ISSN: 2366-1313

FINGER VEIN RECOGNITION SYSTEM WITH TEMPLATE PROTECTION

[1]Mr. Audi Reddy Kayithi,[2]Allu Sai Vineetha,[3]Moses Aashray Kyarem,[4]D Jagadeshwar

[1]Assistant Professor, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

adireddyk.cse@gcet.edu.in

[2, 3, 4,BTech] Student, Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

20r11a6206@gcet.edu.in,20r11a6234@gcet.edu.in,21r15a6205@gcet.edu.in

ABSTRACT:

The finger vein features have received extensive attention due to their high safety and stability characteristics, and are gradually being used in various fields. However, studies have shown that finger vein recognition systems based on convolutional neural networks are at huge security risks. Criminals can obtain part of the user information of the system through certain illegal operations on the recognition results or the system database stored in the recognition system, which puts the original vein data at huge security risks. Once compromised, the user information stored in the system will be permanently leaked, and the individual's vein features will no longer be safe. In order to solve these problems, we propose a new finger vein image recognition, which applies Convolution Neural Network. To enhance the overall performance analysis. Develop a CNN-based model capable of accurately identifying individuals based on their finger vein patterns. Evaluate the performance of the developed model using appropriate metrics such as accuracy, precision, recall and F1-score. Compare the performance of the CNN- based approach with traditional finger vein recognition methods.

Keywords*:* CNN, finger vein features.

ISSN: 2366-1313

I INTRODUCTION

Biometric recognition technology that uses the inherent physiological and behavioral characteristics of the human body for authentication has received widespread attention, and has shown lots of advantages in many applications such as identity authentication, security defense and access control, it has become one of the fastest-growing new technologies. Compared with traditional recognition technology, biometric recognition technology uses the unique features of the human body such as face, fingerprint, iris and vein to perform identity authentication. Because biometrics is not easy to be lost and duplicated, biometric recognition technology is considered a reliable and efficient solution. Among many biological characteristics, the finger vein has become the most popular due to its vitality, uniqueness, and presence inside the finger. Unlike the iris or gait that can be seen or tracked, the finger vein must be captured with an infrared sensor with a specific wavelength, which cannot be directly observed or left traced. A lot of research work has been done on the finger vein recognition system, and various excellent recognition algorithms have been proposed, including both the traditional method of manually designing features by analyzing vein characteristics, and the design network based on deep learning (mainly convolutional neural network (CNN)) for feature extraction through independently learning. The recognition performance of the finger vein recognition systems continues to improve. However, most existing finger vein recognition systems do not pay attention to the protection of finger vein templates or features stored in database, and many systems even show the original images of the finger vein directly in the database.

Although the finger vein features exist inside the human finger and cannot be stolen or duplicated directly, an attacker can hack into the database of the finger vein system or analyze the network output for finger vein information, especially finger vein recognition systems based on CNN. The main component of CNN is convolution operation, which can be restored to a certain extent by DE convolution. Zeiler et al. proposed a DE convolutional network. Different from the forward operation of mapping image pixels to feature space through CNN, the DE convolution network reversely maps the feature map 2 back to pixel space. The main operations include DE

convolution, unpooling, rectification and filtering.

While finger vein characteristics are unique to the human finger and cannot be directly copied or stolen, an attacker can obtain finger vein information via breaking into the database of the finger vein system or by examining the network output. Thesis particularly true for CNN-based finger vein recognition systems. Convolution is the primary function of CNN, and it can be partially restored by DE convolution, which is suggested by a DE convolutional network. The DE convolution network maps the feature map backwards, from pixel space to feature space, in contrast to the forward process of mapping image pixels to feature space by CNN. DE computation, unspooling, rectification, and filtering are the primary operations. Given that CNN is reversible and needs a substantial amount of original finger vein pictures for recognition or training. In this project, we aim to develop a finger vein recognition system using Convolutional Neural Networks (CNNs), a deep learning approach known for its effectiveness in image recognition tasks.

