Fingerprint Recognition System

Disha Sejpal
Student at *NMIMS Mukesh Patel School of Technology Management and Engineering*
Mumbai, India
disha.sejpal131@nmims.edu.in

Krish Shah
Student at *NMIMS Mukesh Patel School of Technology Management and Engineering*
Mumbai, India
krish.shah067@nmims.edu.in

Aditya Shah
Student at *NMIMS Mukesh Patel School of Technology Management and Engineering*
Mumbai, India
aditya.shah91@nmims.edu.in

Jesleena Gonsalves
Assistant Professor in Department of Computer Engineering at *NMIMS Mukesh Patel School of Technology Management and Engineering*
Mumbai, India
jesleena.gonsalves@nmims.edu

***Abstract*—** The abstract provides a brief study of the widely used technology that is fingerprint, discussing issues and challenges in the field. It highlights fingerprint databases and evaluation campaigns, specifically focusing on the Bio Secure Benchmarking Framework for Fingerprints. The framework utilizes the NIST Fingerprint Image Software (NFIS2) and the MCYT-100 database, employing two evaluation protocols. The abstract compares two research systems within the proposed framework, detailing their different approaches to fingerprint processing. Fusion experiments involving various combinations of these systems are discussed, and the NFIS2 software is used to obtain fingerprint scores for multimodal experiments conducted in the Bio Secure Multimodal Evaluation Campaign (BMEC'2007).

Keywords—Computer graphics, Artificial intelligence, Image recognition, Fingerprint recognition.

I. INTRODUCTION

Technology is every growing industry and fingerprint is one of the widely used user recognition patterns in the modern world and can be used in a variety of scenarios and provide a range of solutions. Some of the key advantages of using fingerprint recognition are mentioned below: -

- Everyone has a different fingerprint hence has a high level of security.
- The accuracy level of recognition is high.
- It can be used in small-sized and low-cost devices which makes it possible to be widely used in a variety of applications and devices, e.g., access control, Health care, Airport, mobile phones, Net banking, etc.

Whilst having many advantages fingerprint recognition also has a wide range of disadvantages and weaknesses in certain cases:

- The accuracy can be a huge problem, that is, if the fingerprint sensor is not maintained properly, it can continuously throw and error and lock one out of its own account/device.
- It is difficult to change a fingerprint hence ones the fingerprint is compromised it can be a huge threat to anyone.
- Factors such as finger injuries which results in the user not being able to use the fingerprint sensor is another big problem.
- Some fingerprint sensors may not as well be able to differentiate between a live finger and a fake one which causes a threat to privacy.

II. STATE OF ART IN FINGERPRINT RECOGNITION

In this section we will look at the basic introduction to how we use fingerprint system and its main parts, including a summary of the steps needed for a fingerprint recognition system.

The main process of a fingerprint recognition system are as follows:

- Fingerprint sensing: In this step the system acquired the fingerprints of an individual and creates a raw digital representation of the same.
- Preprocessing: In this step the fingerprint acquired the fingerprint and made changes to make the task of features extraction easy.
- Feature Extraction: In this step the fingerprint acquired will be further studied to identify the unique properties in it, this feature is also knowing as vectors.
- Matching: In this step the acquired fingerprint is compared with the templates which already existed. These existing templates are acquired from other clients and are usually stored in the database.

A. Fingerprint sensing:

In history the fingerprints have been acquired through pressing the fingers on ink and pressing them against a paper card. This paper card is later scrutinized and a visual representation of the point acquired is stored. This process is known as offline accession. These days it is also to take a fingerprint by keeping the fingers on flat surface. This process is known as online accession. The 3 families of detectors grounded on the technology called sensing:

- Silicon detectors: They correspond to several pixels where one is recorded pixel is a detector itself. People keep their fingers on the surface of the detector and four ways are used to change the valuable piece of information into the signal which is electrical and which are present in the electric field, also in the form of heat. The sizes of these detectors are small and they can be fluently bedded. On the other hand, these detectors are veritably precious and the sensing area for the finger detection is small.

