RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt25410

SCCM: A Novel Hybrid Framework for Dual Biometric Authentication for Identity Enhancement

Saurav Verma [a, *], Ashwini Rao [a], Ketan Shah [a]

[a] Mukesh Patel School of Technology Management & Engineering, SVKM's NMIMS, Mumbai, India

* Corresponding Author Email: saurav.verma@nmims.edu

DOI: https://doi.org/10.54392/irjmt25410

Received: 12-02-2025; Revised: 25-06-2025; Accepted: 10-07-2025; Published: 15-07-2025

Abstract: The increasing need for secure identification has led to advancements in biometric authentication. Traditional single-factor methods, such as passwords or tokens, are vulnerable to cyber threats, necessitating more robust alternatives. This study proposes a Dual Biometric Authentication System (DBAS) based on SCCM (SIFT-CNN-MLP), integrating fingerprint and iris recognition to enhance security, precision, and reliability. The system leverages state-of-the-art machine learning and computer vision techniques, including Multilayer Perceptron (MLP), Convolutional Neural Networks (CNN), and Scale-Invariant Feature Transform (SIFT). MLP and CNN models analyze intricate iris patterns, while SIFT and CNN extract distinguishing features from fingerprint ridge-valley structures. By intelligently combining authentication results from both biometrics, DBAS ensures seamless access for authorized users while effectively blocking imposters. The proposed SCCM framework demonstrates high performance in terms of accuracy. For iris authentication, MLP achieved 97.33% accuracy, while CNN outperformed with 97.92% accuracy. Similarly, for fingerprint authentication, SIFT yielded 91.30% accuracy, whereas CNN excelled with 99.23% accuracy. The SCCM-based DBAS significantly enhances authentication accuracy and robustness compared to traditional methods. It is highly effective for computer logins, mobile security, and critical infrastructure protection, making it a novel, future-proof solution for secure authentication.

Keywords: Dual Biometric Authentication, SCCM Framework (SIFT-CNN-MLP), Machine Learning in Biometrics, Iris and Fingerprint Recognition, Secure Identity Verification.

1. Introduction

Dynamic landscape has made robust and dependable identification solutions increasingly important. Authentication is a revolutionary method that uses physical or behavioral attributes to affirm personal identity. To enhance the security of computer systems, this project seeks to implement Dual Biometric Authentication System incorporating iris and fingerprint recognition to capitalize on their strengths. The system overcomes the limitations of relying on a single meth-od by integrating modalities. This groundbreaking technique involves combining fingerprint and iris recognition algorithms for accuracy, dependability, and access control purposes. Hoping to foster stronger security measures in the computer vision field through machine learning as implemented in authentication modalities such as Apple's iPhone. This decision comes from the specific benefits of using iris and fingerprints as identifiers for this project [1]. The technique records unique patterns for each individual's eye which are stable over time while fingerprinting is one of the most reliable methods used in identity verification processes worldwide. These two combinations aim to strengthen defenses against entry attempts. This study explores how different biometric technologies can work together to fulfill the in-creasing demand for secure authentication methods.

In this research, the Dual biometric authentication combines two separate biometric identifiers, such as iris pattern and fingerprint, using biometric factors that require authentication to provide a robust and secure user interface role, the system significantly reduces the risk of unauthorized access and identity fraud. Today the use of identification with two types of palm prints has become prevalent in new generation gadgets like smart phones and high-security portals and additional options, face and iris recognition in Apple iPhone the integration monitors are introduces that access is allowed only when the two biometric components of the palm prints are also authenticated. This research endeavours in the use of machine learning and computer vision contribute towards the advancement of the biometric authentication solutions which has the potential towards offering high end security solutions.

Biometric authentication is widely used in different security systems as a tool to provide individual's identity by an organism's distinctive characteristics. Previous techniques use one or more biometric modes including finger print or face recognition which have various disadvantages. Multi-biometric systems that combine two separate templates of different modalities are improved in terms of security and recognition because of the limitations of the single modality system. These systems involve executing multiple models of machine learning (ML) to improve the results achieved through diverse "algorithms and features". Multi-modal biometric authentication means where the biometric data of a person are checked using two different modalities. For example, as an option, an approach that integrates fingerprint and facial recognition will be much more secure than separated methods one of which does not work under certain circumstances. This is where multi-model ML techniques found their use as these are the ones that allow the processing of multiple data types, and simultaneously make the process more accurate and reliable [1, 2]. Of the various ML algorithms adopted for use in dual biometric system, the most common is the Multi-Layer Perceptron (MLP). Neural networks are a class of MLPs that are designed to model data with nonlinear relationships. They excel at fusing components from dissimilar biometric modalities that include fingerprints and facial structures. These inputs MLP is able to weigh and correlate hence improving the accuracy and precise nature of identity verification [3]. Due to their capabilities to process big volumes of data and accommodate irregularities in the various biometric parameters, they are an essential factor of the DBS.

Convolutional Neural Networks (CNNs) are one of them; they function well for image-based biometric modalities like facial recognition. CNNs are excellent at extracting hierarchical features from photos, like form, texture, and edges, which improves biometric recognition accuracy. CNNs can identify face pictures in a dual biometric system with an accuracy level that is equivalent to that of professionals [5].It offers enhanced authentications when combined with other models such as the fingerprint analysis model. Another useful method in dual biometric systems is called Scale-Invariant Feature Transform (SIFT). SIFT is applied for finding certain features in the image and for matching them and this algorithm has plenty advantages in cases with the difference in size, rotate and brightness [6]. In the case of dual biometric systems SIFT can enrich the extraction and matching of special features in fingerprint as well as facial images. This capability contributes greatly to the enhancement of the system's ability to perform well in the event of change of certain biometric data, and therefore increases system accuracy [7].

The use of MLP, CNN, and SIFT in dual biometric authentication systems offers multi-model ML techniques to effective prove the idea. All these methods work in harmony with each other since all of them focus on various aspects of biometrical data processing. For managing several kinds of relationships in data, there are MLPs; for improving image identification, there is CNNs; and for effective feature matching, there is SIFT. This means that the synergy produces an entire authentication system that is more secure and accurate than a single modality system [8]. Hence, the multi-model ML methods are essential in enhancing the sophisticated dual biometric authentication frameworks. These systems get the best performances and security by merging a single biometric modality with a number of powerful algorithm strengths. Integration of MLP, CNN and SIFT overcomes the drawbacks of applying a single biometric and serves as a solution for verifying people's identity in the context of modern technologies [9].

2. Literature Review

In response to growing security needs biometric authentication systems have generated significant analysis in recent times. Biometric techniques that include fingerprint and iris recognition belong to the most popular category along with extensive investigation and implementation. The research analyzed two biometric identification methods integrating both fingerprint and iris recognition systems throughout the investigative period. Which needed multiple models and systems. The main methods of detecting irises in published research receive discussions in the subsequent literature section. PCA and LDA represent the main dimensionality reduction methods which operate effectively within biometric recognition systems that focus on iris recognition: Thus PCA functions as an unsupervised technique of focalization at a low business level. LDA operates under supervised conditions because it works to reduce class dispersion while enhancing class discrimination [10]. PCA together with LDA are widely studied dimensionality reduction techniques for feature extraction across various research papers and studies in iris detection.

Multilayer Perceptron (MLP) functions as one type of artificial NN which researchers extensively use for regression and classification activities [11]. The mesh finds its application in identifying irises for recognition purposes. The application of Multilayer Perceptron (MLP) functions as a classifier to translate iris image features toward their classification groups that function as individual identifiers. The MLP operated through connecting various nodes or neurons across each successive layer. A nonlinear activation function is applied to the system after which a weight value is added to all inputs before delivering output to the layer [11]. Training processes modify the weight values only between neurons that are part of two neighboring layers in this network. The preexisting ADAM and gradient descent and stochastic gradient descent optimization methods can fulfill this purpose. During the training process the objective is to minimize the loss function that

measures the average numerical distances between actual ground truth scores and predicted results. The training of MLP occurs for iris recognition through data pairs combined with identity or subject labels (from certain iris image sets) A nonparametric pattern segmentation technique based on K-Nearest Neighbors (KNN) in a feature space operates as a classifier for iris recognition systems [12]. This method proves to be an efficient solution for iris detection which serves as a pattern classification task. The system finds neighbors near test instances across the feature space by considering sets of k neighboring elements and uses them to classify all instances. The KNN algorithm relies on an essential parameter k where the selection of numerical value depends on the most accurate outcome during validation that is achieved either through cross-validation methods or traditional empirical observation. A low value of k results in overfitting and a high value of k produces under fitting because it simplifies the decision boundaries.

Deep neural networks that are particularly adept at learning hierarchical representation from natural input data are known as convolutional neural networks (CNNs). This makes CNNs extremely helpful for deaking image recognition tasks like iris recognition. Several CNN architectures, including the use of pre-trained models like MobileNetV2 and built systems, have been suggested and tested in the field of iris recognition [13, 14]. Regarding model architectures, in addition to using trained models like MobileNetV2, several CNN architectures have been developed and tested specifically for iris detection. By optimising the architecture and utilising optimisation and domain specificity with the information to be used, these CNN architectures have nearly improved iris detection performance and efficiency.

