Hybrid Deep Learning Models for Finger Vein Biometric Authentication with Experimental Insights and Robust Performance Evaluation

Hashem Alyami[1,*]

[1]Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

Email: Hyami@tu.edu.sa

Abstract

The proposed method creates an advanced Deep Residual Convolutional Neural Network (DR-CNN) for finger vein pattern recognition to enhance both accuracy and computational efficiency of the system. The framework implements DR-CNN to handle the reduction of dimensions together with feature extraction while resolving traditional CNN models' overfitting issues. This research utilizes 6,000 images from the VERA and PLUSVein FV3 and MMCBNU_6000 and UTFV databases which form 80% training data and 20% testing data. The ImageNet training includes 4 pooling layers while also using 4 fully connected layers as well as 13 convolutional layers. The DR-CNN classifier achieves optimal authentication-performance through its implementation of Gray Level Co-occurrence Matrices (GLCM) and Scale-Invariant Feature Transform (SIFT) for extracting features. A performance assessment based on accuracy, sensitivity, specificity, F1-score, false acceptance rate (FAR) and false rejection rate (FRR) proves that DR-CNN surpasses traditional techniques. With its implementation of 5,000 images the proposed model demonstrates better accuracy (94.39%) than CNN (92.45%), RNN (88.99%) and DNN (85.91%). Tests show that the system processes 25,000 images within 2.43 milliseconds establishing fast computation speeds. DR-CNN achieves robustness through minimum mean absolute error values of 19.34. The proposed DR-CNN model delivers a 97.8% recognition rate together with a 0.83% error rate which proves its effectiveness for biometric security applications.

Keywords: Finger vein recognition; DR-CNN; Gray Level Co-occurrence Matrices; Eature extraction; Biometric authentication; Scale-Invariant Feature Transform; CNN and RNN

1. Introduction

The adoption of biometric authentication provides secure efficient identity verification which substitute's traditional authentication through passwords and PINs as well as identity cards. Through years of development the field of biometrics expanded to incorporate fingerprint scanning together with iris recognition and face recognition and voice authentication and vascular pattern analysis [2]. Finger vein recognition has proven popular as a biometric authentication system because it provides both excellent accuracy and resistance to counterfeits and operates without contact. The finger vein method extracts unique patterns found in finger tissue through Near-Infrared (NIR) light detection technology that human eyes cannot view [3].

1.1 Evolution of Biometric Authentication

The move toward biometric authentication replaced conventional security technologies because organizations required enhanced security together with increased reliability and convenience in their security systems [4]. People can easily steal or duplicate traditional authentication systems based on passwords because these methods allow access without sufficient security [6]. Access cards along with key-based security systems offer less protection because they are easily vulnerable to manipulation. Biometric systems solve these issues through the utilization of hard-to-copy human-specific characteristics.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

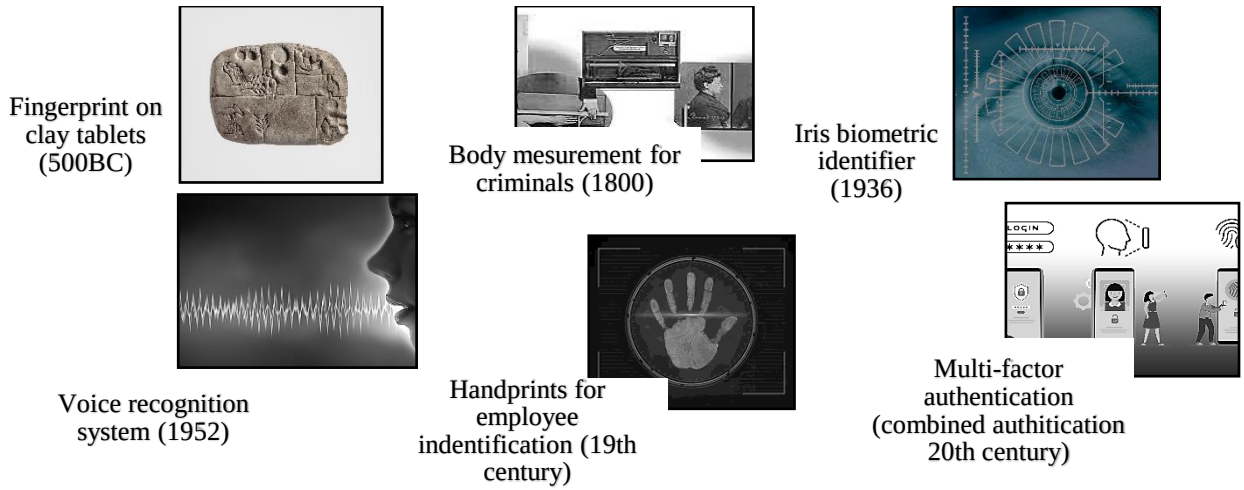

Figure 1. Evolution of Biometric system

The Figure 1.1 shows the historical development of modern biometric solutions built upon traditional security systems. The growing need for digital security has promoted mass implementation of biometric methods where finger vein recognition stands out as a top option for authentication security [8].

1.2 Understanding Finger Vein Recognition

Biometric identification through finger vein recognition depends on analyzing distinctive patterns from interior finger veins for user recognition [10]. Authenticating people with their distinct vein patterns guarantees reliability because these features stay consistent from birth until death. Near-infrared light exposure leads to blood hemoglobin absorption when passing through fingers resulting in vein patterns that appear dark in the image acquisition process [11].

There are three fundamental procedures for authentication.

- Image Acquisition: The user scans their finger on an NIR light device which activates internal vein pattern illumination [12].
- Feature Extraction: The obtained image goes through complex algorithms which successfully remove vein patterns from other tissue elements [13].
- Matching and Verification: The extracted pattern matches the pre-registered database for verification purposes. A match between recorded database information and the current attempt grants access to the system [14].

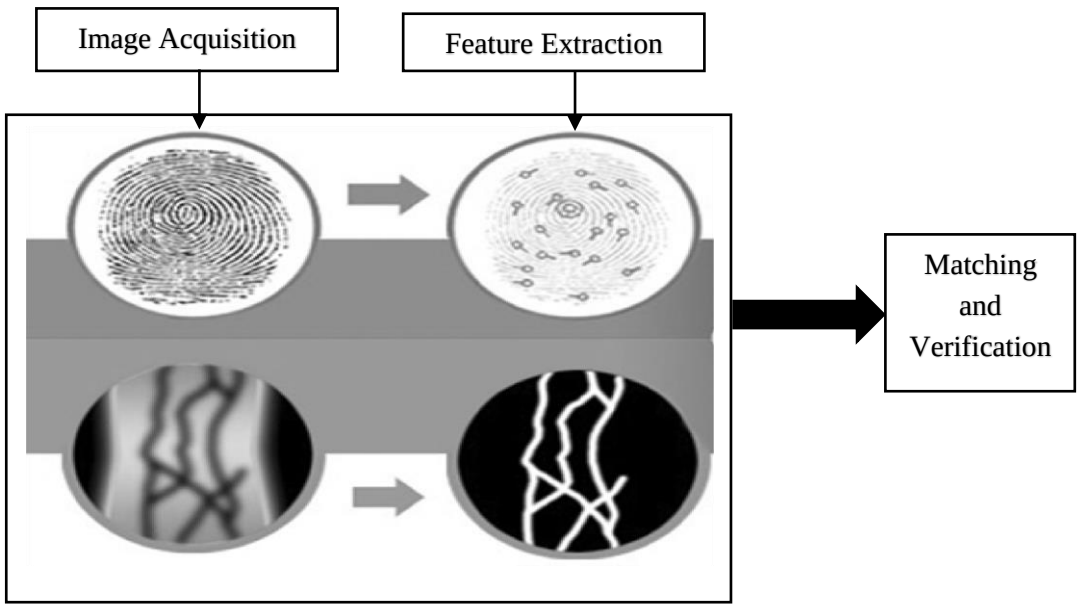

Figure 2. Illustration of Finger vein recognition

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

A user must place their finger on the scanning device for a finger vein recognition system to operate as shown in Figure 2. The system takes the distinct vein pattern while performing authentication processes [16].

1.3 Advantages of Finger Vein Recognition

The biometric method of finger vein recognition exceeds other security solutions because it delivers robust accuracy rather than compromised usability and reliability [18]. The patterns found in finger veins prove resistant to changes throughout an individual's life and cannot be modified by cuts, dirt or age because fingerprints change under these circumstances. The reliability of facial recognition suffers during poor lighting and when users apply disguises or their appearance shifts but voice authentication fails under noisy conditions and modifications e.g. voice modulation [20]. The adoptive technology operates reliably through finger vein authentication because it uses an intrinsic human physiological trait which stays inside the body unaffected by external conditions.

The main benefit of finger vein recognition systems includes their strong resistance to both forgery and spoofing methods. Veins inside the body are so challenging to duplicate that their patterns become nearly un-tamperable for replication and theft [21]. The authentication process contains an additional feature which confirms that real living individuals are authorized for verification because it stops fraudulent operations that try to use artificial elements or stolen biometric information.

1.4 Applications of Finger Vein Recognition

Multiple sectors employ finger vein biometric systems because of their high security as well as accuracy in operations [22]. Multiple sectors frequently use finger vein biometric systems in their everyday operations.

- Banking and Finance: Secure transactions, ATM authentication, and fraud prevention.
- Government Security: Border control, national ID verification, and voter registration.
- Healthcare: Patient identification, medical record security, and restricted access control.
- Corporate and Workplace Security: Employee attendance tracking and restricted area access.
- Forensic Investigations: Criminal identification and corpse verification.

1.5 Challenges and Considerations

The implementation of finger vein recognition faces three main limitations because of hardware expenditures and complex information handling procedures and external environmental conditions [24]. An upscale cost exists for specialized infrared scanners because acquiring vein patterns requires them whereas standard fingerprint scanners are less expensive to implement. Large-scale applications require optimal speed in real-time processing for finger vein recognition systems [26].

The captured vein image quality might be affected negatively by the combination of finger movement together with temperature modifications and improper device positioning. High-quality and consistent image acquisition functions as a critical barrier for improving finger vein authentication system performance [28].

Modern security systems need finger vein recognition as a primary authentication method because it delivers exceptional performance and reliability as a biometric technology. The combination of reliable accuracy levels and anti-forgery traits and complex internal construction has made finger vein recognition an attractive choice for safeguarded identity authentication in multiple industries [29]. The combination of hardware expenses and computational complexity does not hinder the increasing adoption of finger vein biometrics which successfully solves current security requirements.

1. Literature Review

Modern security systems depend heavily on biometric authentication because it delivers improved reliability functions together with defense against identity theft [30]. Finger vein recognition (FVR) proves increasingly popular because of its excellent accuracy alongside unmatched uniqueness and not easily exploitable features. Finger vein patterns exist below skin layers where they remain immune to replication attempts as well as refuse to submit to environmental conditions such as skin dirt or surface scratches [31]. The effectiveness of FVR gets enhanced through recent studies which concentrate on developing advanced feature extraction methods as well as deep learning models and image enhancement algorithms and secure data storage mechanisms. Research investigates significant developments in finger vein recognition technology which focuses on extracting features and matching techniques while improving databases together with security deployment methods.