II. LITERATURE SURVEY

1.A fingerprint and finger-vein based cancelable multi-biometric system Authors: Yang Wencheng, Wang Song, Hu Jiankun, Shang Guanglou , Craig Valli Compared to uni-biometric systems, multi-biometric systems, which fuse multiple biometric features, can improve recognition accuracy and security. However, due to the challenging issues such as feature fusion and biometric template security, there is little research on cancelable multi-biometric systems. In this paper, we propose a fingerprint and finger-vein based cancelable multi-biometric system, which provides template protection and revocability. The proposed multi-biometric system combines the minutiabased fingerprint feature set and image-based finger-vein feature set. We develop a feature-level fusion strategy with three fusion options. Matching performance and security strength using these different fusion options are thoroughly evaluated and analyzed. Moreover, compared with the original partial discrete Fourier transform (PDFT), security of the proposed multi-biometric system is strengthened, thanks to the enhanced partial discrete Fourier transform (EP-DFT) based non-invertible transformation. Local Kernel Feature Analysis (LKFA) for object recognition. Multibiometric feature fusion is non-trivial for the reason that feature representation of multiple traits may be different and

incompatible to one another, e.g. minutia-based fingerprint features and image-based finger-vein features. The only reported work on the feature fusion of fingerprint and finger-vein data is found in, the image-based fingerprint and finger-vein codes are first extracted using a unified Gabor filter, and then a supervised local-preserving canonical correlation analysis (SLPCCA) algorithm is proposed to implement feature fusion. In this method, feature representation for both fingerprint and finger-vein information is image-based. The performance of this image-based multibiometric system can be seriously affected by non-linear distortion and noise present in the fingerprint image. Therefore, in general, for the fingerprint image which has a set of salient points, minutia-based techniques are preferred to image-based ones.

2,A novel finger vein verification system based on two-stream convolutional network learning Author : Fang Yuxun

Convolutional neural networks have been proven to have strong feature representation ability; however, they often require large training samples and high computation that are infeasible for real-time finger vein verification. To address this limitation, we propose a lightweight deep-learning framework for finger vein verification. First, we designed a lightweight two-channel network that has only three convolution layers for finger vein verification. Then, we extracted the mini-ROI from the original image to better solve the displacement problem based on the evaluation of the two-channel network. Shared Representation Learning for Heterogeneous Face Recognition. Biometric authentication systems are becoming increasingly important in various sectors, ranging from financial transactions to access control. Among these, finger vein recognition has gained traction due to its high accuracy and robustness. In this paper, we propose a novel approach named Vein Guard, which utilizes a two-stream convolutional neural network (CNN) architecture for finger vein verification. Vein Guard consists of two streams: the spatial stream and the temporal stream. The spatial stream processes static images of finger veins, capturing the structural information inherent in the vein patterns. On the other hand, the temporal stream processes sequences of vein images captured over time, exploiting the dynamic characteristics of vein patterns such as blood flow. The two streams are jointly trained using a Siamese architecture to learn discriminative features for finger vein verification. The Siamese architecture

facilitates learning by presenting pairs of vein images along with their corresponding labels (i.e., same or different identity). Through the use of contrastive loss, the network learns to minimize the distance between images of the same identity while maximizing the distance between images of different identities. To evaluate the performance of Vein Guard, we conducted experiments on a publicly available finger vein dataset. Our results demonstrate the effectiveness of the proposed approach, achieving state-of-the-art performance in terms of verification accuracy. Furthermore, Vein Guard exhibits robustness against various challenges such as illumination variations, finger positioning.

