Journal of Telecommunication, Electronic and Computer Engineering
ISSN: 2180 – 1843 e-ISSN: 2289-8131 Vol. 17 No. 3 (2025) 35-41
jtec.utem.edu.my
DOI: https://doi.org/10.54554/jtec.2025.17.03.005

Automated Real-time Door Access Control using Finger-vein Recognition

A. R. Syafeeza[1], Albert Ngan Ban Chew[1], Asar Khan[1], Norihan Abdul Hamid[1], Wira Hidayat Mohd Saad[1], and Airuz Sazura A. Samad[2]

[1]*Machine Learning and Signal Processing (MLSP) Research Group, Fakulti Teknologi dan Kejuruteraan Elektronik dan Komputer (FTKEK), Universiti Teknikal Malaysia Melaka, 76100, Durian Tunggal, Melaka, Malaysia.*

[2]*Ges Venture Manufacturing Sdn. Bhd, Johor Bahru, Johor, Malaysia.*

Article Info

Article history:
Received Dec 23rd, 2024
Revised June 13th, 2025
Accepted Sep 24th, 2025
Published Sep 30th, 2025

Index Terms:
Real Time
Finger Vein Recognition
Raspberry Pi 3
NOIR Raspberry Pi Camera
Modified Hausdorff Distance (MHD)

Abstract

The article focuses on developing an automated and real-time finger-vein identification device for door access control. This device records an individual's finger-vein image to grant access to authorized users. The door opens if the user is authorized and remain closed otherwise. The finger-vein image is captured by a Raspberry Pi camera (CMOS NOIR) when a matrix of near-infrared light-emitting diodes (NIR LEDs) illuminates the finger inside the acquisition box. In the captured image, the finger or the background appears lighter, while the veins appear darker. The image then undergoes several processing stages to enhance its quality before the Modified Hausdorff Distance (MHD) technique compares the minutiae points with the template stored in the database. The 2D Entropy algorithm performs further analysis to identify the correct user. If the user is authorized, the door opens; otherwise, it remains closed. The device is developed using Raspberry Pi 3 as the microcontroller, which processes the image, controls the camera, manages NIR LED lighting, and operates the door motor. The device achieves an Equal Error Rate (EER) of 7.88%, corresponding to an accuracy of 92.12%. This study's contribution includes detailed development specifics and proposed solutions to issues encountered during the research.

*Corresponding Author: syafeeza@utem.edu.my

I. INTRODUCTION

There are now numerous ways to lock or unlock a door. The traditional method using a key and a standard lock, while a more contemporary approach uses a passphrase or a password, often a series of digits, in place of a physical key. Both methods, however, share a vulnerability to human error. The ability to unlock a door may be compromised if a key is lost or a password forgotten.

Furthermore, conventional key and password-based systems cannot verify the identity of the person access to the premises. For instance, a stolen key can grant the unauthorized access to a building, and the same is true for a password; anyone who knows it can enter the building. This situation demonstrates that neither the key nor the password demonstrates that neither a key nor a password inherently distinguishes the rightful user. Consequently, the traditional use of keys and passwords has limitations regarding security and reliability [1].

Biometrics authentication, which utilizes unique human characteristics, present a promising alternative to conventional keys or passwords. Biometrics use physical traits that are distinct for each individual, such as fingerprints [2], veins [3], iris patterns [4], facial features [5], and voice [6]. These characteristics are unique to each person, making biometric-based security inherently personal. When a biometric trait serves as the password, human carelessness is no longer a risk; it is impossible to “lose” a fingerprint or accidentally forget a person's biometric trait. Furthermore, biometric traits are extremely difficult to forge [7].

Among biometric methods, finger-vein recognition stands out by using the unique vein patterns within a person’s fingers for identification. These patterns differ for person to person and even among individual fingers on the same hand, and since they lie beneath the skin, they are highly resistant to forgery [8]. Additionally, finger-vein biometrics offer several advantages over other biometric methods, as shown in Table 1, making it a preferred choice for secure authentication.

