e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

AN ENHANCED BIOMETRIC AUTHENTICATION SYSTEM FOR INNOVATIVE VEIN PATTERN ANALYSIS

Sivamurugan G[*1], Tamilselvan S[*2], Vetrivel K[*3], R. Gnanaprakasam[*4]

[*1,2,3,4]Department Of Electronics And Communication Engineering, Kongunadu College Of Engineering And Technology, Trichy, India.

DOI: https://www.doi.org/10.56726/IRJMETS71544

ABSTRACT

Finger vein authentication is a highly secure and credible biometric identification technique based on the unique vein structures found in an individual's finger. This work presents a method for finger vein authentication using machine learning, which involves feature extraction, feature selection, and optimization techniques to achieve superior recognition accuracy. The proposed work adopts a sequential workflow, starting from image acquisition and preprocessing, followed by feature extraction in time, frequency, and special domains. A selective optimization mechanism is performed to avoid redundancy and improve efficiency. In training, an optimized set of detectors is used to identify vein patterns via an evolutionary optimization mechanism, such as selection, mutation, and crossover. During testing, the trained model works on the test data matching observables features against the optimized set of detectors for verification. Experimental analysis indicates that the suggested technique improves authentication accuracy, minimizes false positives, and enhances operational speed. It can be well-imagined in high-security applications such as financial transactions, access control systems, and identity verification systems. In this regard, a CNN-inspired evolutionary optimization approach is applied for training. Basically, it comprises initialization, evaluation, selection, mutation, and crossover processes that reward in producing a set of optimized detectors meant for classification. It is especially effective in high-security applications such as banking, secure access control, and identity authentication in critical infrastructures.

Keywords: Finger Vein, Authentication, Biometric Recognition, Security, Machine Learning, Feature Extraction, Feature Selection, Optimization, Image Preprocessing, Time Domain Features, Frequency-Domain Features, CNN.

I. INTRODUCTION

The Global Knowledge Society and Diversity-The life of the average person now faces threats of crime anywhere in the world. Terrorism is such a phenomenon that may spread instaneously throughout the world and escalate the intensity of the threat. In dealing with the very high security demands, biometric systems have become the ideal answer with better accuracy and ease of use. The pattern of human vascular pattern is different for each individual, difficult to forge, unchangeable by color and pigmentation of the skin, and does not change with age. The purpose of vein detection, where infrared light of wavelength 700nm - 1000nm can penetrate most human tissues but blood hemoglobin can completely absorb infrared light, is perplexing. We compare Near-Infrared (NIR) and Far Infrared (FIR), as the former is capable of best capturing larger vein patterns. Then we capture the vein pattern using a light transfer technique. The finger is then placed in IR light such that the pattern of the veins is taken as a shadow pattern beneath the finger by a web camera. Figure 3 displays the final authentication process diagram. All published papers must and have generally proved that human waterways can be applied for human self-identification systems. Our research assists in personal biometric recognition. This paper deals with testing the identification of arteries and discusses various difficulties in this respect: a. Photo captured using common web cameras contains salt and pepper noise and the gray matter distribution in different experiments tends not to match for the mismanaged of all the camera.

b. Under usual conditions, the dimension of the vein in the image that presents it is extremely small. Good outline separation must be done to produce a working binary image that provides good details of finger veins. The applied pressure on our finger will result in the shrinkage or deformation of the inner vein, and thus it is essential, in this case, to form a weak border for the finger so that the user can keep the finger in a relaxed position. Additionally, this near-infrared imaging technology is important for capturing vein patterns that offer

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

high contrast. Infrared light penetrates the skin and highlights the hemoglobin-rich veins, making them more distinguishable from surrounding tissues. Fine-tuning the illumination conditions and optimizing the image processing mirrors constantly along with enhancing clarity and differentiation of the captured vein patterns would go a long way in boosting the overall efficiency of the biometric system.