- Optical detectors: Then the cutlet just touches the prism of the glass, where the prism is with diffused light. The light is touching the surface and bounce back at the dens and absorbed at the crests. This reflected light is farther concentrated on a CMOS detector. These types of point detectors give a good quality of images and generally, have a large seeing area. The size of these detectors cannot be changed as they've a fixed quantum of difference between the prism and the image detector.
- Ultrasound: Signals are transferred by landing the echo sounds that are bounced back at the point face. These aural signals are suitable to abate the oil painting and dirt which is on the fingers, thus furnishing high quality images. These detectors are huge and precious and may take some time to capture the acquired image. Pre-processing and point birth- A fingerprint, is composed of a pattern of crisscross crests and dens. They flow in resemblant and occasionally terminate. This pattern is classified into some of the figures called curiosities, and it can even be classified into 3 shapes which are circle, delta, and spirals. At an original position, these crests and dens may parade a particular shape called minutia. We are going to study two types of ramifications: crest ending and crest bifurcation. The utmost of the point matching algorithms uses features which are uprooted from Argentine scale images. To make this process easy and dependable, preprocessing step are performed, calculation of original crest frequency and original crest exposure, improvement of point image. The original crest exposure at a pixel position which is the angle at which the point crests form with the vertical axis. The utmost of the algorithms does not cipher the original crest exposure at each pixel but over a square meshed grid.

The ridge present which is local is the number of ridges present on the statement which is proved to be hypothetical along the length which is created at the pixel and the figures which is lying at right angles to the ridge which was local according to the orientation. The total number of ridges frequency is computed according to the grid which is meshed and square in shape.

In a fingerprint image that is acquired the ridges and valleys flow smoothly in a constant direction. However, during practice there are multiple factors that affect the quality of the acquired fingerprints image. These factors could be anything ranging from many medical conditions of the skin to the dirt present on the skin to the noise that the sensor makes. The pattern of ridges and valleys hold several shapes called singularities. After the acquired image is pre-processed, a feature extraction is performed. Several fingerprint detectors are based on matching of dens and crests so, the reliable extraction is quite needed. The already processed fingerprints is changed to binary image, the resolution of the binary image is then changed using morphology. The above step reduces the number of pixels to one pixel only. During the above step a lot of spurious imperfections can occur which needs a post-processing step to fix it.

The image changing into binary and changing of the image to make it thin suffer from various problems:

- Imperfections.
- Loss of information.
- Cost used to compute or making the image.
- Lack of copying the particular image.

III. FINGERPRINT MATCHING

The first step is to create a file containing n processes. During the fingerprint comparison process, the fingerprint which is to be tested will be compared by other fingerprints from the list of fingerprints present in the data. When comparing fingerprints, the system produces a match score or rejection decision. Various fingerprint comparison methods involve comparing the fingerprint input with small images stored in the model, and these small images are stored in grayscale. Most fingerprint algorithms use grayscale images to ensure consistency between the pattern and the grayscale image. One of the main problems in fingerprint recognition stems from the fact that different fingerprints are different sizes. These changes, collectively known as class changes, are caused by many factors, including 1) change or rotation, 2) temporary skinning, 3) interaction half-section, and 4) noise in the sensor.

The difficulty of fingerprint identification is compounded by the difficult task of comparing fingerprints, a process greatly influenced by one or more of the factors mentioned above.

Different fingerprint identification methods can be divided into two main groups:

- Relationship-based methods and detailed methods: In correlation-based methods, the input fingerprint is directly compared to the fingerprint pattern represented as a grayscale image using a correlation measure. Due to the factors which were mentioned before in the paper, the pattern of the finger which is to be checked shows different same patterns. Additionally, comparing two fingerprints is computationally expensive.
- Detail-based methods are widely accepted and have similar properties that allow forensic experts to use them when comparing fingerprints. The expansion process reveals unexpected extractions and is used in poor conditions. Fingers can also convey information because there are ridges and valleys determined by local orientation. Although informative information is less distinctive than detailed information, it can be more reliable than detailed information in some cases.

IV. CURRENT ISSUES AND CHALLENGES

The recognition which is effective depends on the fingerprint depends on the condition of the image of the fingerprint. Fingerprint quality is affected by many conditions such as skin inflammation and sensor pain. Insufficient images will reduce the overall recognition process. Depending on its quality, we can choose to estimate the quality of the fingerprint recognition or rejection system. Due to cost effectiveness and reducing the size of fingerprints, many devices now include fingerprints, including but not limited to mobile phones, PC peripherals. However, the use of small detectors in the limited space of fingerprint data leads to minimal overlap between connections of the same fingerprint. This limitation affects authentication performance. While some fingerprint sensors use mechanical instructions to calibrate fingerprints, other techniques involve taking multiple fingerprints during registration. This facilitates the collection of partially overlapping data, allowing the fingerprint image to be reconstructed.