Table 1 indicates that vein biometrics exhibit superior features compared to other biometric methods. As seen in Table 1, the cost of vein biometrics is moderate while providing excellent accuracy and strong anti-forgery characteristics. Finger-vein recognition can be conducted using two approaches. The first approach employs conventional image processing methods, which utilize algorithms to manipulate pixel values to achieve the desired result. The second approach involves computational intelligence (CI), primarily using systems developed with machine learning techniques. CI is the preferred modern approach, as shown in Table 2. This paper adopts the conventional image processing method due to the limitations of the Raspberry Pi 3, which is unable to handle the complex machine learning algorithms and large data requirements associated with the CI approach.

Table 1
Comparison of Major Biometrics Method [1]

Type of Biometrics	Security		Convenience		
	Anti-Forgery	Accuracy	Speed	Cost	Size
Fingerprint	Bad	Average	Average	Good	Good
Iris	Average	Good	Average	Bad	Bad
Face	Average	Bad	Average	Bad	Bad
Voice	Average	Bad	Average	Average	Average
Vein Pattern	Good	Good	Good	Average	Average

For vein recognition to achieve widespread acceptance, it is essential to reduce equipment costs; however, using low-resolution cameras can lead to poor image quality. Additionally, increasing the number of individuals in the recognition dataset may introduce people with similar recognition features, potentially degrading the system's response time and stability, thus complicating practical application. Existing vein recognition devices often require users to press their fingers directly onto a sensor, which can lead to sensor contamination from finger grease and raise sanitary concerns. Therefore, it is crucial to develop recognition devices that enable contactless data acquisition. Three key issues were addressed in [9]: (1) developing low-cost, contactless devices, (2) achieving a high accuracy rate, and (3) ensuring real-time processing.

Table 2 illustrates the utilization of Raspberry Pi as an embedded platform for finger-vein recognition in biometric verification mode in existing research. While the specific model of Raspberry Pi remains unspecified, it is presumed that the recent Raspberry Pi 4 model was employed. The absence of related work implementing identification mode is likely attributable to the significant computational requirements associated with comparing the test image against ground truth images of all users in the database. Each of these studies utilized its own dataset and achieved relatively favorable Equal Error Rate (EER) values of less than 2% through the utilization of machine learning approaches.

The remainder of this paper is organized as follows. In Section II, we discuss the proposed approaches. Results and discussion follow this in Section III. Finally, this paper is concluded with a summary of the work.

Table 2
Related Work implemented on Raspberry Pi platform

Ref.	Preprocessing	Feature Extracted	Matching Strategy
[9]	Adaptive image contrast enhancement	Repeated line tracking (RLT) method, histogram of oriented gradient (HOG)	Support vector machine (SVM)
[10]	RGB to gray scale conversion, image resizing and filtering	K-Means Segmentation and canny edge detection	Support vector machine (SVM)
[11]	Semantic segmentation DeepLabv3+	Enhanced maximum curvature (EMC) method	Support vector machine (SVM)
[12]	PCA filter, binary hashing, histograms.	Block-wise histograms	k-Nearest Neighbour

II. METHODOLOGY

A. Finger Vein Recognition

A suitable design model was identified and upgraded with the required specifications to establish the topological structure of the final model. This step aims to determine the equivalent mechanism skeleton and kinematic chain required for developing the new design.

B. Types of Finger-Vein Recognition System

There are two types of finger vein recognition systems: identification and verification, as shown in Figure 1. Verification systems are described as 1-to-1 matching systems because the system matches the extracted feature to only a particular entry in the database. The purpose of verification is to check whether the presented features correspond to the claimed individual. For example, if a person presents themselves as a specific individual, the system will compare their finger-vein features only to that person's record in the database. This function reduces the time required for feature comparison.

Identification systems, on the other hand, are described as 1-to-*n* matching systems, where *n* represents the total number of records in the database. In this system, the extracted features are matched against the entire database to identify the individual based on the features presented.

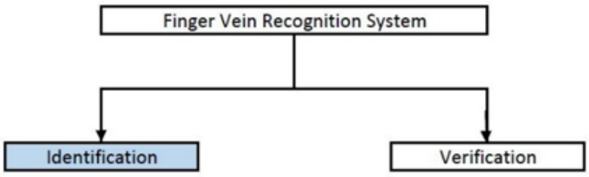


Figure 1. Type of Finger-vein Biometric Recognition Systems

The Python programming language and the OpenCV library were used to develop algorithms for the image-processing tasks. The logos of each library are shown in Figure 2.

