High-Density Grid Segmentation Matching Versus Global Matching

Ian Wilson
dept. College of Sciences (of Aff.)
California State Univ., Fresno (of Aff.)
Fresno, California
ianwilson2@mail.fresnostate.edu

Jonathan Garza
dept. College of Sciences (of Aff.)
California State Univ., Fresno (of Aff.)
Fresno, California
jonathangarza559@mail.fresnostate.edu

Marlon "Zeke" Branham
dept. College of Sciences (of Aff.)
California State Univ., Fresno (of Aff.)
Fresno, California
zekebranham@mail.fresnostate.edu

***Abstract*—This paper proposes a novel approach to fingerprint matching through a High-Density Grid-Based method. Our algorithm segments a fingerprint into grids, calculates minutiae density in each, and focuses on High-Density Grids for enhanced matching efficiency. Our algorithm specifically focuses on grids with above-average minutiae density, within which it employs advanced techniques involving minutiae triplets. This focus on minutiae triplets in high-density areas not only refines the detection and matching of fingerprint features but also significantly improves the efficiency and effectiveness of biometric systems.**

I. Introduction

Fingerprint authentication remains a pivotal element in biometric security, with the integrity of minutiae matching critically influencing system efficacy. Traditional minutiae matching techniques, while robust, often struggle with the challenges posed by partial prints and varying fingerprint qualities. These challenges necessitate advancements that not only enhance accuracy but also optimize computational efficiency.

In reviewing fingerprint recognition models, mostly all methods involve storing an entire fingerprint for matching. This being a template of fingerprint data, for example, uses an entire fingerprint to store during enrollment. Methods like matching global and local structures as proposed in [5], using local structure similarity [9], and point-pattern matching [4]. In all the methods we reviewed and learned from, we found that these methods are increasingly more effective with speed when they are computing less data and more accurate when using more extensive data extraction processes. We saw this as a potential hurdle in identifying situations with a database as large as the adult males within the East Los Angeles area, or within a worksite that holds thousands of employees.

Our project introduces an innovative high-density grid-based fingerprint-matching algorithm for identification purposes that strategically divides the fingerprint into grids, assessing each for minutiae density. This approach allows for a targeted analysis where only grids exhibiting higher than average densities—areas most likely to yield distinctive minutiae configurations—are processed further. This refinement is critical, as it reduces computational overhead by focusing efforts on the most information-rich sections of the fingerprint.

Central to our method is the novel application of minutiae triplets within these high-density grids. By analyzing sets of three minutiae, our algorithm enhances the precision of matching by establishing more complex local structures that are robust against common distorting factors such as rotation and translation. This method not only builds on the traditional uses of ridge ending and bifurcation but also introduces a more nuanced approach to capturing the uniqueness of each fingerprint.

In essence, this report details the design and implementation of our grid-based algorithm, discusses its integration with advanced minutiae triplet techniques, and presents a comparative analysis with existing methods. The aim is to demonstrate a measurable improvement in both accuracy and processing speeds, supporting the feasibility of this method for real-world applications in biometric security systems.

II. Methodology For Division into High-Density Grids

A. Grid Segmentation

Our algorithm begins by segmenting the fingerprint image into 80x80 pixel grids. This segmentation size was selected to balance between resolution and computational efficiency, providing a sufficient area to detect significant minutiae while maintaining manageable data sizes for processing. The segmentation process involves a systematic division of the fingerprint area, ensuring that each section is analyzed independently.

In cases where grids fall on the edges of the fingerprint or in areas with less density, our algorithm dynamically adjusts the grid sizes to smaller dimensions. This flexibility in grid sizing is crucial for maintaining the integrity of feature extraction, particularly in regions where a standard grid might extend beyond the useful boundary of the fingerprint image.

B. Minutiae Counting within Grids

Within each grid, our primary focus is the detection and counting of two key types of minutiae: bifurcations and terminations. Bifurcations are points where a fingerprint ridge splits into two branches, while terminations are where a ridge ends. Counting these features within each grid allows us to assess the minutiae density, which is pivotal for identifying High-Density Grids.

