Deep Learning-Based Pattern Recognition Model in Biometrics

Dr.S.L.Jany Shabu[1], Dr.J. Refonaa[2], Dr.M.Maheswari[3], Dr.D.Poornima[4], Dr.Maheshwari A[5],Dr.S. Gayathri[6]

[1, 2, 3,4,6] Sathyabama Institute of Science & Technology, Chennai, India-600119

[5]SRM Institute of Science and Technology, Kattankulathur – 603203.

.

Abstract. In recent years, pattern recognition and biometrics have seen a rise in the use of machine learning and deep learning (DL). Intelligent systems that accurately recognize patterns and biometric data like fingerprints, facial recognition, voice recognition, and more have been developed with the help of machine learning and deep learning approaches. These algorithms can recognize biometric data and patterns that would be extremely challenging, if not impossible, for a human to recognize. The many obstacles faced by researchers in the area of pattern recognition and biometrics, including the difficulty of collecting accurate data, the ambiguity of pattern representation, and the importance of maintaining privacy. In this paper Deep Learning-Based Pattern Recognition Model (DL-PRM) such as convolutional neural networks (CNNs) can be used to identify patterns in biometric data providing accurate, reliable, and efficient solutions. A DL-PRM architecture is designed which is capable of extracting meaningful features from raw biometric data and helps to handle high-dimensional inputs and large-scale datasets. Transfer learning is used to further improve the performance of the DL-PRM and this can be done by reusing the learned parameters of a pre-trained model and fine-tuning it with the current dataset. DL-PRM recognizes patterns in biometric data with high accuracy can be used for a variety of applications, including identification, authentication, and access control. Anomaly detection in biometric data can be accomplished with the help of DL-PRM. Anomalies like fraudulent transactions and malicious actions can be uncovered with the help of the DL-PRM. This can aid in securing biometric infrastructure against intrusion attempts.

Keywords: Pattern Recognition, Biometrics, Deep Learning, Biometric Data, Machine Learning.

1. Introduction

Personal biometric identification has developed into a crucially needed technic, employed in airport terminals, buildings, cellular phones, id cards, and etc, especially to the rise of smart artificial systems and e-technologies [1]. To train robust recognition algorithms, biometrics data is crucial [2]. Face, iris, fingerprints, palm-print, biometric traits, ear, and other physical characteristics, as well as behavioural characteristics like stride, signature, and tone, are all used for positive identification [3]. These features are permanent and can be used to tell one person apart from another [4]. Combining two or more of these features helps boost security, exhibit high performance, and address the shortcomings of single-modal biometric systems [5]. Real-world scenarios show that possession and knowledge-based approaches are largely ineffective since they are vulnerable to theft and forgetfulness [6].

More security can be achieved through the employment of biometric-based recognition methods as opposed to possession- or experience and understanding methods [7]. Hence, biometric human recognition has become increasingly common [8]. Every biometric feature has pros and cons, and it is generally agreed that there is no single biometric feature that can be used in every situation [9]. The purpose of a face detection task is to identify individual human faces within a given image or set of photos [10]. Focusing on a pattern recognition technique that requires biometrics data about people based on their physical and behavioural characteristic, biometric authentication is one of the finest options for information security [11].

The capacity to use several layers to extract higher characteristics the deeper the network is central to the deep learning (DL) paradigm of machine learning algorithms [12]. In contrast to more conventional neural networks, which typically simply consist of an input node, a few hidden layers, and an output unit, deep neural networks contain an input and output layer and many additional hidden layers in between [13]. For the purposes of this research study, its primary application is in Convolutional Neural Networks (CNN) [14], that are employed to extract data from images by applying a series of convolutional filters in a sweeping motion to the input image [15] and then passing the result through a pooling layer to reduce the size of the image before passing it on to the next filter [16].

Several biometric features similarly show negligible variation over time. Because of this, they have found use in a wide variety of fields, including forensic science, security checks, and smartphone authentication [17]. Nonetheless, it may be difficult because of how easily it may be altered by things like expression or getting older [18]. Because of advancements in technology, biometric security is now widely preferred over traditional password-based authentication techniques all around the world [19]. Using machine learning techniques makes sense when trying to identify something among millions of records [20], and deep learning techniques' versatility in identifying data accurately makes them the best option compared to more conventional classification algorithms [21]. In addition, real - time intrusion detection and other machine learning approaches that protect template databases are increasingly making use of machine learning algorithms [22].

The main contribution of this research is given below,

- Pattern recognition in biometric data can be identified using (DL-PRM) such as convolutional neural networks (CNNs) to provide precise, trustworthy, and time-saving answers.
- DL-PRM is a pattern recognition method that may be applied to biometric data for tasks such as identification, authentication, and access control due to its high level of accuracy.
- With DL-PRM, anomalies in biometric data can be identified.

This paper will continue with the following structure: Section 2 provides background study context through a variety of research on pattern recognition in biometrics. Section 3 describes in detail the suggested DL-PRM model for pattern recognition utilizing CNN. Results from the examinations are discussed in Section 4. Section 5 will cover the additional comments and next steps.

2. Related study

Many studies by a wide range of researchers are discussed;

Recently, deep learning-based algorithms (DL-As) were proven to be highly effective, with state-of-the-art results being achieved in a broad range of computer vision, voice recognition, and processing of natural languages tasks by Minaee S, et al. [23]. These models appear tailor-made for tackling the growing complexity of biometric recognition issues, such as those encountered in mobile device identification and security checks. Here described the characteristics of the most popular datasets used in the literature for each biometric, for the development of a number of interesting deep learning solutions to this biometric and demonstrate their effectiveness on widely used public benchmarks.

