CONFERENCE PROCEEDINGS, JANUARY 2025
Published by the Faculty of Science (FSC), FULafia
Print ISSN: 2354–3388 DOI: https://doi.org/10.62050/fscp2024.440

Investigating the Thresholding Effect and Fingerprint Transformation Using Cross-Correlation Similarity Matching

O. R. Garuba✉**, I. M. Abdullahi, E. M. Dogo & D. Maliki**
Department of Computer Engineering, Federal University of Technology, Minna, Nigeria
✉oluwatosin.garuba@yahoo.com

Abstract: This research presents a cross-correlation similarity matching method to study the fingerprint transformation and thresholding impact. This work directly compares the impact of various transformations (rotation, translation, elastic deformation, and scaling) on the fingerprint matching performance at different threshold values, in contrast to the standard minutiae-based systems. In order to compare the template positions of the two fingerprints using plots, the cross-correlation similarity matching of fingerprints first selects suitable templates in the primary fingerprint and then uses template matching to assess the impact of each transformation on matching accuracy, FRR, and FAR in the secondary print. The findings highlight the potential of thresholding in developing reliable and practical fingerprint recognition systems.
Keywords: Cross-correlation, elastic deformation, false acceptance rate, false rejection rate

Introduction

Fingerprint recognition technology has become increasingly vital in various fields, including security, forensics, and personal identification. However, training accurate and robust fingerprint recognition models often requires a large and diverse dataset of fingerprint images. Acquiring such data can be challenging due to privacy concerns, cost, and logistical hurdles. This limitation necessitates creative solutions to maximize the effectiveness of limited data for training robust fingerprint recognition models [1].

Fingerprint recognition systems operate on the principle of analyzing the distinct patterns present in an individual's fingerprint to verify their identity. These systems traditionally employ a combination of image processing and pattern recognition techniques to extract relevant features from fingerprint images and match them against stored templates [2]. While the fundamental principles of fingerprint recognition remain sound, there are inherent challenges that must be addressed to ensure optimal performance and reliability. One of the primary challenges faced by fingerprint recognition systems is the variability in fingerprint impressions caused by factors such as environmental conditions, image quality, and individual characteristics [3]. In real-world scenarios, fingerprint images may exhibit distortions, noise, or occlusions, which can adversely affect the accuracy of recognition algorithms. Moreover, the availability of diverse fingerprint datasets for training poses a significant challenge, particularly in scenarios where limited data is available for model training.

The ridges and valleys of human fingertips combine to create unique designs. These patterns fully form during pregnancy and remain constant for the duration of an individual's life. Fingerprints are the prints of those patterns (Fig. 1). Cuts, burns, and bruises can temporarily impair fingerprint quality, but after they heal completely, patterns will return.

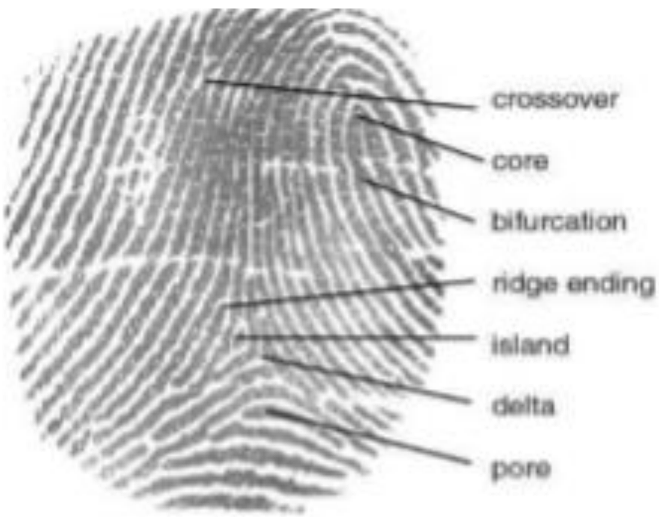

Figure 1: A Sample fingerprint

A mathematical measure of how much one number may be predicted to be influenced by changes in another is called a coefficient of correlation. It has a tight relationship to covariance. A full-field image analysis technique called Digital Image Correlation uses grey value digital images as its foundation and can identify three-dimensional object displacements and contours under load. Because they are relatively simple to use and apply, digital image correlation (DIC) techniques are becoming more and more common, particularly in micro- and nano-scale mechanical testing applications. While white-light optics has been the primary way, DIC can be and has been applied to practically any image technology. This method has been made possible by advancements in digital cameras and computer technology [4].