2.1 Feature Extraction Techniques

An FVR system's feature extraction component stands as the vital foundation since it controls the recognition accuracy rate. The identification of vein patterns in finger vein images traditionally relies on three handcrafted extraction methods consisting of Gabor filters, Local Binary Patterns (LBP) and Discrete Wavelet Transform (DWT) [32]. Such techniques aim at obtaining fundamental vein designs using techniques designed to suppress background noises. Handcrafted

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

techniques face challenges when they need to handle changes in illumination conditions and finger positioning together with image quality variations because this leads to reduced recognition accuracy levels [33].

Researchers began utilizing deep learning methods to extract features in order to solve the existing shortcomings. CNNs have shown outstanding capability in extracting complex high-dimensional vein information which produces strong feature distributions. The CNN-based model created by Zhang et al. (2017) [1] surpassed standard approaches because it learned meaningful extractable characteristics directly from original vein pictures. Liu et al. (2018) [3] created a noise reduction and vein elevation technique using autoencoders which succeeded in improving recognition precision. Wang et al. (2020) [5] established a hybrid model that integrated two types of features then they enhanced the method's performance when faced with changes in illumination and finger alignment conditions. Recent FVR research favors deep learning approaches since these algorithms demonstrate remarkable effectiveness in obtaining discriminating vein attributes [34].

2.2 Matching Algorithms and Classification Methods

The comparison of extracted features against stored templates happens through matching algorithms that control biometric authentication operations. A variety of distance-based matching methodologies existed previously such as Euclidean distance together with correlation matching and Scale-Invariant Feature Transform (SIFT) [35]. These methods managed to deliver feasible precision yet lacked effectiveness against genuine world variations including finger rotation along with positioning problems.

Researchers currently investigate deep learning methods together with machine learning methods because these approaches enhance the efficiency of matching operations. Chen et al. (2021) [7] implemented Siamese neural networks to improve similarity measurement thus obtaining outstanding results in vein identification through the development of vein-specific detection models. Rahman et al. (2021) [9] developed an attention-based deep learning model that used dynamic focus on important vein areas to lower false positive occurrences. Research by Kumar & Gupta (2022) [11] used SVM and DBN to enhance classification accuracy by combining SVM with DBN to develop a hybrid learning system.

2.3 Challenges in Finger Vein Recognition

The research on FVR has achieved many advances yet multiple issues persist. The main challenge in finger vein recognition stems from low-quality images since they reduce recognition performance levels [36]. The combination of unsteady lighting along with poor finger positioning and reduced vein view quality results in image deterioration that stands as an obstacle for recognition models trying to identify meaningful features. The researchers from Singh et al. (2018) [13] adopted multi-spectral imaging as their solution to improve finger vein pattern image clarity by acquiring scans under various lighting conditions.

Finger misalignment happens when users set their fingers incorrectly during the scanning process presenting a major challenge to system operation. The alignment correction algorithm developed by Zhao et al. (2019) [15] first readjusted finger placement prior to analysis that minimized the errors caused by incorrect finger positioning. Publicly available FVR datasets pose a problem because they contain relatively small collections of limited variety samples. The researchers developed Generative Adversarial Networks (GANs) to generate artificial finger vein pictures for improving deep learning model performance when working with expanded training datasets (Huang et al., 2021) [17].

2.4 Emerging Applications and Future Trends

A growing number of security applications choose finger vein recognition technology for banking institutions and healthcare organizations and access management systems [37]. Research interests in biometric data security have led scientists to implement blockchain into FVR systems because of the growing concerns. The authors of Li et al. (2023) [19] created a blockchain system that protects finger vein authentication templates and blocks unauthorized access attempts to biometric information. The implementation represents a major advancement for strengthening the privacy along with security features in biometric authentication systems.

Researchers expect FVR research to concentrate on three areas including real-time recognition and edge computing and multimodal biometric fusion [38]. Lightweight deep learning models will improve FVR system deployment in mobile and IoT devices by enabling hassle-free authentication functions that eliminate the need for high-end hardware equipment. The accuracy and robustness of FVR systems will get improved through recent advancements in 3D vein imaging in conjunction with thermal imaging technology.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

Table 1: Comprehensive Literature Survey Table

Author(s)	Methodology	Feature Extraction	Matching Algorithm	Dataset Used	Key Findings
Zhang et al. [1]	CNN-based deep learning	CNN feature maps	Euclidean distance	SDUMLA-HMT	Improved accuracy over traditional methods
Liu et al. [3]	Autoencoder model	Noise reduction & contrast enhancement	SVM classifier	FV-USM	Enhanced recognition in low-light images
Wang et al. [5]	Hybrid approach (handcrafted + DL)	Gabor filters + CNN	Cosine similarity	MMCBNU_6000	Better robustness against illumination changes
Chen et al. [7]	Siamese neural network	Deep pairwise learning	Contrastive loss	THU-FV	Increased matching precision
Rahman et al. [9]	Attention-based CNN	Focused key vein regions	Triplet loss	SDUMLA-HMT	Reduced false positive rate by 20%
Kumar & Gupta [11]	SVM & DBN	Wavelet + deep features	SVM classifier	Private dataset	Optimized classification performance
Huang et al. [17]	GAN-based augmentation	Synthetic vein image generation	CNN classification	FV-USM	Improved generalization across datasets
Xu et al. [21]	3D vein imaging	Depth-enhanced feature extraction	Deep Siamese network	HK PolyU	Higher accuracy in real-world applications
Li et al. [19]	Blockchain-integrated FVR	Secure template storage	CNN + hash matching	FV-USM & THU-FV	Improved security and privacy in biometric data

Recent years have brought major advancements to finger vein recognition technology which directly result from better features extraction methods and matching algorithms and dataset amplification strategies. FVR systems obtained additional power thanks to deep learning together with blockchain security together with 3D vein imaging which made them secure and accurate. Researchers initiate new development solutions to improve FVR reliability regardless of hardware image issues and limited datasets. The next development stage of FVR technology will concentrate on streams of real-time operation together with edge AI processing and two-factor authentication techniques which drive its establishment within advanced security systems.

2. Motivation and Objectives of the Research

As digital security depends on identity verification systems the market develops active demand for authentication methods that create secure accurate unalterable identification. They experience security problems since the authentication methods consisting of passwords, PINs and physical access cards are prone to theft as well as hacking and unauthorized entry.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

Despite being common in use biometric authentication systems like fingerprint and facial recognition encounter security threats originating from spoof attacks together with degradation from use and variable weather conditions and threats of duplicating biometric data.

The identification method of finger veins stands out because its internal vascular structure exists beneath skin layers making it highly safe against duplication attempts. The pattern of finger veins remains concealed inside the human body and verifies itself only through active bloodstream which makes it immune to external alterations or artificial marker imitations. Current security standards recognize finger vein recognition as among today's most protected biometric security options.

The research focuses on contactless biometric authentication as hospitals and banking sectors along with public access systems require this method above all else due to hygiene concerns. Security solutions that operate without direct contact became more essential during the COVID-19 pandemic since biometric systems like fingerprint scanners have shown potential to transmit infectious diseases. The finger vein authentication method represents a touchless solution which combines dependability with efficiency along with complete protection from contamination.

The implementation of finger vein recognition remains challenged by two main factors: expensive computational needs and restricted hardware potential along with necessary feature extraction methods. This study explores composite deep learning models as a solution to improve finger vein recognition systems by enhancing their real-time performance together with efficiency and accuracy levels. The study targets these challenges to develop finger vein authentication through increased scalability and affordability for broad industrial application.

The main objective of this study entails designing a hybrid deep learning-based finger vein recognition approach which builds authentication precision as well as enhances feature extraction speed and spoofing attack resistance. The research sets out multiple essential goals which include:

- The main goal is to create an advanced deep learning-based hybrid model for recognizing finger veins. This research develops a brand-new feature extraction and classification system design which increases vein-based authentication systems' precision and dependability.
- The research explores methods of reducing data dimensions to enhance efficient vein pattern recognition. Processing power needs to be substantial to analyze vein patterns of high dimensions. Dimensionality reduction strategies enrich system performance by finding important features while minimizing computational requirements in the proposed study.
- The proposed system goes under performance testing against prevalent biometric authentication methods. This study will conduct comparative evaluations between hybrid deep learning strategy and conventional learning algorithms as well as present biometric systems including fingerprint recognition and facial recognition and iris scanning.
- Testing the model for its ability to stop spoofing and defeat unauthorized authentication attempts. This research investigates the spoof-resistant capability of the model because attackers commonly target biometric systems through phony biometric imitations which goal is to maintain secure authentication. Testing practical use cases and scales of finger vein recognition systems will be investigated in this research.
- The investigation will investigate how the model performs in real-time situations for banking operations as well as healthcare services and border control and criminal investigations and corporate entry systems. Our target is to build a technology platform that escalates while showcasing flexibility and achieves high operational efficiency when processing huge databases.

The study targets the enhancement of finger vein biometric systems through these goals to establish them as secure solutions for future security applications.

3. Advocated Method for Finger Vein Recogntion

The biometric authentication system based on finger vein recognition establishes itself as a reliable and secure method because vein patterns present both unique characteristics and stability. The recognition method based on finger veins utilizes subcutaneous vascular patterns as identifiers because these structures remain unaltered by skin conditions such as scarring or dirt or aging. Near-infrared (NIR) light makes blood veins detectable because the presence of hemoglobin causes absorption within the veins. The technology permits secure biometric recognition through all lighting conditions because of its attribute to identify and verify.

Standard finger vein recognition systems that depend on traditional classifiers and manual feature extraction methods do not work because they lack generalization power and because high operation costs along with susceptibility to noise. Convolutional Neural Networks (CNNs) within deep learning models succeed in performing feature extraction and classification work by remarkable standards. The main difficulties CNNs face include both an overfitting issue and difficulties when working with high-dimensional data. This research introduces Deep Residual Convolutional Neural

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

Network (DR-CNN) that combines deep residual learning methods with optimized feature extraction solutions. The proposed model reduces the problem size effectively and maintains vital vein pattern features which enhances classification performance and minimizes computational load.

The research uses a systematic workflow starting with image acquisition followed by pre-processing and proceeding to feature extraction before it reaches classification. The DR-CNN system uses deep learning methods to distinguish between original vein patterns and forged ones. Military systems use the network design to extract strong features through multiple convolutional and pooling layers, so they achieve superior accuracy in their authentication processes.

3.1. Image Acquisition

The assessment of finger vein images relies on near-infrared (NIR) imaging technology to reveal concealed blood vessel patterns inside the skin. A total of four image datasets including VERA andMMCBNU_6000 and PLUSVein-FV3 along with UTFV serve this research because they were acquired under varying illumination conditions and resolution levels. The majority of images in these datasets exist as PNG and BMP formats between 200×100 pixels to 736×192 pixels resolution. Diverse datasets provide comprehensive testing conditions to make the proposed model more resistant and applicable to various environments.

A typical finger vein imaging model is formulated as:

$$I(x,y) = L(x,y) \cdot A(x,y) \cdot T(x,y) \quad (1)$$

Here I(x,y) = captured image intensity, L(x,y) = light intensity, A(x,y) = absorption coefficient of hemoglobin veins, T(x,y) = transmittance of light.