II. LITERATURE REVIEW

Finger vein authentication is an emerging form of biometric identification that uses the unique vein patterns of an individual's finger. This technology is finding wider application due to its reliability, security, and forgery resistance for secure access control, banking, and critical infrastructure systems. The objective of this literature review is to discuss the development of finger vein authentication systems with particular emphasis on the rollout of machine learning and optimization techniques to improve recognition accuracy and operational efficiency. Four main steps in any finger vein authentication system involve: image acquisition, preprocessing, features extraction, and matching. The near-infrared imaging is responsible for the image acquisition through the capturing of the subcutaneous vein patterns. Subsequently applied preprocessing techniques such as noise reduction, contrast enhancement, and region of interest (ROI) extraction are done in order to obtain good quality images from the acquired signals (Kumar & Prathyusha, 2009).

Feature extraction plays an important role in finger vein recognition. Techniques such as Gabor filters, Local Binary Patterns (LBP), and Wavelet Transform have been explored to extract vein pattern features from both spatial and frequency domains. According to Miura et al. (2004), in terms of vein feature extraction, repeated line tracking has been proven to be an effective approach, while Wang et al. The continuous enhancements in machine learning have further enhanced the performance of finger vein authentication systems. The Convolutional Neural Networks have shown great promise in learning features and classification owing to their ability to automatically learn hierarchical features from images (Zhang et al., 2019). Hybrid models combining machine learning algorithms with optimization techniques have been explored for enhanced recognition accuracy.

For finger vein authentication, various optimization techniques are very crucial to reduce redundancy and improve computational efficiency. Genetic algorithms from evolutionary algorithms, which perform selection, mutation, and crossover operations, are an optimization of the feature set iteratively into a much smaller and refined set of detectors, thus minimizing the false acceptance and rejection rates and improving the accuracy of the intended system. Experimental studies came to support the fact that finger vein authentication systems based on conditions like DFUs. Meanwhile, Ragnarson Tenn Vall, and Apelqvist highlight the substantial economic burden of DFUs, pointing out the high healthcare costs associated with ineffective management. Earlier research has demonstrated various feature extraction techniques for finger vein recognition. Miura et al. [2] proposed a repeated line tracking method to enhance vein pattern detection. However, this method faced challenges with image noise and illumination variations. Similarly, Wang et al. [3] explored the use of Gabor filters for vein extraction, which improved accuracy but was computationally expensive. Recent advancements have incorporated machine learning for vein authentication. Convolutional Neural Networks (CNNs) have been widely adopted to automate feature extraction and improve classification accuracy [4]. Deep learning-based methods, such as those proposed by Yang et al. [5], have shown remarkable performance in vein pattern recognition but require extensive computational resources and large datasets. Optimization techniques have also been applied to improve vein authentication systems. Genetic Algorithms (GAs) and Particle Swarm Optimization (PSO) have been used to select the most discriminative features while minimizing redundancy [6]. These evolutionary algorithms enhance the model's efficiency and accuracy by dynamically selecting relevant vein features. Despite these advancements, challenges remain in vein pattern variations caused by pressure differences, image acquisition inconsistencies, and environmental factors. Some studies have introduced multi-frame averaging techniques and pose correction algorithms to mitigate these effects [7].

However, there is still a need for a more robust and adaptive system that can handle real-world variations effectively. This paper builds upon these existing studies by integrating CNN-based feature extraction with evolutionary optimization mechanisms. By addressing the limitations of traditional feature extraction and classification methods, the proposed approach aims to enhance accuracy, efficiency, and robustness in biometric authentication systems.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

III. METHODOLOGY

A. Experiment Setup

To ensure accurate and repeatable results, the experimental setup was designed in a controlled environment to mimic real-world biometric authentication conditions. The following components were used:

- In order to capture high-definition finger vein images, a Near-Infrared camera was used with light in a range from 850nm to 950nm that allowed for a visible contrast of veins underneath the skin surface.
- This was made possible by the use of infrared LED arrays as the source of illumination, placing the hand as in reference to the specially designed finger placement module to achieve consistency and decrease variances from hand movements.
- The computing unit was basically a high-performance or station configured with the desired deep learning frameworks for image processing and analysis such as TensorFlow.

