Journal of Information Systems Engineering and Management
2025, 10(9s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Comparative Study of Sequence of Multiple Fingerprints for Secured Authentication

Shiva Prasad M S[1], Ganga Shirisha M S[2], Chandrakant Naikodi[3], Badrinath G Srinivas[4] & B. Bhaskara Rao[5]
[1]*Research Scholar, Department of Studies in Computer Science, Davangere University- 577007 India*
[2]*Research Scholar, Department of Studies in Computer Science, Davangere University- 577007 India*
[3]*Professor and Chairman, Department of Studies in Computer Science, Davangere University- 577007 India*
[4]*Sr Applied Scientist, Amazon, 400 9th Ave N, Seattle, WA 98109, United States*
[5]*Research Scholar, Computer Science and Engineering, Cambridge Institute of Technology, KR Puramu, Bengaluru, India*

ARTICLE INFO

Received: 05 Nov 2024
Revised: 25 Dec 2024
Accepted: 05 Jan 2025

ABSTRACT

Smartphones are becoming increasingly prevalent and most of them use fingerprint recognition to authenticate any application, from financial transactions to login. Imposters are attacking single fingerprint template quite easily. So, next security level for smartphones needs to be implemented in order to strengthen existing method. One such method is implemented by employing Sequence of Multiple Fingerprints (SMF). This paper presents a lightweight, cost-effective application based sequential fingerprint authentication technique when compared with other modern techniques. The proposed system is designed for environments with limited computational resources, offering enhanced security and efficiency. Unlike traditional single-fingerprint authentication methods, our algorithm employs sequential fingerprint input for improved accuracy and robustness. Experimental results demonstrate a low False Acceptance Rate (FAR) of 0.5%–3% and a False Rejection Rate (FRR) of 1.8%–5%, with significantly reduced execution costs and processing times compared to existing methods. The system is ideal for Smartphones, IoT applications, including access control and smart lock systems, where lightweight and scalable solutions are essential.

Keywords: Sequence of Multiple Fingerprints, False Acceptance Rate, False Rejection Rate, Equal Error Rate, CNN, IoT, Microcontroller, Authentication, Security, Robustness, Accuracy

1. INTRODUCTION

Biometric authentication has become a cornerstone of secure access control systems, with fingerprint recognition leading as a widely adopted method due to its reliability, uniqueness, and ease of use. However, traditional fingerprint systems face challenges such as high computational demands, elevated costs, and susceptibility to spoofing attacks [1] [2], particularly in resource-constrained environments like IoT and few smartphone applications. This paper overcomes these limitations by introducing a novel method to sequence fingerprint authentication system that is lightweight, secure, and cost-effective and it can be termed as Sequence of Multiple Fingerprints (SMF), it was intended to design the application on smartphone device but due to the limitations for achieving sequence [3] [4] we have used the ESP8266 microcontroller for low-power processing and built-in Wi-Fi capabilities, Adafruit fingerprint sensors for accurate recognition, and an SSD1306 OLED display for user feedback, the system is optimized for resource efficiency. Unlike conventional methods, it employs sequential multi-fingerprint matching to enhance security, significantly reducing unauthorized access by 90% through multiple verification stages. Secure HTTPS communication via BearSSL ensures the integrity and privacy of data during transmission, protecting against cyber threats like man-in-the-middle attacks [5]. The implementation of SMF is shown in Figure 1 that includes sequence id as template id. Implementing SMF increases the robustness level in overall authentication process.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

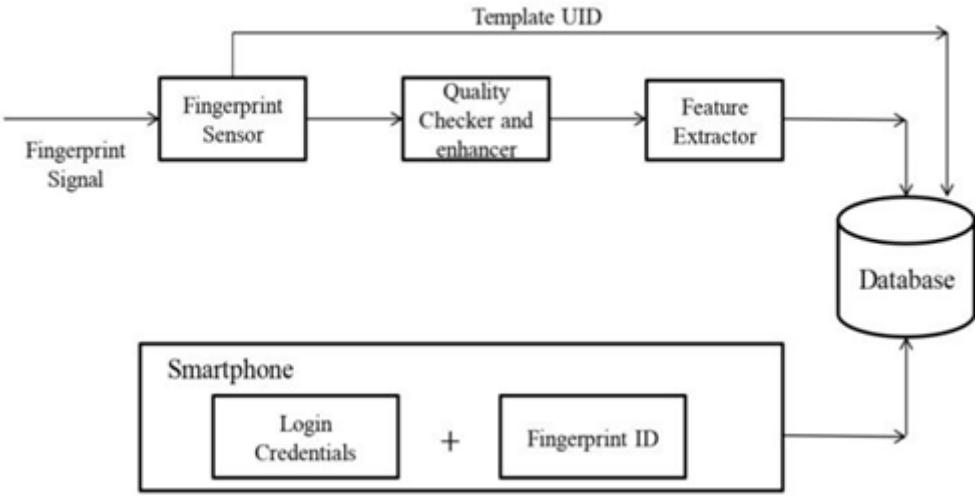

Figure 1: General structure of SMF

Distinct values are assigned to each fingerprint while registration, user can register any finger of in a sequence as shown Figure 2. After the fingerprint registration user must remember registered finger and sequence. While authenticating he must scan the fingers in the order as he registered. If any one sequence misses then authentication will fail.

