individual, it makes use of the individual's biological attributes, such as fingerprints, iris patterns, facial features, and voice recognition. We will present an overview of the various biometric technologies that are used for secure authentication and access control, as well as examine their strengths, shortcomings, and prospective applications, here in this literature review that we are conducting.

Among all of the different kinds of biometric technologies, fingerprint authentication is one of the ones that is utilized most frequently. For the purpose of authenticating and verifying an individual's identity, it analyzes the distinct patterns of ridges and furrows that are seen on the surface of the fingertips. The verification of a user by their fingerprints is quick, trustworthy, and simple to perform. It is utilized in a variety of applications including mobile devices, access control systems, and financial transactions, amongst others. However, fingerprint authentication does have significant drawbacks, including the fact that fingerprints can be forged or spoofed, and that it is susceptible to assaults such as template attacks and replay attacks. Despite these drawbacks, fingerprint authentication is still widely used [3].

Iris Recognition: Iris recognition is yet another common form of biometric technology that is utilized for secure authentication and access control. In order to identify and verify the identity of a person, it examines the distinct patterns found in their iris. Iris recognition is widely regarded as one of the most precise and secure forms of biometric identification due to its resistance to impersonation fraud. It finds widespread application in a variety of contexts, including airport security,

border control, and access control systems, among others. Iris recognition, on the other hand, calls for specific technology and is susceptible to interference from a variety of causes, including eye disorders, advancing age, and shifting lighting conditions.

Facial Recognition: Facial recognition is a type of biometric technology that verifies an individual's identity by analyzing and comparing their unique facial characteristics to a database of known identities. It is possible to utilize facial recognition with both still photographs and video footage, and it can serve the objectives of identifying individuals as well as verifying their identities. Applications such as surveillance and monitoring systems, as well as access control systems and mobile devices, are seeing a growing demand for facial recognition technology. Facial recognition does have significant drawbacks, however, including the potential for both false positives and false negatives, as well as the fact that it is susceptible to being influenced by external factors such as lighting conditions, facial expressions, and physical alterations.

Voice Recognition: Voice recognition is a type of biometric technology that authenticates and verifies an individual's identification by using the distinctive qualities of their voice. Applications such as telephone banking, customer support, and law enforcement are some of the most common places you'll see voice recognition being employed. Voice recognition is simple to implement, does not require the user to physically be there, and can be utilized for distant authentication. Nevertheless, factors such as background noise, speech impediments, and changes in the speaker's voice can all have an impact on the accuracy of voice recognition.

Multi-Modal Biometric Systems In order to improve the accuracy and dependability of the authentication process, multimodal biometric systems combine two or more biometric technologies into a single authentication system. A multimodal biometric system, for instance, could integrate fingerprint authentication with iris recognition or facial recognition in order to verify a person's identity. It has been demonstrated that the accuracy and reliability of authentication systems can be improved by using multi-modal biometric systems. These systems can also be utilized in applications such as border control and law enforcement.

The use of biometric technology as a tried-and-true strategy for implementing foolproof identification and access management is becoming increasingly common. It provides a number of benefits, including improved accuracy, dependability, and convenience, among others. However, biometric technology also has some limits and security difficulties, such as the possibility of spoofing or forging biometric data and the vulnerability to assaults such as template attacks and replay attacks. These are only two examples of the limitations and issues that are associated with biometric technology. Researchers have come up with a number of potential alternatives, including the utilization of multi-modal biometric systems and various methodologies for liveness recognition, in order to circumvent these restrictions. Additional study is required to develop biometric technologies that are both more reliable and secure, and which are also capable of being applied in a wider variety of contexts [4].

Fundamental Elements That Make Up a Fingerprint Recognition System:

The common components that make up a fingerprint recognition system are a sensor, a feature extractor, and a matcher. These three elements work together to create the system. A picture of the fingerprint is taken by the sensor, and this picture is given to the feature extractor to be processed so that it may extract features such as the ridge patterns, the ridge ends, and the ridge bifurcations. In order to establish whether or not the fingerprint is a match for an existing record, the matcher examines the extracted features and compares them with those stored in the database.

Techniques for Recognizing Different Kinds of Fingerprints There Are: There are three primary categories of fingerprint recognition methods: those that focus on minutiae, those that focus on ridge features, and those that focus on pattern recognition [5].

The approach that focuses on minute details is by far the most popular method, and it is predicated on the detection of singular characteristics like ridge ends, bifurcations, and islands, amongst others. The ridge feature-based approach examines the fingerprint in order to determine the geometric qualities of the ridges and valleys that make up the print. The approach that is based on pattern recognition uses machine learning algorithms to identify the one-of-a-kind ridge and furrow pattern that is found on each individual fingerprint.