The environment was controlled to spend minimal external noise and variability, allowing for reliable extraction and acquisition of data.

B. Image Acquisition and Preprocessing

Finger vein images were acquired under standardized conditions to enhance uniformity. The preprocessing pipeline included:

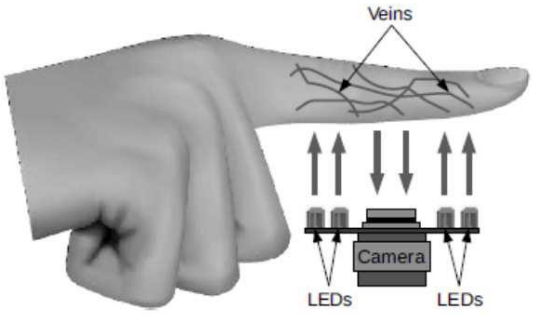

Fig 1: Preprocessing

- Grayscale Conversion: Convert the raw image to grayscale to enhance computational efficiency.
- Contrast Enhancement: Adaptive histogram equalization to improve the visibility of the veins.
- Noise Reduction: Median filtering for background noise reduction to improve clarity of the image.
- Region of Interest Extraction: Scheming and separating the region of the finger to exclude unnecessary backgrounds.

C. Feature Extraction

Feature extraction will be a combination of traditional and deep learning-based techniques:

- Morphological analysis: Patterns of vein are extracted through Gabor filters and some morphological operations.
- Wavelet transform: Frequency-based analysis is employed to enhance the detection of the structure of veins.
- High-level features of the vein patterns: a CNN is trained for the extraction of high-level representations related to the vein pattern.

D. Feature Selection and Optimization

To improve recognition accuracy and reduce computational load:

- Attenuation Analysis: In order to other things augment recognition exactitude and lessen the computational load, redundancy among features was caused out by applying PCA, while GA was put into application to optimize feature selection.
- Classification and Authentication: A CNN-based module was used to perform vein pattern classification and authentication.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

- The model was trained with the following: Supervised learning a set of labelled vein patterns was used to train the model Cross-validation - K-fold was used to ascertain an all-around performance evaluation; Decision thresholding - a similarity score was determined to evaluate the success of the authentication process.

E. Prediction

When speaking about a rotation of up to 90 degrees, the horizontal and vertical flipping of pictures, the amount of alterations introduced into position, one might mention that we train on a variable test set and use Image Data Generator to create a stream of somewhat worse pictures during the training of the model. This gives rise to a discussion on the operations which perform the Exponential Linear Unit (ELU) One layer fully incorporated just after the last major integration. [`same`] simply means that the output volume pieces will be the same size as the input.

Batch normalization is a way to use data for informing just such layers of a hidden network, typically producing the hidden layer activations of each mini-batch (hence the name) in a manner that keeps the mean activation near 0 and the standard deviation close to 1. The layers now have a fast quit surf train after them assigned on very high learning.

F. Limitations and Controls

Several measures were taken to ensure validity and reliability:

- Standardized Environment: The experiments were conducted in controlled light and temperature settings.
- Consistent Finger Placement: To reduce variation, a placement guide helped.
- Repetitive Trials: A number of images were captured for each subject to make sure that, for their robustness, errors were minimized.
- Cross-Dataset Validation: The model was evaluated using external datasets to check how well generalization happened.

G. Summary of Methodology

The following research utilizes a systematic approach for biometric authentication based on the analysis of vein patterns. A controlled experimental setup for making measurements was constructed in order to achieve an accurate and verifiable repeatability. High-resolution images of fingers are captured with a Near-Infrared (NIR) camera operating in the wavelength range of 850nm–950nm, using infrared LED illumination for enhancement. equalization, performing median filtering for noise reduction, and eliminating background interference by performing extraction of the ROI. The feature extraction procedure depicts a combination of conventional and deep-learning-dependent methods like morphological analysis by means of Gabor filter, wavelet transform, and also uses CNN for high-level pattern recognition.