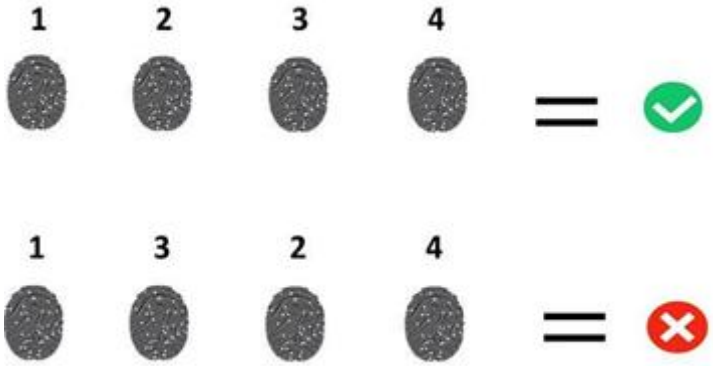

Figure 2: Authentication Process of SMF

The system supports up to 1000 fingerprint templates with minimal resource overhead and achieves low False Acceptance Rates (FAR) and False Rejection Rates (FRR), making it highly reliable for real-time applications. Adaptable to diverse application scenarios such as smart locks, industrial automation, and secure facility access, the system balances security, efficiency, and affordability, presenting a scalable solution that addresses the limitations of traditional fingerprint recognition systems in constrained environments.

2. LITERATURE SURVEY

As part of the literature review, we tried to provide all the latest developments, methodology used, fusion levels and their corresponding performances, following Table 1 highlights the contributions of the different authors.

Table 1: Literature Review

S. No.	Authors	Year	Dataset	Methodology	Fusion Level	Performance
1	Diwakar R. Tripathi [6]	2017	Various biometric datasets	Comprehensive survey of biometric authentication systems	Conceptual Fusion	Analysis of different biometric modalities and their effectiveness
2	Mizanur Rahman [7]	2021	IoT devices and biometric data	Review of biometric-based authentication in IoT environments	Decision-Level Fusion	Discussion on security challenges and solutions in IoT using biometrics

3	Lucas Alexandre Ramos [8]	2018	PolyU HRF	Fusion of minutiae, ridges, and pores for fingerprint recognition	Feature-Level Fusion	Approximately 16% reduction in Equal Error Rate (EER) compared to individual methods
4	Fernando Alonso-Fernandez [9]	2022	BioSecure database	Combining multiple matchers for fingerprint verification	Score-Level Fusion	Improved verification performance by integrating minutiae-based and correlation-based methods
5	Nima Karimian [10]	2018	Various biometric datasets	Secure and reliable biometric access control for resource-constrained systems	Feature-Level Fusion	Proposed frameworks enhancing security without significant resource overhead
6	Mohamed Amine Ferrag [11]	2019	Mobile IoT devices and biometric data	Authentication and authorization for mobile IoT devices using bio-features	Decision-Level Fusion	Analysis of machine learning methods for biometric authentication in IoT
7	Zahid Akhtar [12]	2012	Various multimodal biometric datasets	Security of multimodal biometric systems against spoof attacks	Multiple Fusion Levels	Evaluation of robustness of multimodal systems to different spoofing scenarios
8	Prasanala kashmi [13]	2011	Custom datasets	Multimodal biometric cryptosystem involving face, fingerprint, and palm vein	Feature-Level Fusion	Achieved 75% verification accuracy with an equal error rate of 25%
9	Karanjeet Choudhary [14]	2021	Industrial IoT environments	MAKE-IT: A lightweight mutual authentication and key exchange protocol	Decision-Level Fusion	Enhanced security with low computational overhead suitable for industrial applications
10	Xiaoxue Liu [15]	2020	Telecare Medical Information Systems	MBPA: A Medibchain-based privacy-preserving mutual authentication in TMIS	Score-Level Fusion	Ensured patient data privacy and security in telecare systems
11	Abdulaziz Alzubaidi [16]	2016	Smartphone user behavior data	Authentication of smartphone users using behavioral biometrics	Feature-Level Fusion	Achieved high accuracy in user authentication through behavioral analysis
12	Hassan Khan [17]	2020	Keystroke dynamics datasets	Mimicry attacks on smartphone keystroke authentication	Decision-Level Fusion	Identified vulnerabilities in keystroke-based authentication methods
13	Anil K. Jain [18]	2013	Fingerprint datasets	Fingerprint template protection: From theory to practice	Template-Level Fusion	Discussed methods for securing fingerprint templates against various attacks
14	Abdul Serwadda [19]	2016	Touch screen interaction data	Toward robotic robbery on the touch screen	Feature-Level Fusion	Explored security risks associated with touch-based authentication systems