3. Finger-vein image matching based on adaptive curve transformation Author: Jinfeng Yang

Extracting reliable finger-vein features directly from original finger-vein images is not an easy task since the captured finger-vein images are always poor in quality. This paper proposes an effective method of finger-vein feature representation based on adaptive vector field estimation. Considering that the vein networks consist of vein curve segments, a set of spatial curve filters (SCFs) with variations in curvature and orientation are first designed. To fit vein curves locally and closely, SCFs is then weighted using a variable Gaussian model. Due to the fact that finger veins vary in diameters naturally, an effective curve length field (CLF) estimation method is proposed to make weighted SCFs adaptive to vein-width variations. Finally, with CLF constrain, vein vector fields (VVF) are built for finger-vein network feature description. Experimental results show that the proposed method is highly powerful in improving finger-vein matching accuracy. The quality of finger-vein images is not always good owing to light attenuation in tissues. The NIR lights penetrating a human finger can be refracted, absorbed and scattered by the biological tissue. Since the biological tissue can be viewed as a complex heterogeneous optical medium, the NIR lights suffer from significant scattering in addition to absorption when they propagate into this medium. This can greatly reduce the contrast between the venous and no venous regions, and further impair the accuracy of finger-vein image matching.

III SYSTEM ANALYSIS

EXISTING SYSTEM

Finger vein biometric systems have emerged as a promising modality for personal identification due to their distinctiveness and

ISSN: 2366-1313

robustness. Traditionally, these systems have primarily relied on vein pattern information for authentication. However, recent advancements in machine learning techniques have opened up new avenues for enhancing the accuracy and reliability of such systems. One significant approach involves incorporating texture features into the biometric recognition process.

This approach aims to leverage residual information surrounding vein patterns to improve authentication accuracy. By analyzing not only the vein patterns themselves but also the texture characteristics of the surrounding tissue, the system can achieve better discrimination between individuals. In a recent study, researchers proposed a finger vein biometric system that integrates texture features into the authentication process. The system is built upon the Support Vector Machine (SVM) algorithm, a powerful machine learning technique known for its effectiveness in classification tasks. By training the SVM model on a standardized finger vein database, the researchers evaluated the performance of the proposed system in comparison to traditional approaches. The key innovation of this system lies in its utilization of texture features extracted from the regions surrounding vein patterns. These texture features capture subtle variations in the skin's surface, which can serve as additional discriminative information for authentication. By analyzing both vein patterns and texture features, the system can more accurately distinguish between genuine users and impostors. To evaluate the effectiveness of the proposed approach, the researchers conducted experiments using a standardized finger vein database. The database contains a diverse set of finger vein images captured under various conditions, allowing for comprehensive testing of the system's performance.

Through rigorous experimentation and analysis, the researchers were able to assess the impact of incorporating texture features on authentication accuracy. The results of the study demonstrate that adding texture features significantly improves the authentication accuracy of finger vein biometric systems. By considering residual information around 7 vein patterns, the system achieves higher levels of discrimination between individuals, thereby enhancing overall security and reliability. Moreover, the use of the SVM algorithm ensures robust performance across different

datasets and conditions. Beyond its immediate implications for biometric authentication, this research highlights the broader potential of machine learning techniques in enhancing security systems. By leveraging advanced algorithms and incorporating additional features such as texture information, researchers can continue to push the boundaries of biometric technology and improve its real-world applicability.

Disadvantages

• Doesn't Efficient for handling large volume of data.

• Theoretical Limits

• Incorrect Classification Results.

• Less Prediction Accuracy.

PROPOSED SYSTEM

The proposed system leverages the power of Convolutional Neural Networks (CNNs) for image recognition and classification tasks, specifically aimed at distinguishing between normal and abnormal images. CNNs are a class of deep learning algorithms wellsuited for processing visual data, making them ideal for tasks such as image recognition. In this system, CNNs are employed to analyze the characteristics of input images and predict whether they are normal or abnormal. CNNs are particularly effective for image recognition tasks due to their ability to automatically learn hierarchical features from the input data. By employing layers of convolutional, pooling, and fully connected layers, CNNs can effectively capture both low-level and high-level features present in the images. One common preprocessing step in this system is grayscale conversion.