Feature selection is optimized using Principal Component Analysis (PCA) to remove redundant data and Genetic Algorithms (GA) to enhance classification accuracy. A CNN-based classifier is trained using supervised learning with cross-validation to improve performance. Authentication is determined using similarity scores, and statistical metrics such as accuracy, precision, recall, FAR, FRR, and ROC curves assess model efficiency. Environmental controls, consistent finger placement, and repetitive trials ensure reliability, providing a strong foundation for secure and accurate vein-based biometric authentication systems.

IV. EXISTING SYSTEM

Fingerprint verification is a safe and secure technique employed to authenticate an individual's identity by scanning and examining their distinctive fingerprint layer and patterns. The technology is extensively applied in device such as smart phones, security systems, and access controls, because of its dependability and convenience. This is a process of taking an individual's fingerprint and matching it with stored fingerprint information to verify their identity.

The system starts with a fingerprint sensor, which captures the user's fingerprint when he puts his finger over the device. This image is then processed to make it clear by eliminating noise or distortion. Once the image is clean, the system extracts unique characteristics like the pattern of the ridges, minutiae points (ridge endings and bifurcations), and other unique markers. These characteristics are mapped into a fingerprint template, which is a digital signature of the key details of the fingerprint.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

During the enrollment phase, the system captures the fingerprint of the user through a biometric sensor. Thereafter, a feature extraction algorithm processes the fingerprint image,

Seventh Crossroads of these are minutiae points, ridge bifurcations, and ridge endings. Eventually, these features are converted into a biometric template, which is securely stored in a database. Encryption mechanisms safeguard the stored templates from unauthorized access to assure privacy and security. The authentication phase takes the new fingerprint sample, extracts its features, and matched it against a stored template using a comparison algorithm. If the similarity score is more than a prespecified threshold, access is granted; otherwise, it is denied.

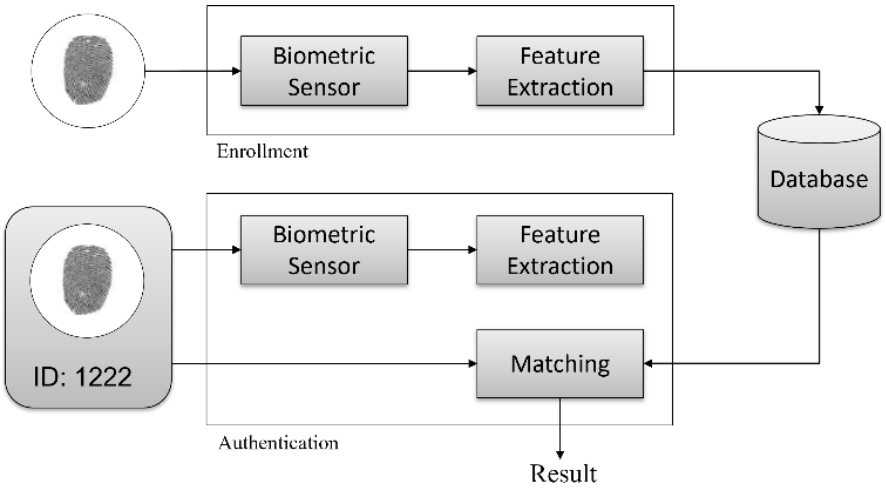

Fig 2: Existing Block Diagram

In order to improve security, the system introduces various types of protection such as template encryption, liveness detection against spoofing attacks, and multi-factor authentication. Key metrics such as False Acceptance Rate, False Rejection Rate, Equal Error Rate, and the Receiver Operating Characteristic curve provide measures of performance that help determine accuracy and reliability. The application of fingerprint authentication includes access control systems, banking security, healthcare, and smartphone authentication.