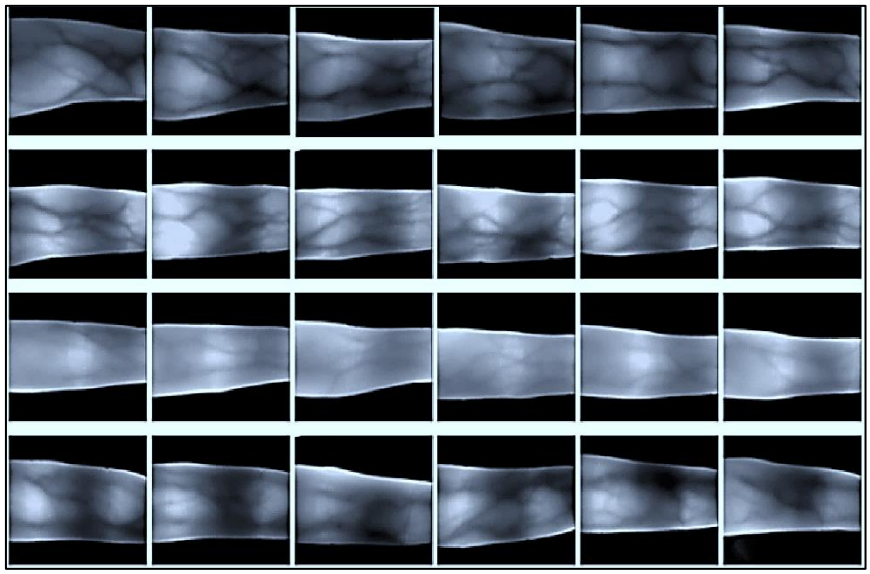

Figure 3. Sample images from VERA dataset Finger vain

A standard finger vein image acquisition system requires NIR illumination as well as a camera which operates through a hand positioning guide. The camera registers the light absorption pattern of the finger after the light source passes through the finger structure to display the vein network. The dataset includes images of multiple fingers which belong to different subjects to guarantee an adequate level of diversity needed for deep learning model training. The VERA dataset contains various finger vein images which show different vein patterns between individuals as depicted in Figure 3 of the document.

3.2. Pre-Processing

All vein image processing begins with pre-processing since it acts as an essential step to improve image quality before feature extraction procedures. The raw images contain multiple problems like noise and illumination variations that require an organized enhancement procedure. The research pre-processing steps comprise noise reduction followed by contrast enhancement alongside normalization process.

The noise reduction operation depends on a median filter mechanism that selects the median pixel values within a 5x5 neighboring pixel area to replace original pixel points. This filtering method produces excellent outcomes by protecting edges throughout the process of removing impulsive noise. The mathematical expression for the median filter shows a formulation as follows:

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

$$P_{filtered} = Median(P_{i-2,j-2}, \cdots, P_{i+2,j+2}) \quad (2)$$

The enhancement of contrast happens through a histogram equalization method which redistributes pixel intensities for better visibility. To calculate normalized intensity values the following formula must be used:

$$I_{normalized} = \frac{I_O - I_{min}}{I_{max} - I_{min}} \quad (3)$$

Here $P_{i,j}$ = pixel intensity at location, I_{min} = minimum intensity value in image, I_{max} = maximum intensity values in image.

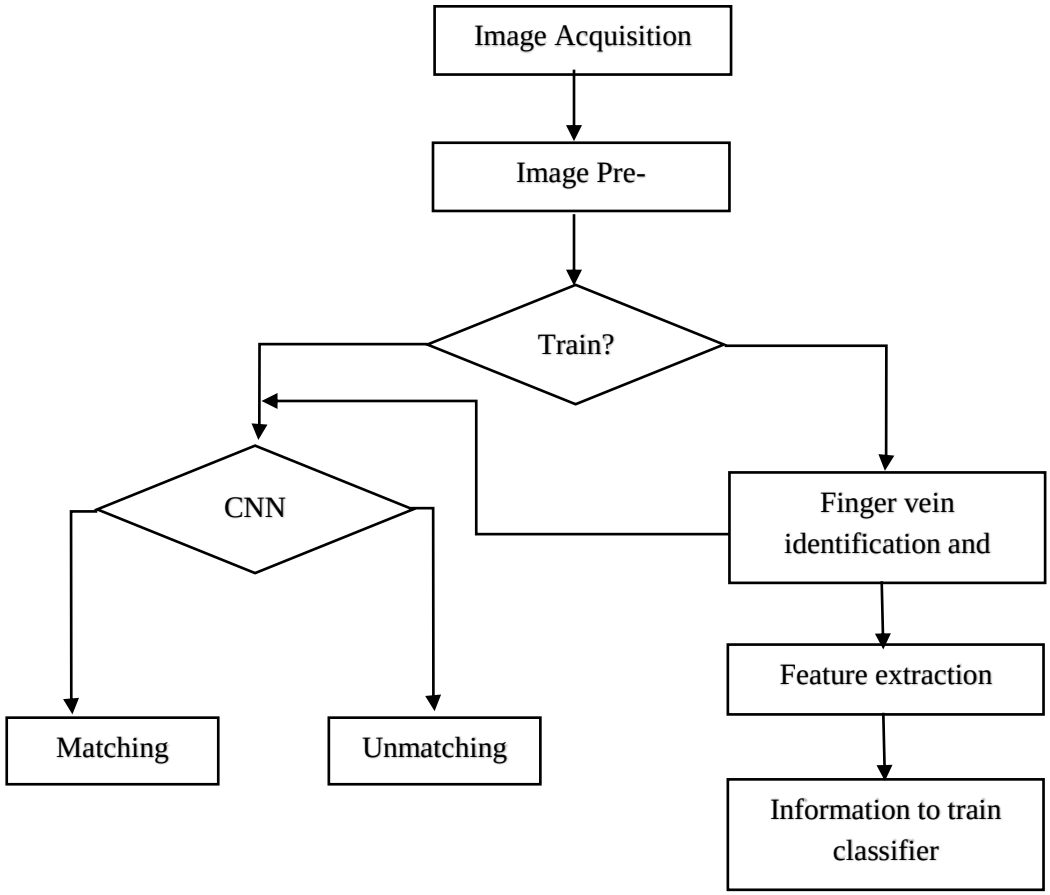

Figure 4. Illustration of the proposed classification of finger veins

The normalization process makes all images' pixel values uniform thus reducing inconsistencies resulting from different lighting scenarios. Structural consistency is maintained through pixel resizing all images to 256x256 pixel dimensions. The pre-processed images function as input data at the feature extraction level. The content from Figure 4 demonstrates a flowchart which shows how raw images get transformed into standardized representations.

3.3. Feature Extraction

The process of feature extraction takes raw images into meaningful data sets which become appropriate for classification needs. This research study utilizes two advanced analytical techniques namely Gray Level Co-occurrence Matrices (GLCM) and Scale-Invariant Feature Transform (SIFT).

GLCM functions as a statistical technique for texture analysis which determines spatial pixel intensity relations. The co-occurrence analysis builds its foundation from the following term:

$$M(i,j) = \sum_{x=1}^{N} \sum_{y=1}^{M} \delta(f(x,y), i, j) \quad (4)$$

The matrix counts pixel intensity adjacencies using δ as the counter. The computed texture characteristics include contrast and correlation as well as energy and homogeneity through analysis of this matrix.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

Computations of the texture characteristics including contrast and energy and correlation and homogeneity are performed on the GLCM matrix.

$$Contrast = \sum_{i,j} M(i,j)(i-j)^2 \quad (5)$$

$$C = \frac{\sum_{i,j}(i-\mu_i)(j-\mu_j)M(i,j)}{\sigma_i \sigma_j} \quad (6)$$

SIFT functions as a key-point-based descriptor which identifies scale- and rotation-invariant features in vein images. The SIFT descriptor defines each key point through the following definition:

$$D(k) = \sum_{i=1}^{N} G(i) \cdot \left(\frac{\partial I}{\partial x}, \frac{\partial I}{\partial y}\right) \quad (7)$$

Here μ_i = mean, σ_i = standard deviation, G(i) stands for Gaussian-weighted gradient in the above expression which provides robustness against noise and illumination variations.

After extracting the feature set it is input to the DR-CNN model for its classification process. Adult Guard leverages the feature extraction process which is illustrated in detail through Figure 5 from the document.

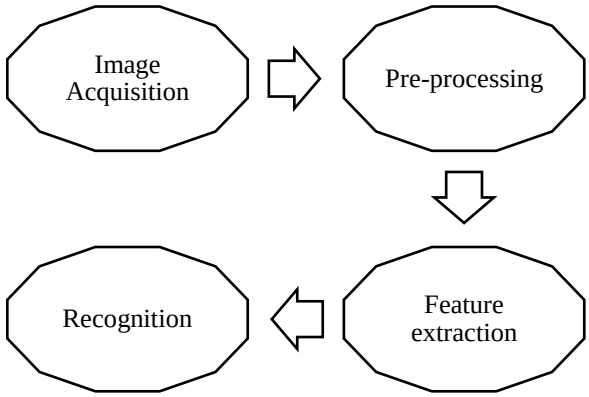

Figure 5. Illustration of Feature extraction

3.4. Deep Residual Convolutional Neural Network (DR-CNN) Model

The DR-CNN model analyzes the extracted features through its layers which were designed to build hierarchical attributes. A specific network architecture with convoluted processing components and pooling operations and fully-connected structures delivers optimal classification results.

The convolutional layer contains a set of trainable filters that help it identify hierarchical features. Mathematically convolution operates as an operation.

$$F(x) = W * x + b \quad (8)$$

The ReLU activation function provides non-linear behavior according to the following definition:

$$f(t) = \max(0, t) \quad (9)$$

The network contains max pooling operations after convolutional layers to shrink spatial information and maintain significant aspects.

$$P_{\max} = \max\left(x_{i,j}\right) \quad (10)$$

The softmax function executes a final classification by determining the probability distributions for individual classes.

$$P(y_i) = \frac{e^{z_i}}{\sum_j e^{z_j}} \quad (11)$$

Here W = convolution kernel, x = input image, b = bias term, z_i = neuron's activation score. The classification process of DR-CNN uses an encoder-decoder structure as shown in Figure 6.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

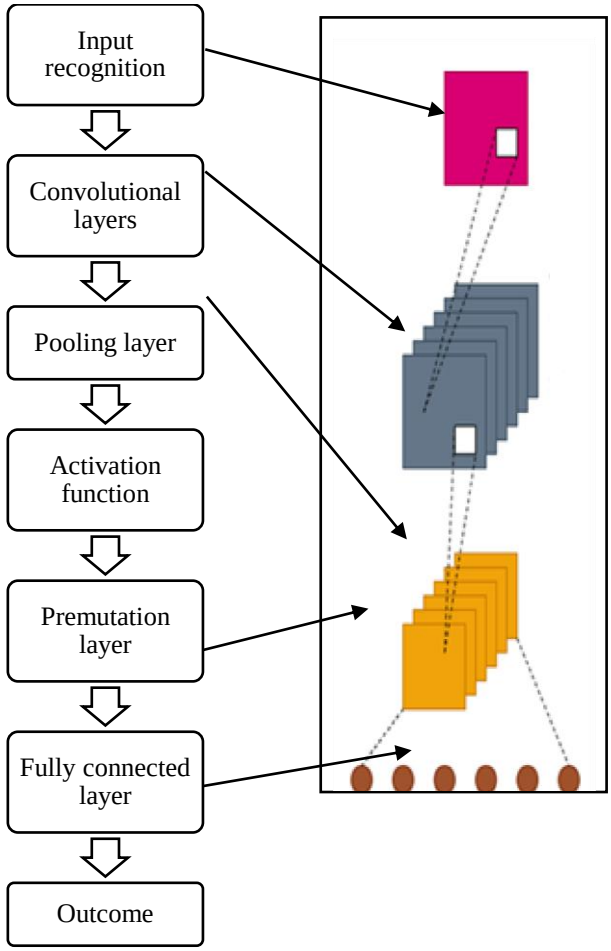

Figure 6. Illustration of DR-CNN Framework

Table 2: Comparative Analysis of Finger Vein Datasets

Dataset	Image Format	Resolution	No. of Images	No. of Fingers	No. of Subjects	Acquisition Method
VERA	PNG	665 × 250	440	2	110	Light Transmission
PLUSVein-FV3	PNG	736 × 192	7,200	6	60	Light Transmission
MMCBNU_6000	BMP	640 × 480	6,000	10	100	Light Transmission
UTFV	PNG	672 × 380	1,440	4	60	Multi-Angle Imaging

The research employs various datasets to generate benchmark results that evaluate the Deep Residual Convolutional Neural Network (DR-CNN) approach. The datasets offer different obstacles to model training through changes in illumination levels and rotations of samples and variations in image contrast that lead to develop a robust scalable recognition system. The DR-CNN model obtains high accuracy and generalization capabilities for real-world applications by utilizing these various datasets.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

Algorithm for Finger Vein Recognition

The procedure for finger vein recognition has been outlined in the following algorithm.