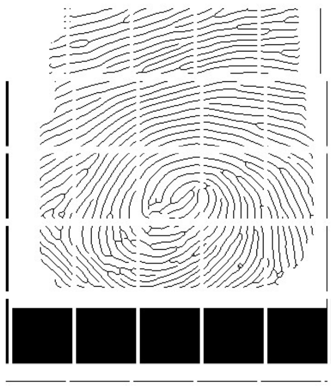

Fig. 1. Example of Segmented Enhanced Fingerprint after singularity centering. The black boxes and lines are the self-centering/resizing components of the algorithm, ignored during later calculations.

Given that the grids are fixed, this presents an issue when a finger is not placed in the exact same position as the enrolled template, an example of this would be a finger that is slightly angled or translated in reference to the scanner, the location of the high-density grids could vary significantly affecting future identification. To combat this, after the skeleton fingerprint image undergoes singularity detection, the image is then centered around the detected singularity prior to minutiae coordinate extraction.

The minutiae are detected using a combination of image enhancement techniques [8] including normalization, segmentation, skeletonization, and singularity detection, followed by a global analysis of the enhanced image's minutiae coordinates by using line-scan minutiae detection techniques. Each grid's minutiae count is then tallied, providing a quantitative basis for selecting grids for further analysis.

C. Selection of High-Density Grids

After counting the minutiae in each grid using a line-scan approach, we assess their densities to identify which grids are the most information-rich. The algorithm selects the top 7 grids with the highest minutiae density for further processing. High-density grids are presumed to contain the most distinct and informative features of the fingerprint, making them critical for the subsequent stages of minutiae triplet formation and feature extraction.

The choice of focusing on the top 7 high-density grids is strategic, enhancing the efficiency and accuracy of the matching process. These grids are likely to contain the most critical and distinguishing features of the fingerprint, which are essential for robust matching. By concentrating our analysis on these high-density areas, we significantly reduce the potential for noise and irrelevant data impacting the matching outcomes, thereby streamlining the identification process.

III. Minutiae Triplets Extraction

A. MinutiaPoint Class Definition

To facilitate the extraction of minutiae triplets, we define a class, MinutiaPointHD, which encapsulates the properties of each minutia point, including its coordinates (x and y). The class also includes methods for calculating the hash (to enable unique identification of minutia points) and for checking equality, which is crucial for ensuring that each minutia point is unique within our dataset

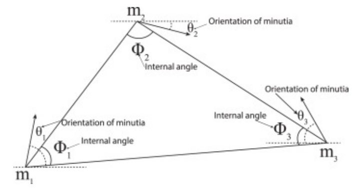

Fig. 2. Example from [1] of minutiae triplet from our implementation.

B. Triplet Formation

The process begins by retrieving minutiae data from a JSON file, which includes the output from our grid segmentation phase. This data is crucial as it contains the coordinates and the grid identification of each minutia, which we use to form triplets. To form these triplets, we iterate over the list of minutiae points, selecting groups of three to create a set of unique triplets. This uniqueness is ensured through a combination of hashing and equality checks, allowing us to avoid redundant calculations and reduce the computational overhead significantly. Each triplet consists of three distinct minutiae points, and our selection process is guided by the spatial relationship between these points within their respective High-Density Grids.

C. Feature Extraction from Triplets

For each triplet, we calculate critical geometric features that are instrumental in the matching process. These include the Euclidean distances between each pair of minutiae in the triplet and the angles formed by these points. The Euclidean distance provides a measure of the spatial separation between points, while the angles offer insight into the relative positioning of the minutiae, which is essential for establishing a robust fingerprint-matching criterion.