V. PROPOSED SYSTEM

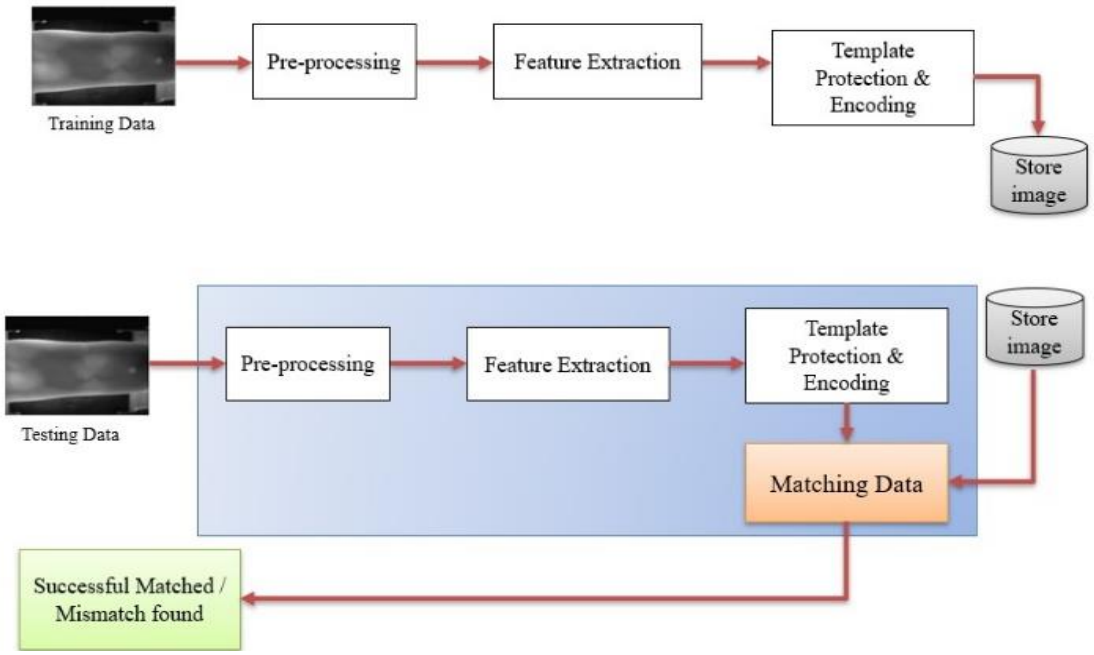

Fig 3: Systematic Architecture

The proposed vein-based biometric authentication system takes a structured approach towards enhanced

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

security and accuracy through feature extraction, feature selection, and an ML-based classification method. The system operates in a sequential pipeline process, starting with image acquisition from a NIR imaging device, and then the acquired training and testing images are preprocessed to improve the visibility of veins and remove noise. In the feature extraction stage, the techniques used to derive meaningful information from the vein patterns include time-domain analysis, frequency-domain transformation, and spatial feature extraction. The features extracted from such analysis will be high-dimensional, and thereafter, they will go through a feature selection process to trim them down in order to be more efficient computationally and at the same time increase classification accuracy. This feature selection process relies on tree-based or genetic algorithms in order to identify the relevant features. The selected features, in turn, should be used for training and testing in a machine learning framework. The training phase consists of an optimization-based approach whereby the dataset undergoes evaluation, selection, mutation, and crossover to derive an optimized detector set. After that, the classifier matches the input vein pattern to an existing template stored in the database. The system, based on the similarity threshold, makes a final decision to ensure a high authentication accuracy.

Common biometric metrics are used to evaluate performance, including False Acceptance Rate, False Rejection Rate, and Equal Error Rate, while a Receiver Operating Characteristic curve is analyzed to assess the trade-off between sensitivity and specificity. Integrated feature selection with machine learning optimization techniques enhances model robustness: reducing error rates and improving overall security. The proposed system can be applied to high-security contexts, such as banking, health access, and border patrol.