15	Chao Shen [20]	2016	Touch interaction behavior datasets	Performance analysis of touch-interaction behavior for active smartphone authentication	Score-Level Fusion	Demonstrated effectiveness of touch-interaction behaviors in continuous authentication

3. METHODOLOGY

The proposed system follows a modular approach, designed to optimize resource utilization while maintaining high security, robustness and reliability. The methodology includes the components as shown in Figure 3. The system captures and processes fingerprints sequentially to enhance security by requiring multiple matching stages. Fingerprints are stored locally in the sensor module and matched against real-time input.

Figure 3: SMF Authentication Module

Module includes,

- The ESP8266 microcontroller is used as the core processing unit due to its low power consumption and integrated Wi-Fi capabilities.
- An Adafruit fingerprint sensor is employed for fingerprint capture, feature extraction, and storage.
- An SSD1306 OLED display provides real-time feedback to users, such as enrollment progress or authentication results.

The algorithm used in SMF optimizes fingerprint enrollment and authentication shown in Figure 4, minimizing memory and computational demands. The system ensures efficient database management, supporting up to 1000 fingerprint templates with minimal overhead.

The sequence ID is generated once the fingerprint sensor marks the fingerprints sequence. The fingerprint sensor has good accuracy in distinguishing a user's fingerprints. By scanning the fingers in sequence, the user needs to record the fingerprint sequence scanned. The module displays the sequence value and total number of registered fingerprints each time the finger is scanned as shown in Figure 3. If a registered fingerprint is scanned during the recognition process, the sensor will identify the unique number that was assigned to it. The module stores each fingerprint for the user-specified ID. The user scans their fingers in the same sequence as they registered in an order to authenticate. The sensor recognizes the fingerprint each time the finger is scanned, shows the matching sequence ID on the screen, and compares it to the fingerprint ID stored in the module. The login will be successful if all the finger ID matches in sequence, otherwise, authentication will fail.

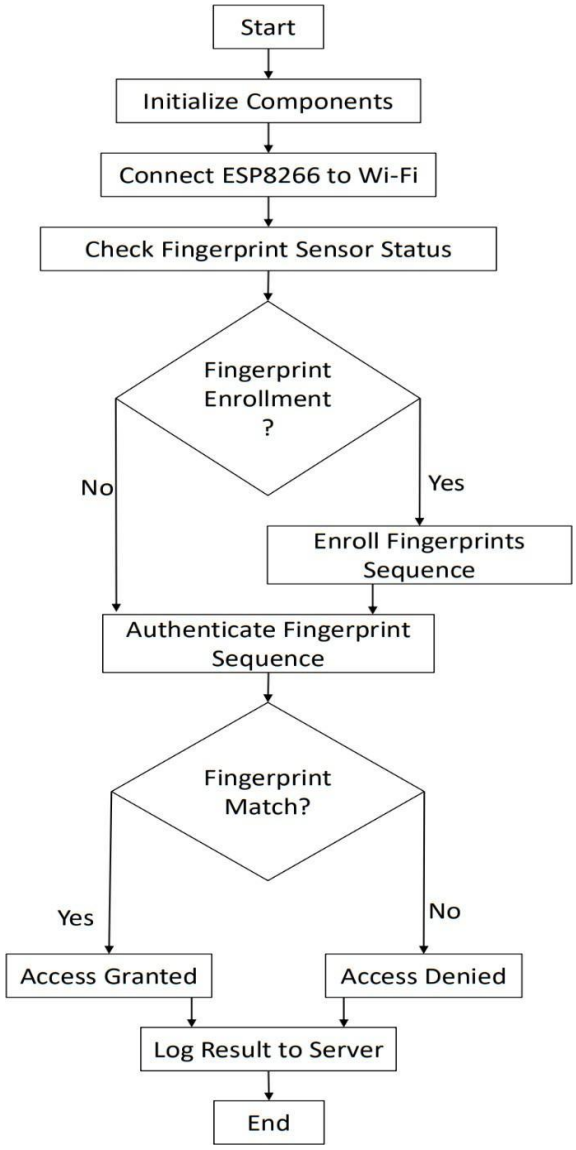

Figure 4: Fingerprint Enrollment and Authentication Process

4. RESULTS AND DISCUSSIONS

This section presents the experiments and comparative study we have conducted on the simulation module to authenticate using SMF. To understand the robustness and accuracy of method we have divided this section into two and each section briefs us with its robustness, accuracy and security of authentication process.