One of the popular method for object recognition and annotation is Scale Invariant Feature Transform (SIFT) algorithm. It is extensively used in various applications of computer vision such as fingerprint recognition and image stitching and object recognition. In fingerprint recognition, the SIFT is used mostly to extract complex and unique features from the fingerprint images. SIFT is very often used to extract annotations and to locate points in fingerprint images [15]. Query fingerprints are compared against those in the database to find the best match and do so by identifying the best match from comparing the query fingerprints' identifiers to those in the database. The current trend of biometric authentication has emerged as a very powerful and truly reliable technique to verify an individual's identity compared to prior techniques such as passwords or PINs. Biometric systems use unique physiological or behavioral characteristics that make security more secure and convenient. But as security threats grow more diverse, there is a growing need for stronger authentication mechanisms. Another approach is in the realm of dual biometric authentication, the use of two overlapping biometrics for a higher security factor. Biometric authentication systems rely critically on feature extraction. It converts raw biometric data into a human identifiable set of features that can be used in identity verification. High accuracy, efficiency, and robustness in biometric system require effective feature extraction techniques. In dual biometric authentication, feature extraction becomes even more important as it must capture and fuse features of at least two biometric sources. As discussed in this research we that proceedings as illustrated as the greatest one.

The complex texture descriptor known as Local Binary Patterns (LBP) is used in a variety of computer vision tasks, such as iris detection, which uses the difference between the central pixel and neighbouring pixels to identify local texture patterns in an image. The LBP function operates by comparing the intensity values of the central and surrounding pixels within a predetermined radius, each of which provides its value in relation to the initial pixel's intensity value; two result numbers activate the local texture model on the portion of this time; LBP codes are computed for each pixel in the image, and a histogram is created to show the frequency of each code.. This histogram can be considered as a feature vector that essentially encodes the texture information found in the iris image [16].

MobileNetV2, an effective method for mobile and embedded devices, is based on the convolutional neural network (CNN) architecture. It's an enhanced version of it with better energy efficiency and performance. MobileNetV2, a potent feature extractor that learns discriminative features in raw iris pictures, offers iris recognition. Depthwise separable convolutions, as in MobileNetV2, split the convolution operation into 2 parts—spatial convolution and pointwise convolution—and the whole computational cost is greatly reduced. It also introduces inverted residual blocks consisting of an expansion layer, followed by a depthwise convolution and a projection layers linearly. In addition, linear bottlenecks between layers are used to further reduce computational requirements, minimizing intermediate representations. In the case of MobileNetV2 applied to iris recognition, the model can be fine-tuned or trained from scratch on iris datasets using pre trained weights over the iris datasets [17]. At present, minutiae-based feature extraction from fingerprint ridge pattern is a common approach for fingerprint recognition, as it tries to find specific points within the fingerprint's ridge pattern, called minutiae. These minutiae points are usually classified into two main types: either ridge endings (where a ridge ends), or ridge bifurcations (where a ridge divides into two). Fingerprint image preprocessing is the initial process of minutiae based feature extraction. The second step of this is to enhance the fingerprint image, then binary it, then thin the ridges to create a skeleton rendered version of the fingerprint. The next step is to minutiae extraction after this prepared skeletonized ridge map. This step

uses algorithms to scan the ridge map and identify their minutiae points, looking for ridge endings and bifurcations as determinate by the combination of grid pixels. Then each minutia is represented with coordinates (x, y) and ridge angle at the minutia. Quality measures and additional information about the minutiae can be added such as whether the minutia is a ridge ending or a bifurcation [18]. Finally, minutiae from the fingerprint to be analyzed are matched against and compared to a minutiae set from the fingerprint stored in the database. The study is based on minutiae spatial relationships and orientations. To match the two fingerprints, we calculate a similarity score using one of various algorithms (such as the Bald Ridge Curve Hough Transform or the minutiae cylinder code). Since such methods can capture highly discriminative and stable features, marrying them to the power of matching performance, minutiae based methods become more popular. However, they are prone to noise, low quality images, and nonlinear distortions and may thus affect the detection and localization of minutiae points with a precise location [19].

The Hough Transform is a well-known and effective feature extraction method, particularly for fingerprint identification. Accurate fingerprint recognition and analysis requires the identification and representation of certain little characteristics in a picture, which is what this is intended to do. This method works particularly well for identifying and characterizing parametric curves in a picture, such as lines, circles, and ellipses. These characteristics are necessary for fingerprint recognition since a fingerprint is made up of intricate ridges and valleys [20-22]. The Hough Transform is typically used for fingerprint recognition on the thinned ridge map of a fingerprint image. Originally, the fingerprint image is thinned ridge map, where the ridges are thinned to one pixel wide lines. This transformation enables the focused analysis of the fingerprint's most important structural features. This ridge map is very good at finding fine details in this ridge map: bifurcations, where a ridge forks into two, and ridges that terminate at or very close to the end. Accurate identification and matching of fingerprints depends on these minutiae [23].

3. Data Acquisition

In terms of data acquisition, biometric authentication systems are of dual type: the first one is collecting biometric information from users, like fingerprint and facial images. This is absolutely critical in order to produce a secure system which accurately identifies individuals. If the collected data is not precise, and contains no errors, then the system is not reliable. In addition, proper secure handling of data during acquisition is paramount in order to protect users sensitive information when acquiring data, data acquisition serves as the beginning step of increased security for computer systems. The main component are explained as:

The CASIA-Iris-Syn, the synthetic dataset which is developed from the Chinese Academy of Science's Institute of Automation (CASIA), is a synthetic iris images data set generated by the mathematical model [24]. The included dataset is 6,000 synthetic images created from 600 iris models, with each model having 10 images that are progressively blurred, noisy and off angling. CASIA-Iris-Syn database aims to provide a very rich, but also diverse, collection of synthetic iris images for developing and evaluating iris recognition algorithms. Few samples images shown in figure1.

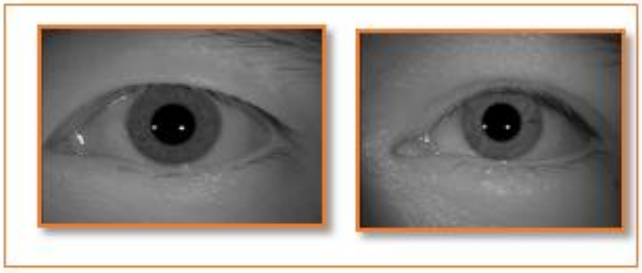

Figure 1. Iris dataset sample images

The CASIA-Iris-Syn dataset has some controlled variations, better privacy protection and scalability. This dataset is generated from such a mathematical model that simulates how iris textures form with such features as generation of mesh, radial and concentric furrows and pigment spot patterns. CASIA-Iris-Syn dataset provides great value for algorithm development, robustness testing, and benchmarking and data augmentation in iris recognition research. We therefore recommend that users of CASIA-IrisV4 use CASIA-Iris-Syn to improve their iris recognition studies [25]. However, it is important to understand that although this dataset gives us some of the insights we desire, it does not necessarily accurately reflect the whole issue of real world iris image challenges. This suggests that evaluation on both synthetic and real world datasets is desired in order to assess algorithm performance comprehensively.

Table 1. Iris dataset Distribution

Attribute	**Description**
Total Number of Images	10,000
Number of Classes	1,000
Images per Class	10
Image Format	PNG
Image Resolution	640 × 480 pixels
Type	Synthetic iris images
Intra-class Variations	Deformation, blurring, rotation

The Sokoto Coventry Fingerprint Dataset (SOCOFing) dataset is a comprehensive collection of fingerprint images intended for academic research purposes. It contains 6,000 fingerprint images sourced from 600 African individuals, with each contributor providing 10 fingerprints. All individuals in the dataset are aged 18 years or older. In addition to the original fingerprint images, the SOCOFing dataset includes distinctive attributes such as gender labels, hand identifiers (left or right), and finger names (e.g., index, middle, ring, or little finger).

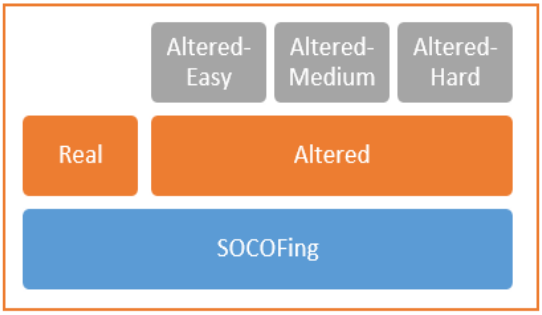

Figure 2. Fingerprint Dataset Categorization

As shown in figure 2, within the SOCOFing dataset, three types of alterations obliteration, central rotation, and z-cut have been applied to the original fingerprints at varying levels: easy, medium, and hard, utilizing corresponding parameter settings within the STRANGE toolbox. The altered fingerprint images within the SOCOFing dataset have been derived from the original images with a resolution of 500 dpi. The dataset comprises a total of 17,934 altered images with easy parameter settings, 17,067 with medium settings, and 14,272 with hard settings [26-31]. It's worth noting that in some instances, certain images did not meet the criteria for alteration with specific settings using the STRANGE toolbox, leading to an uneven distribution of altered images across the three alteration categories.