Grayscale conversion involves transforming the input images from color (RGB) to grayscale, where each pixel is represented by a single intensity value. This preprocessing step is beneficial for several reasons. Firstly, it reduces the dimensionality of the input data, making it more manageable for the CNN model to process. Secondly, grayscale conversion helps preserve important features in the images while removing color information, which may not be relevant for the classification task. By focusing solely on 8 intensity values, the model can better discern patterns and structures present in the images. The effectiveness of the proposed system is enhanced by its performance analysis using CNN algorithms. CNNs have demonstrated state-of-the-art performance in

various image recognition tasks, owing to their ability to learn complex patterns and relationships directly from the data. By utilizing CNNs for performance analysis, the system can accurately evaluate its classification capabilities and identify areas for improvement

Advantages

• High performance.

• Provide accurate prediction results.

• It avoid sparsely problems.

• Reduces the information Loss and the bias of the inference due to the multiple estimates.

IV IMPLEMENTATION

Architecture:

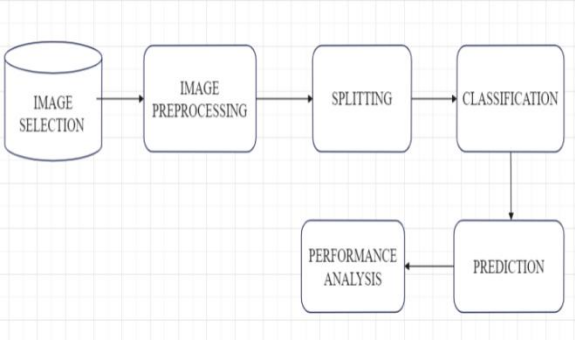


Fig-1. Architectures of the system model

The responsible for receiving input images or data, which could be from various sources such as finger vein images, databases, or files. The input data undergoes pre-processing, including grayscale conversion, resizing, normalization, and data augmentation to prepare it for further processing and analysis. The heart of the system, CNNs consist of multiple layers that learn hierarchical representations of the input data. These layers include convolutional layers for feature extraction, pooling layers for dimensionality reduction, and fully connected layers for classification. The CNN is trained using the preprocessed data. It involves optimizing the model's parameters iteratively using optimization algorithms such as gradient descent to minimize a predefined loss function. Once trained, the model's performance is evaluated using validation data. Metrics such as accuracy, sensitivity, specificity, precision, and F1-score are computed to assess its effectiveness in classification. The trained model is tested on unseen data to assess its real-world 22 performance. This module generates predictions for input images and computes performance metrics similar to the evaluation module.

MODULES

1. Data Selection and Loading

• This step involves identifying and gathering the dataset that contains the images to be used for classification. The dataset should ideally be diverse and representative of the problem domain. It may include both normal and abnormal images.

• Once the dataset is selected, the next step is to load the data into memory or the computational environment where the classification algorithm will be executed. This typically involves reading the image files and converting them into a format suitable for processing, such as arrays or tensors.

2. Data Pre-processing

• Data pre-processing is essential for preparing the raw image data for input into the classification algorithm. Common pre-processing steps include resizing the images to a uniform size, normalizing pixel values to a certain range (e.g., [0, 1]), and performing data augmentation techniques such as rotation, flipping, or cropping to increase the diversity of the dataset.

• In the context of medical imaging, additional preprocessing steps may be required, such as demising, contrast enhancement, or normalization specific to the imaging modality.

3. Data Splitting

• After preprocessing, the dataset is typically divided into two or more subsets for training, validation, and testing. The most common split is between training and testing sets, with a portion of the data reserved for model training and the rest for evaluating model performance.

• Optionally, a validation set may be created from the training data to tune hyper parameters and monitor the model's performance during training. Cross- 23 validation techniques may also be employed to ensure robustness and mitigate over fitting.

4. Classification

• The classification step involves training a machine learning model, such as a Convolutional Neural Network (CNN), on the training dataset. During training, the model learns to map input images to their corresponding labels (e.g., normal or abnormal).

• CNNs consist of multiple layers, including convolutional, pooling, and fully connected layers, which learn hierarchical

ISSN: 2366-1313

representations of the input data. The model's parameters are optimized iteratively using optimization algorithms such as gradient descent to minimize a predefined loss function.

