INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING TECHNOLOGY AND APPLIED SCIENCES (IJIETAS)

Enhancing Data Protection through an Advanced Biometric Security Framework

Aman Kumar[1], Subrata Sahana [2] [0000-0002-9183-2237]

[1,2]Department of Computer Science and Engineering, School of Engineering and Technology
Sharda University, Greater Noida-201308, India

ABSTRACT

Data privacy has happened as a major concern for both individuals and corporations in this technologically advanced world. The persistent risk of individuality theft draws attention to the shortcomings of conventional security protocols like encrypted passwords and verified identification documents. This work offers a novel biometric security model that focuses on fingerprint identification in particular to solve the escalating cybersecurity challenges. Since each person's fingerprints are distinct, they have long been a trustworthy means of identifying themselves. Our study promotes the incorporation of fingerprint recognition into conventional password-based authentication procedures by utilizing its shown accuracy and effectiveness. Passwords and fingerprint recognition work together to protect sensitive data from theft and misuse by limiting access to it to authorized people only. The growing use of biometric data is being driven by the pressing need for strong information security. In addition to talking his dual objectives of user authentication and privacy, this study offers a thorough examination of biometrics as a viable substitute for conventional techniques. Excellent security against theft, loss, or unauthorized access is offered by biometric authentication based on a person's physical and behavioural traits. gives a thorough rundown and offers information about its advantages and disadvantages. By pointing out gaps and offering ideas for future research directions, this work supports continuing efforts to fix weaknesses in present authentication methods. In the digital age, the suggested biometric security approach is a significant step in improving data security and thwarting changing cyber threats.

Keywords: Biometric Security, Fingerprint matching, Information Security, User Authentication, Privacy Protection.

DOI:

1 Introduction

Through a careful examination of biometric security, our research study addresses the urgent need for improved information insurance in an era where mechanical walking and growing security issues are coming together. Fingerprints, facial features, iris samples, voice, and more are all included in biometrics, a computerized recognition system that takes into account exceptional natural or social characteristics. The comprehensive biometric security model dis cussed in this research aims to increase information on security by utilizing contemporary validation methods. Biometrics, including voice recognition, iris scanning, and fingerprints, provide a safe and trustworthy way to identify someone. They offer improve d security and client comfort because they are not easily lost or misused.

Nevertheless, biometrics are also susceptible to brute-force attacks, replay, and data breaches. In addition to its use in advanced criminology, A I, and criminal investigations, biometrics has grown in distinction in fields like banking and security records that demand stringent personality assessments. By demystifying the intricacies of biometric verification and its various uses, this study adds to the ongoing conversation about information security. The term biometrics, which comes from the Greek words "bios" (life) and "metrics" (measuring), refers to the automatic identification and verification of a person using distinctive biological characteristics such as fingerprints or facial features. Biometric technology has numerous uses that entail human identification and verification. Applications for authentication include timekeeping, government systems, automobile locks and ignitions, fraud prevention, and physical access control.

A. BIOMETRIC CHARACTERISTICS

The table lists common human physiological and behavioral characteristics that are used when implementing biometric systems. These characteristics have certain qualities:

- **Universality:** Each person must have characteristics that the system uses.

- **Distinctiveness:** Features must be recognizable, guaranteeing that no two people have the same qualities.
- **Performance:** Each person should have their own optimal EER.
- **Acceptability:** The system should be easy to use and the capturing process should not be laborious.

B. IDENTIFICATION OF FINGERPRINTS

Fingerprint biometrics is a very accurate way to biometric identification that depends on the complex web of valleys and ridges at our fingertips and small, unique minutiae, which are indicators. The introduction of fingerprint scanners two primary categories: contactless and touch-based optical technologies.

Commonly found on laptops, touch-based devices work Similar to digital cameras, visible light is used to record digital pictures of the fingertips. But there are problems with this approach. such as the skin's elastic deformation upon contact and use of pressure influencing the outcome. Fingerprint contactless However, scanners expose the finger to light and Examine the transmitted or reflected signals to determine the distinct fingerprint. Additionally, some systems have a layer of Detecting liveness by using the body's natural sweat as a recognizable indication of an actual finger. lenses with high magnification and Sweat on the fingertips is captured by specialist lighting equipment. calculation out if they are still alive.