These geometric features are calculated using methods defined within the MinutiaPointHD class. The distance between any two points is computed as the square root of the sum of the squared differences in their x and y coordinates. To compute the geometric relationships necessary for fingerprint matching, we use the following formulas:

$$\text{Distance}_{i,(i+3)\%3} = \sqrt{(x_{(i+1)\%3} - x_i)^2 + (y_{(i+1)\%3} - y_i)^2} \tag{1}$$

$$\theta_i = \cos^{-1}\left(\frac{d^2_{(i+1)\%3} + d^2_{(i+2)\%3} - d_i^2}{2 \cdot d_{(i+1)\%3} \cdot d_{(i+2)\%3}}\right) \tag{2}$$

$$\theta_{i \text{ in degrees}} = \theta_{i \text{ in radians}} \times \frac{180}{\pi} \tag{3}$$

This method ensures that the distances are invariant to the orientation of the fingerprint, making them reliable indicators of the relative positions of minutiae in a fingerprint.

By focusing on unique triplets and extracting detailed geometric features, this part of the algorithm enhances the precision of the fingerprint-matching process. The use of unique triplets ensures that each combination of minutiae is considered only once, optimizing the computation and avoiding redundancy. The detailed feature set derived from these triplets provides a robust foundation for the subsequent matching stages, where these features are compared against known templates to establish identity matches.

IV. Implementation of Matching

Our matching algorithm is designed to identify the most likely match for a given probe fingerprint from a database of candidate fingerprints. It employs a multi-step approach that includes feature extraction, data normalization, distance calculation, and similarity scoring.

A. Feature Extraction and Data Normalization

Initially, the algorithm processes the probe fingerprint to extract key features, such as minutiae points, which are small, distinctive patterns found in the ridges of a fingerprint. This feature extraction is crucial as it forms the basis for comparison. Once extracted, these features undergo a normalization process to standardize the data, making it suitable for accurate comparisons. This may involve scaling of distances between features or normalization of angles, adapting the data into a uniform scale that ensures consistency across different fingerprints.

$$N(x) = \frac{x - \min(X)}{\max(X) - \min(X)} \tag{4}$$

Where *X* is the original set of feature values, *x* is an individual feature value, and *N(x)* is the normalized value.

B. Comparison and Distance Calculations

For each candidate fingerprint in the database, the algorithm calculates the distances between corresponding features of the probe and the candidate fingerprints. This involves computing the Euclidean distances between corresponding minutiae points. The algorithm also considers the geometric relationships between features, such as the relative angles and spatial arrangements, which are crucial for matching fingerprints that may have been distorted by elastic deformations during the capture process.

$$d(\mathbf{p}, \mathbf{q}) = \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2} \tag{5}$$

Where *p* and *q* are n-dimensional points representing corresponding minutiae points from the probe and candidate fingerprints, respectively.

C. Similarity Scoring

After calculating distances and angles, the algorithm aggregates these measurements to compute a similarity score for each candidate fingerprint. This score is typically computed by integrating various metrics, including point-to-point distances, differences in angles, and other structural similarities. The weights assigned to each of these metrics can be adjusted based on their relative importance and the specific characteristics of the fingerprint data being analyzed.

$$S = \omega_1 \cdot \overline{D} + \omega_2 \cdot \overline{\Delta\theta} + \omega_3 \cdot \overline{\Delta d} \tag{6}$$

- *D* is the average Euclidean distance between corresponding minutiae points.
- *delta-theta* is the average difference in angles between corresponding features.
- *delta-d* is the average difference in distances between feature sets.
- *w1*, *w2*, and *w3* are weights assigned to each component, reflecting their relative importance in the similarity calculation.

D. Decision Making

The algorithm then compares the similarity scores of all candidate fingerprints and identifies the one with the highest score as the best match. This process involves evaluating the overall closeness of the probe fingerprint to each candidate, based on the computed similarity scores, to determine the most likely identity.

$$M = argmax_{i \in \{1,\ldots,k\}} \cdot S_i \tag{7}$$

Where *M* is the index or identifier of the candidate fingerprint that has the highest similarity score *S* of *i* among all *k* candidates.

