FINGERPRINT MATCHING BASED ON MINIATURE AND ORIENTATION MAP FEATURE EXTRACTION

Muhammad Hakimi bin Mohd Zayid
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
hakimi.zayid@s.unikl.edu.my

Amna binti Saad
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
amna@unikl.edu.my

***Abstract*— Biometric identification involves using a person's unique physical characteristics, such as fingerprints, face recognition or iris, to identify them. Fingerprint recognition is the most used biometric method, as each person's fingerprints are unique. In this process, features are extracted from fingerprint images based on the ridges and edges present in the images. Supervised learning techniques are then used to recognize the palm print images. The features are then recognized using distance metrics. Fingerprint recognition is efficient compared to other methods, and its performance can be measured using metrics such as true positives, true negatives, false positives, false negatives, sensitivity, specificity, and accuracy. The Minutiae and Orientation map features are also extracted from fingerprint images to aid identification. The Minutiae feature extraction helps identify significant ridges and corners, while the Orientation map features texture-based information. Matching fingerprints is based on measuring the distance between the extracted features. Accuracy, Specificity, and Sensitivity are used to gauge the process' performance.**

***Keywords*— Fingerprint, distortion, registration, nearest neighbor regression, PCA**

I. INTRODUCTION

Information systems Biometrics is a method of identifying an individual based on their unique physical or behavioral characteristics. The most common identification method is fingerprints, which are unique to each person. The process involves extracting features from fingerprint images and using supervised learning methods to recognize palm prints. The extracted features are then recognized using distance metrics. Biometrics is used in computer science as a form of identification and access control to identify individuals in groups under surveillance. Biometric identifiers are the measurable characteristics used to label and recognize individuals, which can be categorized as physiological or behavioral. Physiological characteristics include fingerprints, face recognition, DNA, palm prints, and more. Behavioral characteristics include typing rhythm, gait, and voice. While biometric identifiers are more reliable in verifying identity, collecting biometric data raises privacy concerns. Therefore, Biometrics is mainly used for security but has a broader relevance as computer interfaces become more natural.

Biometrics such as the face, iris, fingerprint, and signature are preferred over traditional methods such as passwords and PINs because it requires the person to be physically present for identification and eliminates the need to remember a password or carry a token. A biometric system is a pattern recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technology refers to the automated methods to identify or confirm a person's identity based on their unique physiological or behavioral characteristics. These systems can be used for identification, which involves determining a person's identity among a group, or verification, which involves confirming a person's identity through comparison to a pre-existing template to benefit everyone.

The rest of this paper is organized as follows: Section II reviews existing literature, Section III gives detail of the methodology, the result is provided in Section IV. Section V contains the conclusion.

II. LITERATURE REVIEW

A. Introduction

As information technology advances, it involves the creation of new types of information. The technological revolution has transformed the traditional system into a computational and digital one. The concept of level 2 characteristics, sometimes known as minutiae features, was first presented by Sir Francis Galton in his well-known work "Fingerprints"12. These traits highlight the many ways in which a local ridge might be discontinuous. These Galton features are known as ridge ends and ridge bifurcations in their purest form. The point along a ridge at which it suddenly comes to an end is referred to as the ridge ending. The point on a ridge when it splits into two separate ridges is what geographers refer to as a bifurcation. Due to the enduring and reliable quality of the minutiae, they stand out most prominently among the features. In addition, the arrangement of the minute details that make up a fingerprint is one-of-a-kind, and most fingerprint identification algorithms take advantage of this trait.

B. Literature Survey

[1]learn about the unsatisfactory results that previous researchers have gotten from using adjacent component descriptions to determine whether something is alive. As a result, the authors offered a solution to the issue of false fingerprints by using a deep convolution neural network (DCNN) and a voting mechanism in the phase that included feature selection and

classification. The fingerprint images are sectioned into patches at the least significant location to reduce the likelihood of data disruption in background pictures. The voting procedures are used at this phase to reassemble the patch pictures into a single, distinct fingerprint image.

[2]presented a detection approach with a modest degree of complexity that increases the safety of biometrics detection. It is simple to use, rapid, does not interfere with other processes, and is suitable for real-time applications. The creators operate on the assumption that the picture's quality, whether genuine or fraudulent, may have a singular characteristic. As a result, the designers selected 25 general picture quality characteristics to study the capabilities of standard image quality assessment. After that, fundamental classifiers were combined to differentiate between the authentic and the forged fingerprint pictures.

