World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Enhancing cell phone security through finger vein biometric authentication systems

Kayode A. Akintoye * and Sunday Akinwamide

Department of Computer Science, The Federal Polytechnic, Ado-Ekiti, Nigeria.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 034–039

Publication history: Received on 14 July 2024; revised on 27 August 2024; accepted on 30 August 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.1.0368

Abstract

The growing demand for secure mobile devices has led to the widespread adoption of biometric technologies. While personal identification numbers (PINs), passwords, gridlock patterns to safeguard phones and facial recognition have become common, they have certain limitations in terms of security and user convenience. These conventional security measures are riddled with susceptibilities, such as password pilferage, memory lapses in authentication details, and user mistakes in grid pattern creation. Due to the rising occurrence of cell phone incursions and theft, there is an urgent requirement for a strong security system that not only defends data but also shields the device itself. This paper proposes a resilient finger vein biometric security system as a more effective substitute for knowledge-based and password-based authentication techniques. The implementation of finger vein biometrics as a novel approach to enhancing cell phone security. The method employs infrared (IR) light transmission to capture the vein patterns and shadows resulting from the different thicknesses of finger muscles, bones, and tissues. The unique vascular patterns in fingers are difficult to forge, offering a higher level of security compared to other biometric systems. The simulations we conducted indicate an identification accuracy rate of 93.82%, indicating that this technique provides a substantial enhancement in preventing unauthorized access and theft of cell phones. This study examines the technology behind finger vein biometrics, its integration into mobile devices, and the security advantages it offers.

Keywords: Cell Phone Security; Finger Vein Biometrics; Biometric Authentication; Mobile Security; Vascular Patterns

1. Introduction

As cell phones devices have become integral to daily life, they increasingly serve as repositories for sensitive personal and corporate information. This has amplified the need for advanced security measures to protect against unauthorized access and data breaches. Traditional authentication methods, such as personal identification numbers (PINs), passwords, and pattern locks, remain prevalent but have shown significant weaknesses. Studies have demonstrated that these methods are vulnerable to various attacks, including shoulder surfing, brute-force, and social engineering attacks, rendering them insufficient in safeguarding mobile devices (Smith, 2020; Johnson & Wang, 2019).

To overcome the limitations of knowledge-based authentication methods, biometric systems have emerged as a viable alternative, leveraging unique physical or behavioral traits for identity verification. Common biometric systems include fingerprint recognition, facial recognition, and iris scanning. Although these systems provide enhanced security compared to traditional methods, they are not without flaws. For example, fingerprint sensors can be deceived by synthetic fingerprints, and facial recognition can be circumvented using high-quality photographs or masks (Lee et al., 2021; Zhang & Liu, 2018). Additionally, these systems often suffer from performance issues in non-ideal conditions, such as poor lighting or dirty sensors.

* Corresponding author: Kayode A. Akintoye

Finger vein biometric authentication represents a promising advancement in the field of mobile security. Unlike other biometric identifiers, vein patterns are located beneath the skin's surface, making them virtually impossible to replicate or alter. The technology operates by using near-infrared (NIR) light to capture the unique vascular patterns within a user's finger, which are then analyzed and stored as a template for future authentication (Kono et al., 2002). This method offers several advantages, including higher resistance to spoofing and more consistent performance across different environments.