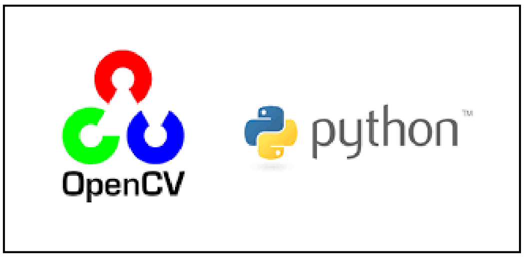


Figure 2. OpenCV and Python Logos

C. Image Quality Assessment

The image quality assessment was carried out using a modified version of the 2D entropy equation as described by Y.H Lee, 2017 [13][14]. The method begins by applying Pulse Width Modulation (PWM), starting at 20% PWM and gradually increasing to 100%, while capturing five finger-vein images at different PWM levels. All saved images then undergo entropy calculation, and the result with the highest entropy value is selected as the best. The equation for the Modified 2D Shannon Entropy is shown in Equation 1. The flowchart for image quality assessment is shown in Figure 3.

$$H_{2D} = \frac{1}{m\,X\,n} \sum_{i=j>T}^{L} L_{ij}\; x\; \left(log_2(m\,X\,n) - log_2(L_{ij})\right) \tag{1}$$

where, the coordinate of one pixel in the grayscale image with gray level, L and the size of m*n is (i,j). This formula can also increase computation speed as $\log_2$ (m *n) is constant and can be reused to optimize performance [2].

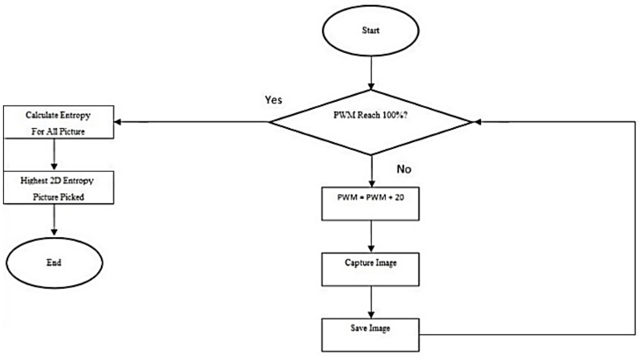

Start
PWM Reach 100%?
Yes
No
Calculate Entropy For All Picture
Highest 2D Entropy Picture Picked
End
PWM = PWM + 20
Capture Image
Save Image

Figure 3. Flowchart of the image quality assessment

D. Image Processing

As shown in Figure 4, after quality inspection, the selected finger-vein image proceeds through three additional image processing steps: preprocessing, feature extraction and matching strategy.

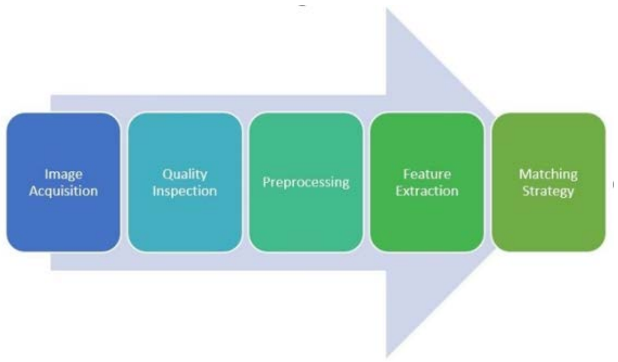


Figure 4. Flow of the utilized algorithm

E. Image Processing

Preprocessing is an essential step in the finger-vein biometric system as the raw image captured by the camera contains extraneous information and noise that prevents direct processing. Thus, a series of image processing techniques must be applied to the raw image before feature extraction can occur.

As shown in Figure 5, preprocessing consists of seven steps after converting the image to gray scale: contrast-limited adaptive histogram equalization (CLAHE), image normalization or segmentation, non-local denoising, low pass Gaussian filter, adaptive thresholding, binary median blurring, and finally inverting the image.