V. FINGERPRINT SYSTEM COMPARISON

In this comparison table below, the table gives us an important difference between fingerprint recognition, facial recognition and iris recognition based on the environmental factors, contact required or not, accuracy and many other factors.

Aspect	Fingerprint	Facial	Iris
Biometric Feature	Unique fingerprint	Facial features	Unique iris pattern
Accuracy	High	Moderate to High	Very High
Ease of Use	Convenient	Convenient	Convenient
Speed	Fast	Fast	Fast
Contact requirement	Contact	Non-contact	Non-contact
Environmental	Dirt and moisture	Lighting conditions	Stable across

Fig 1 Comparison of fingerprint, facial and iris systems

VI. NIST MINUTIAE INTEROPERABILITY EXCHANGE TEST

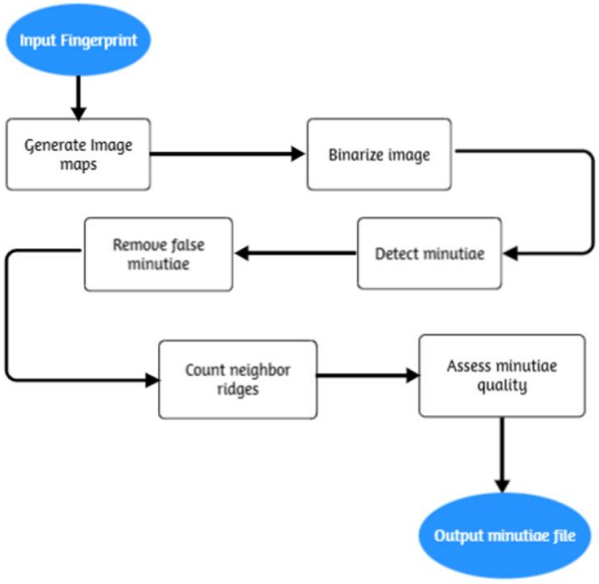
The primary reason of the NIST Detail Interoperability Exchange Test (MINEX) is to test how to use detail data to exchange fingerprint data between multiple fingerprint scanners. This test is designed to measure the number of changes in identification accuracy when using detail data from different systems for fingerprint matching. The interaction between templates is affected by the content of the coding scheme and the specific matchers used for template matching.
There are many ways to describe the process of finding, extracting, formatting, and comparing details from fingerprints. The information used in the evaluation consists of images from several sensors, including both the one which can see the live sample and which is not live scan roll representations and different types. Latent fingerprints were removed from the database.

Key findings from the MINEX evaluation include:
- The design has better performance compared to ANSI INCITS 378-2004 templates.
- Different models of different generators and competitors do not always come first in matching and repeating service providers from the same generation.
- By replacing one vendor's renderer template with another vendor's renderer.
- Sensitivity of the method's performance to the quality of the dataset; better data drives appropriate interactions, while lower quality data does not.

VII. FINGERPRINT MATCHING USING BOZORTH3 ALGORITHM

The BOZORTH3 matching algorithm is designed to calculate the match score of details of a pair of fingers to determine their origin from the same finger. This mapper shows rotation and interpretation differences using positional information and orientation of detail points, specifically for finger comparison.
The algorithm can be compiled from the following three methods:

a) Create two tables comparing fingerprints, each for one of the two fingers.
b) Development of the matching table of fingers.
c) Calculate the comparison score using the comparison of fingerprints.



VIII. PAIRING OF MINUTIAE

It is a technique for fingerprint recognition by pairing minutiae, the unique fingerprint features. Inspired by triangular matching, the method involves forming triangles with corresponding minutiae. Additional attributes, like distance and angles, are calculated for each minutia. Pairs of minutiae are chosen based on local similarities, focusing on those with a shared minutia. Verification of neighbors using closing angles helps identify corresponding minutiae pairs, forming equivalent triangles in both fingerprints. The most connected pair, along with its associated neighbors, is then stored in a pairing list for subsequent fingerprint matching.

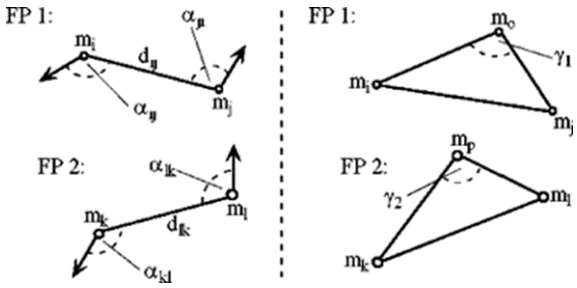


Fig 3 The above diagram shows the calculation of triangles to establish correspondence between two fingerprints.