C. CONTRAST AMONG VARIOUS BIOMETRIC TECHNOLOGIES

Table 1: Comparison of Biometric Technologies Based on Universality and Distinctiveness

Biometric Technology	Universally	Distinctiveness
Face geometry	High	Low
Facial thermogram	High	Low
Fingerprint	Medium	High
Hand geometry	Medium	Medium
Iris	High	High
Retina	High	High
Voice	Medium	High
Calligraphy	Low	Low

Table 2: Comparison of Biometric Technologies Based on Performance and Acceptability

Biometric Technology	Performance	Acceptability
Face geometry	Low	High
Facial thermogram	Low	High
Fingerprint	High	Medium
Hand geometry	Medium	Medium
Iris	High	Low
Retina	High	Low
Voice	Low	High
Calligraphy	Low	High

D. PRINCIPLE OF OPERATION

Based on the idea of taking precise pictures of distinctive characteristics, the most cutting-edge technologies used are silicon, optical, and ultrasonic. In the field of Two main groups of algorithms for fingerprint identification are utilized: 1. Minor detail coordination entails contrasting particular areas of the fingerprint patterns that are of interest. The enrolment procedure includes determining specific details with their position and orientation, which are subsequently contrasted with a to ascertain whether the fingerprints match using "fingerprint memory" like comparing a map to the real one, the saved template terrain. 2. Coordination of design contrasts the overall fingerprints' traits, not as if they were someone focus. Distinctive features of a finger imprint can include sub-areas of specific interesting counting edges. ebb and flow, thickness, or thickness. During enrolment, not much sections of the distinctive finger imprint and their relationship to The distinct fingerprint imprint is extracted. Zones of fingerprints are characterized by separate patterns close to minutiae, low ridge flow, and unusual combinations of edges. Systems for recognizing fingerprints store and compare distinct fingerprint information, utilizing a variety of storing techniques and compression. These methods confirm a correspondence between stored as well as scanned prints. Fingerprint readers concentrate on particular regions where ridges meet, produce loops, or form patterns, comparable to the middle "whorl" of fingerprints. These distinct traits are transformed into a code, serving as a safe identification number for the person.

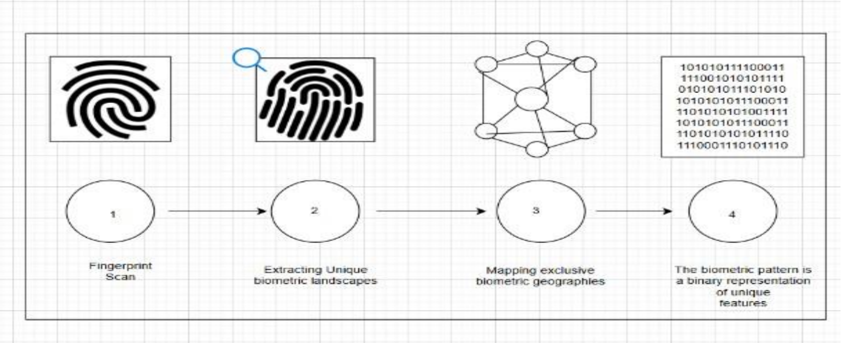
101010111100011
111001010101111
010101011101010
101010101100011
110101010100111 1
101010101100011
110101010101110
111000111010111 0
1
2
3
4
Fingerprint Scan
Extracting Unique biometric landscapes
Mapping exclusive biometric geographies
The biometric pattern is a binary representation of unique features