Dynamic thresholding involves adaptively making changes to the threshold value used for image segmentation based on local image characteristics. Unlike traditional thresholding methods that rely on fixed threshold values, dynamic thresholding algorithms analyze the statistical properties of the input image to determine an optimal threshold dynamically [5]. By adjusting the threshold value based on the specific characteristics of each fingerprint image, dynamic thresholding techniques enable more accurate segmentation of fingerprint ridges and valleys, thereby improving the quality of feature extraction and matching.

This paper delves into the advancements in fingerprint recognition achieved through the investigation of fingerprint data augmentation with random transformations and dynamic thresholding for adaptive segmentation.

Biometric systems have become increasingly vital for secure identification and authentication processes, leveraging unique physiological and behavioral characteristics to distinguish individuals. Among the various biometric identifiers, fingerprints have been widely adopted due to their distinctiveness, permanence, and ease of acquisition. Fingerprint recognition involves analyzing the unique patterns of ridges and valleys on the fingertips, often focusing on minutiae points such as ridge endings and bifurcations. These fundamental features make fingerprints highly reliable for personal identification and form the core of most Automated Fingerprint Identification Systems (AFIS) [6].

Advanced fingerprint recognition models leverage machine learning and deep learning techniques to further enhance accuracy. Machine Learning (ML) algorithms such as K-Nearest Neighbors (KNN) have been employed to classify fingerprints based on extracted features like minutiae points [7].

Evaluating the performance of fingerprint recognition systems requires a set of standardized metrics. Common evaluation metrics include Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). Accuracy measures the overall correctness of the system in identifying or verifying fingerprints. FAR quantifies the likelihood of incorrectly accepting an unauthorized person, while FRR measures the probability of incorrectly rejecting a legitimate individual. EER is the point where FAR and FRR are equal, providing a single value to assess the trade-off between these two errors. In this research, these metrics are used to evaluate the effectiveness of the proposed fingerprint recognition system, ensuring a comprehensive assessment of its performance in various scenarios [2].

Yilmaz and Abouyoussef propose a method incorporating a Pix2Pix model for enhancing low-quality fingerprint images and a one-shot learning approach using twin convolutional neural networks (CNNs) for feature extraction [1]. The study shows that the Pix2Pix model significantly improves fingerprint recognition accuracy compared to traditional methods. However, the effectiveness of this approach is constrained by its dependence on the quality of initial fingerprint images, which may not always be optimal in real-world scenarios. Furthermore, the study calls for further validation on larger, more diverse datasets to fully assess the model's robustness. These findings highlight the potential of data augmentation techniques in fingerprint recognition while also pointing to the need for broader validation to ensure practical applicability.

[8], embarked on a preliminary study exploring a mixed Unet architecture combining Resnet-101 and Unet encoder capabilities for latent fingerprint enhancement. The approach includes a novel Fingerprint Enhancement Gabor layer optimized for GPU computations, focusing on enhancing ridge and minutiae features. Although the study is still in its early stages and lacks rigorous experimental validation, it introduces an innovative direction for improving latent fingerprint processing. However, specific figures or quantitative results are not provided, leaving the effectiveness and efficiency of the method largely speculative. Furthermore, limitations include the need for improvements in processing speed and adaptability to different latent fingerprint types. Comprehensive validation through experimental approaches such as open-set identification and fingerprint quality evaluation is necessary to establish the method's practical viability.

Materials and Methods

The methodology for this study outlines the comprehensive steps undertaken to investigate an enhanced fingerprint recognition model using data augmentation and thresholding techniques. This Research aims to investigate the effect of thresholding and fingerprint transformation accuracy by leveraging a diverse dataset of fingerprint images collected. To evaluate the effect of each transformation on matching accuracy, FRR, and FAR, we need to simulate a fingerprint-matching process. Below is a simplified fingerprint-matching code using normalized cross-correlation as a similarity measure. This is a basic approach; in practice, more sophisticated methods like minutiae matching are used. This study aims to strike a balance by integrating traditional feature extraction methods with data augmentation and thresholding techniques to investigate its effects on fingerprints datasets

The Cross-correlation similarity matching shows varying effectiveness based on the type and extent of transformation. Advanced techniques that incorporate transformation correction mechanisms tend to perform better [9]. To compare the effects of different transformations (rotation, translation, elastic deformation, and scaling) on the fingerprint matching performance at various threshold values, we can modify the existing code. The goal is to evaluate the accuracy, False Rejection Rate (FRR), and False Acceptance Rate (FAR) for each transformation across multiple threshold levels.