E. Summary

This fingerprint matching algorithm stands out for its detailed focus on geometric and structural aspects of fingerprint features, leveraging advanced mathematical models to enhance the accuracy and reliability of fingerprint matching. This approach not only improves the robustness of the matching process against common issues like partial prints and distortion but also enhances the algorithm's ability to handle a wide range of fingerprint qualities and capture conditions.

V. Performance Evaluation

A. Experimental Setup

The dataset for this study was obtained from the Fingerprint Database provided by the Institute of Automation, Chinese Academy of Sciences, accessible via the CASIA Fingerprint Database. Each image in this dataset represents a unique fingerprint, offering a broad spectrum of patterns that are essential for the rigorous testing of fingerprint analysis algorithms.

The primary condition for selecting a fingerprint sample from the database was the presence of a clear point of singularity. A singularity point in fingerprint analysis refers to a local ridge discontinuity, typically manifesting as either a loop or a whorl. These points are crucial for accurate fingerprint matching and identification. If a fingerprint did not exhibit a discernible singularity, it was excluded from the sample set. This criterion ensured that only fingerprints with distinct and identifiable features were included in the study, thereby enhancing the reliability of the matching process.

Prior to analysis, each fingerprint image was processed to enhance clarity and contrast, ensuring that the singularity points were prominently visible. This step was vital for the subsequent feature extraction and matching phases.

The effectiveness of the fingerprint matching algorithm was assessed using triplet Euclidean distance (5) and the angle measurements (2) of the triplets. Triplet Euclidean Distance involves calculating the Euclidean distance between corresponding singular points across three dimensions. It is a quantitative measure that evaluates the spatial discrepancies between similar features in different fingerprint images.

The analysis also involved measuring angles formed by lines connecting the triplet minutiae points. This angular measurement evaluates the geometric arrangement of the minutiae, adding a layer of comparison that enhances matching accuracy. Angles between minutiae are critical for determining the precise orientation and relational positioning within the fingerprint patterns, offering a robust metric for comparing the overall alignment of fingerprint features. The use of minutiae triplets are considered costly when using entire fingerprints, but when using select parts of the fingerprint, we are significantly reducing computational effort while still using a more invariant method of minutiae comparison.

B. Results and Analysis

TABLE I
DATABASE ENROLLMENT PROCESSING TIMES

Database Size	Loading Program (s)
10 Fingerprints	43.4018
20 Fingerprints	99.3641
50 Fingerprints	194.8053
100 Fingerprints	430.4079
500 Fingerprints	1771.6308
1,000 Fingerprints	4672.5168

TABLE II
MATCHING USING HIGH-DENSITY GRIDS

Database Size	Matching (s)	Total HDG Processing (s)
10 Fingerprints	0.0546	2.6148
20 Fingerprints	0.0978	2.4933
50 Enrollments	0.2259	2.6330
100 Enrollments	0.4320	2.8155
500 Enrollments	2.4986	4.9328
1,000 Enrollments	8.0966	10.5574

Experimental data reveals that the average processing time for a single fingerprint using Global Matching is 0.120 seconds per fingerprint. In contrast, the High-Density Grid matching

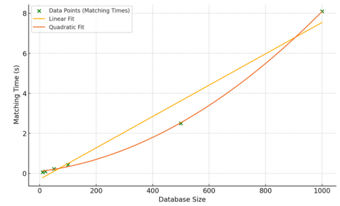

Fig. 3. Linear and Quadratic Fitting to Matching Times

method demonstrates exponentially faster performance with an average time of 0.036 seconds. This makes our method a little more than 3x faster per fingerprint. In terms of a database the size of the ones we tested with, this increase plays a significant role in computational effort and overall CPU execution time and stress. With a database the size of 500 individual images, our method successfully identifies a match in under 2.5 seconds, while its counterpart would preform at around 60 seconds of computational time.

Global Matching involves a straightforward implementation as it examines the entire fingerprint for matching. Conversely, High-Density Grid matching requires multiple computational steps to partition the fingerprint into grids and identify regions with the highest density. This added complexity of implementation is a trade-off for enhanced performance in matching efficiency on large-scale databases. The increase complexity is displayed in Table 1 and where the enrollment phase takes majority of the computational time of the program.