Fig 1: Generating binary code through finger print

II. LITERATURE REVIEW

Combining biometrics with reversible biometrics encryption, which scrambles data using a one-way transformation biometric information into a permanent format, offering an additional layer of protection in contrast to storing data in its unprocessed form. This section explores previously suggested related projects intended to at setting up a mechanism for user authentication. The method includes using fuzzy and soft biometric traits. vault plans. According to Nand kumar et al., a multi Fuzzy-Vault is a biometric template security technique. Stressing how crucial it is to protecting biometric information It cannot be restored and is irreplaceable. Protecting various templates for individuals individually is not very helpful. for concerns of security. Consequently, our suggestion offers a technique to combine many user generated templates into a one item. A two-phase plan was developed by Abhilasha et al. Federated identity management authentication method systems. In the first stage, biometric two-factor authenticating using evidence with no prior knowledge. They created biometric cryptographic keys utilizing methods from models in vector space. These secret keys make use of the benefits of biometric verification while safeguarding the confidentiality of biometric information. Sunil and colleagues created a safe Using a distinct, erasable biometric fingerprint storage technique characteristic, creating a safe feature matrix, and data encryption and decryption using cryptographic keys. A new A technique has been introduced. They presented a technique for making fingerprint-based erasable keys with the goal of overcoming the limitations imposed by traditional methods. The Combining biometrics with encryption is a characteristic of the Biometric Cryptography System, also known as the Biometric Cryptographic System. In this system, they presented the idea of biometrics that may be cancelled, which has been suggested earlier in. In, Souter et al. expected a more advanced, contemporary use of biometric keys authoritative computation with an optical connection based on a distinctive mark coordinating structure. Their computation connects a cryptographic key to the individual's images of finger impressions taken during enrolment and uses Fourier processing to compensate for special move the mark image. A channel is organized and set up. to obtain a balance between resistance to mutilation and separation of these images.

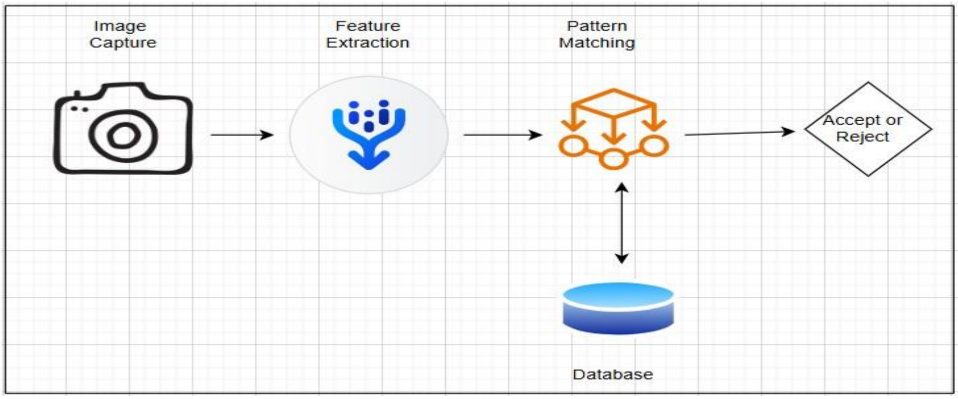

Fig 2: Biometric System

III. PROPOSED APPROACHES

The study suggests a new fingerprint based on minutiae. matching method that increases the resilience of systems for biometric security. The method makes advantage of scale resilient key extraction using the invariant feature transform (SIFT) points and characteristics from fingerprint photos that have already been processed, rendering them unresponsive to variations in rotation, scale, and illumination. This resistance to changes in entrance greatly increases the accuracy of matching, particularly in real-world situations where outside influences and sensor noise are unavoidable. Additionally, the minutiae approach produces unexpected computational effectiveness, as it employs a matcher based on furans to swiftly determine the important areas that correlate between input and saved pictures of fingerprints. This cuts down on processing time and enhances the system's scalability, enabling it to manage big datasets without compromising precision. This technique opens the door for incorporation into different security applications like mobile devices and border control validation, when quick and accurate identification is paramount. The novel fingerprint-matching system based on minutiae Biometric security has advanced significantly thanks to technology. systems, increasing their effectiveness and dependability. By maximizing the matching process and utilizing SIFT capabilities procedure, this strategy will result at a time when fingerprint based security grows increasingly robust to the actual difficulties, safeguards private data, and safeguards vital infrastructure while offering further convenience and safety for users.

A. ACTIONS TAKEN IN THE OPERATION

I. Fingerprint Image Acquisition: Acquiring photographs of fingerprints using biometric sensors or gadgets is the first stage of the biometric identification procedure.

II. Enhancing Image Quality: Improving the quality of fingerprint photos using pre-processing techniques for removing noise and correcting distortions, ensuring data that is clearer and more trustworthy.

III. Feature extraction with SIFT integration: Scale-Invariant Feature Transform Implementation (SIFT) to extract reliable descriptors and critical points from previously processed photos of fingerprints, guaranteeing ability to withstand changes in fingerprint patterns.

IV. Minutiae Point Identification: Recognizing conventional details seen in fingerprint pictures, identifying distinctive ridge features that contribute according to unique biometric characteristics.