IX. FINGERPRINT RECOGNITION

In the process of fingerprint recognition, the paragraph discusses how two fingerprints are aligned globally. This alignment is treated as a rigid transformation, meaning it involves only translation and rotation. The parameters for this transformation are calculated using established pairs of minutiae. The translation parameter is determined by the subtraction in the position of the vectors for the first pair of minutiae and the parameter which is rotated among the vectors while connecting the first pair to other minutia pairs. After estimating these efficient factors, representation of coordinates is applied to several points in linear symmetry. Notably, no additional refinement, such as fine adjustments, is carried out during this alignment process. The

primary focus is on aligning the fingerprints globally for subsequent analysis, considering only translation and rotation.

X. MATCHING OF FINGERPRINTS:

In the final step, a straightforward matching process is conducted using normalized correlation at various locations on the fingerprints. Small areas around the identified minutiae points in the fingerprint which was represented are correlated with areas which corresponded in the fingerprint which was marked second. The areas only with a symmetry which is linear and is average too holds a specific threshold which is considered, keeping it well-defined regions of fingerprints, which are present only for comparison. The ultimate score of matching of fingerprints is determined by the value which is average of all the similarity values obtained from comparison of various fingerprints.

XI. UPM

The UPM Ridge-based Fingerprint Verification System uses special features to compare the fingerprint ridges. The fingerprint image is divided into small pixels, and variation in the responses caused by features among these pixels form a feature vector called Finger Code. This system has an automatic alignment process based on correlation, determining the optimal offset between Two Finger Codes. The UPM ridge-based matcher involves two main steps: extracting the Finger Code and then comparing or matching these Finger Codes.

Under UPM two methods must be done.
Extraction of Feature Code: To create the Finger Code, the system uses three steps. First, it applies eight special filters called Gabor filters the fingerprint image. Then, it divides the filtered images into equal-sized squares. Finally, for each square in each filtered image, it calculates the variation in pixel intensities. These variations, known as standard deviation values, make up the Finger Code for the fingerprint image. It is worth mentioning that no efforts are made to enhance the image because Gabor filters are good at capturing specific information and are not easily affected by noise. You can see an example of this process in figure below.

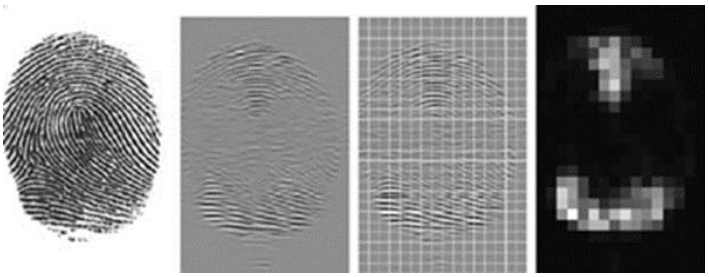


Fig 4 Example of how the fingerprint process works

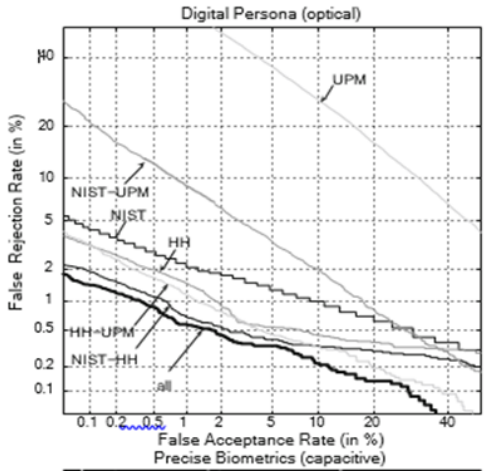
Matching of Finger Codes:

- Alignment: Making sure the two fingerprints are in the right position.
- Similarity Calculation: Figuring out how similar the Finger Code are.

The system calculates a score based on how different the Finger Code is to align the fingerprints, it uses a method that looks for the best match between corresponding parts. However, it does not consider rotations between fingerprints. For the database used, typical rotations are handled by the tessellation method.