High-Density Grid matching shows strong potential for commercial and other applications where medium-sized fingerprint datasets require timely processing. Despite the higher complexity of implementation, its performance benefits make it suitable for environments where accuracy and speed are paramount. Conversely, Global Matching remains a viable option for singular fingerprint matching, where speed is less critical, and simplicity in implementation is prioritized.

$$y = 2.261 \times 10^{-3} x^2 + 2.3309x + 73.4123 \tag{8}$$

Quadratic relationship between the database size and the direct matching times from Table 2.

VI. IMPLICATIONS FOR THE FIELD OF BIOMETRIC SECURITY

The theoretical framework and initial performance evaluations of our high-density grid-based segmentation approach carry promising implications for the field of biometric security, particularly in enhancing fingerprint recognition systems. While our current implementation primarily quantifies improvements in processing speeds, the conceptual underpinnings suggest several key benefits that could significantly influence biometric practices. Potential for Enhanced Efficiency By selectively analyzing High-Density Grids that likely contain critical fingerprint features, our algorithm is designed to reduce computational overhead significantly. This method shows potential for much faster processing compared to traditional global matching techniques, which is particularly advantageous for real-time biometric systems.

A. Theoretical Robustness Against Variability

The use of minutiae triplets within targeted high-density areas theoretically enhances the system's robustness against distortions such as rotation and translation. Although direct accuracy metrics were beyond the scope of our current testing, this approach is expected to improve the fidelity of matches in varied operational conditions.

B. Scalability and Application in Large Databases

Our algorithm's methodical approach to data segmentation positions it as a viable solution for handling large-scale biometric databases efficiently. This scalability is crucial for extensive applications like national identity programs and large corporate security systems.

C. Cross-Modal Biometric Potential

While implemented for fingerprints, the principles underlying our grid segmentation and triplet analysis hold potential for adaptation across other biometric modalities, such as iris or facial recognition. This adaptability invites further exploration and could lead to comprehensive security solutions that span multiple biometric indicators

D. Inspirational Basis for Ongoing Research

Our study contributes to the biometric security discourse by proposing a method that addresses both speed and potential accuracy enhancements. As real-world applicability and further validation are pursued, our work could inspire and benchmark future innovations in biometric technologies, particularly in optimizing performance under practical constraints.

In summary, the proposed fingerprint-matching algorithm, while currently validated in terms of speed improvements, lays a solid foundation for future advancements in biometric security. It invites a reassessment of conventional matching techniques and suggests a pathway toward developing more sophisticated, efficient, and scalable biometric systems. Further research and practical testing will be crucial in fully realizing and substantiating the theoretical advantages posited by our approach.

VII. Observations/Applications For Future Research

A. Incorporating Singularity Data for Matching

During our project, we identified potential improvements that could significantly enhance our fingerprint-matching algorithm. Currently, the algorithm uses singularity points as primary anchors for alignment and matching. While this method is generally effective, its reliability can be compromised by fingerprints that lack clear singularities due to poor quality or natural variations. Future enhancements could involve integrating a broader array of anchor points, such as ridge bifurcations and unique pattern formations, to improve versatility and robustness. This expansion is expected to bolster the system's performance across a wider variety of fingerprint types and qualities.

Additionally, our testing predominantly involved high-quality scans, which may not adequately represent the diverse conditions typically encountered in practical scenarios. To assess the true robustness of our algorithm, future studies should test with a broader spectrum of print conditions, including smudges, partial captures, and other anomalies. Such testing will help validate the algorithm's effectiveness under adverse conditions and guide enhancements to accommodate real-world variations in fingerprint quality.

B. Enrollment Enhancement

In terms of the enrollment process, our current approach captures only a single image for each fingerprint during enrollment. To reduce the False Non-Match Rate (FNMR) and improve the matching success rate, it would be advantageous to collect multiple instances of each fingerprint during the enrollment phase. This data could then be normalized and stored as a collection of instances per individual, rather than a single entry per person. This method would necessitate additional storage, especially as data volume could grow significantly.