By offering both original and synthetically altered fingerprint images alongside gender, hand, and finger name labels, the SOCOFing dataset serves as a valuable asset develop and assess fingerprint recognition algorithms, particularly regarding their resilience to various types of distortions, alterations, and degradations. The sample of one person having four fingerprints captured is shown in figure 3.

Figure 3. Sample images of right hand 4 fingerprints of same person

4. Methodology

In proposed framework, the Iris and Fingerprint Authentication System represents sophisticated approach to biometric security by combining two distinct modalities: It emphasizes the fields of iris recognition and fingerprint analysis. Iris recognition uses the characteristics patterns in the iris making it accurate and resistant of external changes while fingerprint analysis examines the unique ridge patterns in the fingers. The integration of these two biometric methods meanwhile improves security through a layered verification. In addition to both approaches enhancing identity validation, the dual approach bridges the gap of relying on single biometric modality as a solution to secure access control. Flow of methodology is shown in figure. 4 and figure 5 shows the flowchart of iris fingerprint recognition algorithms. The following figure no. 4 also shows the decision points to authenticate users based on accurately verified iris and fingerprint biometrics.

Table 2. Fingerprint Dataset Distribution

Category	Description	Count of Images
Original Fingerprints	Fingerprint images from 600 African subjects (10 fingerprints per subject)	6,000
Synthetically Altered Fingerprints - Easy Settings	Fingerprint images with easy-level alterations (obliteration, central rotation, z-cut)	17,934
Synthetically Altered Fingerprints - Medium Settings	Fingerprint images with medium-level alterations (obliteration, central rotation, z-cut)	17,067
Synthetically Altered Fingerprints - Hard Settings	Fingerprint images with hard-level alterations (obliteration, central rotation, z-cut)	14,272
Total Fingerprint Images	**Original fingerprints and Synthetically altered fingerprints**	**61,273**

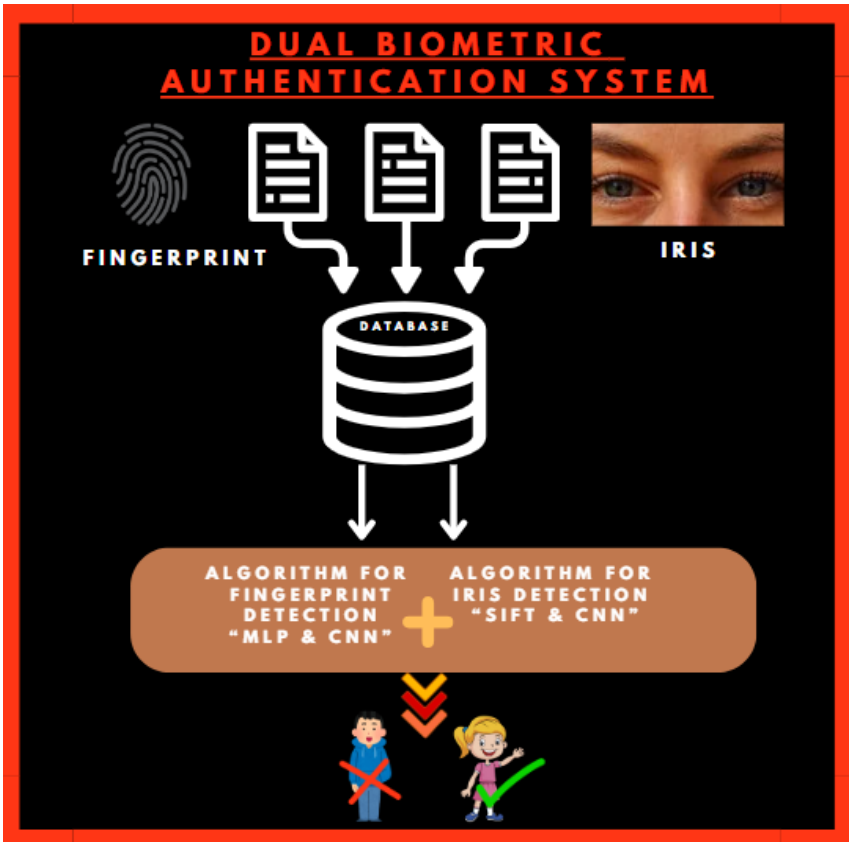

Figure 4. Methodology Flow

This broad trend highlights how many algorithms and modalities have been integrated to achieve strong and secure user authentication. This study digs into the analysis of a flow diagram shown in figure 4 for an iris and fingerprint identification system. The system verifies user identity using image processing techniques and machine learning algorithms. This study goes down each flowchart component, demonstrating how it fits into the overall authentication process. The system runs two independent but concurrent workflows: one for iris authentication and another for fingerprint authentication. Both processes share common processing stages until the feature extraction stage, at which point distinct approaches are used for each biometric modality. Figure 4, depicts the whole study technique, including a step-by-step procedure for both fingerprint and Irish detection, with the findings of both methods being combined for authentication. The following is a discussion of each step's explanation.

A) Image Acquisition: The process begins with picture acquisition. This entails taking digital photographs of both irises and fingerprints. This is often accomplished through the use of specialized hardware, such as iris scanners and fingerprint scanners. The collected images are used as raw data for the subsequent image processing and feature extraction steps.

B) Preprocessing: Preprocessing is the enhancement in quality of iris and fingerprint images so as to ready them for effective feature extraction as shown in figure.6. This involves greyscaling, normalizing, noise reduction, segmenting, edgding. The result of these techniques is simplification of the data, noise reduction, and consistency which improve the effectiveness of downstream analysis, and the performance of the model. After the Iris and fingerprint settings were acquired preprocessing is done with those images. The aim of this step is to increase quality of the image and to be ready for feature extraction. These preprocessing techniques consist of a number of important operations.

First to deal with the data is a grayscale conversion shown in figure.7 which simplifies the data, converting the RGB (Red, Green, Blue) images to grayscale thus reducing the computational complexity of the data when being processed. Without this next step, the image data would be more complex making the analysis more complicated. First, normalization changes the intensity levels of image pixels to the set range that is commonly between 0 and 1. This helps to have a uniform image, that is, all images have a common intensity scale. This facilitate the extraction of meaningful features where all images have a common intensity scale. Another preprocessing is important noise reduction, which is often carried out employing Gaussian blur.