CLAHE is used to enhance the image contrast, while image normalization isolates the Region of Interest (RoI) and reduces the image size to improve computation speed. Adaptive thresholding converts the grayscale image into a binary format, followed by the binary median blurring to further refine the image before inverting it for the feature extraction process. Non-local denoising and low-pass Gaussian filters reduce noise in the image, producing higher image quality before adaptive thresholding.

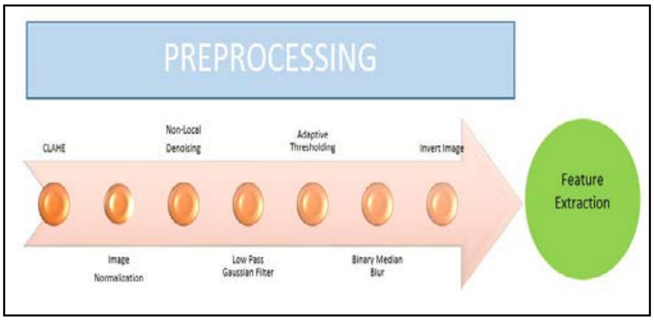


Figure 5. The seven preprocessing steps before feature extraction

F. Feature Extraction

After undergoing preprocessing, the finger-vein images now have their veins exposed in binary form. However, the entire finger-vein image cannot be used directly as features, as the shape of the vein is highly dependent on the geometry of the finger during image capturing. Hence, specific vein features must be extracted from the finger-vein images.

The feature extraction step consists of two processes: applying the thinning algorithm and extracting minutiae points. The thinning algorithm is used to transform the binarized image from the preprocessing stage into a finger-vein image that is only 1 pixel wide. This facilitates the subsequent extraction of minutiae points from the finger-vein lines, which will serve as the extracted features. The thinning algorithm used is a fast method developed by Zhang Suen, designed to reduce the width of the finger-vein while preserving most of the original vein shape.

After thinning, features known as minutiae points are extracted. Minutiae points, commonly used in the fingerprint biometric system, are also adopted in this work since the structure of finger-veins resembles fingerprint patterns. Various types of minutiae points are used, as shown in Figure 6.

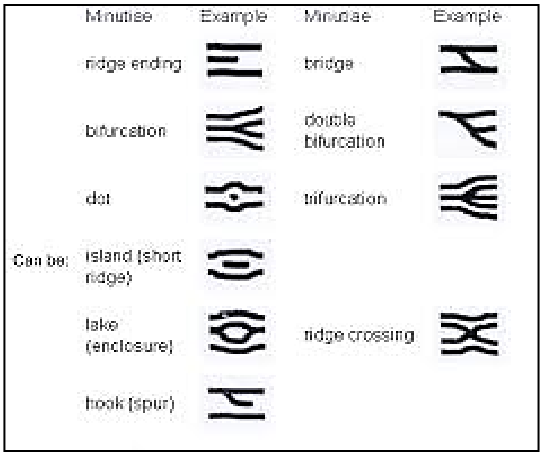


Figure 6. Type of Minutiae Points [15]

In this system, only two types of minutiae points are considered: the ridge ending or end points and the bifurcation points. The endpoints are locations where the veins terminate abruptly, whereas the bifurcation points are where a vein diverges into two or more branches of veins. The minutiae points of these two types are identified in the image and then saved into a text file if the image is part of a template. The end and bifurcation points are determined by checking the cross-number values shown in Table 3.

Table 3
Cross Number Property for Minutiae Points [16]

Cross Number	Property
0,1	Isolated Point
2,3	Ending Point
4,5	Connecting Point
6,7	Bifurcation Point
8	Cross Point

The cross number is used by applying a window size of 3*3 over each pixel in the thinned image to count the number of '1's in the window. If the count is 0 or 1, the pixel is classified as an isolated point.

G. *Matching Strategy*

The proposed methodology employs the Modified Hausdorff Distance (MHD) as the matching strategy, leveraging its robust algorithmic framework. Prior to the implementation of the matching procedure, an alignment of points in both the query and template images is required.