VI. RESULTS AND DISCUSSION

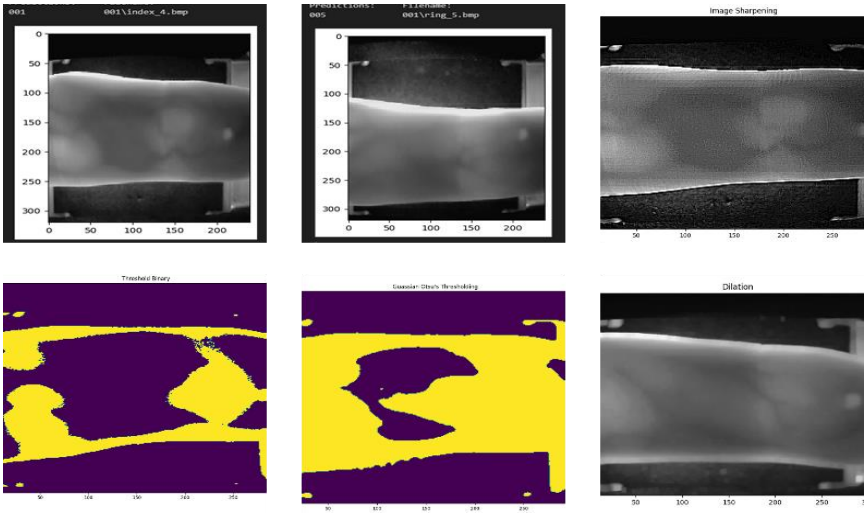

Fig 4: Preprocessing image

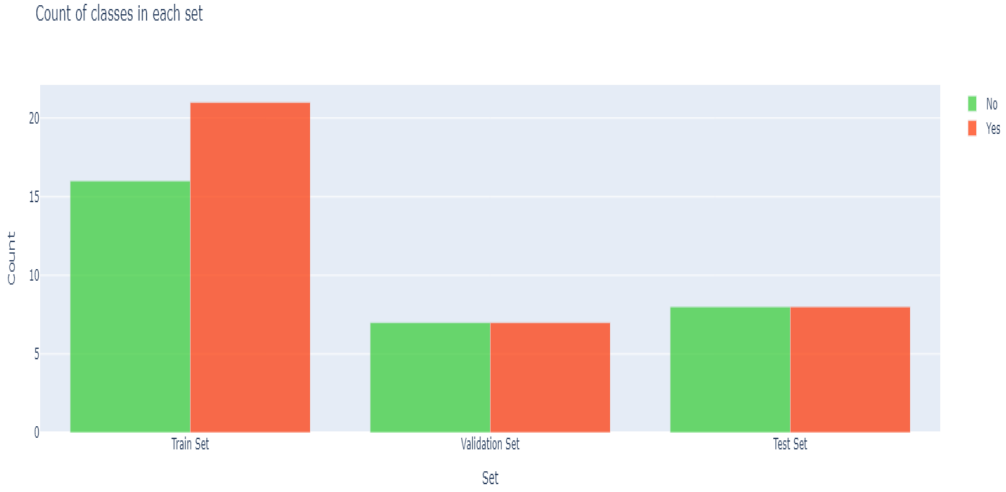

Fig 5: Training and Validation set

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

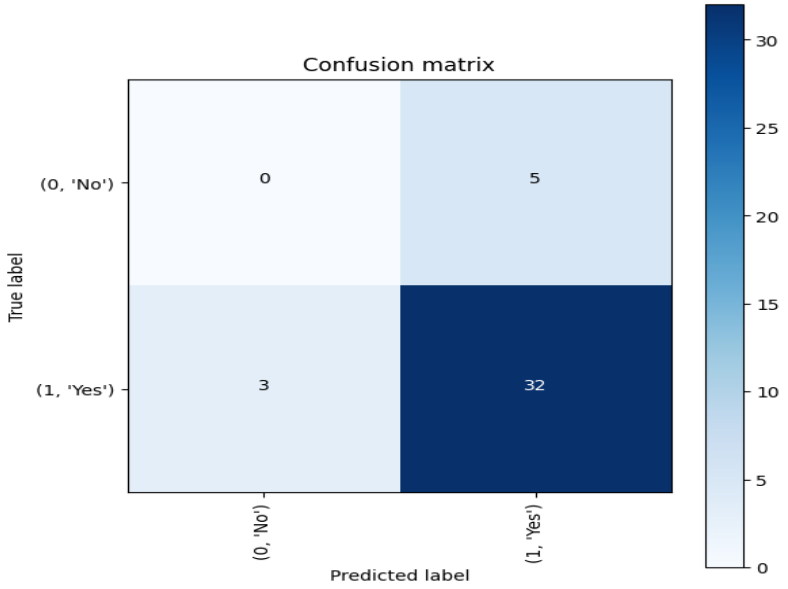

Fig 6: Confusion Matrix

According to figure 6, the confusion matrix is a basic, useful tool for evaluating the performance of binary classification tasks in machine learning. In this matrix, two classes are defined, No (0) and Yes (1), while the model evaluates TP, TN, FP, and FN. In this case, the model correctly predicted 32 instances of Yes (TP) and misclassifies 3 true Yes cases as No (FN). The 5 No cases are all misclassified as Yes (FP), and there are no correctly predicted No cases (TN=0). Overall, the model achieved an 80% accuracy: 32 correct out of 40 predictions. However, the predictive bias of the model seems to lean towards Yes: high Recall (91.4%) but no identification of No cases (0% precision for class 0). There may be class imbalance or other issues that need to be addressed in model predictions. This conflict between the two metrics can be handled in terms of resampling, cost-sensitive learning, or optimizing decision thresholds.

VII. CONCLUSION

This method as proposed in the paper is applicable for Measurement One and is employed for measuring large volumes of the system, which can be reached in the limited time expected; instead, ordinal measurements are used. This paper provides an analysis