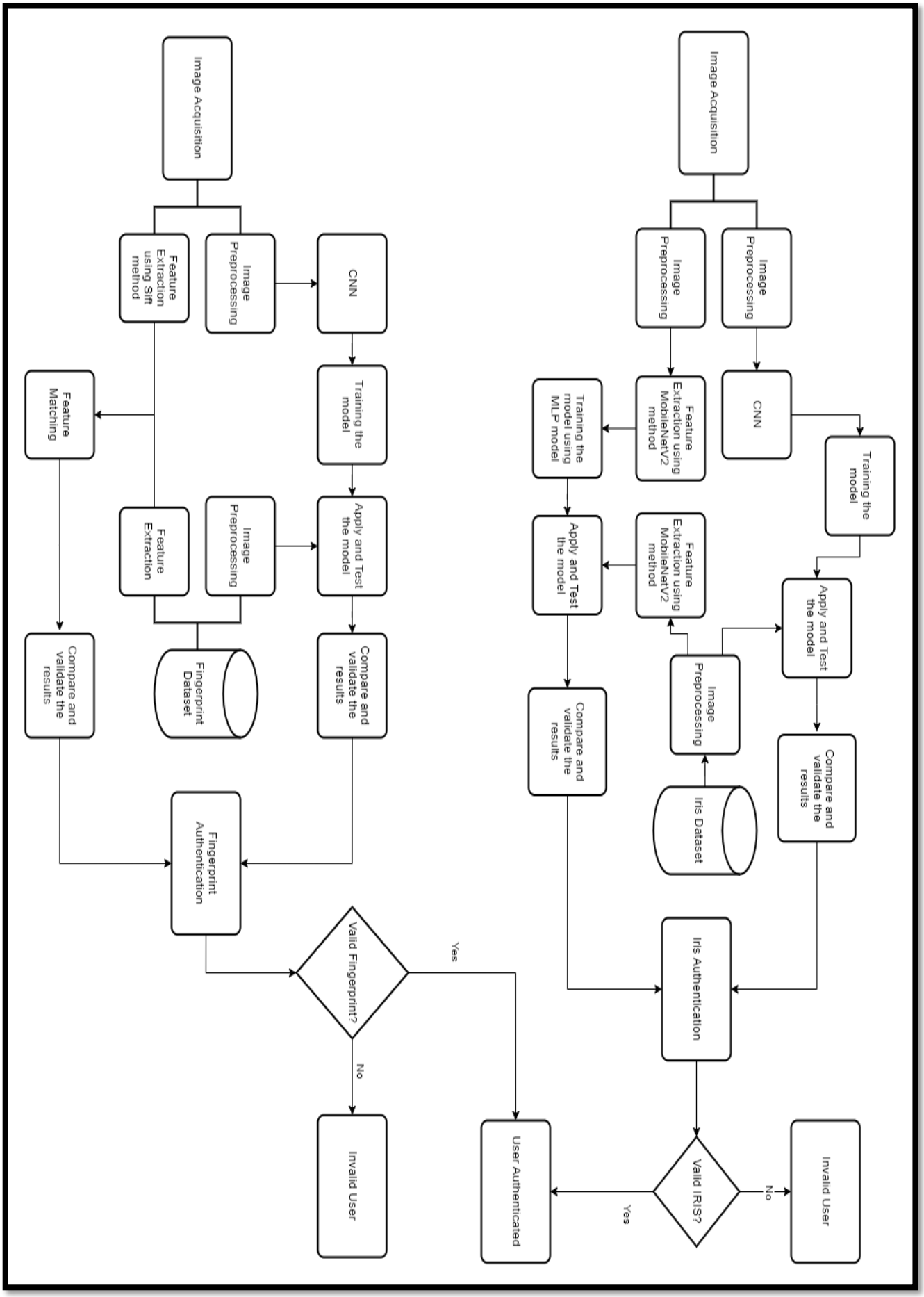

Figure 5. Iris and Fingerprint Authentication System

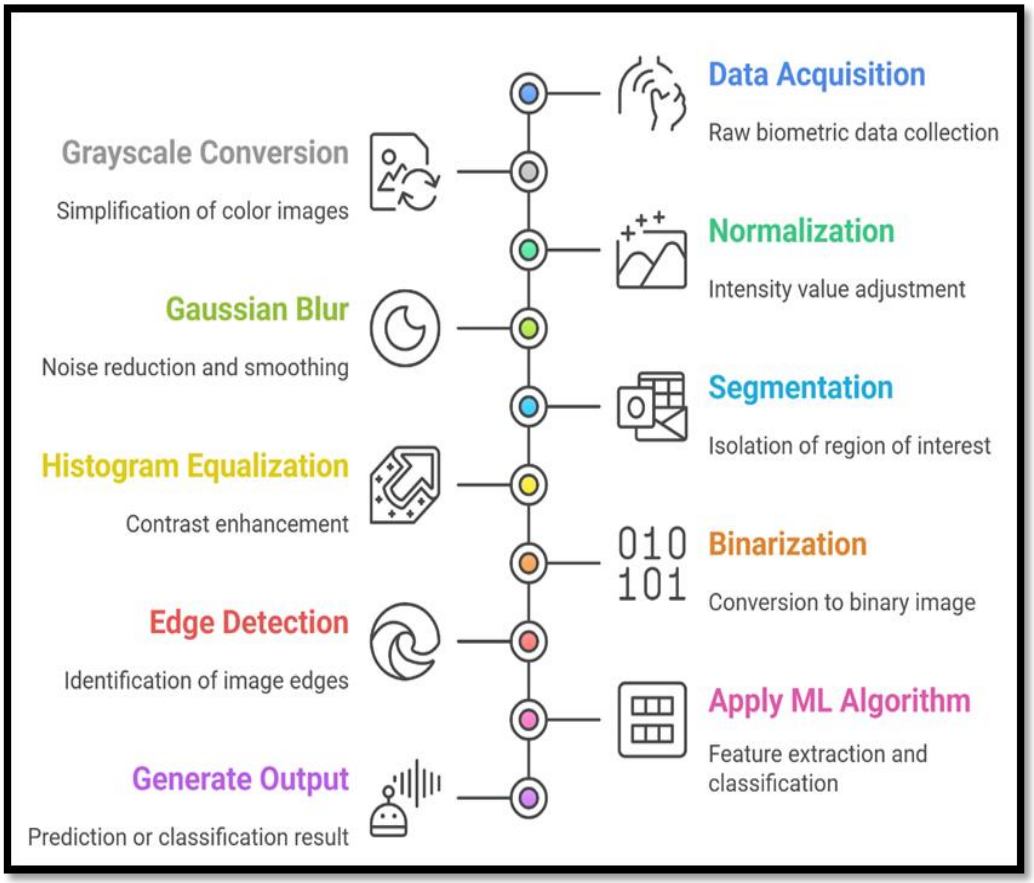

Figure 6. Various Preprocessing Steps

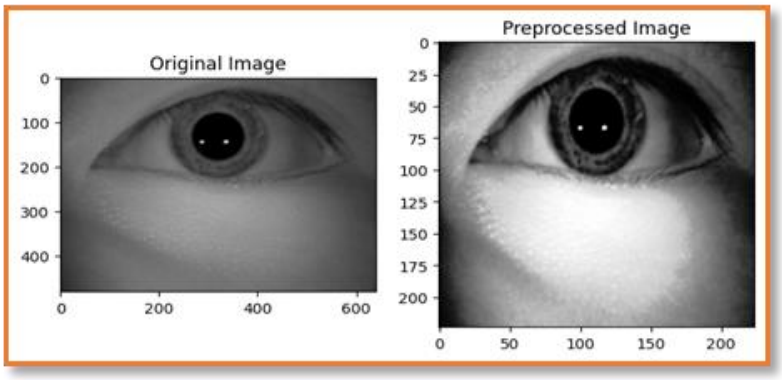

Figure 7. Sample images (Original image and Preprocessed image)

This technique reduces noise present at acquisition due to imaging or sensor imperfection, effectively smoothing out the image and reducing the likelihood of false features during subsequent analysis via convolution of image with a Gaussian kernel.

In this, segmentation is applied for isolation of particular regions of interest throughout an image. For example, in iris images, the iris is segmented from the rest of the image: sclera and eyelids. The process involves dividing the image into meaningful sections through segmentation, and the nature of the image and what we want to achieve out of it determines which segmentation algorithm we choose, edge detection, region growing or model-based segmentation.

Binarization, or simple thresholding, is another technique that converts grayscale images into binary format based on a fixed threshold, simplifying the image and making it easier to identify and extract relevant features. Here, Edge detection, particularly using the Canny algorithm, is a technique used to identify edges within an image by detecting local intensity gradients. This method is especially useful in fingerprint analysis, where edge detection helps in identifying the ridges and valleys that form the unique patterns used for identification. Morphological operations, such as erosion, dilation, opening, and closing, are used to manipulate the shapes and structures within an image. These operations are essential for tasks like noise removal, where unwanted small objects are removed,

and segmentation, where specific structures are enhanced.

To simplify the images and reduce the number of features amenable to identification, another technique is binarization (or simple thresholding), which converts grayscale images the binary way by simply applying a fixed threshold. In this case, we consider the use of Edge detection, in particular the use of the Canny algorithm to identify edges within an image by detecting local intensity gradients. In fingerprint analysis, however, edge detection in combination with this method is particularly useful because it allows the ridges and valleys that make up fingerprint patterns to be identified. Manipulating the shapes and structures within an image is done by using these morphological operations, namely erosion, dilation, opening or closing. For tasks such as noise removal, which needs to remove unwanted small objects, and segmentation, which is needed to enhance specific structures, these are essential operations.

Finally, we apply data augmentation in order to artificially augment the dataset with varieties of the same original data samples. But the wider utility of this technique comes from the fact that it helps expose models to new input data variances (which are often unseen), with the result being improved robustness and generalization performance. In the dataset, the image rotation rotates the image by a certain angle around its center, however, through this data augmentation models are better able to handle real world scenarios where the input data may be quite different from the training data in the given dataset. Rotation angles can be small angles (e.g. ±15°, ±30°), larger angles (e.g., ±45°, ±90°). Horizontal flipping, is mirroring the image with respect to the vertical axis; Vertical flipping, is mirroring the image with respect to the horizontal axis; Scaling, means resizing the image to larger or smaller size and cropping, is selecting a region of interest in the image. In order to adjust the brightness and contrast of images, intensity values must be adjusted on pixels. Varying between bright and contrast levels at random makes the model more resilient to variation in lighting conditions and makes it perform well in all scenarios.

C) Feature Extraction: The preprocessing is done on the iris image and it goes to the feature extraction phase. The first basic step takes a preprocessed image and extracts key, distinctive and familiar features. To extract features from this iris, the system uses a special technique called MobileNetV2. MobileNetV2 relatively small model size, this convolutional neural network (CNN) architecture is well known for its efficiency in extracting features from images to extract high-quality features. MobileNetV2 uses convolution ally pre-processed iris images in successive layers. These exceptions reflect the unique properties of the iris such as detailed shapes and textures Feature Extraction – Fingerprint Authentication. A new feature extraction technique called SIFT (Scale-Invariant Feature Transform) is used for fingerprint images. By using SIFT technique, the main details of the fingerprint image that are least affected by changes in illumination, rotation, and scale are extracted Unique fingerprint sample features such as bifurcations and ridge ends form these keypoints. Each keypoint is given a descriptor vector by the SIFT method, which captures the local fingerprint characteristics around that point.