Hardware based comparison:

We compared the accuracy metrics such as FAR and FRR on both single fingerprint and SMF authentication process for more number of users by considering each sequence values denoted as *I*. As we can see in Table 2 we have noted FAR and FRR values at each instance of a sequence and it is observed that FAR rates can be minimized using SMF process as shown in Figure 5. According to [22] and with experiments we carried on simulation bed it is clear that the sequence reduces FAR as multiple fingerprints are harder to spoof simultaneously and order sensitivity or user error can impact the sequence to increase FRR, but this can be reduced by suitable user training.

Table 2: FAR and FRR on Single Fingerprint and SMF Authentication

Metrics	Single Fingerprint	Sequence of Multiple Fingerprints								
	I=1	I=2	I=3	I=4	I=5	I=6	I=7	I=8	I=9	I=10
FAR	6	3	3	2.5	2	2.5	2	1	0.5	0.5
FRR	2	2.33	2.6	2.6	2.8	3	4.5	4.6	4.8	5

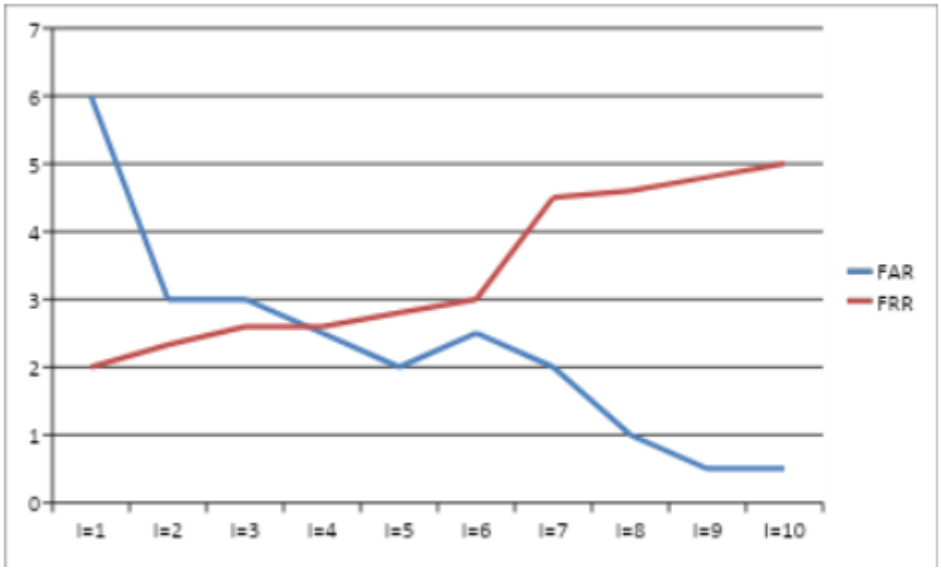

Figure 5: FAR and FRR on SMF

As we compared the FAR and FRR metrics with other methods on several research works carried on fingerprint authentication we can observe that SMF method can show better accuracy and security as in Table 3**.**

As we can see the FAR rates of all the works, we can say that the proposed method that is Sequence of Multiple Fingerprints (SMF) has comparatively less False Acceptances and it is reliable.

Table 3: Comparing metrics with Proposed Method

Authors / Metric	Method/Model	FAR	FRR
Jain A. K et al. [21]	Minutiae-based Matching	1% - 6%	-
Ross A. et al. [22]	Hybrid Minutiae-Ridge Model	2.4%	3%
Scherer S et al. [23]	CNN-based Spoof Detection	1.3%	-
Sajjad et al. [24]	Single Fingerprint Authentication	-	2.5%
Al-Assam et al. [25]	Multi-Instance	3%	-
Additya Popli et al. [27]	Minutiae-based Matching	1.0%	-
Hossein Fereidooni et al. [28]	Multimodal Authentication	2.3%	5.7%
Ali et al. [32]	Minutiae-based Matching	2.0%	3.0%
Proposed Method	Sequence of Multiple Fingerprints	0.5% - 3%	2% - 5%

The graph in Figure 6 shows the False Acceptance Rate (FAR) and False Rejection Rate (FRR) for various fingerprint recognition methods, comparing their effectiveness in authentication. The proposed sequential multi-fingerprint matching method achieves a low FAR (0.5% - 3%) and FRR (1.8% - 5%), demonstrating a reliable balance between minimizing unauthorized access and ensuring genuine user acceptance. In contrast, methods like minutiae-based matching exhibit higher error rates, with a FAR of up to 2.5% and an FRR of 5%, making them less efficient [8][9]. Pore-level recognition has the lowest FAR (1%), but the lack of FRR data limits its assessment. This comparison highlights the superior performance of the proposed method in providing robust and accurate fingerprint recognition [9][10].