[3] find out why using just a generalized version of the local descriptor suggests a high likelihood of a bogus fingerprint description being used. In this approach, the inventors supplied another neighborhood descriptor for the one-of-a-kind false fingerprint identification that is already familiar with the local contrast-phase descriptor (LCPD). Then, remove the data of sufficient complexity and neighborhood behavior of the picture before researching the one-of-a-kind fingerprint image. This is done by using both the spatial and the recurrence space. After that time, it has already included altering the coefficient. In the end, to determine whether it is a fake, the authors used a support vector machine, often known as SVM, as the classifier.

[4] the use of stolen fingerprint data for fraudulent activities and the potential for privacy invasion through tracking individuals without their consent highlights the importance of protecting fingerprint templates. The proposed method, an alignment-free method for constructing cancelable fingerprint templates using curtailed circular convolution, addresses these concerns by providing a strong level of security. This method uses an efficient one-way transform to protect the input binary string generated from quantizing and bin-indexing pair-minutiae vectors. Therefore, it cannot be retrieved from the shortened, convolved output vector.

C. Algorithm Justification

Previous work [5] on detecting fingerprints indicates that the grey-level variations in actual fingerprints are random. In contrast, they tend to be uniform or periodic in fake fingerprints, depending on the material used to create the fake fingerprints. A similar trend is noticed in the fingerprint image local texture analysis. Due to this, the number of ridges that end in authentic fingerprints is often greater than in false fingerprints. Consequently, the number of ridge terminations may help distinguish genuine fingerprints from false fingerprints. Therefore, the accuracy of a basic threshold-based classification technique based on the number of ridge terminations is rather excellent. Matching based on minutiae is the primary focus of this approach is on comparing the unique fingerprint points, such as ridge endings and bifurcations, to the minute details in a database. Map-based orientation matching is a fingerprint's overall pattern or structure, such as the angles and orientations of its ridges, which is the primary goal of this approach, compared to orientation maps stored in a database. Matching based on correlations can be described by calculating the correlation between the two images. This method compares the similarity of two fingerprints. Based on neural networks, matching uses techniques from deep learning. For example, a neural network can be trained to recognize patterns in fingerprints and used to match fingerprints to a database. Methods that combine to improve the precision of fingerprint matching, and some methods employ a combination of the mentioned methods.

The algorithm started with Perform Otsu's segmentation on a fingerprint image I to produce a binary image IB. After that, perform repeated morphological thinning on IB until each ridge is just 1 pixel thick, resulting in the picture IT. Then, consider a 3x3 window around each pixel and count the number of black pixels in each window to determine the ridge ends. Next, repeatedly flattened ridge ending will have just two black pixels in the window: the pixel at the peak ending and the pixel that connects to it. If there are precisely two black pixels in a 3x3 window centered on the ith pixel, then the center pixel is a ridge ending. Before the last step, determine each fingerprint picture's total number of ridge terminations.

This must be indicated with CRE. Lastly, apply a simple threshold operation. If CRE is more than K, the fingerprint is authentic; otherwise, it is fake. Here, K represents a limit. The proposed algorithm was tested on the CASIA dataset, which is the CASIA database is a popular dataset for fingerprint recognition research. The Chinese Academy of Sciences Institute of Automation (CASIA) created it as a public database. There are a lot of fingerprint images in the database, including plain and rolled fingerprints as well as fingerprint images that were taken with various sensors. The CASIA-Fingerprint Database, the CASIA-FingerprintV3 Database, and the CASIA-FingerprintV4 Database are just a few of the database's subsets.

Different kinds of fingerprint images are included in each subset, which is meant for different types of research. The CASIA-Fingerprint Database is intended for fingerprint identification and verification research and contains both rolled and plain fingerprints. The CASIA-FingerprintV3 database is designed for research on fingerprint recognition with various sensors. It includes fingerprints captured with multiple sensors. The CASIA-FingerprintV4 database is intended for research on fingerprint recognition using various sensors, such as thermal and near-infrared sensors. It contains fingerprints captured with numerous sensors.