V. Safe Matching and Quick Decision-Making: using a furan to match comparable critical areas based matcher to facilitate effective comparison and guaranteeing a secure process by setting a threshold for decision-making to ascertain positive identity.

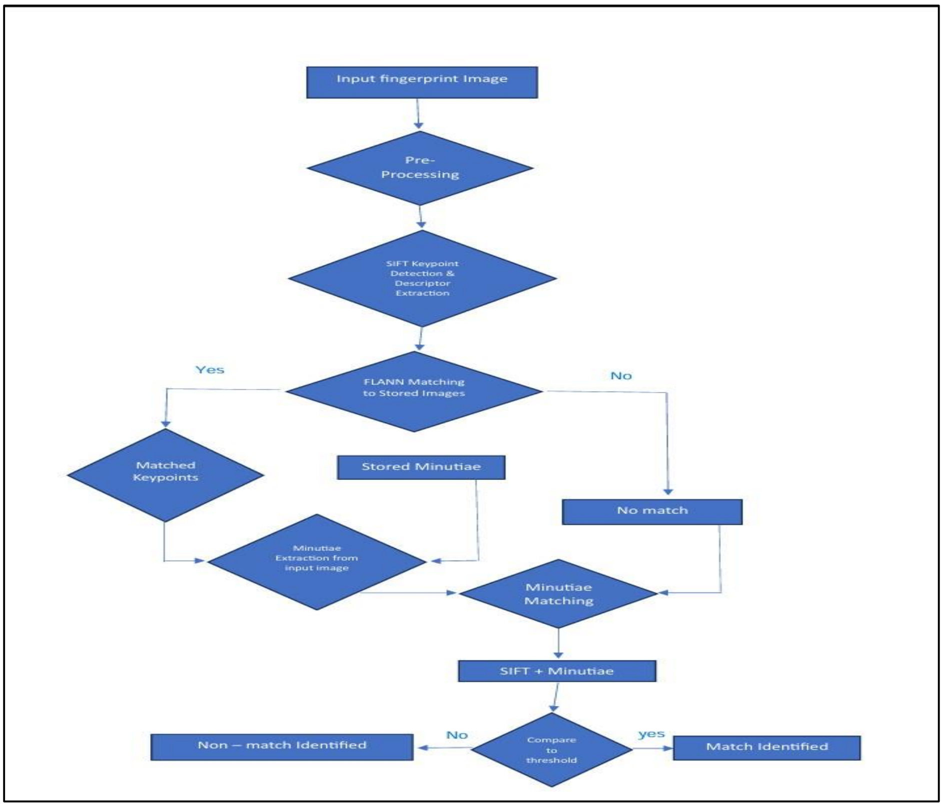

Fig 3: Flow chart showing Enhanced Fingerprint Matching

IV. IMPLEMENTATION

Reading a sample fingerprint picture is the first step in this methodology. Next, we use the SIFT (Scale-Invariant Feature Transform) technique to identify critical points and their descriptors. We next calculate the SIFT key points and descriptors for each of a set of real fingerprint photographs.

The Fast Library for Approximate Nearest Neighbours, or FLANN, is used to efficiently match the dataset's key points with the sample's key points. To guarantee accuracy, we filter the matches according to distance ratios. The ratio of genuine matches to the total number of key points found is then used to determine the match score.

We record the best match discovered and its associated score as we traverse through the dataset. When the procedure is complete, we output the fingerprint image's filename and match score that most closely resembles the sample. We use the OpenCV library to show any valid matches that are found.

In order to facilitate fingerprint identification or authentication in biometric applications, the primary goal of this solution is to determine which genuine fingerprint picture most closely resembles the sample that was supplied.

V. RESULT AND ANALYSIS

Among the outcomes of the deployment is the recognition of the authentic fingerprint picture that displays the greatest correspondence with the given sample. The SIFT OpenCV-implemented technique is used to identify important details and calculate descriptors for the sample and actual pictures of fingerprints. FLANN-based matching allows potential Key points that relate with one another are formed, and distance ratios are used to select matches.

The true fingerprint image that matches the best, coupled with its linked matching score, which is established by monitoring the greatest score during the iteration of the contest. If the matches are legitimate are discovered, the program displays the matches using the OpenCV library. In the end, the code's power resides in its capacity to determine the authentic fingerprint picture that corresponds most closely resembles the provided sample, helping to Biometric fingerprint recognition or authentication systems.