5. Prediction

• Once the model is trained, it can be used to make predictions on new, unseen data. This involves passing input images through the trained model and obtaining output predictions, typically in the form of class probabilities or discrete labels.

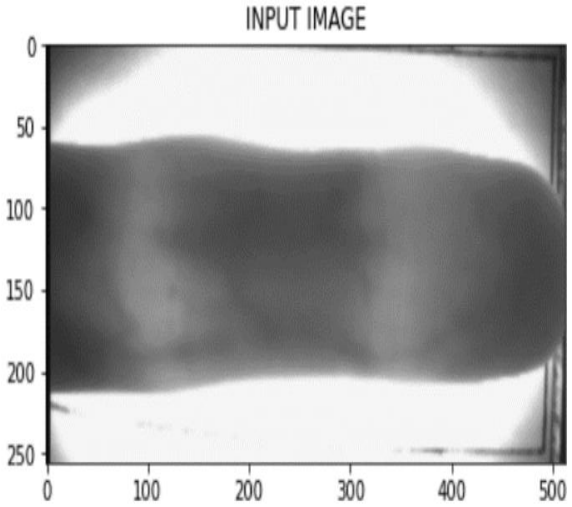
• The predictions can then be evaluated using performance metrics such as accuracy, precision, recall, and F1-score to assess the model's effectiveness in classifying normal and abnormal images.

6. Result generation

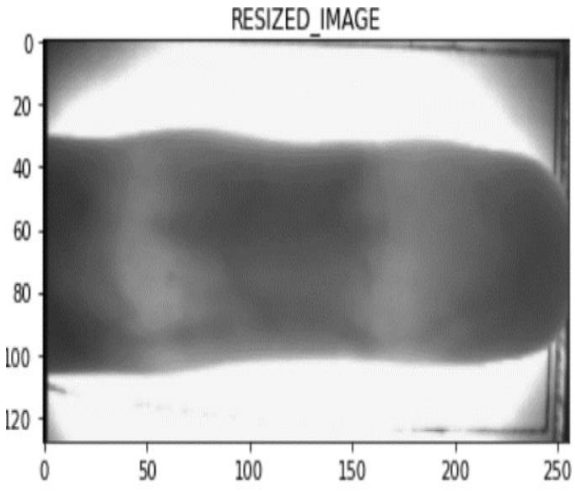
In the result, the input image is classified as either normal or abnormal, providing accuracy, sensitivity, and specificity metrics. Accuracy denotes overall correctness, sensitivity indicates the model's capability to detect true positives, and specificity measures its proficiency in identifying true negatives. These metrics offer a comprehensive evaluation of the model's performance, helping assess its effectiveness in correctly identifying both normal and abnormal images while minimizing false positives and false negatives