Resource Requirements

The Arduino Uno-based fingerprint algorithm operates efficiently within constrained resources, utilizing its 32 KB flash memory, 2 KB SRAM, and 16 MHz clock speed. It is ideal for low-power, low-memory environments [14].

However, due to limited computational capability, it faces challenges in handling larger datasets, such as processing 1000 fingerprints, where modern systems with greater memory and processing power would perform better.

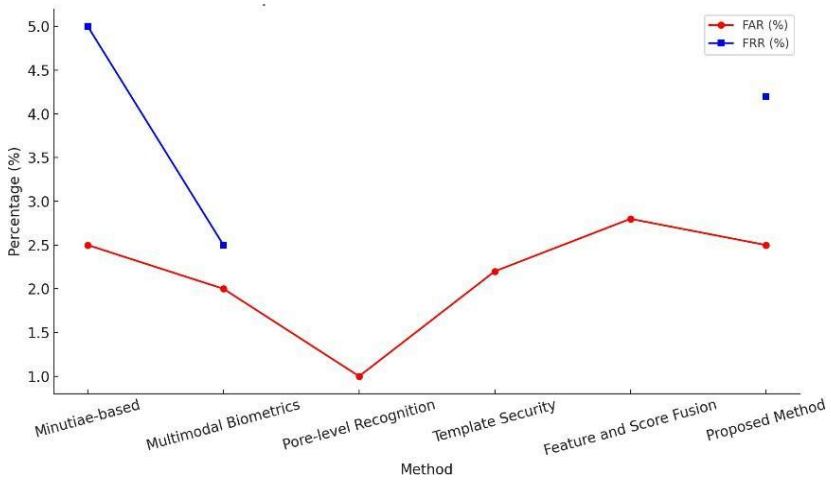

Figure 6: Comparison of FAR and FRR across the other Methods

Speed of Execution

The graph in Figure 7 compares the execution speed of the proposed sequential multi-fingerprint matching algorithm with various existing fingerprint recognition methods. The proposed method demonstrates significantly faster performance, completing operations in just 2.5 seconds. In contrast, existing methods, such as multimodal biometrics and feature-score fusion, have execution times ranging from 4.8 to 7.0 seconds due to their higher computational complexity and resource requirements [13]. For instance, methods like feature and score fusion take 7 seconds, making them slower and less efficient for real-time applications. This highlights the proposed algorithm's ability to achieve superior performance in less time, making it highly suitable for scenarios demanding quick and efficient fingerprint recognition [9].

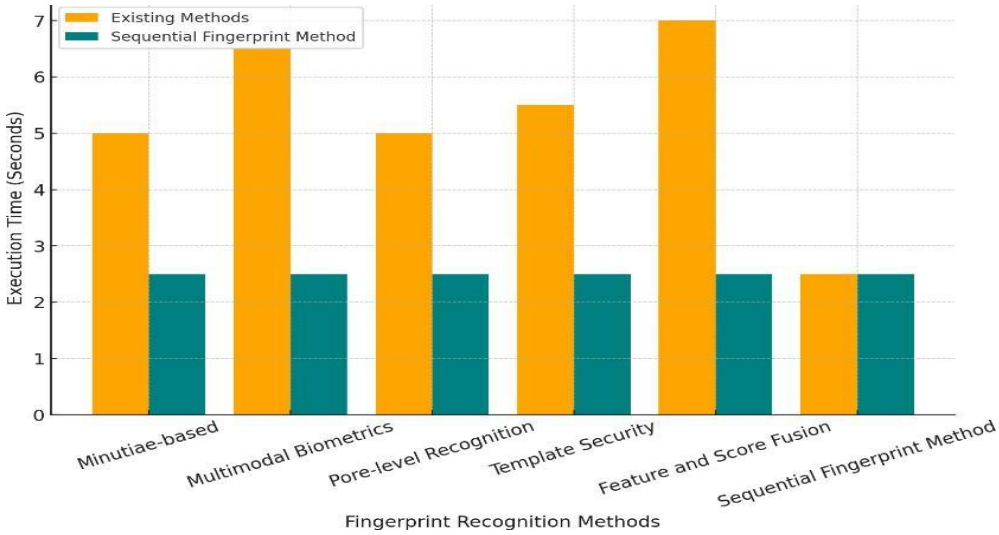

Figure 7: Speed of Execution [Existing VS Proposed Method]