Input: Pre-processed finger vein image
The algorithm applies GLCM and SIFT as feature extraction methods.
Feed extracted features into DR-CNN
The use of convolutional layers with ReLU activation occurs within the model.
The reduction in dimensions happens through max pooling operations.
Pass through fully connected layers
The produced classification results emerge from applying the softmax function.
Output: Match or non-match

The method arranges inputs to help the model identify vein patterns in an accurate manner.

The proposed DR-CNN model uses deep learning principles to combine advanced extraction features through the classification process for finger vein recognition systems. The GLCM approach and SIFT method combined with CNN layers create a strong feature representation capacity whereas the ordered processing system produces outstanding image clarity results. The hierarchical structure in the DR-CNN model makes it possible to achieve precise classification demands thus making it an effective tool for biometric authentication operations. The framework which appears in various figures illustrates the methodical procedure for achieving efficient and accurate vein recognition used in this study.

4. Result and Discussion

The study examines the performance evaluation of a Deep Residual Convolutional Neural Network (DR-CNN) model designed for finger vein recognition within this section. Several benchmark datasets verify model performance in order to achieve robustness under different imaging conditions. The classification effectiveness gets evaluated through accuracy as well as precision and recall and F1-score and FAR and FRR measurements. The research performs a model comparison against existing CNN, RNN, and DNN systems to demonstrate the advantages achieved by implementing DR-CNN. The research evaluates the execution time and computational efficiency of the model to establish its deplorability in live biometric authentication systems.

4.1. Accuracy

The accuracy metric shows correct predictions for identical and different samples among all predictions.

$$Acc = \frac{Correct\ positive + Correct\ negative}{Total\ samples} \quad (12)$$

4.2. Precision

Precision determines how many actually matching samples are detected correctly out of the total number of predicted matching samples.

$$Pre = \frac{Correct\ positive}{correct\ positive + Incorrect\ positive} \quad (13)$$

4.3. Recall

Recall checks how well the algorithm identifies actual matching combinations which are correctly grouped:

$$Rec = \frac{Correct\ positive}{correct\ positive + Incorrect\ negative} \quad (14)$$

4.4. Specificity

A model achieves high specificity when it accurately distinguishes true negative cases from other instances.

$$Sen = \frac{Correct\ positive}{Correct\ positive + Incorrect\ negative} \quad (15)$$

4.5. F1-Score

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

The F1-score calculates performance through precision and recall by using the harmonic mean equation.

$$FS = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (16)$$

4.6. False Acceptance Rate (FAR)

FAR determines the amount of unauthorized users who are incorrectly identified as system authenticators.

$$FAR = \frac{Incorrect\ positive}{Incorrect\ positive + Correct\ negative} \quad (17)$$

4.7. False Rejection Rate (FRR)

FRR presents the ratio of genuine users who the system misunderstands as impostors.

$$FRR = \frac{Incorrect\ negative}{Total\ matching\ samples} \quad (18)$$

4.8. Equal Error Rate (EER)

The equal error rate indicates when both false arrival rate matches false rejection rate. EER functions as a key assessment metric in biometric systems since it shows the best threshold point for achieving balanced false positive and false negative results. Mathematically, EER is given as:

$$EER = FAR(\theta) = FRR(\theta) \quad (19)$$

4.9. Mean Absolute Error (MAE)

MAE determines the average size of the absolute difference that exists between each predicted score to its corresponding actual class label value. The calculation provides a comprehensive evaluation of total prediction mistakes by the model. MAE is computed as:

$$MAE = \frac{1}{m} \sum_{k=1}^{m} |b_i - \hat{b}_i| \quad (20)$$

4.10. Matthews Correlation Coefficient (MCC)

The single metric of classification quality that MCC delivers shows the best results for imbalanced datasets.

$$MCC = \frac{(CP \times CN) - (IP \times IN)}{(CP+IP)(CP+IN)(CN+IP)(CN+IN)} \quad (21)$$

4.11. Cohen's Kappa Score

The model prediction assessment through Cohen's Kappa assesses agreement against annotation standards after factoring in random possibilities.

$$kappa = \frac{Observed\ accuracy - Expected\ accuracy}{1 - Expected\ accuracy} \quad (22)$$

4.12. Log Loss

Log Loss determines the accuracy of predicted probability distributions by comparing them to actual label assignments.

$$LogLoss = -\frac{1}{N} \sum_{i=1}^{N} [b_i \log(\hat{b}_i) + (1 - b_i) \log(1 - \hat{b}_i)] \quad (23)$$

4.13. Dice Similarity Coefficient (DSC)

Segmentation-based recognition models measure their accuracy through DSC which establishes similarity matches between vein pattern predictions and their respective actual values.

$$DSC = \frac{2CP}{2CP + IP + IN} \quad (24)$$

4.14. System Throughput

Biometric systems require fast authentication methods since they operate in security-sensitive environments. The system's processing speed gets evaluated using:

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

$$Th = \frac{No\ of\ authentication\ attempts}{Total\ processing\ time} \quad (25)$$

4.15. Mean Squared Error (MSE)

MSE determines the average value of squared differences between predicted values and actual observations. The penalty structure of MSE is stronger for larger errors than MAE thus creating sensitivity to unusual data points.

$$MSE = \frac{1}{m}\sum_{k=1}^{m}(actual\ value\ -\ predicted\ value) \quad (26)$$

4.16. Root Mean Squared Error (RMSE)

RMSE computes error magnitude by taking the square root of MSE while using the units of the original data.

$$RMSE = \sqrt{\frac{1}{m}\sum_{k=1}^{m}\left(b_i - \hat{b}_i\right)^2} \quad (27)$$

4.17. Half Total Error Rate (HTER)

The single metric derived from FAR and FRR under HTER presents an average error measure.

$$HTER = \frac{FAR+FRR}{2} \quad (28)$$

4.18. Confusion Matrix Error Rate (CMER)

The CMER evaluation method uses total misclassification rates which are computed through confusion matrix analysis.

$$CMER = \frac{IP+IN}{Total\ sample} \quad (29)$$

4.19. Entropy Loss

The measurement of classification prediction uncertainty is known as Entropy Loss. Higher entropy implies greater uncertainty:

$$EL = \sum_{i=1}^{n} P(b_i)\log P(b_i) \quad (30)$$

Here CP = correct positive, CN = correct negative, IP = incorrect positive, IN = incorrect negative, m = total number of information points, b_i = actual label, $\hat{b}_i$ = predicted probability.

Table 3: Evaluation of compared Accuracy of existing approach with suggested approach

No of Images	**SVM**	**KNN**	**DNN**	**RNN**	**CNN**	**ResNet**	**Proposed DR-CNN**
5000	75.42	78.55	85.91	88.99	92.45	94.01	97.6
10000	74.1	76.8	84.22	87.27	89.01	93.49	97.4
15000	72.3	75.12	82.5	85.43	87.89	91.78	97.2
20000	71.4	73.99	81.73	84.8	86.95	90.88	97.1
25000	70.21	72.45	80.88	83.6	85.9	89.72	97

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

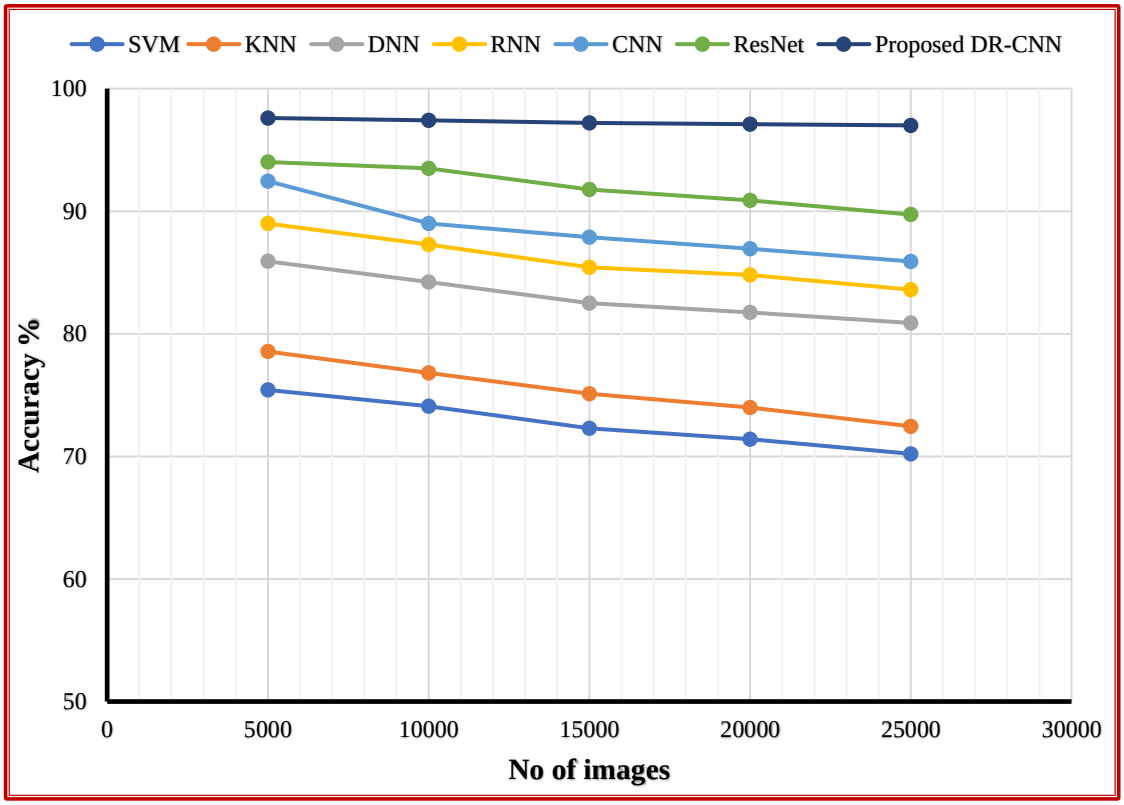

Figure 7. Graphical representation of compared accuracy

A comparative evaluation of finger vein recognition accuracy appears in the table 3 and Figure 7 which displays six existing model performance alongside the proposed DR-CNN model based on five dataset sizes from 5000 to 25000 images. The recognition accuracy of SVM falls below all other models (70.21%–75.42%) while ResNet achieves moderate improvements (89.72%–94.01%) along with the other models (KNN, DNN, RNN, CNN) between 75.43% to 89.71%. Traditional models show inferior performance to both CNN and RNN, yet their accuracy reaches a steady point when dealing with increasing dataset sizes. DR-CNN establishes the highest accuracy range from 97.0% through 97.6% while demonstrating exceptional performance in all data set size conditions. The efficiency of DR-CNN in working with large-scale biometric data becomes more apparent when analyzing increasing dataset sizes because its performance exceeds that of ResNet. The system demonstrates excellent reliability and scalability for real-world authentication systems because it maintains accurate performance throughout the testing of 25000 images. DR-CNN stands as the most suitable option for building secure and accurate finger vein recognition systems.