V RESULT AND DISCUSSION

Input image

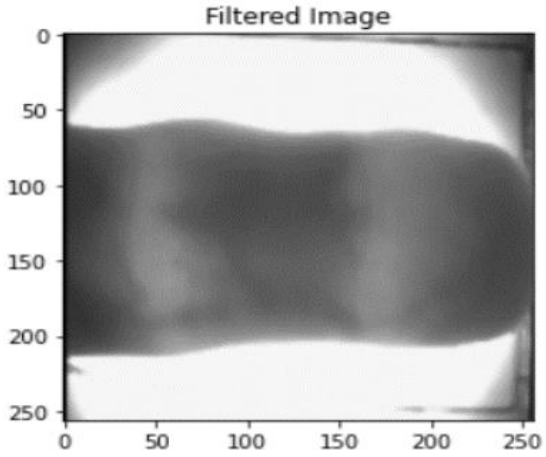


Resized image

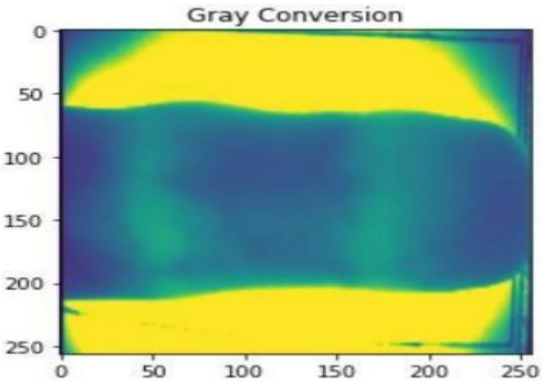


Filtered image

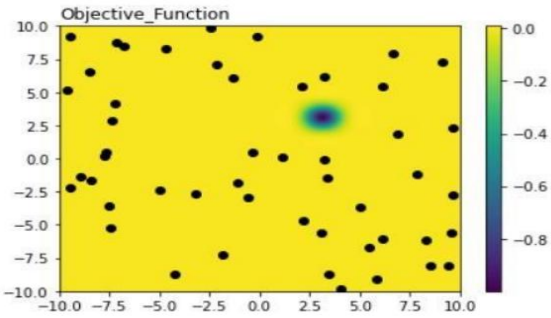
ISSN: 2366-1313



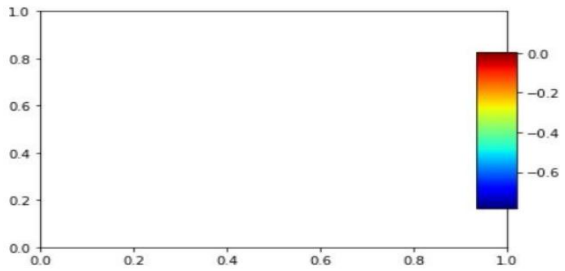
Gray Conversion



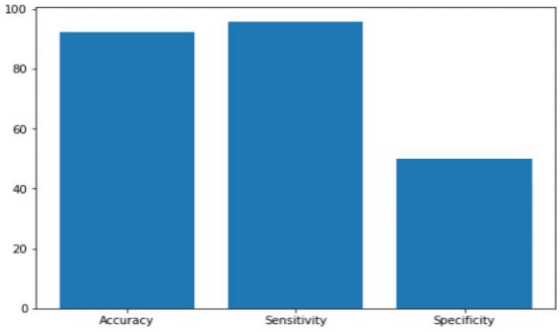
Objective function



Graph



Comparison Graph



Classification result

```
 Shape of Input Image:  (256, 513, 3)
Resized Dimensions using Preprocessing :  (128, 256, 3)
******** Classification Result ********
Identified as - Normal Image
WARNING:tensorflow:From C:\Users\DELL\anaconda3\Lib\site-packages\keras\src\losses.py:2976: The
name tf.losses.sparse_softmax_cross_entropy is deprecated. Please use
tf.compat.v1.losses.sparse_softmax_cross_entropy instead.

(80, 18)
(20, 18)
```

Model Layers

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 26, 26, 32)	320
max_pooling2d (MaxPooling2D)	(None, 13, 13, 32)	0
flatten (Flatten)	(None, 5408)	0
dense (Dense)	(None, 100)	540900
dense_1 (Dense)	(None, 10)	1010

Values

ISSN: 2366-1313

```
Sensitivity 95.83333333333334
Specificity 50.0
Precision 95.83333333333334
Recall 95.83333333333334
NPV 0.5
FPR 0.5
FNR 0.041666666666666664
FDR 0.041666666666666664
Accuracy 92.3076923076923
Kappa Coeffient 0.4583333333333339
Jaccard Coeffient 0.92
False Acceptance Rate 50.0
False Rejection Rate 4.166666666666657
F-Measure 0.9583333333333334
```