Implementing High-Density Segmentation in environments where cloud storage is feasible could greatly enhance the overall effectiveness of the algorithm. By leveraging cloud capabilities, we can accommodate the increased data requirements without compromising system performance, thereby improving the enrollment process and enhancing the algorithm's accuracy and reliability in practical applications.

VIII. Casade-Like Identification

In order to increase efficiency for large-scale uses, we have outlined an application derived from our proposed High-Density Grid-Based Segmentation draws inspiration from the Viola-Jones Boosted Cascade approach to object detection [5], which efficiently processes data through cascading classifiers rather than evaluating the entire dataset simultaneously. This methodology is adept for real-time applications and has been adapted to our fingerprint recognition system to enhance performance in large-scale databases.

In our suggested approach, fingerprint data is segmented into three key categories: fingerprint singularity, High-Density Grids, and minutiae triplets. These vectors serve as the foundation for a cascading classification system:

1) **Initial Screening:** The algorithm first searches for matching singularities between the probe fingerprint(s) and potential candidates in the database. Candidates with matching singularities are flagged for deeper analysis.
2) **High-Density Grid Comparison:** Next, the algorithm compares the High-Density Grids of these flagged fingerprints against a pre-defined dictionary of grid locations. Only candidates whose grid similarities exceed specific thresholds proceed to the next stage. This step effectively narrows down the pool of potential matches, significantly reducing computational load.

3) **Detailed Minutiae Analysis:** For the remaining candidates, the algorithm extracts and analyzes minutiae triplets to finalize identification. This stage provides a detailed and precise matching process, ensuring high accuracy.

By employing a hierarchical, cascade-like classifier system, our algorithm efficiently manages computational resources. Each stage filters and refines the candidate pool, focusing resources only on the most probable matches, which mirrors the effectiveness seen in real-time face recognition technologies.

REFERENCES

[1] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "A Novel Minutiae Triangulation Technique for Non-invertible Fingerprint Template Generation," Expert Systems with Applications, vol. 186, p. 115832, Dec. 2021, doi: https://doi.org/10.1016/j.eswa.2021.115832.

[2] N. K. Ratha, K. Karu, Shaoyun Chen, and A. K. Jain, "A real-time matching system for large fingerprint databases," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 8, pp. 799–813, 1996, doi: https://doi.org/10.1109/34.531800.

[3] M. Tico and P. Kuosmanen, "An algorithm for fingerprint image post-processing," An Algorithm for Fingerprint Image Postprocessing, Nov. 2002, doi: https://doi.org/10.1109/acssc.2000.911285.

[4] S.-H. Chang, F.-H. Cheng, W.-H. Hsu, and G.-Z. Wu, "Fast algorithm for point pattern matching: Invariant to translations, rotations and scale changes," Pattern Recognition, vol. 30, no. 2, pp. 311–320, Feb. 1997, doi: https://doi.org/10.1016/s0031-3203(96)00076-3.

[5] X. Jiang and W.-Y. Yau, "Fingerprint minutiae matching based on the local and global structures," IEEE Xplore, Sep. 01, 2000. https://ieeexplore.ieee.org/abstract/document/906252 (accessed Apr. 03, 2022).

[6] P. Viola and M. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," IEEE Conf Comput Vis Pattern Recognit, vol. 1, Feb. 2001, doi: https://doi.org/10.1109/CVPR.2001.990517.

[7] A. M. Bazen and S. H. Gerez, "Segmentation of Fingerprint Images," vol. 12, pp. 276–280, Nov. 2001.

[8] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 777–789, 1998, doi: https://doi.org/10.1109/34.709565.

[9] N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish, "Robust fingerprint authentication using local structural similarity," IEEE Xplore, Dec. 01, 2000. https://ieeexplore.ieee.org/abstract/document/895399 (accessed Mar. 26, 2021).