D) Model Training and Testing: The extracted iris segments are then used to train machine learning. This system uses a multilayer perceptron (MLP). Multi-layer perceptron (MLP) feed-forward artificial neural network topology is suitable for classification problems. This system is composed of an input layer, one or more hidden layers of networked neurons, and an output layer. The MLP receives labeled iris datasets during training. The data set consists of the labels (such as individual user IDs) of the pre-processed iris image. MLP acquires knowledge by mapping the retrieved attributes to relevant users. After training, the system uses independent iris data to evaluate the efficiency of the learned MLP model. This data set includes the user labels of the pre-processed track images just like the training set. When presented with these unseen iris images, the model attempts to classify them using features taught in training. In Performance evaluation, the user ID predicted by the model is compared to the actual characters in the system test dataset. Quantitative measures such as recall, precision, and accuracy are calculated to assess the ability of the model to generalize to unknown inputs.

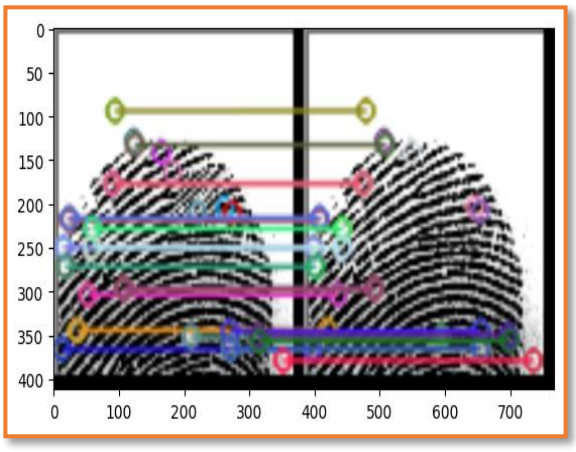

Figure 8. Sample image of key point descriptors matching using SIFT

Based on performance analysis and classification results, the system issues a message indicating the certification status of the iris. The system displays a "Valid IRIS" message, indicating that the user is successful, if for example it correctly segments the iris feature and matches a known user in the training data.

Conversely, if the model could not reliably classify the iris objects or find a match in the training data, the system will display the message "Invalid User", which means that they have failed.

The fingerprint verification performance proceeds with feature extraction using the SIFT method as shown in figure.8, as mentioned earlier, while the iris verification performance is improved by model training and testing. After feature extraction, the fingerprint validation process uses model training to resemble its iris equivalent. Here, a different machine learning model can be used based on the information of the extracted fingerprint features. In Model selection, Support Vector Machines (SVMs) and Convolutional Neural Networks (CNNs), specially developed for fingerprint recognition, are popular choices for fingerprint authentication models Using a labeled fingerprint dataset, with images each associated with a user ID is used to train these algorithms. The model finds a complex relationship between the retrieved fingerprint characteristics and the matching users' identifications during training. Using a different fingerprint dataset, the system checks the performance of the fingerprint recognition model after training. This dataset includes a pre-processed fingerprint image with additional user characters, such as the training set. These unseen fingerprint images are presented to a trained artist, who tries to classify them using the material he learned in training. For Performance evaluation, as with iris validation, the system evaluates model performance using metrics such as accuracy, precision, and recall. This analysis determines how effectively the model generalizes to unseen fingerprint data. After performance analysis, the system issues a message based on classification results for fingerprint authentication. Fingerprint Validation process where the system displays a "fingerprint validation" message, which indicates a successful authentication by the user, for example classifying the fingerprint type correctly and with a known user of the training data in the corresponding. Whereas for Invalid User, conversely, if the model could not reliably classify the fingerprint features or find a match in the training data, the system will display the message "Invalid User", indicating failure. The entire novel process in shown in Figure.4 for the iris fingerprint authentication system illustrates how graphics and machine learning can be used to create a robust and secure user authentication system. The approach improves security and reduces the potential for errors associated with the use of a single biometric identifier by combining two different biometric strategies.

E) Hardware Resource: High performance GPU powered desktop system was used to carry on in this research. There were 2 nodes namely Dell PowerEdge R760 Server Master Node, Dell PowerEdge R760XA Server GPU Node. Master node had configure as 2* Intel Xeon Gold 5420+, Cores=28, 2.00 GHz, Memory= 256 GB, SSD = 480GB x 2, SSD = 7.68TB x 5 and other compute node had configure as 2 * Intel Xeon Gold 6438Y+, Core = 32, 2.00 GHz, Memory = 512GB, DDR5 4800MT/s, SSD = 1.92TB x 2.

6. Experiential Result and Analysis

The result and analysis section focuses on evaluating the effectiveness of the dual biometric authentication system. This is a check to see how well the system works for user's identification and how well it prevents unauthorized access. Through the analysis of the system's performance metrics including accuracy, false acceptance rate, and false rejection rate it can find the reliability and robustness of the system. Finally, this section discusses both implementation challenges encountered and possible improvements to increase system security and efficiency. This research results with all implemented methods summarized in Table 3.

Results of the study show performance of different methods used for iris and fingerprint authentication as well as the difference between the accuarcy afforded by traditional machine learning methods and advanced deep learning approaches. Several techniques were evaluated for Iris Authentication. For feature extraction, Local Binary Patterns (LBP) have been used with an SVM classifier in PCA with an accuracy of 85.17% Although effective, however, it failed to completely capture the fine details required for highly accurate iris recognition. In PCA with KNN classifier, the LBP features performed slightly better than was probable in PCA with a KNN classifier using LBP features: accuracy of 88.50%. We found that an accuracy of 86.50% was improved further with LDA (Linear Discriminant Analysis) with SVM classifier, which implies that LDA may give a more discriminative feature space for SVM, though there is still room for improvement. LDA with KNN classifier achieved an accuracy of 88.42%, nearly matching PCA-KNN, but the difference was marginal, emphasizing that both PCA and LDA provide similar effectiveness when paired with KNN. A Multi-Layer Perceptron (MLP), utilizing MobileNetV2 for feature extraction, significantly outperformed the above methods with an accuracy of 97.33%.

This result highlights the power of combining neural networks for both feature extraction and classification, allowing the model to capture more complex patterns within the iris data. The best performance came from a Convolutional Neural Network (CNN), which achieved the highest accuracy of 97.92% as shown in figure.9. CNNs design their own spatial hierarchies of features, and this indicates that CNNs, especially for iris recognition tasks, are very good at it.

Results of fingerprint authentication using different machine learning techniques show considerable variation in performance for Fingerprint Authentication.

Table 3. Accuracies obtained using different methods for iris and fingerprint authentication

Authentication	Method	Accuracy
Iris	PCA with SVM classifier (LBP feature extraction)	85.17%
	PCA with KNN classifier (LBP feature extraction)	88.50%
	LDA with SVM classifier (LBP feature extraction)	86.50%
	LDA with KNN classifier (LBP feature extraction)	88.42%
	MLP (MobileNetV2 feature Extraction)	97.33%
	Convolutional Neural Network (CNN)	97.92%
Fingerprint	SIFT (Altered - Easy)	91.22%
	CNN (3 layers model with batch normalization)	99.23%
	K-Nearest Neighbors (KNN)	87.32%
	Support Vector Machine (SVM)	90.22%
	Random Forest Classifier	89.56%
	Gradient Boosting Machines	88.68%

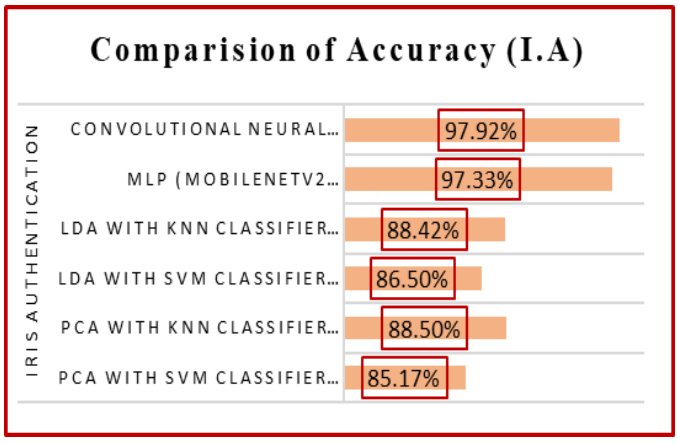

Figure 9. Results of Fingerprint Authentication Methods

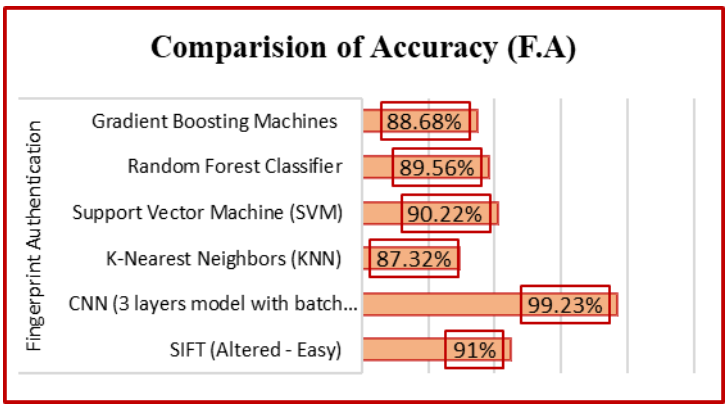

Figure 10. Results of Iris Authentication Methods

Under changed easy conditions, the SIFT (Scale Invariant Feature Transform) method, which was used, showed an accuracy of 91%, however, strong performance in feature extraction and matching. But the Convolutional Neural Network with three layers and batch normalization performed much better than anything else, with an accuracy of 99.23% as shown in figure10. It illustrates CNN's capability of extracting fine details and hot patterns, thereby proving to be the most capable method of fingerprint authentication, in this study. However, in comparison, traditional machine learning methods showed moderate performance.