VI CONCLUSION

In conclusion, the implementation of a finger vein recognition system utilizing Convolutional Neural Networks (CNNs) has demonstrated remarkable efficacy in enhancing security systems across diverse applications. The utilization of machine learning techniques, particularly CNNs, facilitates the extraction of discriminative features from finger vein images, leading to highly accurate and reliable recognition outcomes. CNNs excel in capturing intricate patterns and textures present in finger vein images, enabling precise identification of individuals based on their unique vein structures. Through their hierarchical architecture, CNNs autonomously learn and extract meaningful features directly from the raw image data. This eliminates the need for manual feature extraction, streamlining the recognition process and enhancing efficiency. Moreover, CNNs possess robust feature extraction capabilities, enabling accurate and efficient vein pattern recognition. By learning hierarchical representations of finger vein patterns, CNNs effectively distinguish between individuals, thereby ensuring reliable authentication. Their adaptability to different vein patterns further enhances recognition performance across diverse datasets and environments. Furthermore, CNNs have demonstrated high accuracy in finger vein recognition tasks, outperforming traditional methods and providing superior recognition rates. Their ability to automatically learn discriminative features contributes to improved recognition performance and adaptability to variations in finger vein patterns.

FUTURE ENHANCEMENT

The future of finger vein recognition systems powered by Convolutional Neural Networks (CNNs) holds considerable promise, ripe with opportunities for enhancement. Further refinement of CNN architectures and training methodologies is expected to drive significant improvements in accuracy and robustness. Techniques such as transfer learning and meta-learning could be explored to leverage knowledge from related tasks and adapt models to novel domains, thereby enhancing recognition performance. Moreover, advancements in hardware acceleration and parallel processing architectures could enable real-

time deployment of finger vein recognition systems on resource- 52 constrained devices, opening avenues for applications in mobile and IoT environments. Additionally, the fusion of finger vein recognition with complementary biometric modalities, such as fingerprint or iris recognition, holds potential for enhancing both security and usability in multifactor authentication scenarios. Addressing privacy concerns through techniques such as federated learning and differential privacy will be crucial for fostering user trust and compliance with data protection regulations. Furthermore, efforts to develop interpretable CNN models will provide insights into the decision-making process, enhancing transparency and facilitating trust in the system. As finger vein recognition continues to mature as a biometric modality, interdisciplinary collaborations between researchers, engineers, and practitioners will be essential for driving innovation and unlocking its full potential in diverse applications, from access control and authentication to healthcare and beyond.

VII REFERENCES

1. Finger vein template protection based on alignment-robust feature description and index-of-maximum hashing S Kirchgasser, C Kauba, YL Lai, 2020
2. Towards practical cancelable biometrics for finger vein recognition C Kauba, E Piciucco, E Maiorana, M Gomez-Barrero… - Information …, 2022
3. Finger vein recognition system with template protection based on convolutional neural network H Ren, L Sun, J Guo, C Han, F Wu - Knowledge-based systems, 2021
4. On the recognition performance of biohash-protected finger vein templatesVKrivokuca, S Marcel - Handbook of Vascular Biometrics, 2020
5. Template protection based on chaotic map for finger vein recognition L Shao, H Ren, L Sun, C Han… - IEEJ Transactions on …, 2022
6. A template generation and improvement approach for finger-vein recognition H Qin, P Wang - Information, 2019 vii. W. Yang, S. Wang, J. Hu, G. Zheng, C. Valli, A fingerprint and finger-vein based cancelable multi-biometric system, Pattern Recognition 78 (2018) 242–251.
7. CNN and Genetic Algorithm for Finger Vein Recognition OM Assim, AM Alkababji Finger-vein recognition using a novel enhancement method with convolutional neural network A Bilal, G Sun, S Mazhar, 2021

8. Prasadu Peddi (2015) "A review of the academic achievement of students utilizing large-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.
9. Prasadu Peddi (2015) "A machine learning method intended to predict a student's academic achievement", ISSN: 2366-1313, Vol 1, issue 2, pp:23-37.

AUTHORS

Mr. Audi Reddy Kayithi Assistant Professor Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: adireddyk.cse@gcet.edu.in

Miss. Allu Sai Vineetha, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: 20r11a6206@gcet.edu.in

Mr.Moses Aashray Kyarem, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: 20r11a6234@gcet.edu.in

Mr. D Jagadeshwar Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: 21r15a6205@gcet.edu.in