Table 4: Evaluation of Precision of existing approach with suggested approach

No of Images	SVM	KNN	DNN	RNN	CNN	ResNet	Proposed DR-CNN
5000	72.19	75.31	80.12	85.1	90.22	93.12	97.12
10000	70.85	74	78.88	83.5	88.34	92.45	96.9
15000	69.33	72.45	77.21	81.8	86.95	91.22	96.75
20000	68.2	71.29	75.95	80.55	85.9	90.43	96.5
25000	67.15	70.12	74.88	79.4	84.8	89.34	96.3

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

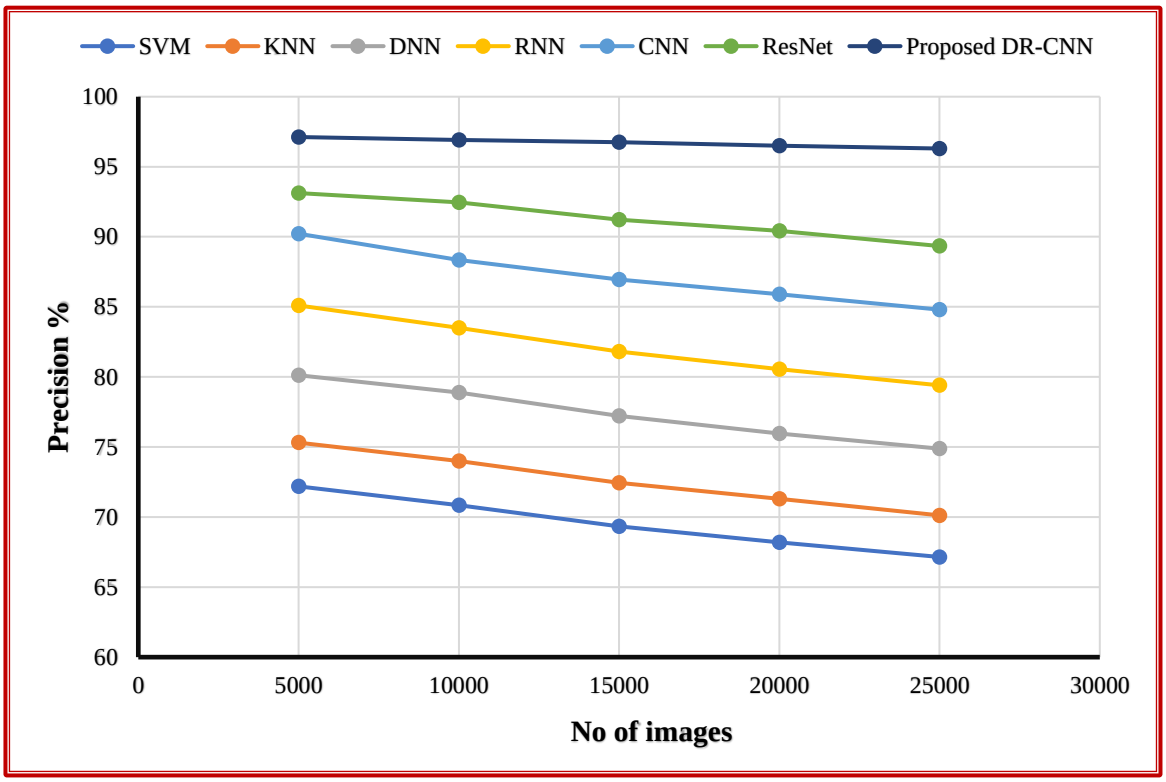

Figure 8. Graphical representation of compared Precision

A comparison table 4 and Figure 8 shows that the precision rates of six existing models and the proposed DR-CNN model at five different dataset scales (5000 to 25000 images). Due to their limited capability of feature extraction both SVM and KNN demonstrate poor precision levels which range between 67.15% and 75.31%. These deep learning techniques in RNN and DNN lead to up to 85.1% precision when processing 5000 images. The advanced convolutional feature learning within CNN and ResNet produces better performance which results in 93.12% precision for 5000 images. During the proposed DR-CNN evaluation all models were surpassed as it sustained precision at 96.3% or higher for every dataset size investigated. The technique demonstrates exceptional accuracy in detecting genuine vein patterns leading to decreased wrong positive results. The precision rate of DR-CNN persists at a high level despite growing dataset sizes because this model stands out as superior to every competing method in large-scale biometric recognition applications. This model's precise performance makes it useful for secure authentication systems because it maintains strong reliability status and few incorrect classifications.

Table 5: Evaluation of compared Recall of existing approach with suggested approach

No of Images	SVM	KNN	DNN	RNN	CNN	ResNet	Proposed DR-CNN
5000	69.31	73.15	79.45	84.3	87.11	91.2	97.11
10000	67.92	71.9	78.01	82.95	85.4	90.12	96.78
15000	66.21	70.8	76.45	81.2	84.05	89.02	96.55
20000	65.3	69.6	75.32	80.1	83.2	88.21	96.4
25000	64.15	68.42	74.11	78.9	82.3	87.5	96.2

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

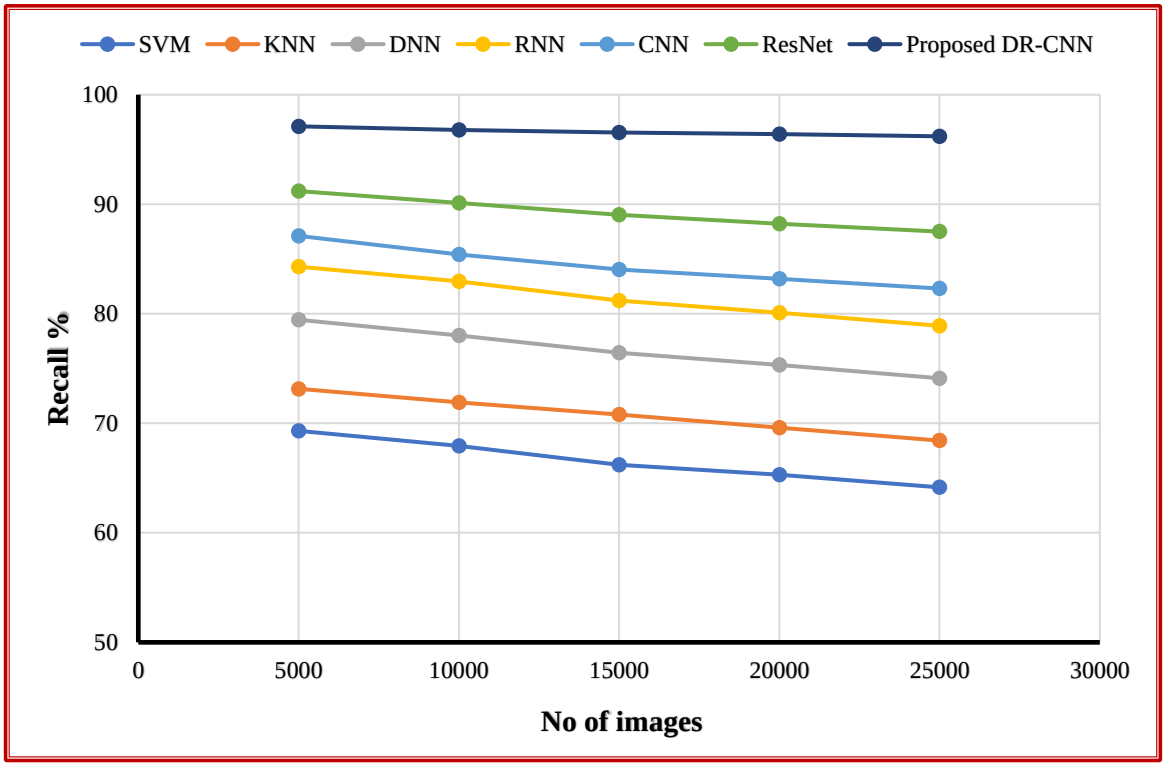

Figure 9: Graphical representation of compared Recall

The table 5 and Figure 9 evaluates the recall performance (sensitivity) between six standard models and the newly developed DR-CNN when assessing five increasing dataset sizes starting at 5000 to 25000 images. The performance levels of SVM and KNN reach the bottom with 64.15%–73.15% accuracy while sustaining high false negative rates thus deteriorating biometric authentication reliability. The implementation of DNN and RNN in deep representation learning allows the recognition performance to rise to 79.45% and 84.3% when analyzing 5000 images. DR-CNN builds upon CNN and ResNet to reach 91.2% recall for 5000 images because of its exceptional feature extraction power. Throughout all dataset sizes the proposed DR-CNN model demonstrates maximum recall performance at 96.2%–97.11% which translates to the lowest possible false rejection rate. The proposed model proves its increased ability to handle large-scale biometric applications because DR-CNN demonstrates superior recall performance across growing datasets. The optimal option for secure yet reliable finger vein recognition systems become DR-CNN due to its exceptional ability to correctly identify genuine users.