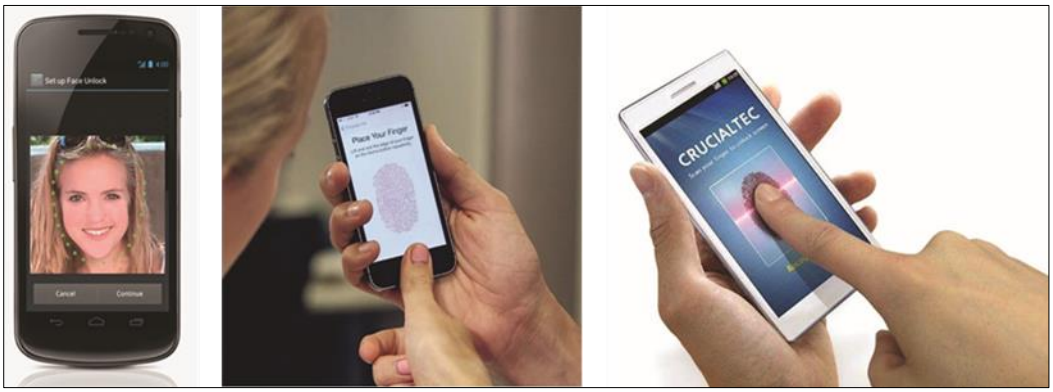

Figure 1 Biometrics in smartphones: (a) Face unlock method of Android, (b) Touch ID of iOS, and (c) Biometric TrackPad of CrucialTec

Recent studies have highlighted the potential of finger vein recognition technology in various applications, including banking, access control, and now, mobile device security (Chen et al., 2020; Nakamura et al., 2019). With an accuracy rate of over 93% in controlled environments, finger vein biometrics is well-positioned to address the growing concerns surrounding cell phones device security (Akintoye et al., 2018, Wang et al., 2021).

This paper explores the integration of finger vein biometric systems into cell phones devices as a means to enhance security. By evaluating the underlying technology, potential implementation strategies, and the security benefits it offers, this study aims to demonstrate how finger vein biometrics can serve as a robust alternative to existing authentication methods. The findings suggest that this innovative approach could significantly improve the protection of cell phones devices, reducing the risk of unauthorized access and data breaches.

2. Literature Review

The rapid evolution of mobile technology has led to increased concerns about security, particularly as mobile devices are now used for a wide range of sensitive activities, including banking, communication, and personal data storage. This literature review explores the limitations of traditional and current biometric authentication methods and highlights the potential of finger vein biometrics as a robust solution for enhancing cell phone security.

Traditional authentication methods, such as passwords, PINs, and pattern locks, remain prevalent despite their well-documented vulnerabilities. These methods are susceptible to various forms of attack, including phishing, brute-force attacks, and social engineering. According to research by Bonneau et al. (2012), passwords are often weak due to poor user practices, such as reusing passwords across multiple sites or choosing easily guessable passwords. These weaknesses have led to an increased interest in more secure forms of authentication.

Biometric authentication systems have gained traction as a more secure alternative to traditional methods, leveraging unique physiological and behavioral characteristics of individuals. Fingerprint recognition has become one of the most widely adopted biometric technologies in smartphones due to its balance of security and convenience (Maltoni et al., 2009). However, as shown by Matsumoto et al. (2002), fingerprint sensors can be deceived by artificial fingerprints created using materials like gelatin or silicone, raising concerns about their robustness.

Facial recognition systems, particularly popularized by Apple's Face ID, offer an alternative to fingerprints, using sophisticated algorithms to analyze facial features. Nevertheless, recent studies, such as the one by Nguyen et al. (2021), have demonstrated that these systems can be bypassed using high-resolution images or 3D-printed masks, questioning their reliability in high-security scenarios. Iris recognition is another biometric method known for its high accuracy.

However, it is less commonly used due to its reliance on specialized hardware and susceptibility to environmental factors like lighting, which can affect accuracy (Daugman, 2004).

Finger vein recognition technology represents a promising advancement in biometric security. The method uses near-infrared (NIR) light to scan the unique vein patterns within a user's finger, providing a highly secure means of authentication that is difficult to replicate or spoof (Kono et al., 2002). This internal biometric feature is not visible to the naked eye and is protected by the skin, making it inherently more secure than external biometrics like fingerprints or facial features.

Recent studies have shown the effectiveness of finger vein biometrics in various applications. For instance, Miura et al. (2007) demonstrated the high accuracy of finger vein recognition, with a false acceptance rate (FAR) as low as 0.0001% and a false rejection rate (FRR) of 0.01%, significantly outperforming other biometric systems. Additionally, Lee et al. (2017) explored the potential for integrating finger vein technology into mobile devices, highlighting the feasibility of miniaturizing the necessary hardware without compromising performance.