of the anatomy structure in the removal of the finger network and simulation, and proposed an effective framework for finger recognition. Contributions of this paper are summarized in the following points. An algorithm extracts a vein pattern using curvature direction along the shape map and anatomical structure upon the basis of the vein network refinement.

VIII. REFERENCES

[1] B. Hou, H. Zhang, and R. Yan (2022), "Finger-vein biometric recognition: A review," IEEE Trans. Instrum. Meas., vol. 71, pp. 1–26.

[2] C. Kauba, B. Prommegger, and A. Uhl (2020), "OpenVein—An open-source modular multipurpose finger vein scanner design," in Handbook of Vascular Biometrics. Cham, Switzerland: Springer, ch. 3, pp. 77–111.

[3] H. Lu, Y. Wang, R. Gao, C. Zhao, and Y. Li (2021), "A novel ROI extraction method based on the characteristics of the original finger vein image," Sensors, vol. 21, no. 13, pp. 4402.

[4] J. Huang,W. Luo,W. Yang, A. Zheng, F. Lian, andW. Kang (2022), "FVT: Finger vein transformer for authentication," IEEE Trans. Instrum. Meas., vol. 71, pp. 1–13.

[5] L. Yang, X. Liu, G. Yang, J. Wang, and Y. Yin (2023), "Small-area finger vein recognition," IEEE Trans. Inf. Forensics Security, vol. 18, pp. 1914–1925.

[6] M. S. M. Asaari, S. A. Suandi, and B. A. Rosdi (2014), "Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics," vol. 41, no. 7, pp. 3367–3382.

[7] P. Tome and S. Marcel (2015), "On the vulnerability of palm vein recognition to spoofing attacks," pp.

319–325.