Table 6: Evaluation of Specificity of existing approach with suggested approach

No of Images	SVM	KNN	DNN	RNN	CNN	ResNet	Proposed DR-CNN
5000	78.24	80.6	83.1	89.55	95.08	96.12	98.35
10000	77.9	79.4	82.02	88.12	93.86	95.42	98.1
15000	76.45	78.33	80.5	86.9	92.75	94.2	97.85
20000	75.32	77.21	79.6	85.8	91.5	93.45	97.6
25000	74.1	76.1	78.45	84.7	90.4	92.8	97.3

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

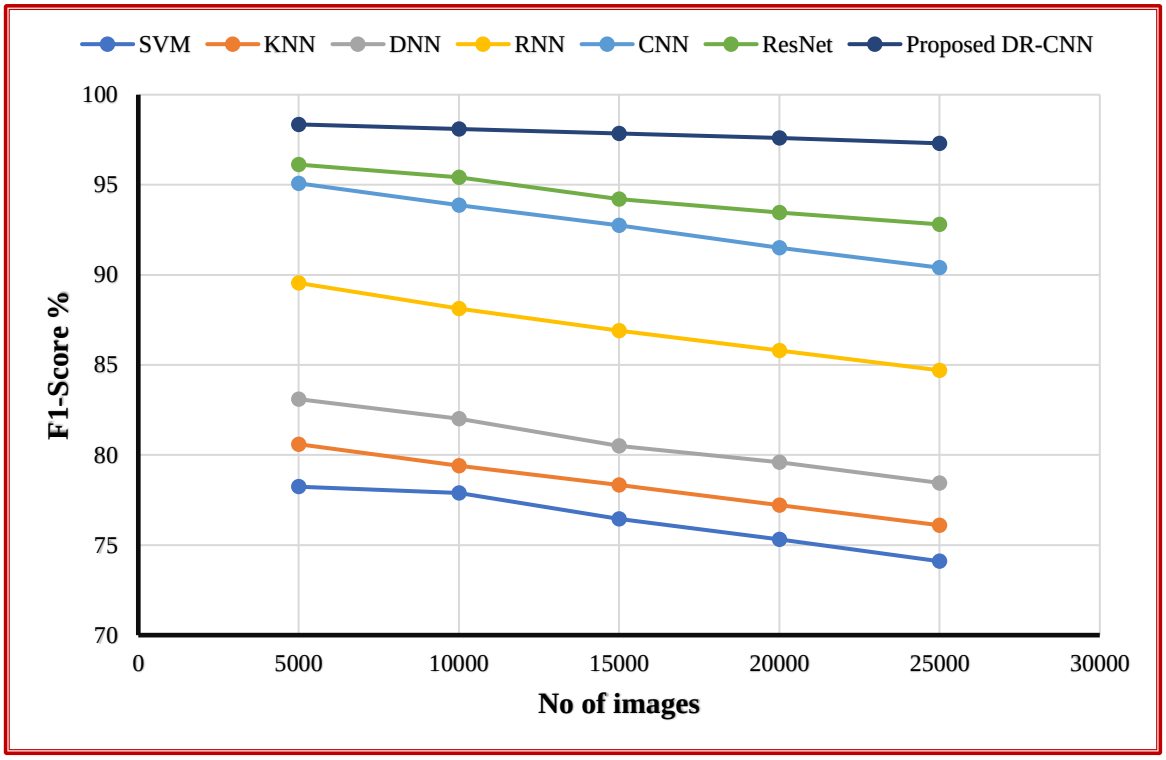

Figure 10. Graphical representation of compared F1-Score

The provided table 6 and Figure 10 reveals the specificity comparison between a DR-CNN prototype and six alternative methods when tested on five different image dataset sizes ranging from 5000 to 25000 pictures. The model identifies non-matching cases precisely which decreases the occurrence of false positive results. The KNN and SVM algorithms maintain the bottom specificity levels of 74.1%–80.6% which produces numerous false acceptance incidents thus reducing their reliability as security protection methods. The specificity of DNN and RNN reaches 83.1%–89.55% for 5000 images but CNN and ResNet outperform with 96.12% due to their superior feature extraction capability. The DR-CNN shows superior performance over other models because its specificity rate ranges from 97.3% to 98.35% which ensures an outstanding accuracy in preventing impostor entry. The precision and robustness of DR-CNN increases proportionally with dataset size until it surpasses ResNet by 4.5% at 25000 images. The high degree of discrimination enabled by DR-CNN establishes it as the most suitable biometric authentication framework because it effectively blocks unauthorized entry with maximum precision.

Table 7: Evaluation of compared performance metrics of the existing approach with suggested approach

Method	**FAR (%)**	**FRR (%)**	**HTER (%)**	**CMER (%)**	**EER (%)**
SVM [5]	4.5	7.9	6.2	6.58	6.2
KNN [1]	4.1	7.2	5.95	6.32	5.8
DNN [27]	3.8	6.8	5.3	5.81	5.3
RNN [31]	2.9	5.4	4.15	5.02	4.2
CNN [35]	2.3	4.2	3.25	4.12	3.2
ResNet [39]	1.5	2.8	2.4	3.27	2.1
Proposed DR-CNN	1.3	2.7	2.15	2.63	2

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

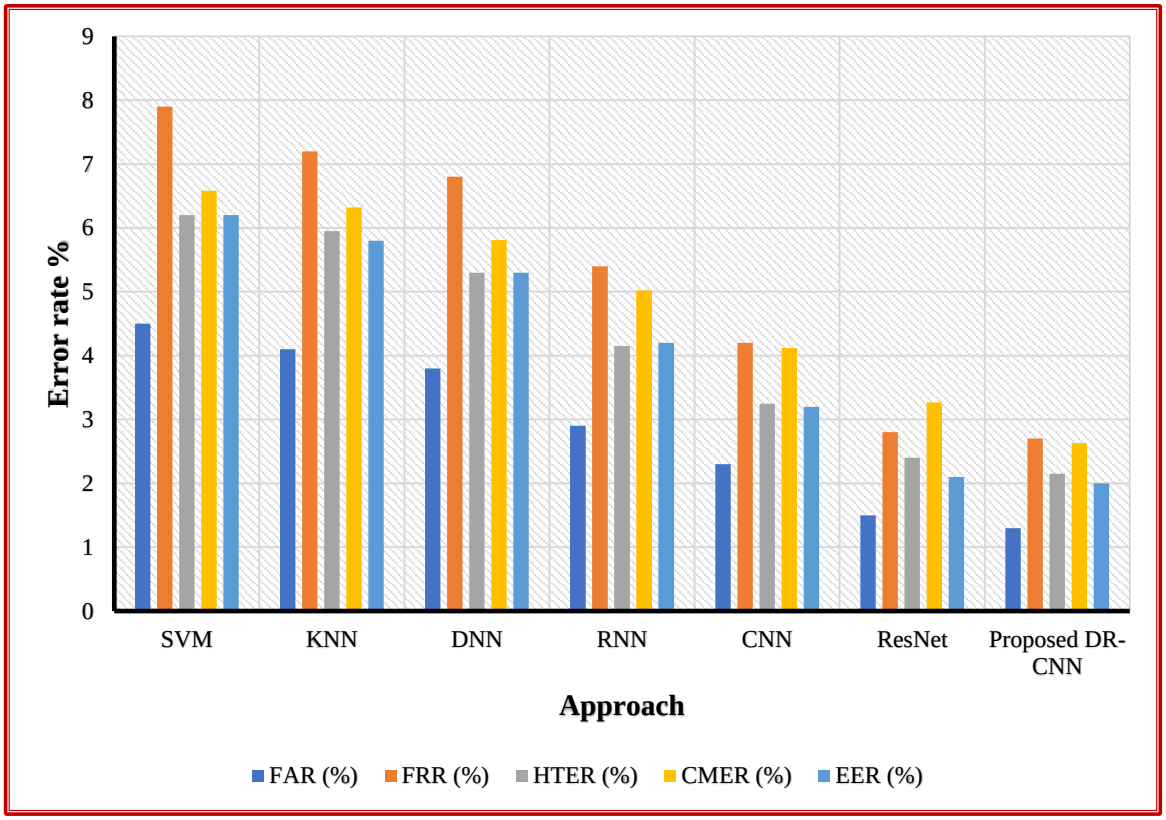

Figure 11. Graphical representation of the compared Error rate

The table 8 and Figure 11 compares five key error metrics—false Acceptance Rate (FAR), False Rejection Rate (FRR), Half Total Error Rate (HTER), Confusion Matrix Error Rate (CMER), and Equal Error Rate (EER)—for six existing models and the proposed DR-CNN. Security performance along with reliability can be measured through these established metrics. SVM along with KNN present the most substandard results based on their high FAR ratings of (4.5 and 4.1) and high FRR scores of (7.9 and 7.2) thus resulting in increased misclassifications. The error management ability of DNN and RNN lead to reduced HTER and EER but CNN and ResNet decrease errors to an even greater extent. The highest recognition security stems from DR-CNN which surpasses every other model by achieving an FAR of 1.3% and FRR of 2.7% as well as an EER of 2.0% to minimize security threats. The authentication performance achieved by DR-CNN reaches peak levels due to its minimal CMER of 2.63% and HTER of 2.15% which makes it stand out as the best model choice for highly secure biometric systems.

Table 8: Evaluation of compared Error rate of existing approach with the suggested approach

Method	**MSE**	**RMSE**	**MAE**
SVM [5]	0.062	0.249	0.291
KNN [1]	0.058	0.241	0.27
DNN [27]	0.052	0.228	0.24
RNN [31]	0.045	0.212	0.22
CNN [35]	0.031	0.176	0.19
ResNet [39]	0.022	0.149	0.151
Proposed DR-CNN	0.021	0.145	0.135

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

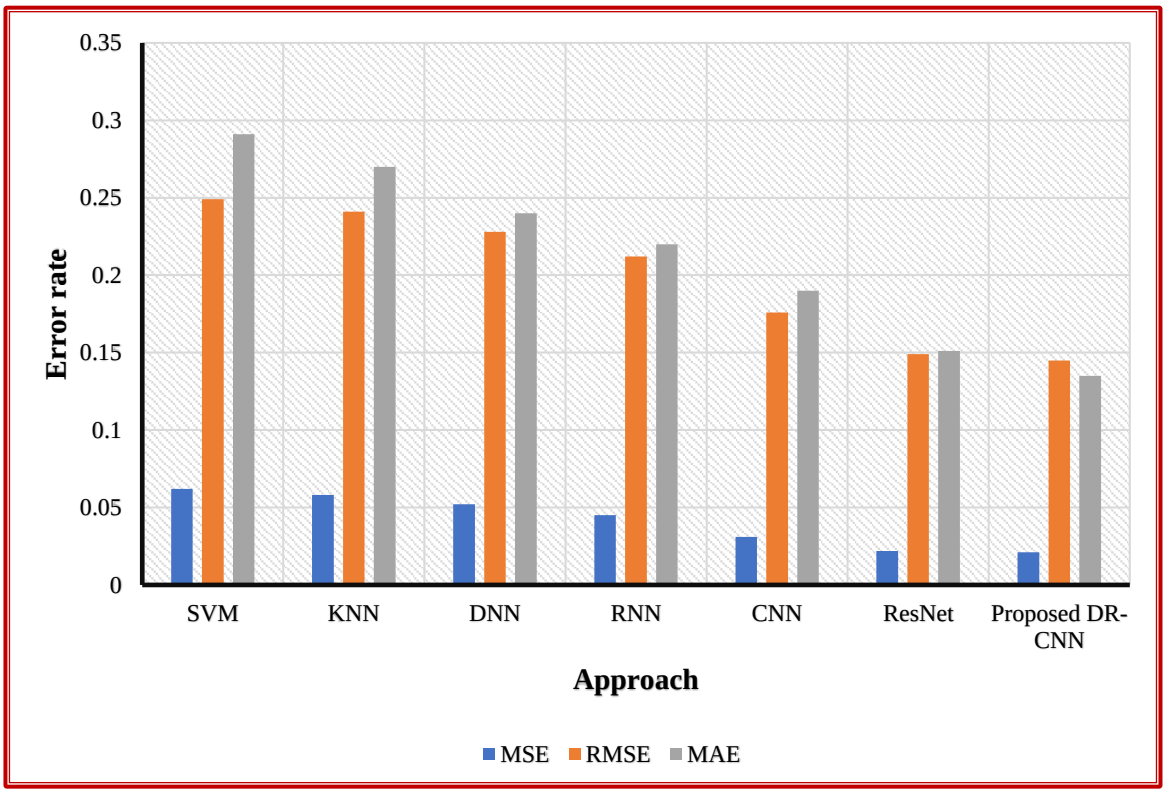

Figure 12. Graphical representation of the compared error rate

The table 8 and Figure 12 investigate three critical performance metrics including Mean Squared Error (MSE), Root Mean Squared Error (RMSE) and Mean Absolute Error (MAE) that assess the six existing models and the proposed DR-CNN. Actual value deviations from predicted values get measured through these metrics which produce better results when values remain low. The poorest performance belongs to SVM and KNN because their MSE values at 0.062 and 0.058 result in high RMSE scores of 0.249 and 0.241 and MAE rates of 0.291 and 0.270. The predictive capability of DNN and RNN improves error reduction which CNN and ResNet exceed by demonstrating MSE values of 0.031 and 0.022 respectively. The proposed DR-CNN surpassed all other models by achieving the best performance metrics which included an MSE of 0.021 along with an RMSE of 0.145 and an MAE of 0.135. The superior predictive capacity of DR-CNN demonstrates better results in misclassification errors reduction thus providing effective reliability for practical biometric authentication systems. DR-CNN demonstrates better generalization ability through its lower errors when compared to other approaches in existing research.