The alignment process is accomplished through a combination of RANSAC (Random Sample Consensus) and Affine Transform techniques. RANSAC is utilized to identify the optimal inlier points among the minutiae, which are then used to determine the best affine coefficients. These coefficients help detect and correct any alignment discrepancies between the query image and the database image. Once aligned, the images undergo the Modified Hausdorff Distance (MHD) calculation to measure their similarity.

III. RESULTS AND DISCUSSION

A. *Finger-Vein Identification*

Figure 7 illustrates the finger-vein identification device, which consists of a simple box with an opening for finger insertion. Figure 8 provides a view of the interior, showing the placement of the Raspberry Pi at the bottom. Directly above the Raspberry Pi is a black box designed to house the camera and the NIR (Near-Infrared) illuminating circuit. The black box serves to minimize interference from external lighting.

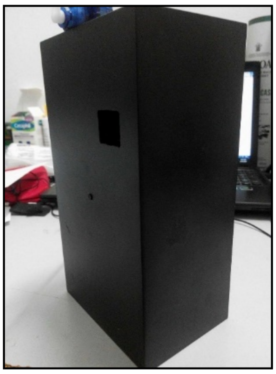


Figure 7. Finger-Vein Identification's Device

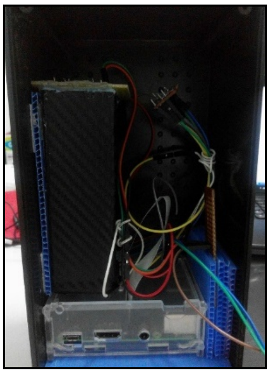


Figure 8. Interior of the Finger-Vein Device

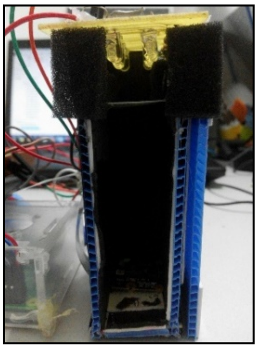


Figure 9. NIR Illuminating Circuit and Camera

The Raspberry Pi camera is positioned at the bottom of the box. Figure 9 shows the NIR illuminating circuit, which consists of 10 IR LEDs, and a plastic slit placed beneath the NIR illuminating circuit to allow the finger to rest on it, helping to slightly restrict finger movement during image acquisition. Figure 10 shows the servo motor used to simulate the door mechanism. The servo motor is attached to a door to act as a latch. If the finger-vein device successfully matches the finger-vein, it will activate the servo motor to grant access through the door.

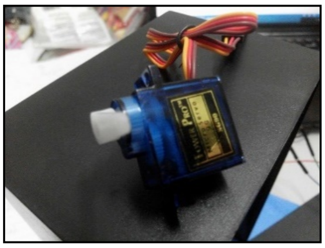
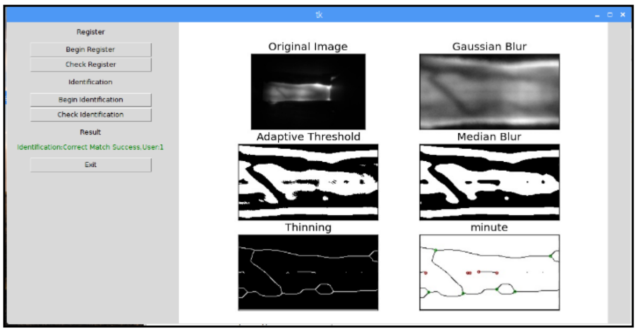


Figure 10. Servo Motor Demonstrating the Door Mechanism

B. Graphic User Interface (GUI)

A GUI was created to facilitate user interaction with the finger-vein identification device. Figure 11 shows the GUI display when a successful match is made. The finger-vein image is displayed to illustrate the process from the original image to the extraction of minutiae points. If the user is successfully matched, a green indicator appears on the left side of the GUI, confirming successful identification for the specific user.