VI. FUTURE ENHANCEMENT

The approach suggested in this article represents a significant advancement in the field of biometric security, according to the methodology described above. With the addition of SIFT, or scale-invariant feature transform, and the use of a matcher based on furan, the fingerprint-based on the minutiae matching strategy exhibits a high degree of precision and effectiveness. The expectation is that, because of its due to its inherent resilience, this model will get a lot of adoption and see further developments in the future.

The scalability of the system combined with the computational effectiveness of the furan-based matcher, which puts it in a position to oversee ever-larger datasets without sacrificing accuracy. As the course of As technology advances, more improvements in Image processing and sensor technologies are anticipated to enhance the model's functionality, increasing its resistance against a range of practical difficulties. The optimal model Speed guarantees prompt and accurate recognition, but also emphasizes fingerprint-based security as a crucial element in protecting sensitive data and protecting vital infrastructure. The extent of this in the future approach applies to a variety of applications, creating an ultimate benchmark for the upcoming generation of systems for biometric identification. Its versatility and To provides the foundation for a future in which Biometric security not only satisfies but also exceeds the requirements of changing security environments, providing improved defence and practicality in a variety of fields.

VII. CONCLUSION

This research study presents a novel approach to biometric security, concentrating on the suggested minutiae-based fingerprint-matching method. It displays a technique to extract important points and descriptions using SIFT from fingerprint images, ensuring their scalability, rotation as well as changes in light. This method discusses the drawbacks of conventional minutiae-based matching, such as fluctuations in visual quality, noise, and subtle distortions. It makes biometric security systems more resilient to real-world difficulties by establishing distinctive anchors in the fingerprint landscape, guaranteeing precise identification despite details that are veiled or incrusted. The matcher based on furan increases the effectiveness of computing and makes quick and trustworthy identity, which is essential in security applications where Time is of the essence. As this strategy becomes more popular, it assures a secure environment where private data is protected by increased resilience. This stands for a ground-breaking move toward a future in which biometric protection reaches previously unheard-of levels of dependability, shielding vital information against changing dangers.

REFERENCES

1 Natgunanathan, Iynkaran, Abid Mehmood, Yong Xiang, Gleb Beliakov, and John Yearwood. "Protection of privacy in biometric data." IEEE access 4 (2016): 880-892.

2 Drozdowski, Pawel, Fabian Stockhardt, Christian Rathgeb, Daile Osorio-Roig, and Christoph Busch. "Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection." IEEE access 9 (2021): 139361-139378.

3 Sumalatha, U., K. Krishna Prakasha, Srikanth Prabhu, and Vinod C. Nayak. "A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection." IEEE Access 12 (2024): 64300-64334.

4 Gomez-Barrero, Marta, Javier Galbally, Aythami Morales, and Julian Fierrez. "Privacy-preserving comparison of variable-length data with application to biometric template protection." IEEE Access 5 (2017): 8606-8619.

5 De Lacerda Filho, Eduardo Magalhães, Geraldo P. Pereira Rocha Filho, Rafael Timóteo De Sousa, and Vinícius P. Gonçalves. "Improving data security, privacy, and interoperability for the IEEE biometric open protocol standard." IEEE Access 10 (2020): 26985-27001.

6 Bassit, Amina, Florian Hahn, Joep Peeters, Tom Kevenaar, Raymond Veldhuis, and Andreas Peter. "Fast and accurate likelihood ratio-based biometric verification secure against malicious adversaries." IEEE transactions on information forensics and security 16 (2021): 5045-5060.

7 Fu, Biying, and Naser Damer. "Biometric recognition in 3D medical images: a survey." IEEE access 11

(2023): 125601-125615.

8 Osorio-Roig, Dailé, Lázaro Janier González-Soler, Christian Rathgeb, and Christoph Busch. "Privacy-preserving multi-biometric indexing based on frequent binary patterns." IEEE Transactions on Information Forensics and Security 19 (2024): 4835-4850.

9 Dinca, Lavinia Mihaela, and Gerhard Petrus Hancke. "The fall of one, the rise of many: a survey on multi-biometric fusion methods." IEEE Access 5 (2017): 6247-6289.

10 Yan, Wenqing, Jingwei Tang, and Sandro Stucki. "Design and implementation of a lightweight deep CNN-based plant biometric authentication system." IEEE Access 11 (2023): 79984-79993.