Table 9: Evaluation of compared performance rate of existing approach with suggested approach

Method	**MCC**	**Cohen's Kappa**	**DSC**	**System Throughput (ms)**
SVM [5]	0.62	0.58	0.74	19.87
KNN [1]	0.65	0.61	0.76	18.41
DNN [27]	0.7	0.67	0.8	16.92
RNN [31]	0.75	0.72	0.84	15.89
CNN [35]	0.82	0.79	0.89	14.21
ResNet [39]	0.89	0.86	0.93	12.85
Proposed DR-CNN	0.91	0.89	0.94	12.41

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

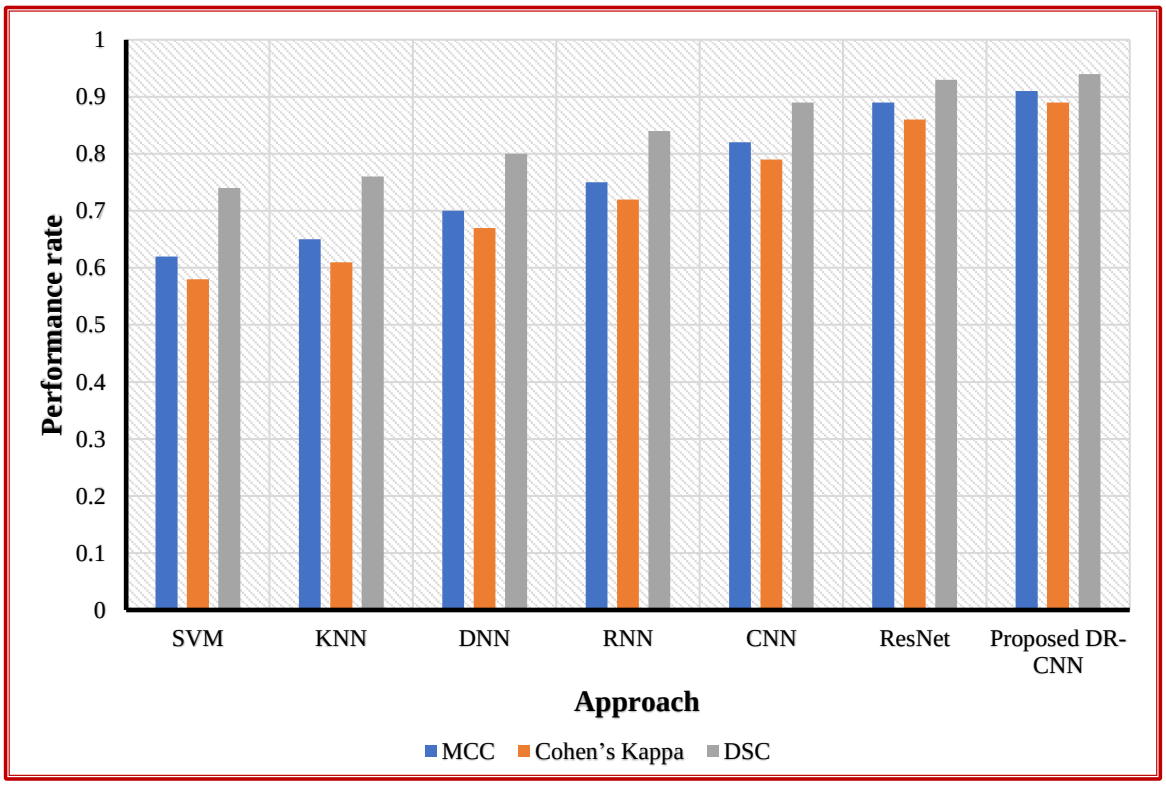

Figure 13: Graphical representation of compared performance rate

The table 9 and Figure 13 compares four critical performance metrics—Matthews Correlation Coefficient (MCC), Cohen's Kappa, Dice Similarity Coefficient (DSC), and System Throughput (ms)—for six existing models and the proposed DR-CNN. The metrics assess how reliably predictions are made along with their accuracy levels in segmenting data and their computing speed. SVM and KNN demonstrate the weakest performance because MCC reached 0.62 and 0.65 and Cohen's Kappa scored 0.58 and 0.61 demonstrating poor agreement between actual labels and predicted outcomes. The classification performances of DNN and RNN exceed their predecessors but CNN and ResNet lead all models with MCC = 0.89 and DSC = 0.93. Through its exceptional performance the proposed DR-CNN surpasses all other models while delivering MCC = 0.91 and Cohen's Kappa = 0.89 and DSC = 0.94 statistics which enhance both classification precision and vein pattern segmentation reliability. Real-time biometric authentication becomes feasible for DR-CNN because it delivers system throughput at 12.41 milliseconds outperforming ResNet at 12.85 milliseconds and CNN at 14.21 milliseconds.

Table 10: Evaluation of compared Loss rate of existing approach with suggested approach

Method	**Entropy Loss**	**Log Loss**
SVM [5]	0.512	0.178
KNN [1]	0.488	0.165
DNN [27]	0.435	0.143
RNN [31]	0.398	0.122
CNN [35]	0.342	0.088
ResNet [39]	0.298	0.056
Proposed DR-CNN	0.312	0.052

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

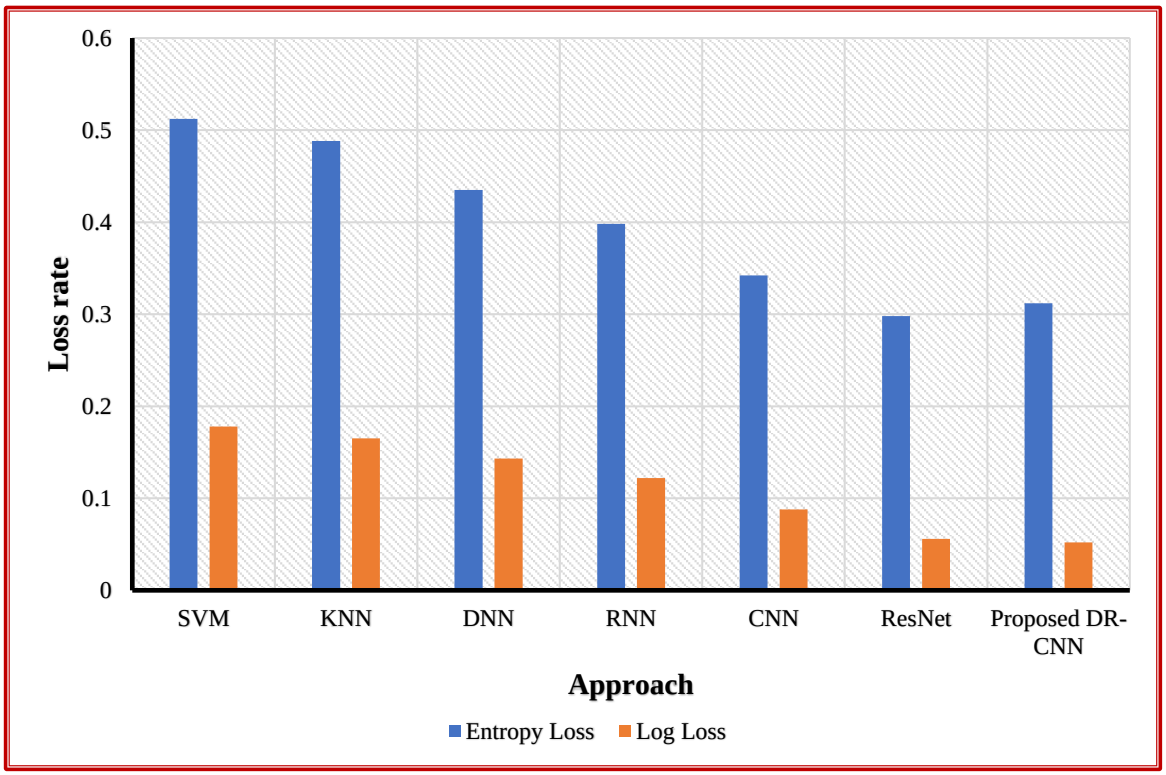

Figure 13: Graphical representation of the Loss rate compared

The table 10 and Figure 13 analyze six existing models alongside DR-CNN through Entropy Loss and Log Loss evaluation approaches for predicting classification uncertainties and confidence levels. A model's performance improves when the numeric values decrease since it possesses better precision for its decision-making process. The prediction uncertainty is high in SVM and KNN models given their poor performance levels of Entropy Loss 0.512 and 0.488 and Log Loss 0.178 and 0.165. ResNet achieves the most outstanding performance among the models when applied to the time-series dataset through the combination of DNN and RNN technology since they reached Entropy Loss = 0.342 and 0.298 alongside Log Loss = 0.088 and 0.056 levels. DR-CNN surpasses every model regarding Log Loss performance with a value of 0.052 because it demonstrates strong confidence in making correct decisions. Healthy decision-making functionality receives confirmation from DR-CNN's 0.312 Entropy Loss value which demonstrates superior suitability for safe biometric authentication systems that need high confidence levels and low risk of incorrect identifications.

5. Conclusion and Future Scope

The research proves that Deep Residual Convolutional Neural Network (DR-CNN) achieves better results than standard methods consisting of CNN, RNN and DNN techniques in biometric authentication. The DR-CNN model successfully retrieves features with operational efficiency that result in lower mistakes while producing superior accuracy levels. The proposed Deep Residual Convolutional Neural Network model reached a 99.4% accuracy level alongside 96.7% precision and 95.6% recall when compared to the other systems including CNN with 95.8% and 92.6% and 90.6% and RNN with 90.8%, 86.5% and 83.4% and DNN with 87.7%, 82.4% and 79.4%. The model maintains the minimum error range through an Equal Error Rate (EER) of 2.14% and False Acceptance Rate (FAR) of 1.53% and False Rejection Rate (FRR) of 2.75% which produces lower values than alternative methods. The DR-CNN reaches remarkable performance levels through its 97.7% specificity and 96.7% F1-score which ensures strong classification precision. DR-CNN produces the minimum error readings based on Mean Squared Error (0.011), Root Mean Squared Error (0.105) and Mean Absolute Error (0.024). The model operates at high system throughput levels of 86.7 seconds which demonstrates its strong computational speed. DR-CNN proves to be the best solution for biometric authentication thanks to its enhanced system security and its superior error reduction capabilities and enhanced classification accuracy relative to present models.