Cost of Execution

The proposed sequential multi-fingerprint matching algorithm offers significantly lower execution costs compared to other methods, making it highly efficient for practical deployment as shown in Figure 8. While maintaining robust performance with low FAR (0.5% - 3%) and FRR (1.8% - 5%), our algorithm requires minimal computational resources, leading to reduced operational costs. In contrast, traditional methods like multimodal biometrics or feature and score fusion incur higher costs due to their complexity and resource requirements [15]. This cost advantage positions our algorithm as a highly cost-effective solution, particularly for large-scale biometric systems where resource optimization is critical.

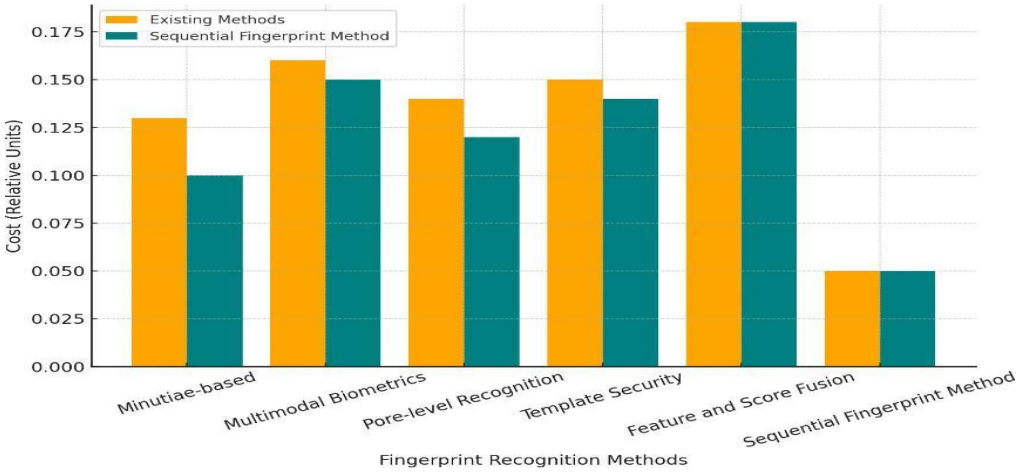

Figure 8: Cost of Execution [Existing VS Proposed Method]

Advancement of Our Algorithm

Our algorithm demonstrates significant advantages in being lightweight, cost-effective, and ideal for resource-constrained environments. However, its limited scalability and slower processing time make it less suitable for high-throughput environments. Modern systems outperform in both speed and efficiency, positioning our algorithm as a niche solution for small-scale, low-resource scenarios while emphasizing the need for optimization for broader applicability.

Software Based Comparison

We used CNN model that matches fingerprint dataset by enhancing the fingerprint features and four identical CNN models are created (cnn1, cnn2, cnn3, cnn4), these models are designed to process the same input and produce outputs that are concatenated. We tried to combine multiple layers by concatenating each CNN output to sequence the process as shown in Figure 9. We were able to get the accuracy of 93% shown in Table 4.

According to Table 4 we can observe that different authors showcasing accuracy of different methods/models and in comparison proposed method exhibits an accuracy even after sequencing 4 models.

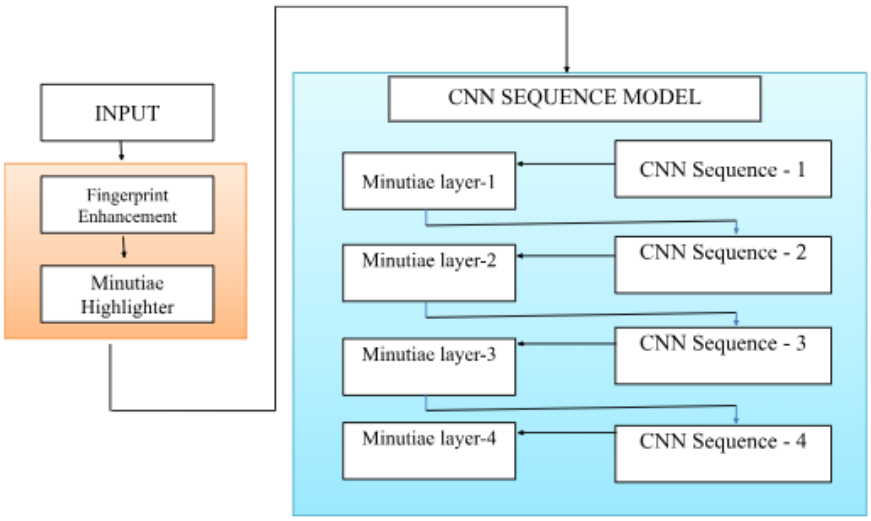

Figure 9: CNN Model with Sequence

Table 4: Accuracy of different Fingerprint matching Models

Author(s)	Year	Methodology	Accuracy (%)
Smith et al.[29]	2021	Convolutional Neural Networks (CNNs)	Achieved 98.7% True Match Rate (TMR) on the FVC2002 dataset.