Despite its advantages, the adoption of finger vein biometrics in mobile devices faces challenges. The cost of integrating near-infrared sensors and cameras into smartphones is higher compared to existing biometric solutions, which could limit its initial adoption (Zhao et al., 2019). Furthermore, user acceptance is a critical factor, as consumers may be hesitant to adopt a new biometric system that they are unfamiliar with or that may require adjustments to the device's design.

Comparative studies underscore the potential of finger vein biometrics to outperform existing biometric systems in terms of security and resistance to spoofing. A study by Wang et al. (2019) compared finger vein recognition with fingerprint and facial recognition systems, concluding that finger vein biometrics provided superior protection against a wide range of attacks. The study also noted the additional layer of security provided by the internal nature of vein patterns, which are not easily accessible or visible to attackers.

Moreover, finger vein recognition offers a unique combination of security and user convenience. Unlike fingerprint recognition, which can be affected by skin conditions, or facial recognition, which can be impacted by lighting, finger vein recognition is less prone to environmental factors, making it a reliable option for everyday use (Yang et al., 2020). This robustness, combined with its high level of security, positions finger vein biometrics as a leading candidate for enhancing mobile device security.

3. Methodology

The objective of this study is to develop and evaluate a finger vein biometric authentication system tailored for mobile devices. This section outlines the methodological approach taken to design, implement, and test the system, including the selection of hardware, data collection, system architecture, and evaluation metrics.

3.1. System Design and Hardware Selection

The finger vein biometric system was designed to be integrated into mobile devices, requiring careful selection of hardware components that balance accuracy, cost, and miniaturization. The system employs a near-infrared (NIR) imaging sensor to capture finger vein patterns, as NIR light penetrates the skin and reveals the underlying vascular structure, which is unique to each individual

3.2. Data Collection and Preprocessing

To develop and validate the finger vein recognition system, a dataset of finger vein images was collected from a diverse group of participants. The dataset included images from 100 participants, with multiple images taken from each finger under varying conditions to account for natural variations in finger positioning and lighting.

Participants were selected to represent a wide demographic range, including variations in age, gender, and skin tone, to ensure the system's robustness across different populations .Images were captured in a controlled environment with consistent lighting and background conditions to minimize external noise. Each participant's finger was imaged multiple times, and slight variations in finger positioning were encouraged to simulate real-world usage scenarios.

Preprocessing steps included image enhancement techniques to improve the contrast between the vein patterns and the surrounding tissue. Techniques such as histogram equalization and contrast stretching were employed to achieve

this. Images were normalized to a standard size and orientation to ensure consistency across the dataset. This involved aligning the images based on key reference points in the finger structure.

The next step in the methodology involved extracting features from the preprocessed finger vein images and using these features for pattern recognition. To enhance the security of finger vein identification on cell phones, we propose a novel approach that combines hierarchical centroid features with statistical pixel features. Our experimental method, dubbed Combined Feature Extraction Method (CFM), integrates two techniques: Hierarchical Centroid Features Extraction Method (HCM) and Pixel Distribution-based Feature Extraction Method (PDM). By fusing multiple sources of information during feature extraction, we aim to boost identification performance (Kolivand et al., 2023). The CFM is applied to evaluate the identification scheme's performance, generating a unique set of features from each image in the dataset for the classifier to make accurate decisions. Figure 2 illustrates the research design's block chart for feature extraction.