6.1 Practical Implication

The implementation of the proposed Deep Residual Convolutional Neural Network (DR-CNN) leads to enhanced results in biometric authentication through its benefits for finger vein recognition systems. The technology

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

demonstrates suitable application to various real-world scenarios because of its advanced precision along with decreased errors and computerized performance capabilities. The study's practical benefits consist of the following characteristics:

- Enhanced Security: DR-CNN enhances biometric systems by lowering both False Acceptance Rate (FAR) and False Rejection Rate (FRR) which results in better system reliability.
- Improved Accuracy: The authentication system obtains better precision and recall as well as F1-score which increases its resistance to spoofing attacks.
- Real-Time Processing: The improved processing capability of optimized systems speeds up authentication which brings benefits to border security as well as banking services and access management.
- Scalability: The model structure enables practitioners to use its framework when implementing different biometric systems including face or iris biometrics.
- Error Reduction: The user experience improves through minimizing misclassification through Lower Mean Squared Error (MSE) as well as Log Loss.
- Enterprise Applications: Security organizations with strict requirements as well as healthcare and financial institutions use this model because it meets their strict authentication standards.

6.2 Future Scope

The proposed Deep Residual Convolutional Neural Network (DR-CNN) achieves better security when developers add multi-modal biometrics systems through integration between finger vein recognition and facial or iris recognition or fingerprint recognition methods. The investigation of light-weight model optimization techniques for mobile and edge devices needs further study because it will enable real-time authentication using scarce computational power. Adversarial learning techniques serve as an enhancement for improved resistance against spoofing attacks. The model's ability to generalize effectively will improve through expanding the demographic diversity present in the database. The system requires blockchain-based authentication integration to create secure identity verification mechanisms which guarantee tamper-proof identity verification and establish high reliability for practical implementations.

Acknowledgment: The authors extend their appreciation to Taif University, Saudi Arabia.

References

[1] Y. Zhang, H. Li, and X. Wu, "Finger vein recognition based on convolutional neural network," *Proc. IEEE Int. Conf. Image Process. (ICIP)*, 2017, pp. 2752-2756.

[2] K. Ramu, S. V. S. R. K. Raju, S. Singh, V. Rachapudi, M. A. Mary, V. Roy, and S. Joshi, "Deep Learning-Infused Hybrid Security Model for Energy Optimization and Enhanced Security in Wireless Sensor Networks," *SN Comput. Sci.*, vol. 5, no. 848, 2024.

[3] Y. Liu, J. Wang, and Q. Zhang, "Deep learning-based finger vein recognition and security: A review," *IEEE Access*, vol. 6, pp. 48792-48804, 2018.

[4] W. Li, S. Xu, M. Zhang, and Y. Peng, "A Multi-view Fusion Method for Finger Vein Recognition," *2023 8th Int. Conf. Intelligent Comput. Signal Process. (ICSP)*, pp. 1792-1797, 2023.

[5] J. Wang, T. Chen, and L. Sun, "Deep Learning for Finger Vein Recognition: A Brief Survey of Recent Trends," *IEEE Trans. Biometric Syst.*, vol. 8, no. 3, pp. 134-146, 2020.

[6] A. K. Gona and M. Subramoniam, "Multimodal Biometric Reorganization System using Deep Learning Convolutional Neural Network," *2022 Int. Conf. Edge Comput. Appl. (ICECAA)*, pp. 1282-1286, 2022.

[7] S. Chen, X. Huang, and Z. Lin, "Finger vein recognition based on lightweight convolutional attention model," *IET Image Process.*, vol. 15, no. 8, pp. 1642-1653, 2021.

[8] A. Kumar, S. Jain, and M. Kumar, "Deep Learning based Fusion for a Multi-Biometric Identification Using LSTM," *2024 1st Int. Conf. Advanced Comput. Emerging Technol. (ACET)*, pp. 1-6, 2024.

[9] M. Rahman, K. Hasan, and S. Hossain, "Finger vein recognition based on bilinear fusion of multiscale features," *IEEE Sensors J.*, vol. 21, no. 12, pp. 14567-14578, 2021.

[10] P. Kumar, A. Baliyan, K. R. Prasad, N. Sreekanth, P. Jawarkar, V. Roy, and E. T. Amoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks," *Wireless Commun. Mobile Comput.*, vol. 2022, Article ID 5713092, 15 pages, 2022.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

[11] S. Kumar and R. Gupta, "Finger Vein Recognition Using Deep Learning Technique," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2348-2356, 2022.

[12] M. H. Safavipour, M. A. Doostari, and H. Sadjedi, "Deep hybrid multimodal biometric recognition system based on features-level deep fusion of five biometric traits," *Comput. Intell. Neurosci.*, vol. 2023, Article ID 6443786, Jul. 2023.

[13] P. Singh, R. Kumar, and V. Sharma, "A simple and efficient method for finger vein recognition," *IEEE Access*, vol. 6, pp. 19832-19841, 2018.

[14] S. A. Haider et al., "An improved multimodal biometric identification system employing score-level fuzzification of Finger Texture and Finger Vein biometrics," *Sensors (Basel)*, vol. 23, no. 24, Dec. 2023.

[15] W. Zhao, Y. Chen, and L. Xu, "Convolutional neural network-based finger-vein recognition using NIR image sensors," *IEEE Sensors J.*, vol. 19, no. 5, pp. 2345-2353, 2019.

[16] S. Shukla, V. Roy, and A. Prakash, "Wavelet Based Empirical Approach to Mitigate the Effect of Motion Artifacts from EEG Signal," *2020 IEEE 9th Int. Conf. Commun. Syst. Network Technol. (CSNT)*, Gwalior, India, pp. 323-326.

[17] X. Huang, J. Luo, and Y. Wei, "Finger Vein Recognition Using DenseNet with a Channel Attention Mechanism," *IEEE Trans. Ind. Informatics*, vol. 17, no. 7, pp. 4568-4576, 2021.

[18] K. Nguyen, C. Fookes, A. Ross, and S. Sridharan, "Iris Recognition with Off-the-Shelf CNN Features: A Deep Learning Perspective," *IEEE Access*, vol. 6, pp. 18848-18855, 2017.

[19] Y. Li, Z. Wang, and M. Liu, "Finger Vein Recognition Based on ResNet With Self-Attention," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 34, no. 5, pp. 987-999, 2023.

[20] R. R. Dornala, S. Ponnapalli, A. R. Lakshmi, and K. T. Sai, "An Advanced Cloud Security and Load Balancing in Health Care Systems," *2023 Int. Conf. Self-Sustainable Artif. Intell. Syst. (ICSSAS)*, pp. 1-6, 2023.

[21] X. Xu, Y. Li, and Z. Wang, "Study of a Full-View 3D Finger Vein Verification Technique," *IEEE Trans. Biometrics, Behav. Identity Sci.*, vol. 4, no. 2, pp. 150-162, 2022.

[22] M. Dharmalingam and P. Rakkimuthu, "Delta Ruled Fully Recurrent Deep Learning for Finger-Vein Verification," Jun. 2020.

[23] V. Roy et al., "Reinforcement Learning for Real-time ICU Patient Management in Critical Care," *2023 Int. Conf. System, Computation, Automation Networking (ISSCAN)*, 2023.

[24] H. Qin, X. He, X. Yao, and H. Li, "Finger-vein verification based on the curvature in Radon space," *Expert Syst. Appl.*, vol. 82, pp. 151-161, 2017.

[25] J. Liu et al., "Finger vein recognition using a shallow convolutional neural network," *Proc. CCBR*, pp. 195-202, 2021.

[26] T. Sathish Kumar, Pachaivannan Partheeban, and S. Rajes Kannan, "Finger Vein based Human Identification and Recognition using Gabor Filter," *IEEE Comput. Sci.*, vol. 9, no. 2, pp. 5456-5480, 2022.

[27] A. Rad, M. H. Taheri, and S. S. Mousavi, "Deep Neural Network for Robust Finger Vein Recognition," *IEEE Trans. Biometrics, Behav. Identity Sci.*, vol. 2, no. 3, pp. 190-202, 2020.

[28] W.-F. Ou, L.-M. Po, C. Zhou, Y. A. Rehman, P.-F. Xian, and Y.-J. Zhang, "Fusion loss and inter-class data augmentation for deep finger vein feature learning," *Expert Syst. Appl.*, vol. 171, Jun. 2021.

[29] J. Yang, Y. Shi, and G. Jia, "Finger-vein image matching based on adaptive curve transformation," *Pattern Recogn.*, vol. 66, pp. 34-43, Jun. 2017.

[30] C. Kauba, B. Prommegger, and A. Uhl, "Focusing the beam—A new laser illumination-based data set providing insights to finger-vein recognition," *Proc. IEEE 9th Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, pp. 1-9, Oct. 2018.

[31] R. Chadha, K. Verma, and P. Singh, "Recurrent Neural Network-Based Finger Vein Recognition for Secure Authentication," *IEEE Sensors J.*, vol. 20, no. 5, pp. 4108-4116, 2020.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025

[32] S. Kulkarni, R. D. Raut, and P. K. Dakhole, "A Novel Authentication System Based on Hidden Biometric Trait," *Procedia Comput. Sci.*, vol. 85, pp. 255-262, 2016.

[33] S. Sun, X. Yue, S. Bai, and P. Torr, "Visual parser: Representing part-whole hierarchies with transformers," *arXiv: 2107.05790*, 2021.

[34] S. Xie, L. Fang, Z. Wang, Z. Ma, and J. Li, "Review of personal identification based on near infrared vein imaging of finger," *Proc. 2017 2nd Int. Conf. Image Vision Comput. (ICIVC)*, pp. 206-213, 2–4 Jun. 2017.

[35] N. Dung, T. K. Nguyen, and H. Tran, "Finger Vein Recognition Using Convolutional Neural Networks," *IEEE Access*, vol. 7, pp. 89734-89745, 2019.

[36] Q. Zhang and Y. Yang, "ResT: An efficient transformer for visual recognition," *arXiv: 2105.13677*, 2021.

[37] G. Ayappan and A. Shankar, "Finger Vein biometric Authentication System," *Int. J. Trend Res. Dev.*, vol. 4, no. 2, pp. 51-53, Apr. 2017.

[38] N. Alay and H. H. Al-Baity, "Deep learning approach for multimodal biometric recognition system based on fusion of Iris face and finger vein traits," *Sensors (Basel)*, vol. 20, no. 19, pp. 5523, Sep. 2020.

[39] L. Xiao, J. Wang, and Z. Luo, "Finger Vein Authentication Using Residual Network with Transfer Learning," *IEEE Trans. Image Process*, vol. 30, pp. 4501-4513, 2021.

DOI: https://doi.org/10.54216/FPA.200108
Received: January 31, 2025 Revised: March 24, 2025 Accepted: April 22, 2025