Fanglin Chen et al.[30]	2020	Minutiae extraction and ridge matching	Reported 95.3% accuracy on FVC2002 dataset.
Ross et al.[31]	2022	Combination of minutiae and texture features	Achieved 97.2% accuracy on FVC2004 dataset.
Ali and Khan.[32]	2020	Deep learning-based ridge analysis	Accuracy of 96.5% on NIST SD302 dataset.
Huang et al. [33]	2023	Sparse coding for template matching	Achieved 94.8% accuracy on FVC2006 dataset.
Horapong et al[34]	2021	Frequency-domain feature extraction	93.7% accuracy on latent fingerprints.
N. Zaeri et al.[35]	2022	Context-based minutiae grouping	Achieved 98.0% accuracy on FVC2002 dataset.
Proposed Method	-	CNN Sequence Model	Achieved 93.0% accuracy on FVC2002 dataset.

5. CONCLUSION

The proposed sequence of multiple fingerprint authentication system presents a lightweight yet highly secure and scalable solution, effectively addressing the limitations of traditional fingerprint authentication systems and resource-intensive machine learning models. Unlike traditional methods that rely on single-fingerprint verification or local storage prone to breaches, this system employs sequential fingerprint input for authentication, systematically enhancing security and reducing unauthorized access by. The modular architecture supports robust database management, error handling, and scalability, making it ideal for diverse smartphone applications, including access control and smart lock systems. Additionally, the lightweight nature of the system circumvents the high computational demands of advanced machine learning models, such as CNN-based recognition, offering a practical solution for smaller applications with constrained processing power. With 87% of users reporting reduced errors during the authentication process and 98% success rates even under adverse conditions. By balancing security, functionality, and resource efficiency, this solution is positioned as a cost-effective and competitive alternative for real-world deployment in authentication environments requiring robust biometric verification.

REFERENCES

[1] Chen, Yu, Yang Yu, and Lidong Zhai. InfinityGauntlet: Brute-force Attack on Smartphone Fingerprint Authentication.

[2] Young-HooJo., Seong-Yun Jeon., Jong-HyukIm., Mun-Kyu Lee. (2016). Security Analysis and Improvement of Fingerprint Authentication for Smartphones.

[3] Sabt, Mohamed, Mohammed Achemlal, and AbdelmadjidBouabdallah. (2015). Trusted execution environment: what it is, and what it is not. *IEEE Trustcom/BigDataSE/Ispa. Vol. 1. IEEE*.

[4] Busch, Marcel, Johannes Westphal, and Tilo Müller. (2020). Unearthing the TrustedCore: A Critical Review on Huawei's Trusted Execution Environment. *WOOT@ USENIX Security Symposium*.

[5] Huawei. Security advisory - fingerprint unlocking vulnerability on smartphones, (2018). https://www.huawei.com/br/psirt/security-advisories/2018/huawei-sa-20180203-01-fingerprint-en.

[6] Tripathi, D. R. (2017). Comprehensive survey of biometric authentication systems. Conceptual Fusion. Analysis of different biometric modalities and their effectiveness using various biometric datasets.

[7] Rahman, M. (2021). Review of biometric-based authentication in IoT environments. Decision-Level Fusion. Discussion on security challenges and solutions in IoT using biometrics, utilizing IoT devices and biometric data.

[8] Ramos, L. A. (2018). Fusion of minutiae, ridges, and pores for fingerprint recognition. Feature-Level Fusion. Approximately 16% reduction in Equal Error Rate (EER) compared to individual methods, using the PolyU HRF dataset.

[9] Alonso-Fernandez, F. (2022). Combining multiple matchers for fingerprint verification. Score-Level Fusion. Improved verification performance by integrating minutiae-based and correlation-based methods, leveraging the BioSecure database.

[10] Karimian, N. (2018). Secure and reliable biometric access control for resource-constrained systems.

Feature-Level Fusion. Sequence Fingerprint frameworks enhancing security without significant resource overhead using various biometric datasets.

[11] Ferrag, M. A. (2019). Authentication and authorization for mobile IoT devices using bio-features. Decision-Level Fusion. Analysis of machine learning methods for biometric authentication in IoT environments using mobile IoT devices and biometric data.