[8] R. S. Kuzu, E. Maiorana, and P. Campisi (2021), "Loss functions for CNN based biometric vein recognition," pp. 750–754.

[9] T. Eglitis, E. Maiorana, and P. Campisi (2023), ''Open-source finger vein acquisition device for biometric applications,'' IEEE Trans. Instrum. Meas., vol. 72, pp. 1–12.

[10] Z. Wang, D. Wu, R. Gravina, G. Fortino, Y. Jiang, and K. Tang (2017), "Kernel fusion based extreme learning machine for cross-location activity recognition," Inf. Fusion, vol. 37, pp. 1–9.

[11] Mendes DJ. M. Ruiz-Echeverri, J. C. Bernal-Romero, J. M. Ramirez-Cortes, P. Gomez-Gil, J. Rangel-Magdaleno, and H. Peregrina-Barreto, ''Dorsal hand veins biometrics using NIR images with fusion of classifiers atscore level,'' in Proc. IEEE Int. Instrum. Meas. Technol. Conf. (I2MTC),May 2021, pp. 1–6.

[12] F. Wilches-Bernal, B. Núñez-Álvares, and P. Vizcaya, ''A database of dorsal hand vein images,'' 2020, arXiv:2012.05383.

[13] D. De Santos-Sierra, M. F. Arriaga-Gómez, G.Bailador, And C. Sánchez-Ávila, "Low Computational Cost Multilayer Graph- Based Segmentation Algorithms For HandRecognition On Mobile Phones," In Proc. Int. Carnahan Conf. Security Technol. (Iccst), Rome, Italy, 2014, Pp. 1–5.

[14] W. Kang And Q. Wu, "Pose-Invariant Hand Shape Recognition Based On Finger Geometry," Ieee Trans. Syst., Man, Cybern.,Syst., Vol. 44, No. 11, Pp. 1510–1521, Nov. 2014.

[15] B. P. Nguyen, W.-L. Tay, And C.-K. Chui, "Robust Biometric Recognition From Palm Depth Images For Gloved Hands," Ieee Trans. Human–Mach. Syst., Vol. 45, No. 6, Pp. 799–804, Dec. 2015.Morales Et Al., "Synthesis Of Large Scale Hand-Shape Databases For Biometric Applications," Pattern Recognit. Lett., Vol. 68 , No. 1, Pp. 183–189, 2015.

[16] R. M. Luque-Baena, D. Elizondo, E. López- Rubio, E. J. Palomo, And T. Watson,"Assessment Of Geometric Features For Individual Identification And Verification In Biometric Hand Systems," Expert Syst.Appl., Vol. 40, No. 9, Pp. 3580–3594, 2013.S. Marcel, M. S. Nixon, And S. Z. Li, Handbook Of Biometric Anti-Spoofing:Springer, 2014.

[17] D. Gragnaniello, C. Sansone, And L. Verdoliva, "Iris Liveness Detection For Mobile Devices Based On LocalDescriptors," Pattern Recognition Letters, Vol. 57, Pp. 81-87, 2015.L.

[18] Yang, G. Yang,Y. Yin, And X. Xi, "Finger VeinRecognition With Anatomy StructureAnalysis," Ieee Trans. Circuits Syst. Video. Technol., 2017.

[19] L. Yang, G. Yang, L. Zhou, And Y. Yin, "Superpixel Based Finger Vein Roi Extraction With Sensor Interoperability," In Proc. 8th Int. Conf. Biometrics (Icb), Phuket, May. 2015, Pp. 444–451.

[20] K. B. Raja, R. Raghavendra, And C. Busch, "Video Presentation AttackDetection In Visible Spectrum Iris Recognition Using Magnified Phase Information," Ieee Transactions On Information Forensics And Security, Vol.10, No. 10, Pp. 2048-2056, 2015.

[21] Nalini, K., and L. Jaba Sheela. "A survey on datamining in cyber bullying." International Journal on Recent and Innovation Trends in Computing and Communication 2.7 (2014): 1865-1869.