Identification:Correct Match Success,User:1

Figure 11. Successful Identification Process

C. 2D Entropy Analysis

Figure 12 shows the 2D Entropy values for three users. The optimal PWM level varies for each user. From Figure 12, it can be seen that user 1 obtained the best vein image at PWM 100%, whereas user 2 achieved the best image at PWM 40% and user 3 at 60%. The result proves that this method is sensitive and effective for evaluating and selecting the best image from multiple PWM levels, enhancing the quality of the verification device.

D. Biometric Performance Evaluation: ERR (Equal Error Rate)

The ERR graph was plotted using the database of 100 index fingers, with each user contributing 10 images of their index finger for the database of the device. The EER was derived by plotting the False Acceptance Rate (FAR) and False Rejection Rate (FRR) graphs. The threshold values of the FAR, FRR and EER graph were based on the MHD values calculated by comparing the query and the template images.
The FAR graph was generated by selecting one user's database as the template image and using the remaining nine images from the same user's database as the query images. For example, User 1’s first image is compared with every image from User 2 to 10. Then, User 1's second image was similarly compared with every other user’s images, except User 2.

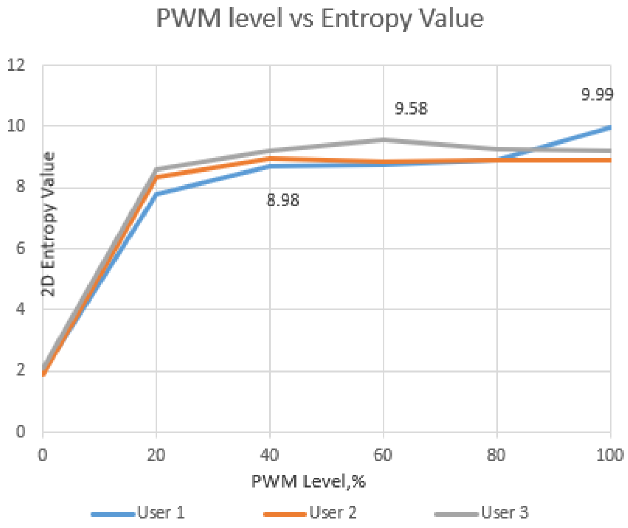


Figure 12. Graph of PWM Level Against 2D Entropy Value

This process continued until each user's images were compared with the entire database, excluding their own images. For example, User 1's first image was not compared with User 1's second image. This approach allowed for determination of the threshold values between templates and queries from different user’s databases.

The FRR graph was generated by comparing a user's images within their own database. For example, User 1's first image was compared with User 1's second image. Rather than using the conventional matching strategy of comparing one query image to one template image, a method was proposed in which one query image was matched with all templates in a user's database. As each user had 10 images in the database, 10 MHD values were generated for each user. The mean of these 10 MHD values was then calculated to serve as the final value for comparison.

From Figures 13 and 14, it is evident that the device achieved an Equal Error Rate (EER) value of 7.8852%, with a corresponding Modified Hausdorff Distance (MHD) threshold value of 18.1976. This EER value was relatively low, indicating a device accuracy of 92.12%. This EER value was attributable to the utilization of identification biometric mode in this study. It is noteworthy that employing verification mode could potentially enhance the EER.