While not to be counted out, the KNN algorithm yielded an accuracy of 87.32% which is far short of the sophisticated techniques. As in SVM classifier, Accuracies of 90.22% was obtained by Support Vector Machine (SVM) in differentiating fingerprint patterns but not up to those of deep learning methods. For the Random Forest Classifier, result got 89.56% accuracy and for Gradient Boosting Machines (GBM) result got 88.68% accuracy which is poor compared to other models. Therefore, the deep learning based CNN model outperform traditional method significantly for the fingerprint authentication task, and other machine learning methods produce respectable, but less accuracy results. Below section discusses the explanation of each technique as 'A' , 'B' and 'C'.

6.1 Iris Authentication

6.1.1 PCA with SVM classifier (LBP feature extraction)

To extract texture, LBP feature extraction technique was used on iris images. Then, principle component analysis (PCA) was applied that reduced the dimensionality of the iris feature vector and classified it as a Support Vector Machine (SVM) that helped to separate the iris shapes into different groups. This method achieves an accuracy rate of 85.17%, as indicated in Table 3. The general LBP operator can be defined as:

$$LBP_{np,R}(x,y) = \sum_{p=0}^{np-1} s(g_p - g) * 2^{np} \quad (1)$$

Where, (x, y) is the coordinates of the center pixel. "g" is the intensity value of the center pixel. "g_p" is the intensity value of the neighboring pixels. "s" is the sign function that returns 1 if its argument is non-negative and 0 otherwise. "np" is the number of neighboring pixels considered. "R" is the radius of the circularly symmetric neighborhood. The mathematical steps involved in PCA include:

a) Computing the covariance matrix of the data.

b) Calculating the eigenvectors and eigenvalues of the covariance matrix.

c) Selecting the top k eigenvectors corresponding to the largest eigenvalues to form the projection matrix.

d) Projecting the original data onto the new subspace formed by the selected eigenvectors.

The SVM mathematical formulation involves finding the optimal hyperplane by solving the following optimization problem:

$$min_{w,b} \frac{1}{2} ||w||^2 + C \sum_{i=1}^{N} \xi i \quad (2)$$

Where, "w" is the weight vector, "b" is the bias term, "ξi" are slack variables and "C" is the regularization parameter. Moderate precision indicates limitations in distinguishing between iris shapes using traditional methods.

6.1.2 PCA with KNN Classifier (LBP Feature Extraction)

The feature extraction technique of local binary patterns (LBP) was used to extract texture features from the iris images. Then, the classifier is reduced by principle component analysis (PCA) reducing the dimensionality of the iris feature vector as K-Nearest Neighbors (KNN) which assigns labels to iris feature vectors based on similarity. This method achieves an accuracy rate of 88.50%, as indicated in Table 3. The same approach, which was used for the LBP and PCA in previous method was used here too and the steps involved in KNN classification are as follows:

a) Compute the distance between the query sample and all samples in the training set.

b) Select the top 'k' samples closest to the query sample.

c) Assign the class label by majority voting among the "k" neighbors.

There is a slight improvement in accuracy compared to SVM, indicating that iris shapes are well clustered in the feature space.

6.1.3 LDA with SVM Classifier (LBP Feature Extraction)

The feature extraction technique of local binary patterns (LBP) was used to extract texture features from the iris images. Then, linear discriminant analysis (LDA) maximizing class separation in the iris feature space was applied. The SVM classifier defines decision boundaries between iris classes. This method achieves an accuracy rate of 86.50%, as indicated in Table 3. The same approach, which was used for the LBP and SVM in previous method was used here too and the steps involved in LDA include:

a) Computing the mean vectors for each class.

b) Computing the scatter matrices (within-class and between-class scatter matrices).

c) Finding the eigenvectors and eigenvalues of the generalized eigenvalue problem.

d) Selecting the top k eigenvectors corresponding to the largest eigenvalues to form the projection matrix.

e) Projecting the original data onto the new subspace formed by the selected eigenvectors.

A comparison of the accuracy of PCA-based methods, showing similar effectiveness in iris pattern recognition.

6.1.4 LDA with KNN Classifier (LBP Feature Extraction)

The feature extraction technique of local binary patterns (LBP) was used to extract texture features from the iris images. Then, linear discriminant analysis (LDA) maximizing class separation in the iris feature space was applied. The KNN classifier assigns labels based on proximity to the reduced feature space. This method achieves an accuracy rate of 88.42%, as indicated in Table 3. The same approach for LBP, KNN and LDA used in previous methods are used over here and performed the method. The similar performance of PCA and KNN classifier, shows the robustness of LDA in iris validation.

6.1.5 MLP (MobileNetV2 Feature Extraction)

Method Description: Here in Multilayer Perceptron (MLP) learning complex iris patterns by features extracted by feature extraction method, MobileNetV2 feature extraction method is used as it extracts high level features from iris image, enabling accurate classification. This method achieves an accuracy rate of 97.33%, as indicated in Table 3.

The steps for MobileNetV2 Feature Extraction [15], "I" represent an input iris image, F(I) represent the extracted features from the MobileNetV2 network. Mathematically, the feature extraction process can be represented as:

$$\mathrm{F(I)} = \mathrm{MobileNetV2(I)} \quad (3)$$

Where, MobileNetV2(I) denotes the output of the MobileNetV2 network when fed with the input iris image "I". Multilayer Perceptron (MLP) for Learning Complex Patterns [16]. Let, x represent the extracted features from MobileNetV2, "W" represent the weight matrix of the MLP, "b" represent the bias vector of the MLP, "σ(·)" represent the activation function, typically a nonlinear function like the sigmoid or ReLU. The output of the MLP can be computed as follows:

$$z = \sigma(W \cdot x + b) \quad (4)$$

where, "z" represents the output of the MLP, "W·x" represents the dot product between the weight matrix, "W" and the input features "x", "+b" represents the addition of the bias vector, "σ (·)" is the activation function applied element-wise. The significant improvement in accuracy compared to traditional methods highlights the effectiveness of deep learning in iris validation.

6.1.6 Convolutional Neural Network

Convolutional Neural Network (CNN) learns a sequence of iris images. Its framework includes convolutional, pooling, and fully integrated layers for feature extraction and classification as shown in figure 11. This method achieves an accuracy rate of 97.92%, as indicated in Table 3. The highest accuracy was obtained among all the methods, indicating the highest capability of CNNs in capturing complex iris shapes.

6.2 Fingerprint Authentication

6.2.1 SIFT (Altered-Easy)

Scale-Invariant Feature Transform (SIFT) extracts distinctive features from fingerprint images invariant to scale and rotation. This method achieves an accuracy rate of 91.30% as indicated in Table 3. Steps involved in performing SIFT [17]:

Scale-Space Extrema Detection where Construct a scale-space representation of the input fingerprint image by convolving it with Gaussian kernels at different scales. Compute the Difference of Gaussians (DoG).

$$DoG(x, y, \sigma) = \big(G(x, y, k\sigma) - G(x, y, \sigma)\big) \quad (5)$$

Where, $G(x, y, \sigma)$ is the Gaussian-blurred image at scale σ, and k is the scale factor. Detect local extrema in the DoG pyramid to identify potential keypoints.

Keypoint Localization which refine the locations of keypoints by fitting a 3D quadratic function to the nearby samples in the scale-space pyramid. Orientation Assignment helps to assign a dominant orientation to each keypoint based on the local image gradient directions. Accumulate gradient orientations into histograms weighted by the gradient magnitude. Select the peak in the histogram as the dominant orientation of the keypoint. The extract a descriptor for each keypoint that captures its local appearance. Exceptional accuracy indicates robustness of SIFT in capturing unique fingerprint characteristics, making it a promising method for fingerprint authentication.

6.2.2 CNN (3 layers' model with batch normalization)

CNN model learns the hierarchical representation of the fingerprint images, the architecture with batch normalization normalizes the layer inputs, accelerates the convergence of the model. This method achieves an accuracy rate of 99.23% as indicated in Table 3. The impressive accuracy demonstrates the effectiveness of batch normalization in improving CNN performance for fingerprint verification.