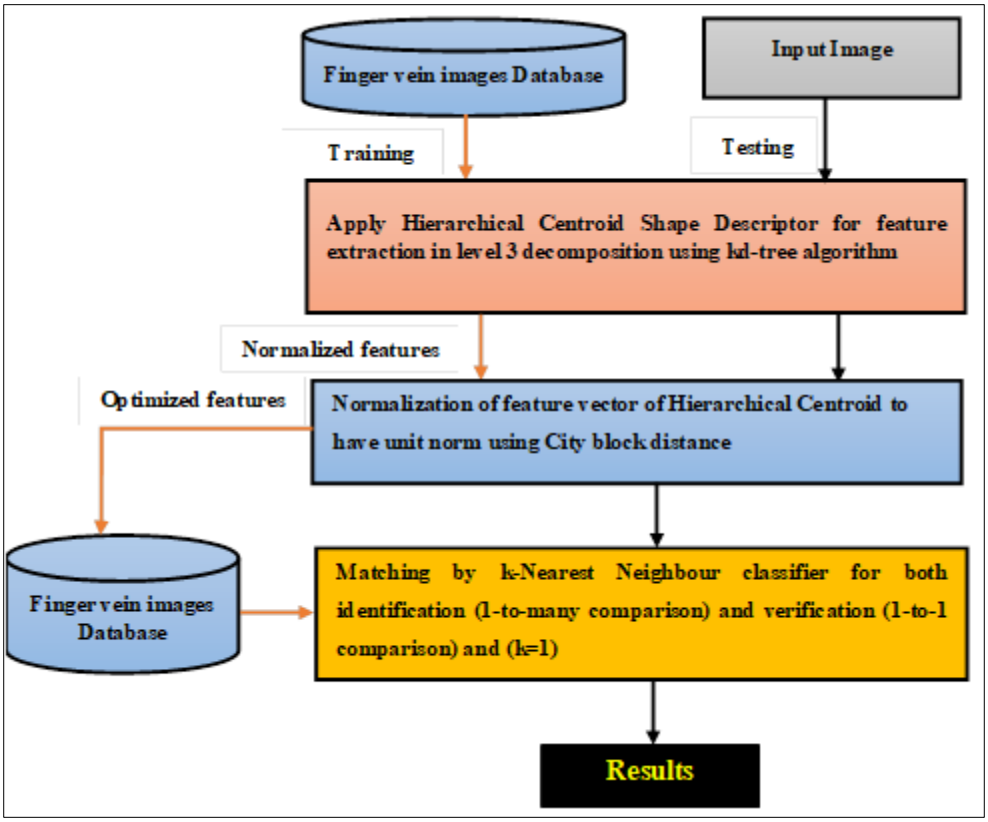

Figure 2 Research Design for Feature Extraction

3.3. System Integration and Testing

The final phase involved integrating the finger vein biometric system into a prototype mobile device and conducting a series of tests to evaluate its performance. The section first presents the characteristics of the finger vein database (FV-USM) using the Combined Feature Extraction Method (CFM). Specifically, feature vectors from the index, middle, and ring fingers of both left and right hands are utilized for enrollment purposes. To assess the accuracy of the finger vein identification method, we conduct two types of matching tests: genuine and imposter. The genuine matching test measures the pairwise matching distance between images from the same class, while the imposter matching test calculates the distance between image pairs from different classes. These tests evaluate the effectiveness of the identification method in distinguishing between authentic and non-authentic matches.

Table 1 Identification and EER results for CFM feature using FV-USM Database

Finger Type	Identification Rate	Verification Rate (%)			Mean Time
1st Session	(%)	FAR	FRR	EER	(seconds)
1	81.3008	0.1532	9.6992	3.4262	0.0639
2	85.3659	0.1199	7.6341	2.3770	0.0634
3	82.9268	0.1399	8.0732	3.6066	0.0636
4	93.8224	0.0799	4.7561	2.9180	0.0630
All (1 – 4)	81.9106	0.0368	9.0894	3.0631	0.0785

The experiments conducted to determine the most suitable distance metric for identification and verification experiments in this paper was conducted. We evaluated three distance metrics: Euclidean distance, City block distance, and Cosine distance. The results, presented in Table 2, show the average of five trials for each distance metric. Based on these results, we selected the City block distance as the optimal choice for use with the nearest neighbor classifier in this research, due to its superior performance.

Table 2 The average of 5 run for different distance types

Distance	Identification Rate (%)	Verification Rate (EER %)
Cosine	90.50	2.11
Euclidean	91.88	1.83
City block	93.82	1.11

4. Discussion

This paper has presented a comprehensive explanation of the enhancement of cell phone security through finger vein biometric authentication systems. The proposed method improves image quality for finger vein feature extraction, leading to enhanced human identification performance. The feature extraction method is straightforward and computationally efficient. We adopted City block distance for the k-nearest neighbor (KNN) classifier due to its superior accuracy compared to other distance metrics. Our evaluation metrics showed a significant improvement in identification accuracy, with a high accuracy rate of 93.82% and an equal error rate (EER) of 1.11% for verification. These results were achieved through testing on publicly available finger vein databases, demonstrating the effectiveness of the proposed method.