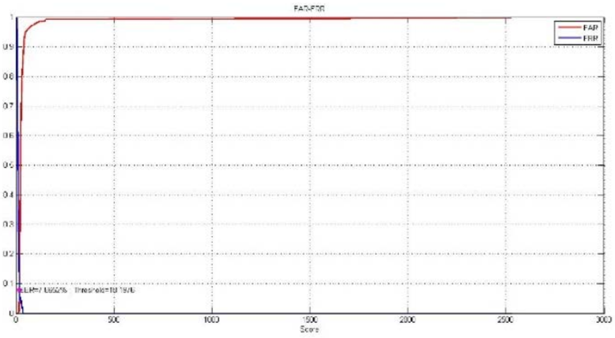


Figure 13. Equal Error Rate of Design's Biometric Device Mean MHD

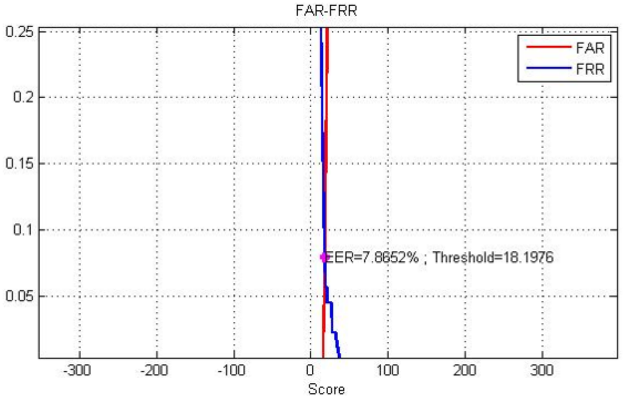


Figure 14. Equal Error Rate of Design's Biometric Device Mean MHD

Table 4 presents a comparative analysis of this study's performance with that of other related works. The Equal Error Rate (EER) achieved in this study differs significantly from that of other works, primarily due to the adoption of identification biometric mode, as opposed to the verification mode utilized in other studies. In identification mode, a specific test sample is compared with the ground truth images of all users in the dataset. Despite this difference, the accuracy attained in this study remains consistent with that of other works. It is worth noting that conducting thorough benchmarking poses challenges, as each study employs its own self-collected dataset and unique personal computer configurations. Nevertheless, the approach proposed in this study shows promise for further refinement.

Table 4
Performance comparison with other related works

Ref.	No. of users	Test samples	Biometric mode	Performance
[9]	32	-	Verification	EER: 1.06% Speed: 0.61 s
[10]	10	100	Verification	EER: 0.0015%
[11]	32	-	Verification	EER: 0.84%
[12]	10	50	Verification	Accuracy: 92.67%
This study	10	100	Identification	EER: 7.18% Accuracy: 92.12%

IV. CONCLUSION AND FUTURE WORK RECOMMENDATION

An automated, real-time finger-vein identification device for door access control was proposed, utilizing the Raspberry Pi 3 embedded platform. This device records an individual's finger-vein image using a matrix of near-infrared light-emitting diodes (NIR LEDs) to grant access to authorized users. The image then undergoes several preprocessing stages to enhance quality before the Modified Hausdorff Distance (MHD) technique compares the minutiae points with the template stored in the database. The 2D Entropy algorithm performs further analysis to identify the correct user. The device achieves an Equal Error Rate (EER) of 7.88%, corresponding to an accuracy of 92.12%. This study's contributions include detailed development specifics and proposed solutions to issues encountered during the research.

Several future works and recommendations can be proposed for improvement. Upgrading the identification process to a verification-like procedure could increase the device's computational speed. The matching method could be replaced with a more robust algorithm, such as machine learning techniques, or the segmentation, feature extraction, and classification stages could be replaced with a deep learning approach. To support these enhancements, the Raspberry Pi platform should be updated to the most recent model, Raspberry Pi 4.

A better finger placement box could also be designed, incorporating a U-shaped area that conforms to the shape of a finger. This design would ensure the sides of the finger are fully covered, facilitating easier background filtering. Additionally, the area beneath the finger should be free from any obstructions during the image acquisition process, as pressing the finger onto a hard surface could cause blood dispersion, thereby affecting the quality of the original finger-vein image.

ACKNOWLEDGMENT

The authors would like to acknowledge the support from the Machine Learning and Signal Processing (MLSP) research group under the Centre for Telecommunication Research & Innovation (CeTRI), Fakulti Teknologi dan Kejuruteraan Elektronik dan Komputer (FTKEK), Universiti Teknikal Malaysia Melaka (UTeM).

CONFLICT OF INTEREST

Authors declare that there is no conflict of interest regarding the publication of the paper.

AUTHOR CONTRIBUTION

The authors confirm contribution to the paper as follows: study conception and design: A. R. Syafeeza and Albert Ngan Ban Chew; data collection: A. R. Syafeeza Albert Ngan Ban Chew; analysis and interpretation of findings: A. R. Syafeeza Albert Ngan Ban Chew, Asar Khan and Norihan Abdul Hamid; draft manuscript preparation: Wira Hidayat Mohd Saad, and Airuz Sazura A. Samad. All authors had reviewed the findings and approved of the final manuscript.