III. PROPOSED APPROACH

Concerns Regarding Safety and Capabilities: In spite of its high level of accuracy and dependability, fingerprint authentication suffers from a number of drawbacks and vulnerabilities. Fingerprints are susceptible to damage and alteration, which is a limitation that might have an effect on the reliability of the authentication process. There is also the possibility that some people do not have unique fingerprints due to a variety of reasons, such as traumas or skin diseases. This is another limitation. There are further security concerns associated with fingerprint authentication, including the chance that fingerprints could be forged or spoofed, as well as the system's susceptibility to assaults such as template attacks and replay attacks [6].

Alternative Courses of Action: Several different techniques have been presented in order to address the constraints and concerns regarding security that are linked with fingerprint authentication. The usage of multi-modal biometric systems, which combine fingerprint authentication with other biometric technologies such as iris recognition or facial recognition, is one approach. Another solution is to use facial recognition technology. The utilization of liveness detection methods is yet another potential answer. These methods can determine whether the fingerprint being given originates from a real or a fabricated source. In addition, cryptographic methods like encrypted hash algorithms and secure hash algorithms can be used to prevent the fingerprint data that is kept in the database from being accessed inappropriately or altered in any way.

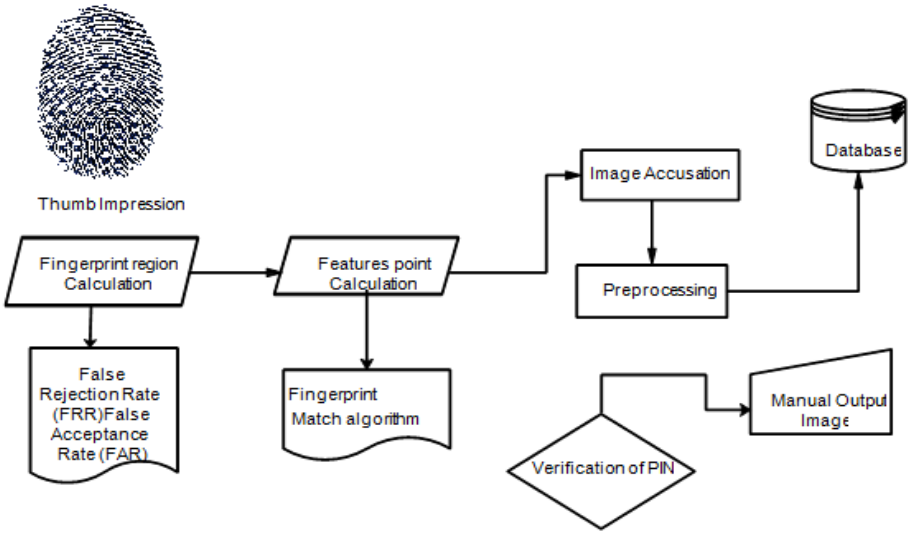

Figure 1: Proposed architecture for finger print authentication

IV. COLLECT INFORMATION AND DO RESEARCH

Collecting data in order to ensure that fingerprints are used securely for authentication and access control, the following data can be collected:

- ***Enrollment Data:*** This comprises the images of the individual's fingerprints as well as other biographical information about them, such as their name, ID number, and contact information.
- ***Authentication Data:*** This includes the images of the user's fingerprints that were recorded during the authentication process, as well as the date, time, and location of the authentication attempt.
- ***Error Data:*** This contains any problems that occurred during the authentication process, such as false acceptances or false rejections. 3. Error Data: This includes any faults that occurred during the authentication process.

Dataset: The system was tested on the FVC 2000 database [8]. The database used was developed using low cost capacitative fingerprint scanners. The database contains a total of about 800 fingerprints of 110 different fingers. The accuracy of the system is quantified in terms of false acceptance ratio (FAR) and the false rejection ration (FRR). An FAR of 1% was obtained for an FRR of 7% for this database. The Equal error rate (FAR=FRR) for the system mentioned was found to be 5% that implies an accuracy of 95%. The system can handle 180O of rotation in a fingerprint image.(see figure 2)

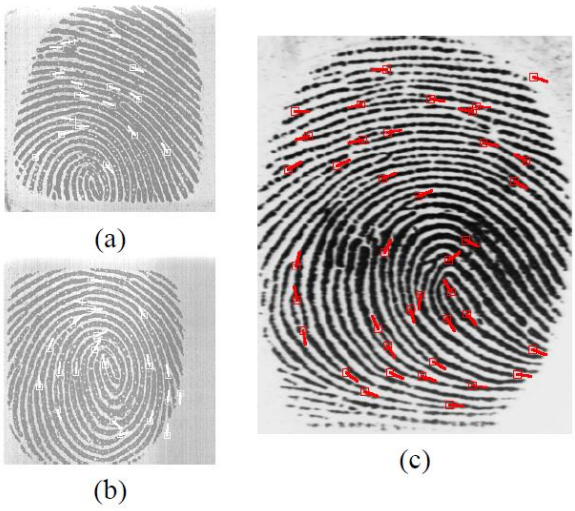

Figure 2: Fingerprint images collection using the solid state Veridicom sensor (a) (b) and the optical Digital Biometrics sensor (c).