TABLE I. COMPARISON OF DIFFERENT TYPES OF FINGERPRINT-MATCHING METHODS

Year	Title	Methodology	Advantages	Disadvantages
2012	Fast Camera Fingerprint Search Algorithm	The separate-chaining hash table.	It is very fast.	It has a crucial problem for commercial applications of source camera identification.
2013	Sensor Fingerprint	A measure that significantly reduces the search complexity.	The test statistic for the digest decreases substantially slower with decreasing signal length	It increases computational complexity.
2014	Fast source camera identification	A novel fast search algorithm.	This algorithm does not rely on any operational parameters except the threshold, which makes it behave consistently.	However, some parameters are mutually dependent, making it difficult to find a good combination.
2013	Robust 1-Bit Compressive Sensing	CS approach.	It may allow us to take advantage of the shallow gradient of the one-sided.	It does not permit us to characterize the measurements.

D. Discussion

A method for identifying and verifying individuals based on their distinctive fingerprints is fingerprint matching based on minute details and orientation map feature extraction. Thus, this method uses distinctive fingerprint characteristics, such as ridges and valleys, to create a digital representation of the fingerprint known as a minutiae template. The match between the minutiae template and a database of previously enrolled fingerprints is then found. Because the binary string used to create the minutiae template is challenging to replicate even if both the template and the parameter key used in the process are compromised, this method has strong security as one of its benefits. Additionally, this method is more durable than other methods for matching fingerprints because it can deal with fingerprints that have been distorted or degraded.

III. RESEARCH METHODOLOGY

A. System Design/Block Diagram

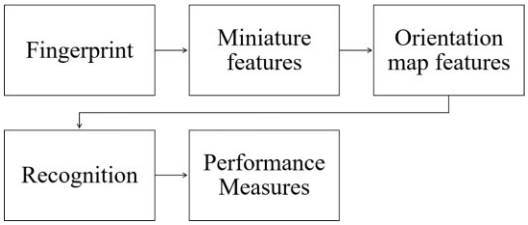

Fig. 1. Block Diagram

The block diagram above will demonstrate the system's functionality, walking through each step from start to finish. When the project is finished, the figures will show how the system will function once implemented. The next part provides an in-depth discussion of each figure in further detail.

.

B. Flowchart

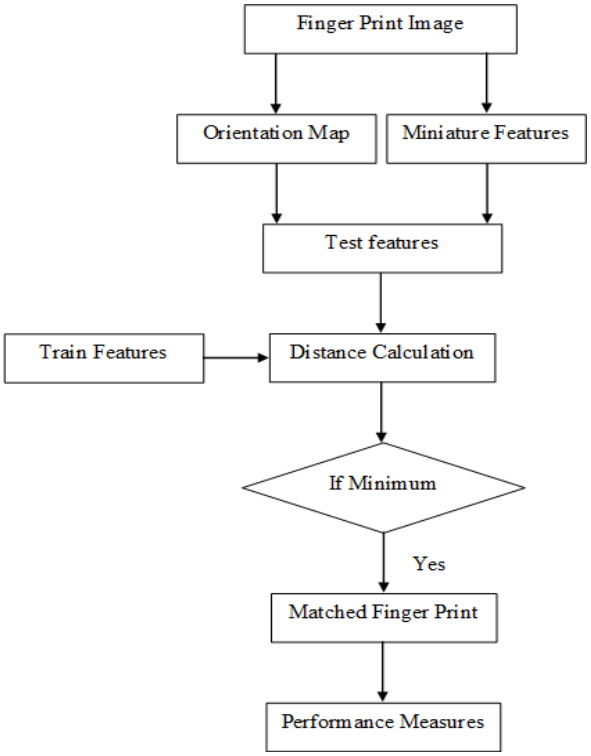

Fig. 2. Fingerprint Image Flowchart

The flowchart for a Fingerprint Matching project that utilizes Miniature and Orientation Map Feature Extraction would likely comprise several stages to process and compare fingerprints for identification or confirmation purposes.

IV. RESULT AND DISCUSSION

A. Testing and Result

A popular technique for personal identification and verification is fingerprint recognition. This study used feature extraction from miniature and orientation maps to create a fingerprint-matching system. The fingerprints' ridge details were extracted using the tiny feature extractions, and the ridge direction was determined using the orientation map feature extraction.