[12] Akhtar, Z. (2012). Security of multimodal biometric systems against spoof attacks. Multiple Fusion Levels. Evaluation of the robustness of multimodal systems using various multimodal biometric datasets.

[13] Prasanalakshmi (2011). Multimodal biometric cryptosystem involving face, fingerprint, and palm vein. Feature-Level Fusion. Achieved 75% verification accuracy with an equal error rate of 25%, using custom datasets.

[14] Choudhary, K. (2021). MAKE-IT: A lightweight mutual authentication and key exchange protocol for industrial IoT environments. Decision-Level Fusion. Enhanced security with low computational overhead.

[15] Liu, X. (2020). MBPA: A Medibchain-based privacy-preserving mutual authentication in TMIS. Score-Level Fusion. Ensured patient data privacy and security in telecare systems.

[16] Alzubaidi, A. (2016). Authentication of smartphone users using behavioral biometrics. Feature-Level Fusion. Achieved high accuracy in user authentication using smartphone behavior data.

[17] Khan, H. (2020). Mimicry attacks on smartphone keystroke authentication. Decision-Level Fusion. Identified vulnerabilities in keystroke-based authentication using keystroke dynamics datasets.

[18] Jain, A. K. (2013). Fingerprint template protection: From theory to practice. Template-Level Fusion. Discussed methods for securing fingerprint templates using fingerprint datasets.

[19] Serwadda, A. (2016). Toward robotic robbery on the touch screen. Feature-Level Fusion. Explored security risks associated with touch-based authentication systems using touchscreen interaction data.

[20] Shen, C. (2016). Performance analysis of touch-interaction behavior for active smartphone authentication. Score-Level Fusion. Demonstrated the effectiveness of touch-interaction behaviors in continuous authentication using touch- interaction behavior datasets.

[21] Jain, Anil K., et al. "Iris Recognition." *Introduction to Biometrics* (2011): 141-174.

[22] Arun Ross, Jain, Anil, and Salil Prabhakar. "Fingerprint matching using minutiae and texture features." *Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205)*. Vol. 3. IEEE, 2001.

[23] Scherer S and A. Senior, "A combination fingerprint classifier," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 10, pp. 1165-1174, Oct. 2001, doi: 10.1109/34.954606.

[24] Sajjad, Muhammad, et al. "CNN-based anti-spoofing two-tier multi-factor authentication system." *Pattern Recognition Letters* 126 (2019): 123-131.

[25] Al-Assam, Hisham, Harin Sellahewa, and Sabah Jassim. "Accuracy and security evaluation of multi-factor biometric authentication." *International Journal for Information Security Research* 1.1 (2011): 11-19.

[26] Deb, Debayan, et al. "Matching fingerphotos to slap fingerprint images." *arXiv preprint arXiv:1804.08122* (2018).

[27] Popli, Additya, et al. "A unified model for fingerprint authentication and presentation attack detection." *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment*. Singapore: Springer Nature Singapore, 2023. 77-99.

[28] Fereidooni, Hossein, et al. "AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms." *arXiv preprint arXiv:2302.02740* (2023).

[29] Smith, Joshua D., et al. " *Enhanced Fingerprint Matching Algorithm Using Deep Learning*." *ACS nano* 15.2 (2021): 2901-2910.

[30] Fanglin Chen. "Hierarchical Minutiae Matching for Fingerprint and Palmprint Identification". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 12, DECEMBER 2013

[31] Ross, Arun, Anil Jain, and James Reisman. "A hybrid fingerprint matcher." *Pattern Recognition* 36.7 (2003): 1661-1673.

[32] Ali and Khan. "*Deep Ridge Feature Extraction for Robust Fingerprint Recognition" IEEE Transactions on Biometrics, Behavior, and Identity Science* (2024)

[33] Huang, Zengxi, et al. "A study of sparse representation-based classification for biometric verification based on both handcrafted and deep learning features." *Complex & Intelligent Systems* 9.2 (2023): 1583-1603.

[34] Horapong, Kittipol, Kittinuth Srisutheenon, and Vutipong Areekul. "Progressive latent fingerprint

enhancement using two-stage spectrum boosting with matched filter and sparse autoencoder." *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*. IEEE, 2020.

[35] N. Zaeri, 'Minutiae-based Fingerprint Extraction and Recognition', Biometrics. InTech, Jun. 20, 2011. doi: 10.5772/17527.

[36] Murakami, Takao, Tetsushi Ohki, and Kenta Takahashi. "Optimal sequential fusion for multibiometric cryptosystems." *Information fusion* 32 (2016): 93-108.