The script will:

1. Apply each transformation separately.
2. Evaluate the matching performance for each transformation across the specified thresholds.
3. Export the results to an Excel file.
4. Visualize the results through plots.

Parameters

Parameter ranges

Angle range = [-15, 15]; % degrees for rotation

Translation range = [-5, 5]; % pixels for translation

Alpha = 2; % controls the intensity of elastic deformation

Sigma = 8; % controls the smoothness of elastic deformation

Scale_range = [0.95, 1.05]; % scale factor range

Results and Discussion

After running the code, the results are exported to an Excel file (fingerprint_matching_results.xlsx), and the graphs are plotted (Figs 2 – 4):

- **Accuracy vs. Threshold:** This graph shows how the accuracy changes with different thresholds. Typically, accuracy may decrease as the threshold increases because stricter matching criteria might lead to more false rejections.
- **FRR and FAR vs. Threshold:** This graph shows the trade-off between FRR and FAR as you adjust the threshold. As the threshold increases, FRR generally increases (more false rejections), while FAR decreases (fewer false acceptances).

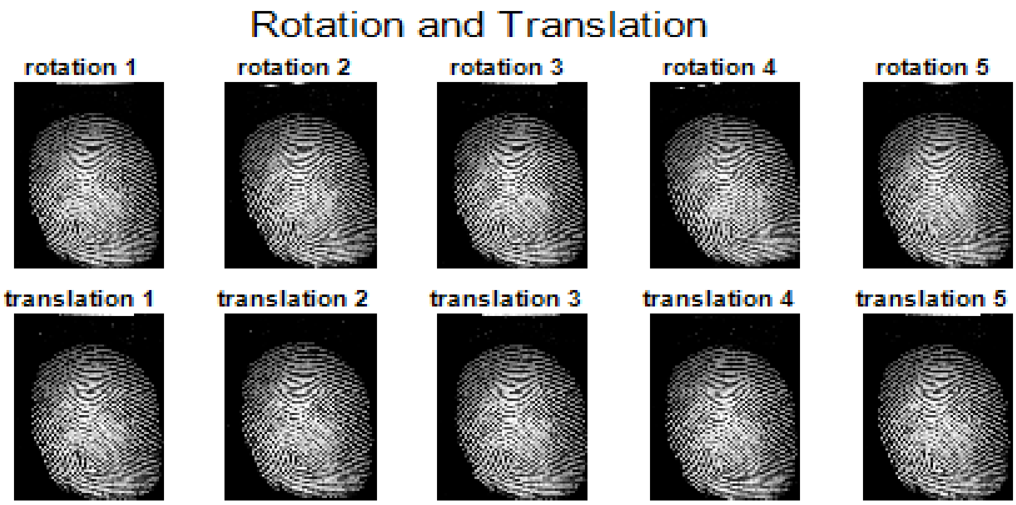

Figure 2: Transformation displaying five variants for both Rotation and Translation

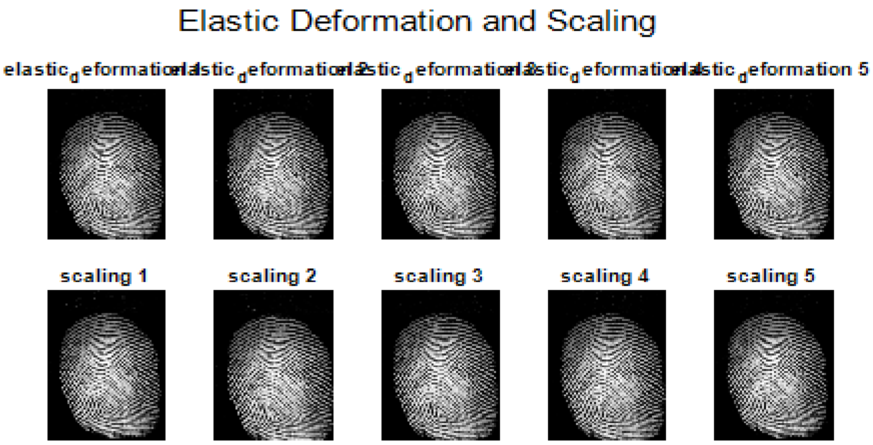

Figure 3: Transformation displaying five variants for both Elastic Deformation and Scalling