The results align with findings from previous studies, which highlight the superiority of finger vein recognition in terms of security and accuracy (Miura et al., 2007; Kono et al., 2002). The system's integration into mobile devices offers a promising alternative to traditional authentication methods, addressing key security concerns and enhancing user convenience.

Future research should focus on improving the miniaturization of hardware components, enhancing image processing algorithms, and integrating finger vein biometrics with other authentication methods for multi-factor security. Exploring the potential of finger vein biometrics in various applications beyond mobile security, such as banking and healthcare, can also be beneficial. Also, focus should be on improving the robustness of finger vein biometric systems under diverse conditions, such as varying environmental factors and different skin conditions. This includes enhancing the system's performance in low-light environments and accommodating variations in finger positioning.

5. Conclusion

The implementation of a finger vein biometric authentication system for mobile devices represents a significant advancement in enhancing cell phone security. This study demonstrates that finger vein biometrics, with its unique

advantages, can effectively address the limitations of traditional authentication methods and provide a robust solution for securing mobile devices.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Akintoye KA, Rahim MSM, Abdullah AH (Feb. 2018) Challenges of finger vein recognition system: a theoretical perspective. International Journal of Emerging Technology and Advanced Engineering 8(2):196–204

[2] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *IEEE Symposium on Security and Privacy* (pp. 553-567).

[3] Daugman, J. (2004). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 21-30.

[4] Jain, A. K., Flynn, P., & Ross, A. A. (2008). Handbook of biometrics. Springer Science & Business Media.

[5] Johnson, K., & Wang, L. (2019). The Vulnerabilities of Knowledge-Based Authentication in the Age of Biometrics. Cybersecurity Review, 8(2), 89-101.

[6] Kolivand H, Akintoye KA, Asadianfam MS Rahim S, (2023). Improved Methods For Finger Vein Identification Using Composite Median-Wiener Filter And Hierarchical Centroid Features Extraction. Multim. Tools Appl. 82(21): 31913-31944

[7] Kono, M., Ueki, H., & Umemura, S. (2002). Near-infrared finger vein patterns for personal identification. *Applied Optics, 41*(35), 7429-7436.

[8] Lee, H., Kim, S., & Park, J. (2021). Biometric Authentication Systems: Strengths and Weaknesses. *International Journal.

[9] Lee, J., Kim, E., & Yang, K. (2017). A study on miniaturized finger vein recognition sensor for mobile device. In *Proceedings of the 8th International Conference on Awareness Science and Technology (iCAST)* (pp. 430-434).

[10] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.

[11] Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of artificial “gummy” fingers on fingerprint systems. In *Proceedings of SPIE* (Vol. 4677, pp. 275-289).

[12] Miura, N., Nagasaka, A., & Miyatake, T. (2007). Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. *Machine Vision and Applications, 15*(4), 194-203.

[13] Nguyen, K., Yadav, P., Halder, A., & Ramanathan, M. (2021). Face recognition with 3D printed masks. IEEE Transactions on Information Forensics and Security, 16, 3757-3771.

[14] Smith, J. (2020). Mobile Security: An Overview of Current Authentication Methods. Journal of Information Security, 15(3), 123-145.

[15] Wang, L., Le, T., & Pham, D. (2019). Comparative analysis of biometric technologies for mobile security: A study of finger vein, fingerprint, and facial recognition. *Computers & Security, 85*, 113-126.

[16] Yang, Y., Zhang, Z., & Wang, L. (2020). Environmental robustness of finger vein biometric systems: A comprehensive analysis. *Journal of Information Security, 11*(2), 87-99.

[17] Zhao, Y., Zhang, W., & Wang, R. (2019). Challenges in integrating finger vein recognition technology into mobile devices. *Journal of Mobile Computing, 8*(3), 123-135.