6.3 Overall Analysis

In figure 12 & 13, analysis of Iris and fingerprint verification presented respectively, where all iris verification methods outperformed the fingerprint verification method, with deep learning-based structure achieving the best accuracy of both methods. In particular, fingerprint authentication using older methods was inferior to iris, highlighting the limitations associated with fingerprint recognition.

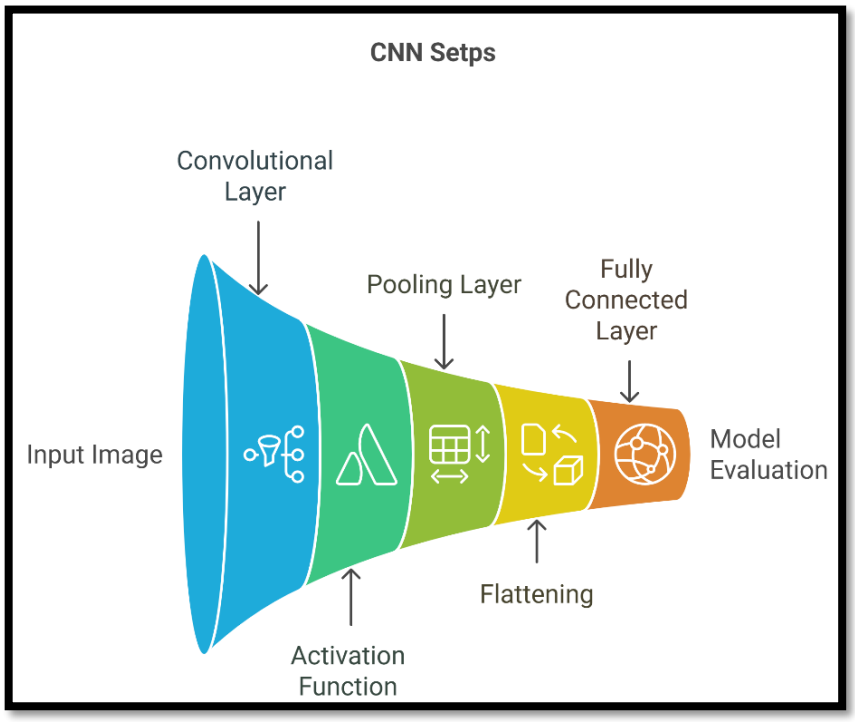

Figure 11. Steps in CNN

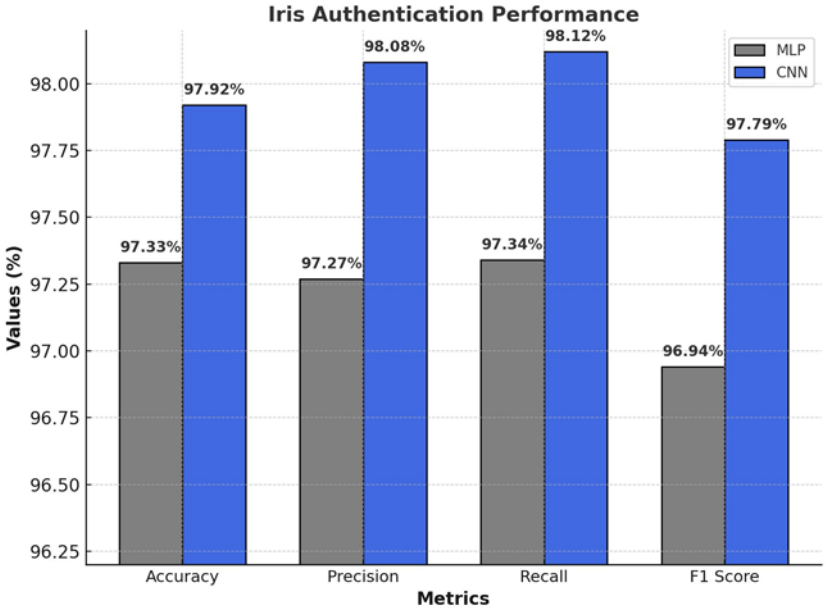

Figure 12. Graph showing different metric values incurred with both methods used for iris authentication

Table 4. Iris and fingerprint authentication performance metrics

Method	Accuracy	Precision	Recall	F1 Score
For Iris Authentication:				
MLP	97.33%	97.27%	97.34%	96.94%
CNN	97.92%	98.08%	98.12%	97.79%
For Fingerprint Authentication:				
SIFT	91.30%	91.17%	91.26%	91.08%
CNN	99.23%	99.33%	99.23%	99.22%

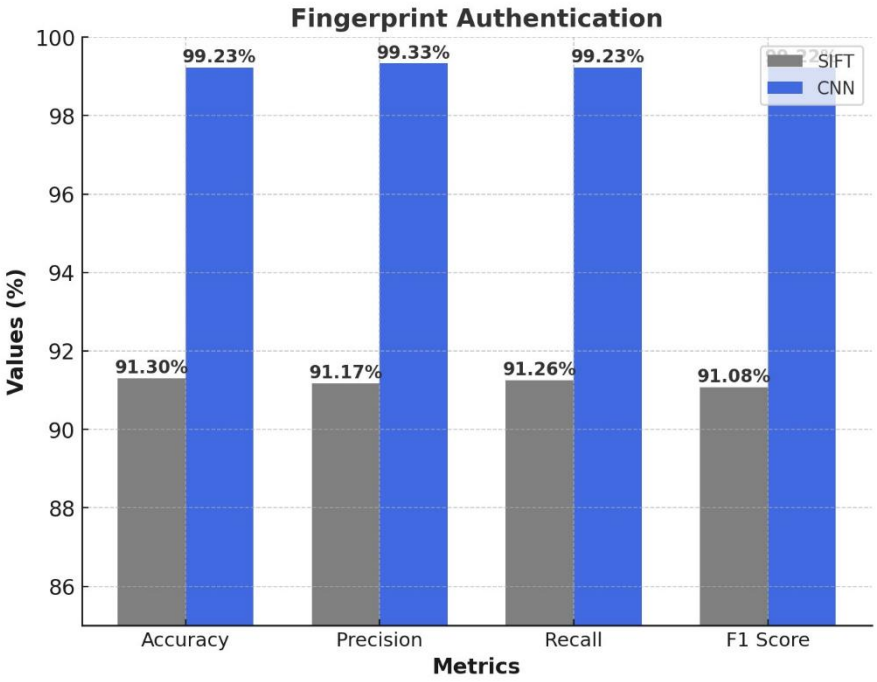

Figure 13. Graph showing different metric values incurred with both methods used for fingerprint authentication

Effective deep learning: Deep learning techniques, especially CNN images, have proven to be highly effective for iris and fingerprint verification, demonstrating the ability to understand patterns and details for accurate recognition. With respect to Challenges and Opportunities, traditional methods such as PCA and SVM failed, especially in fingerprint recognition, highlighting the need for advanced methods. SIFT and CNN with batch normalization have emerged as promising fingerprint authentication algorithms, with high accuracy rates and real-world applications.

The above table 4 mentions the performance metrics of iris and fingerprint verification using different methods. The results for iris and fingerprint authentication reveal the effectiveness of various machine learning models, evaluated through accuracy, precision, recall, and F1 score metrics. In iris. In iris authentication, MLP (Multilayer Perceptron), achieved an accuracy of 97.33%, with a precision of 97.27%, a recall of 97.34%, and an F1 score of 96.94%. This suggests that the MLP model is highly effective in correctly classifying iris patterns, with balanced precision (ability to avoid false positives) and recall (ability to identify true positives). The slightly lower F1 score indicates a minor trade-off between precision and recall but still shows excellent performance overall. Also, CNN (Convolutional Neural Network), outperformed the MLP with an accuracy of 97.92%, a precision of 98.08%, a recall of 98.12%, and an F1 score of 97.79%.

These results demonstrate that the CNN model is superior in iris authentication tasks, delivering even higher accuracy and more balanced precision and recall. The high F1 score reflects its robustness in both predicting positive classes and reducing false predictions. Where as in fingerprint authentication, SIFT (Scale-Invariant Feature Transform): This traditional feature extraction method for fingerprint authentication achieved an accuracy of 91.30%, with a precision of 91.17%, a recall of 91.26%, and an F1 score of 91.08%. The SIFT method provides solid performance in fingerprint recognition, showing a well-balanced ability to correctly identify and match fingerprint features, though not as effective as modern deep learning methods. Using CNN, this deep learning method excelled in fingerprint authentication, with an outstanding accuracy of 99.23%, a precision of 99.33%, a recall of 99.23%, and an F1 score of 99.22%. These metrics indicate near-perfect performance, with the model highly successful in both identifying true positives and minimizing false positives, making CNN the most effective technique for fingerprint authentication in this study.