XII. RESULTS

The experiment looked at different fingerprint recognition systems to see how well they work. They tested systems that focus on specific fingerprint points (minutiae) and others that look at the whole fingerprint pattern (ridge). They found that systems using minutiae (like specific points on a fingerprint) work better. Also, cameras that take better pictures (optical cameras) did a better job than others (capacitive cameras). Among the methods tested, the HH algorithm stood out as the best. It is like a smart filter that pays attention to specific details in fingerprints. On the other hand, methods like the NIST algorithm, which use a binary approach, did not perform as well. They lose some details and add unnecessary points. Making sure the pieces of the fingerprint fit together well (alignment) is crucial. The HH algorithm does this cleverly, making it more accurate. Matching fingerprints is like solving a puzzle. The HH algorithm does this well, combining accuracy with a clever way of comparing fingerprints. In the end, they noticed that systems made by companies tend to work better than those made by schools. Companies put extra effort into making their systems work well. In summary, focusing on specific points in fingerprints, especially with methods like the HH algorithm, works the best. The type of camera and how well the system is fine-tuned also play a big role.



Some results are shown in the form of graphs:

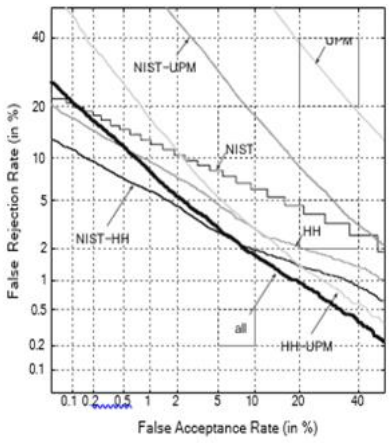


Fig 5 Verification performance of individual systems

XIII CONCLUSION

The study conducted experiments using the database, which contains images of the fingerprints from both sensors one which is optical and other which is capacitive. Three different fingerprint recognition systems were tested, each employing distinct features such as checking the alignment of the fingerprint and matching it with different databases and the feature extraction which is important. The investigation also explored combinations of these systems using simple fusion methods. Several key findings emerged from the experiments. The study confirmed the discriminative power of minutiae, the specific points in fingerprints. It highlighted that incorporating additional information such as higher-order matching of crests and dens, the orientation which is locally present, and ridge features enhances performance, particularly for low-quality fingerprints. Among the tested algorithms, the HH algorithm stood out as the best performer. This algorithm not only combined minutiae-based correspondence and correlation-based matching but also employed complex filtering for minutiae extraction, avoiding information loss associated with binarization. When combining different systems, the study observed that using only two systems which resulted in changes in performance improvement which is again contrasted to including a third system. While the patterns of three systems produced the best Equal Error Rate (EER) for the optical sensor, the study emphasized that its goal was not achieving a perfect verification rate but rather showcasing the benefits of combining different methods within the same modality. The study found that the best pattern of two or three systems consistently included the best of the individual patterns. However, the study acknowledged that the output of individual patterns could be affected by different factors such as the database. This realization prompted the researchers to extend their hands on to different databases and explore different patterns to develop more compact fingerprint recognition systems.

REFERENCES

[1] V. Mehta, J. Tiwari, and J. Shaji, “Face Recognition- Advanced Techniques,” International Journal of Engineering Research & Technology, vol. 8, no. 7, Jul. 2019, doi: https://doi.org/10.17577/IJERTV8IS070178.

[2] Agung, “Impact of Algorithms for the Extraction of Minutiae Points in Fingerprint Biometrics”, J. Comput. Sci., vol. 8, no. 9, pp. 1467–1472, Sep. 2012.

[3] R. K. Y. Chin and J. F. Lim, “Fingerprint Recognition Using a Hybrid of Minutiae- and Image-Based Matching Techniques”, Int. J. Simul. Syst. Sci. & Technol., Apr. 2020. https://doi.org/10.5013/ijssst.a.15.02.07

[4] D. T.Meva, C. K. Kumbharana, and A. D. Kothari, “The Study of Adoption of Neural Network Approach in Fingerprint Recognition”, Int. J. Comput. Appl., vol. 40, no. 11, pp. 8–11, Dec. 2012. https://doi.org/10.5120/5007-7326

[5] J. Rajharia and P. C. Gupta, “A New and Effective Approach for Fingerprint Recognition by using Feed Forward Back Propagation Neural Network”, Int. J. Comput. Appl., vol. 52, no. 10, pp. 20–28, Aug. 2012. https://doi.org/10.5120/8239-1492