V. RESULTS AND DISCUSSIONS

Analysis of the Data The acquired information can be subjected to the following types of analysis:

- ***Correctness of the Authentication Process:*** The correctness of the authentication process may be assessed by comparing the fingerprint pictures that were obtained during the authentication process with the data from the enrollment process. Calculations involving the false acceptance rate (FAR) and the false rejection rate (FRR) are able to be performed in order to determine how accurate the authentication system is?
- ***Performance Metrics:*** In order to determine how effective the authentication system is, it is possible to examine the performance metrics of the system. These metrics include the length of time required for authentication as well as the processing speed of the system.

- ***Error Analysis:*** The error data can be evaluated in order to determine the factors that contribute to errors and to enhance the functionality of the authentication system.
- ***Security Analysis:*** The security of the authentication system can be assessed to see whether or not it contains any flaws or weaknesses, and then measures can be taken to mitigate such vulnerabilities and weaknesses results.

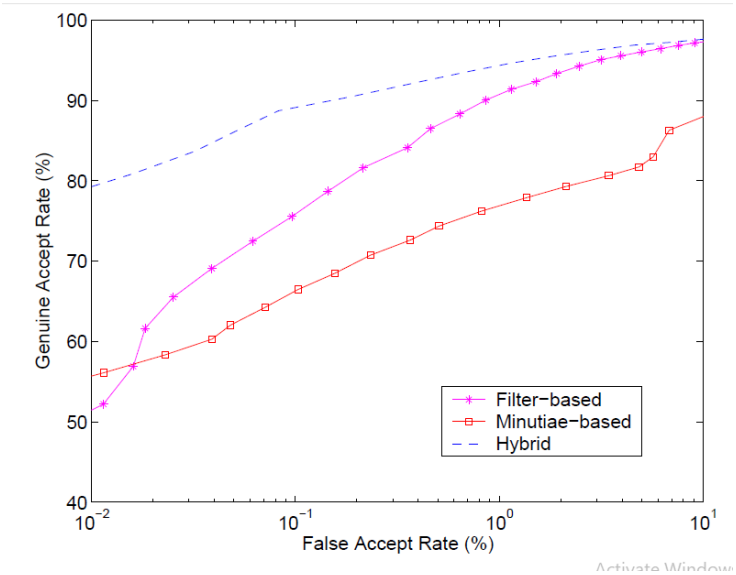

Figure 3: The ROC curve comparing the performance of the minutiae based approach with filter based approach and Hybrid approach.

For the purpose of assessing the efficiency and safety of fingerprint secure authentication and access control systems, it is essential to collect data and perform analysis on such data. It is possible to improve the system's performance and security by doing an analysis of the authentication accuracy, performance metrics, error statistics, and security analysis, and then taking the necessary steps to do so(see figure 3).

VI. CONCLUSION

The use of fingerprint authentication as a method of secure authentication and access control is a biometric technique that has seen widespread use. It is determined by the distinctive ridges and furrows that are found on the top surface of the fingertips. This article has presented a summary of the technology used for fingerprint authentication, as well as its history and the fundamental components.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Afsar, F. A., M. Arif, and M. Hussain. "Fingerprint identification and verification system using minutiae matching." National Conference on Emerging Technologies. Vol. 2. 2004.
[2] Jain, Anil, Arun Ross, and Salil Prabhakar. "Fingerprint matching using minutiae and texture features." Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205). Vol. 3. IEEE, 2001.
[3] Maltoni, Davide, and Rafiaele Cappelli. "Fingerprint recognition." Handbook of biometrics (2008): 23-42.
[4] Chugh, Tarang, Kai Cao, and Anil K. Jain. "Fingerprint spoof detection using minutiae-based local patches." 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2017.
[5] Bhargava, Neeraj, et al. "Fingerprint recognition using minutia matching." International Journal of Computer Trends and Technology 3.4 (2012): 641-643.
[6] John Berry and David A. Stoney, "The history and development of fingerprinting," in Advances in Fingerprint Technology, Henry C. Lee and R.E. Gaensslen, Eds., pp. 1–40. CRC Press, Florida, 2nd edition, 2001.
[7] Federal Bureau of Investigation, The Science of Fingerprints:Classification and Uses, Washington, D.C., 1984, U.S. Government Printing Office
[8] Http://Bias.Csr.Unibo.It/Fvc2004/, the Fingerprint Verification Competition Organization
[9] Tico, M. & Kuosmanen, P, "An Algorithm for Fingerprint Image Post processing" in Thirty-Fourth Asilomar Conference on Signals, Systems, and Computers, October 29, 2000 - November 1, 2000