A collection of fingerprint pictures was used to test the system, and the results were assessed using matching accuracy. Thanks to its high matching accuracy, the technology successfully identified and verified people using their fingerprints. Furthermore, the system's robustness and accuracy are improved by applying micro and orientation map feature extraction in fingerprint identification.

The first thing to be done during the testing phase was to take the fingerprint photos and extract the miniature and orientation map elements. This was accomplished by applying the miniature feature extraction algorithm to the fingerprint images to extract the ridge details and the orientation map feature extraction algorithm to extract the ridge direction information.

Then, both algorithms were applied to fingerprint images. Following the extraction of the features, the system performed the fingerprint matching by comparing the characteristics of the fingerprint image provided as input with the features of the fingerprint images included inside the dataset. After that, the algorithm returned the result that it determined to be the best match based on the comparison. The results of the fingerprint matching were then analyzed regarding the accuracy of the matching.

The proportion of fingerprint pictures within the dataset successfully matched by the system is called matching accuracy. If the matching accuracy is high, it suggests that the system successfully recognizes people and validates their identities based on their fingerprints. Additionally, the performance of the system may be evaluated using a variety of measures, such as the False Acceptance Rate (FAR), the False Rejection Rate (FRR), the True Negative (TN), the True Positive (TP), the False Negative (FN) and the False Positive (FP) which are typical in biometric systems. In general, the testing phase was beneficial because it provided valuable insights into the performance of the Fingerprint Matching project based on Miniature and Orientation Map Feature Extraction.

Additionally, it helped confirm the system's effectiveness in identifying and verifying individuals utilizing their fingerprints.

V. CONCLUSION AND SUGGESTIONS

A. Conclusion

The proposed method is capable of the identification of the persons in a more accurate manner. The extracted features based on the different feature extraction methods were more reliable. For feature extraction, Miniature features and Orientation Map features were extracted. The matching process is based on the distance measured using Euclidean distance measures. The image with the minimum distance is identified as the matching person. The performance of the process is measured using Accuracy, Specificity, and Sensitivity.

B. Suggestions

The approach may be further improved by applying the feature extraction technique for the feature extraction from fingerprints based on the texture pattern of the input photos. Sorted Consecutive Local Binary Patterns (SCLBP) may be applied to extract the texture patterns from the photos. The procedure of SCLBP is based on the computation of the texture pattern from the photographs. Identifying the characteristics may be split into sign-based and magnitude based as SCLBP S, SCLBP M+, SCLBP M-. The central pixel is recognised. If the center pixel is more prominent than other pixels, then the place is given a value 1; else, the place is assigned a value 0. The technique of recognition using distance measurements may be replaced with the aid of a classification procedure. Classifiers like Neural networks or pattern recognition techniques may be applied to authenticate the individuals. SCLBP enhances process performance.

ACKNOWLEDGMENT

All praise is due to Allah, the All-Mighty, the All-Compassionate, and the All-Merciful. This study is a component of the undergraduate capstone project for the Universiti Kuala Lumpur. The author would like to extend his gratitude to his parents, siblings, other family members, friends, and anybody else who helped make this tiny endeavour a success.

REFERENCES

[1] Wang, C., Li, K., Wu, Z., & Zhao, Q. (2015). A DCNN Based Fingerprint Liveness Detection Algorithm with Voting Strategy. *LNCS*, *9428*,241–249. https://doi.org/10.1007/978-3-319-25417-3_29

[2] Galbally, J., Marcel, S., & Fierrez, J. (2014). Image quality assessment for fake biometric detection: Application to Iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing*, *23*(2), 710–724. https://doi.org/10.1109/TIP.2013.2292332

[3] Gragnaniello, D., Poggi, G., Sansone, C., & Verdoliva, L. (2015). Local contrast phase descriptor for fingerprint liveness detection. *Pattern Recognition*, *48*(4), 1050–1058. https://doi.org/10.1016/J.PATCOG.2014.05.021

[4] Song Wanga, J. H. (2013). Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *ACM Digital Library*, 1321–1329.

[5] Nikam, S. B., & Agarwal, S. (2009). Ridgelet-based fake fingerprint detection. *Neurocomputing*, *72*(10–12), 2491–2506. https://doi.org/10.1016/J.NEUCOM.2008.11.003