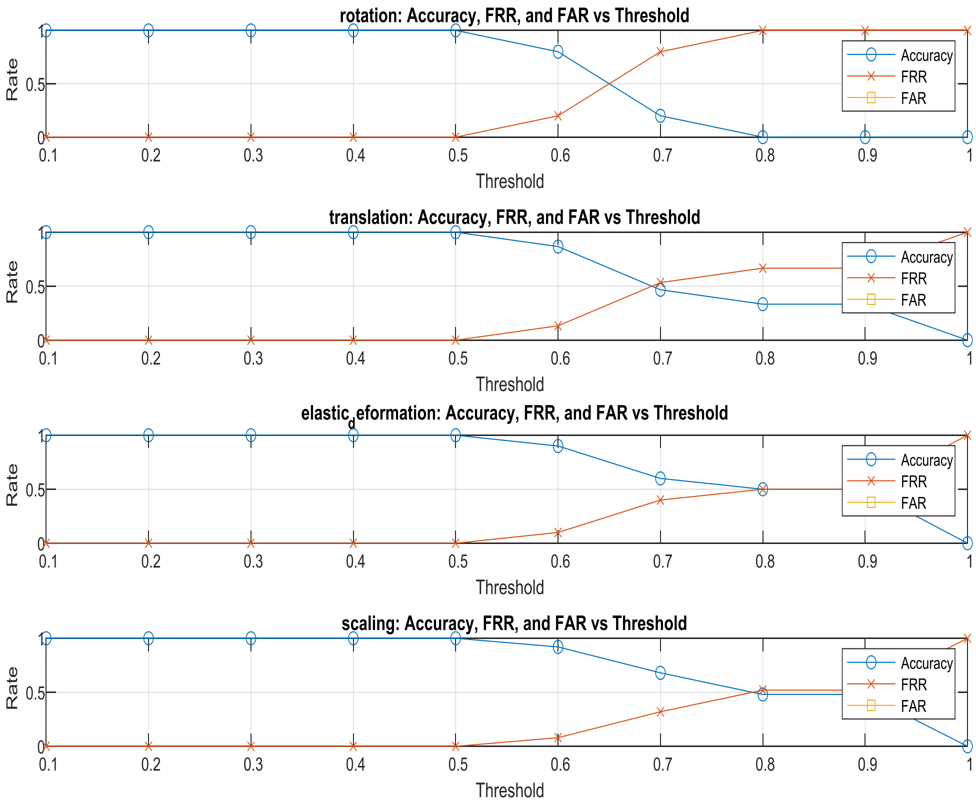

Figure 4: Effect of threshold variation on the performance of each transformation method

In the first graph, as the threshold increases from 0.1 to around 0.5, accuracy is maximized, suggesting that at lower thresholds, the model effectively identifies genuine fingerprints while minimizing errors. However, after this threshold point (0.6 onwards), the accuracy decreases while the FRR increases, indicating that the system starts rejecting genuine fingerprints more frequently. This increase in FRR signifies that the system has become too strict in its matching criteria. At higher thresholds, FAR is almost negligible, implying that the system is highly secure with minimal false acceptances, but at the cost of higher false rejections.

The second and third graphs demonstrate a similar pattern, where optimal accuracy is achieved within a specific threshold range. Notably, there is a clear crossover point where the FRR and FAR curves intersect. This crossover indicates a balance between security and usability. Before this point, the FAR is higher, meaning the system is more permissive and may falsely accept unauthorized fingerprints. After the crossover, the FRR becomes dominant, showing the system's increased reluctance to accept variations, even if they belong to the authorized individual. This balance point is crucial in practical scenarios where the trade-off between security (low FAR) and convenience (low FRR) must be carefully managed.