REFERENCES

[1] Y. Nakamaru, M. Oshina, S. Murakami, B. Edgington, and R. Ahluwalia, "Trends in finger vein authentication and deployment in Europe," Hitachi Rev., vol. 64, no. 5, pp. 275–279, 2015.

[2] G. C. Hembroff, X. Wang, and S. Muftic, "Providing an additional factor for patient identification based on digital fingerprint," in Proc. of 2nd USENIX Work. Heal. Secur. Privacy, 2011, pp. 3–4.

[3] S. A. Radzi, M. Khalil-Hani, and R. Bakhteri, "Finger-vein biometric identification using convolutional neural network," Turkish J. Electr. Eng. Comput. Sci., 2016, vol. 24, no. 3, https://doi.org/10.3906/elk-1311-43.

[4] R. P. Wildes, "Iris recognition: an emerging biometric technology," in Proc. of IEEE, vol. 85, no. 9, pp. 1348–1363, 1997, https://doi.org/10.1109/5.628669.

[5] T. Satonaka, "Biometric watermarking based on face recognition," in Proc. SPIE 4675, Security and Watermarking of Multimedia Contents IV, 2002, pp. 641–651, https://doi.org/10.1117/12.465325.

[6] J. D. Brand, J. S. D. Mason, and S. Colomb, "Visual Speech: A Physiological or Behavioural Biometric?," Third International Conference, AVBPA 2001, pp. 157–168. doi: 10.1007/3-540-45344-X_23.

[7] B. Miller, "Vital signs of identity [biometrics]," IEEE Spectr., vol. 31, no. 2, pp. 22–30, 1994, https://doi.org/10.1109/6.259484.

[8] B. Edgington, "Introducing hitachi's finger vein technology: a white paper," Hitachi's Finger Vein Technology, 2007.

[9] C. H. Hsia and C. F. Lai, “Embedded vein recognition system with wavelet domain,” Sensors Mater., vol. 32, no. 10, pp. 3221–3234, 2020, https://doi.org/10.18494/SAM.2020.2861.

[10] R. Sarala, E. Yoghalakshmi, and V. Ishwarya, “Finger vein biometric based secure access control in smart home automation,” Int. J. Eng. Adv. Technol., vol. 8, no. 6, pp. 851–855, 2019, https://doi.org/10.35940/ijeat.F8044.088619.

[11] C. H. Hsia and C. H. Liu, “New hierarchical finger-vein feature extraction method for iVehicles,” IEEE Sens. J., vol. 22, no. 13, pp. 13612–13621, 2022, https://doi.org/10.1109/JSEN.2022.3177472.

[12] Q. E. Wen, N. M. Kamaruddin, and B. A. Rosdi, “Raspberry pi-based finger vein recognition system using PCANet,” J. Phys. Conf. Ser., vol. 1529, no. 2, 2020, https://doi.org/10.1088/1742-6596/1529/2/022068.

[13] Y. H. Lee, M. Khalil-Hani, and R. Bakhteri, “FPGA-based finger vein biometric system with adaptive illumination for better image acquisition,” in Proc. of 2012 IEEE Symp. Comput. Appl. Ind. Electron., 2012, pp. 107–112, https://doi.org/10.1109/ISCAIE.2012.6482079.

[14] Y. H. Lee, M. Khalil-Hani, R. Bakhteri, and V. P. Nambiar, “A real-time near infrared image acquisition system based on image quality assessment,” J. Real-Time Image Process., vol. 13, no. 1, pp. 103–120, 2017, https://doi.org/10.1007/s11554-016-0586-y.

[15] S. Coletta, “Fingerprints: Points, Type, and Classification.” Accessed: Jun. 13, 2024. [Online]. Available: https://www.suecoletta.com/fingerprints-points-type-and-classification/

[16] A. S. Chaudhari, G. K. Patnaik, and S. S. Patil, “Implementation of minutiae based fingerprint identification system using crossing number concept,” Inform. Econ., vol. 18, no. 1, pp. 17–26, 2014, https://doi.org/10.12948/issn14531305/18.1.2014.02.