7. Conclusion

The use of iris and fingerprint recognition techniques has been assisted by this extensive research into the development along with evaluation of two biometric identification systems. A novel approach responds to the growing need for reliable and robust detection solutions in the dynamic security environment of today. In this research, dual biometric authentication systems provide greater accuracy, reliability and security by combining iris and fingerprints as opposed to single methods of authentication. This research shows that the fusion of these two biometric identifiers significantly improves access control by reducing the threat associated with traditional identification methods such as password or token-based techniques so well.

Research confirms that iris authentication is superior to fingerprint by adopting deep learning algorithms for accurate and reliable biometric authentication The success of these two biometric authentication algorithms in various applications such as electronic access, mobile device security, and in critical infrastructure security It demonstrates its potential as a future-proof solution to meet the growing demand for personalized airtight certification. Future research should refine and improve deep learning models for iris fingerprint recognition, and also test the possibility of blending other biometrics to improve security and performance. To improve security awareness technology in a highly connected world, new ways for embracing biometrics have to be developed. Dual biometric systems may be further improved by developments in AI and machine learning, which would increase their adaptability, scalability, and defence against spoofing attempts. This technology has the potential to be extremely important in fields like border control, finance, and safe access to private data.

References

[1] K. Sasikumar, S. Nagarajan, Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques. IEEE Open Journal of the Computer Society, 6, (2025) 392 – 402. https://doi.org/10.1109/OJCS.2025.3538557

[2] A.K. Gangly, S. Bhattacharya, S. Chattopadhyay, (2024) A Design of Efficient Biometric based Banking System Through AI-Powered Transaction Security Fintech System for Secure Transactions. 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India. https://doi.org/10.1109/ICACITE60783.2024.10617391

[3] Z. Chai, L. Zhang, X. Huang, M. Li, X. Yang, Integration of device fingerprint authentication and physical-layer secret key generation. IEEE Signal Processing Letters, 30, (2023) 1257–1261. https://doi.org/10.1109/LSP.2023.3313004

[4] S. Li, M. Cheng, Y. Cheng, C. Fan, L. Deng, M. Zhang, S. Fu, M. Tang, P.P. Shum, D. Liu, Enhancing the physical layer security of OFDM-PONs with hardware fingerprint authentication: A machine learning approach, Journal of Lightwave Technology, 38(12), (2020) 3238–3245. https://doi.org/10.1109/JLT.2020.2995161

[5] M. Ahsan, M.A. Based, J. Haider, M. Kowalski, An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning. Computers and Electrical Engineering, 95, (2021) 107387. https://doi.org/10.1016/j.compeleceng.2021.107387

[6] H.T. Nguyen, L.T. Nguyen, Fingerprints classification through image analysis and machine learning method. Algorithms, 12(11), (2019) 241. https://doi.org/10.3390/a12110241

[7] PHD TOPIC. (2018) Fingerprint recognition algorithm python programming. https://phdtopic.com/fingerprint-recognition-algorithm-python/

[8] V. Madikonda, (2022). An implementation of fingerprint detection with Python. Spider Research and Development. https://medium.com/spidernitt/an-implementation-of-fingerprint-detection-with-python-f143d20c3a96

[9] M. Gandhi, M. Patel, H. Bhadra, S. Verma, (2024) Automated Detection and Mitigation of Malicious Packages in the PyPI Ecosystem and exe Files: PyGuardEX. First International Conference for Women in Computing (InCoWoCo), Pune, India. https://doi.org/10.1109/InCoWoCo64194.2024.10863220

[10] K. Nguyen, C. Fookes, A. Ross, S. Sridharan, Iris recognition with off-the-shelf CNN features: A deep learning perspective. IEEE Access, 6, (2018) 18848–18855. https://doi.org/10.1109/ACCESS.2018.2825627

[11] M. Oravec, (2014) Feature extraction and classification by machine learning methods for biometric recognition of face and iris. In Proceedings ELMAR-2014, IEEE, Zadar, Croatia. https://doi.org/10.1109/ELMAR.2014.6923301

[12] L. Shuai, L. Yuanning, Z. Xiaodong, H. Guang, C. Jingwei, Z. Qixian, W. Zukang, D. Zhiyi, Statistical cognitive learning and security output protocol for multi-state Iris recognition. IEEE Access, 7, (2019) 132871–132893. https://doi.org/10.1109/ACCESS.2019.2941225

[13] Academic College Projects. (2021) Implementing iris recognition project using Python code development. https://academiccollegeprojects.com/iris-recognition-project-using-python/

[14] R.C. Gonzalez, R.E. Woods, (2018) Digital Image Processing, 4th ed. Pearson, Pearson Education.

[15] A. Sarin, D. Thanawala, S. Verma, C. Prakash, (2020) Implementation of New Approach to Secure IoT Networks with Encryption and Decryption Techniques. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, Kharagpur, India. https://doi.org/10.1109/ICCCNT49239.2020.9225279

[16] I. Goodfellow, Y. Bengio, A. Courville, Y. Bengio, (2016) Deep Learning. MIT Press.

[17] A. Khraisat, O. Alsmadi, M. Al-Ayyoub, (2020) Fingerprint matching based on a combination of SIFT and PCA, In Proceedings of the 4th

International Conference Natural Language Processing and Information Retrieval (NLPIR).

[18] Z. Sun, H. Zhang, T. Tan, J. Wang, Iris image classification based on hierarchical visual codebook. IEEE Transactions on pattern analysis and machine intelligence, 36(6), (2014) 1120–1133. https://doi.org/10.1109/TPAMI.2013.200

[19] I. Goel, N.B. Puhan, B. Mandal, Deep convolutional neural network for double-identity fingerprint detection, IEEE Sensors Letters, 4(5), (2020) 1–4. https://doi.org/10.1109/LSENS.2020.2987863

[20] N.V. Tomin, V.G. Kurbatsky, D.N. Sidorov, A.V. Zhukov, Machine learning techniques for power system security assessment. IFAC-Papers Online, 49, (2016) 445–450. https://doi.org/10.1016/j.ifacol.2016.11.131

[21] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, B. Xiao, Deep-learning-based physical-layer secret key generation for FDD systems. IEEE Internet Things Journal, 9(8), (2022) 6081–6094. https://doi.org/10.1109/JIOT.2021.3109272

[22] S. Verma, K. Jain, C. Prakash, (2020) An unstructured to structured data conversion using machine learning algorithm in Internet of Things (IoT). In Proceedings of the International Conference on Innovative Computing & Communications (ICICC). https://dx.doi.org/10.2139/ssrn.3563389

[23] M.T. Kocyigit, L. Sevilla-Lara, T.M. Hospedales, H. Bilen, Unsupervised batch normalization. In 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), IEEE, USA. https://doi.org/10.1109/CVPRW50498.2020.00239

[24] D. Moreira, M. Trokielewicz, A. Czajka, K. Bowyer, P. Flynn, (2019) Performance of humans in iris recognition: The impact of iris condition and annotation-driven verification, In 2019 IEEE Winter Conference on Applications of Computer Vision (WACV), IEEE, USA. https://doi.org/10.1109/WACV.2019.00115

[25] Z. Wang, M. Wang, Compare the security of biometrics. In 2020 International Conference on Computer Engineering and Application (ICCEA), IEEE, Guangzhou, China. https://doi.org/10.1109/ICCEA50009.2020.00031

[26] F. Alonso-Fernandez, R.A. Farrugia, J. Bigun, J. Fierrez, E. Gonzalez-Sosa, A survey of super-resolution in iris biometrics with evaluation of dictionary-learning. IEEE Access, 7, (2019) 6519–6544. https://doi.org/10.1109/ACCESS.2018.2889395

[27] S. Liu, Y.N. Liu, X.D. Zhu, G. Huo, W.T. Liu, J.K. Feng, Iris double recognition based on modified evolutionary neural network. Journal of Electronic Imaging, 26(6), (2017) 063023-063023. https://doi.org/10.1117/1.JEI.26.6.063023

[28] K. Nguyen, C. Fookes, S. Sridharan, M. Tistarelli, M. Nixon, Super-resolution for biometrics: A comprehensive survey, Pattern Recognition, 78, (2018) 23–42. https://doi.org/10.1016/j.patcog.2018.01.002

[29] T. Singh, Design of a dual biometric authentication system. (2016) International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), IEEE, India.

[30] S.P. Singh, S. Tiwari, A dual multimodal biometric authentication system based on WOA-ANN and SSA-DBN techniques, Sci, 5(1), (2023)10. https://doi.org/10.3390/sci5010010

[31] U. Deshmukh, (2024) Fingerprint Feature Extraction. GitHub.

Authors Contribution Statement

Saurav Verma: Conceptualization, Methodology, Software, Writing – Original Draft preparation. Ashwini Rao: Validation, Writing – Reviewing and Editing. Ketan Shah: Supervision, Writing- Reviewing and Editing. All the authors read and approved the final version of the manuscript.

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

The data supporting the findings of this study can be obtained from the corresponding author upon reasonable request.

Has this article screened for similarity?

Yes

About the License