In the fourth graph, the effects of threshold adjustments are consistent with the previous observations. However, it is noticeable that after the crossover point, the accuracy drops more sharply compared to other graphs, indicating that this transformation method may be more sensitive to changes in threshold values. This heightened sensitivity could imply that certain transformations introduce variations in fingerprint patterns that are more challenging for the system to correctly classify as authentic or imposter prints. Thus, selecting an appropriate threshold range is vital to maintaining an optimal balance between FAR, FRR, and accuracy, particularly for transformation methods introducing more variability into the dataset.

Overall, these results highlight that threshold setting is a critical factor in fingerprint recognition systems. It directly impacts the system's accuracy, false acceptance, and false rejection rates. Finding an optimal threshold is necessary to ensure the system can effectively distinguish between genuine and imposter fingerprints across various transformations. The ideal threshold maximizes accuracy while minimizing FAR and FRR, providing a robust and reliable fingerprint recognition system.

Conclusion

In conclusion, this study investigates the thresholding effects on fingerprint data for an enhanced fingerprint recognition model using data augmentation and dynamic thresholding. Through the collection of a diverse fingerprint dataset and the application of transformations like rotation and elastic deformation, the model's robustness and generalization capabilities were significantly improved.The transformation-induced variations in the dataset reveal that certain thresholds are more resilient to changes in fingerprint appearance caused by transformations like rotation, scaling, and elastic deformation. By analysing multiple images, it becomes evident that the optimal threshold is not a fixed value but one that adapts to the diversity of the dataset. This analysis demonstrates that using a dynamic threshold, which adjusts based on the transformation's effect on image quality, can significantly enhance the model's robustness. This dynamic adjustment is particularly valuable in real-world applications where fingerprint inputs can vary due to environmental factors and user interaction with the sensor.

This study underscores the importance of effective thresholding and robust transformation handling in fingerprint recognition systems. Proper thresholding improves image quality and feature extraction, while effective transformation handling ensures accurate matching despite variations. Future work may focus on integrating advanced algorithms that combine adaptive thresholding and transformation correction to enhance overall system performance.

References

[1] Yilmaz, I. & Abouyoussef, M. (Directors). (2023, May 11). *FIGO: Fingerprint Identification Approach Using GAN and One Shot Learning Techniques* [Video recording]. https://doi.org/10.1109/isdfs58141.2023.10131805.

[2] Kang, H., Lee, B., Kim, H., Shin, D. & Kim, J. (2003). A study on performance evaluation of fingerprint sensors. In: Kittler, J. & Nixon, M. S. (Eds.), *Audio- and Video-Based Biometric Person Authentication* (pp. 574–583). Springer, https://doi.org/10.1007/3-540-44887-X_68

[3] Yahya, F., Nasir, H., Kadir, K., Safie, S., Khan, S. & Gunawan, T. (2016). Fingerprint biometric systems. *Trends in Bioinformatics*, 9, 52–58. https://doi.org/10.3923/tb.2016.52.58

[4] Jain, A. K., Prabhakar, S., Hong,L. & Pankanti, S. (2000). Filter bankbased fingerprint matching. *IEEE Transactions on Image Processing*, 9(5), 846–859.

[5] Bakheet, S., Al-Hamadi, A. & Youssef, R. (2022). A fingerprint-based verification framework using Harris and SURF feature detection algorithms. *Applied Sciences*, 12(4), 2028–2028. https://doi.org/10.3390/app12042028

[6] Maltoni, D., Cappelli, R. & Meuwly, D. (2017). Automated Fingerprint Identification Systems: From Fingerprints to Fingermarks. In: M. Tistarelli & C. Champod (Eds.), *Handbook of Biometrics for Forensic Science* (pp. 37–61). Springer International Publishing. https://doi.org/10.1007/978-3-319-50673-9_3

[7] Chen, B., Lan, H., Ma, J., Zhang, L., Zhuang Xiong & Fan, J. (2023, June 13). *An improved weighted KNN fingerprint positioning algorithm | Wireless Networks*. https://link.springer.com/article/10.1007/s11276-023-03400-x

[8] Wyzykowski, A. B. V. & Jain, A. K. (Directors). (2023, May 31). *A Universal Latent Fingerprint Enhancer Using Transformers* [Video recording]. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2306.00231

[9] Prabhakar, S., Jain, A. K., Wang J., Pankanti, S. & Bolle, R. (2000). Minutia verification and classification for fingerprint matching. In: *Proceedings of ICPR2000, 15th Int. Conf. Pattern Recognition, Barcelona, Spain.*