Compared to traditional unimodal biometrics systems, recognition systems that employ several biometric modalities garner more interest due to their increased efficiency and heightened security. These can be achieved by adding CNNs with deep learning techniques by multimodal biometrics identification system (MmBIS) was described in this paper by Daas S, et al. [24]. Using a deep learning approach using convolutional neural networks, the authors of this study demonstrate a safe multimodal biometrics identification system. According to the findings of the experiments, the proposed fusion structures are 99.89% accurate with a similar error rate of 0.05%. The results show that the deep learning-based biometrics recognition system is trustworthy, dependable, and safe.

In light of rising privacy and safety concerns, biometric human recognition technologies are in high demand. The ear is a very specific and identifying feature of the human body.And though, when there are no limits placed on the photographs, the level of difficulty dramatically increases. The study provides comprehensive information on deep learning techniques (CI-DLt) using databases, evaluation parameters, and current methods. With the release of new datasets here presented a new resource for evaluating unrestrained ear detection as well as recognition by Kamboj A, et al. [25]. To establish a baseline for comparison, they compared this database to six others widely used datasets. Finally, researchers outlined several directions for further research into open questions hoping their study will serve as a starting point for future ear biometrics researchers.

In digital forensics, camera model identification (CMI) refers to the task of pinpointing the camera that captured a suspect image. These aids forensic investigators in connecting a suspect's camera to an unlawful image database or in correctly attributing a questionable image to its proper source. In this paper, authors used a convolutional neural network (CNN) trained with deep learning techniques to determine if a picture has been subjected to a counter-forensic origins anonymization assault and given as CMI-CNN by Sameer V, et. al [26]. Our experiments show that the suggested system has very high detection accuracy and passes the overfitting test.

These days, it's increasingly crucial to be able to accurately identify a speaker. To emphasise, gadgets that depend on voice instructions are especially vulnerable. In this paper, researchers identified at what it would take to develop a voice identification system (IDs) that does not rely on textual cues. A support vector machine (SVM) was developed and evaluated on two data sets to determine how well it can extract Mel-Frequency Cepstral Coefficients (MFCC) by Boles A, et al. [27]. The findings demonstrate the viability of such systems for use in both speaker verification and speaker recognition applications.

Based on the above traditional approaches on pattern recognition in biometrics, MFCC, CMI-CNN, CI-DLt, DL-As, and MmBIS are going to compared with our proposed system DL-PRM. The proposed method aids in the detection of anomalies like fraudulent transactions and harmful behaviours. To better protect biometric infrastructure from unauthorized access, this can be of great help.

3. Proposed System DL-PRM

In this paper, a method for improving the quality of biometric images that is more comparable to human perception by using a convolutional neural network model in conjunction with a proposed method DL-PRM with a convolution operation strategy.Some of these features, however, are challenging to collect, and many algorithms are required for processing and use in security devices. This paper provides a summary of various Machine Learning strategies for identifying individuals by their unique biometric characteristics.

3.1 Process involved in CNN for Pattern Recognition

Image capture and analysis, dimensionality reduction, extraction of features, and classification are the typical processes in the traditional approach to automatically identify, which is additionally utilized for pattern recognition based on biometric features. The recognition system's efficiency therefore relies heavily on the classifier used, which in turn is determined by the feature extraction technique. Finding a classifier that works well in combination with the selected feature extractor to produce optimal classifier is challenging. The overall process of CNN for recognition of patterns are shown in below figure 1.

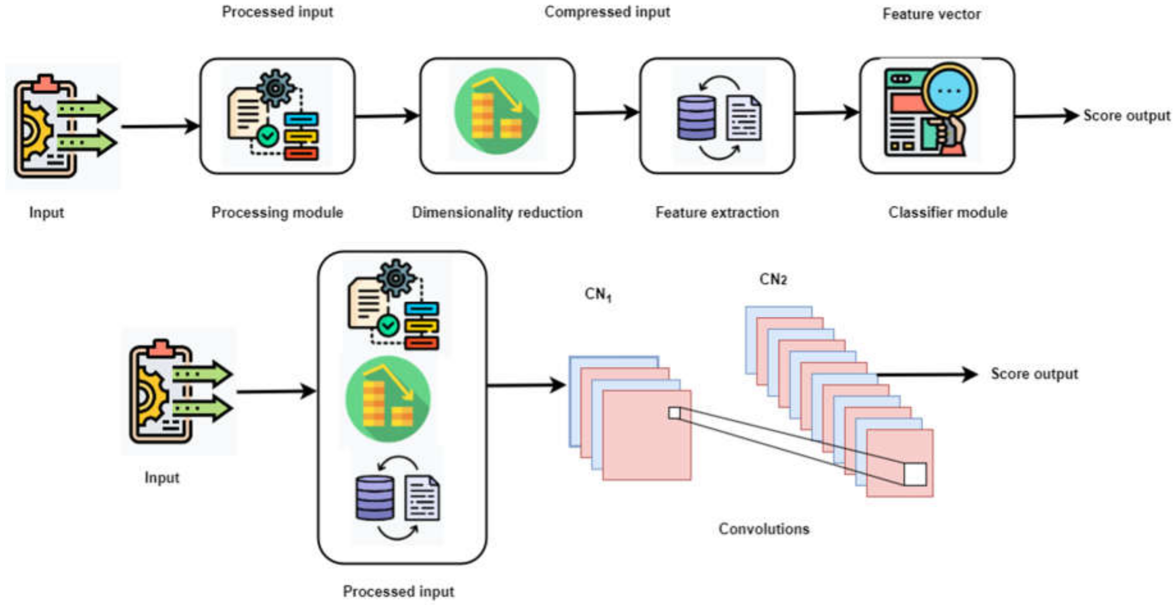


Fig. 1. Overall process of CNN for recognition of patterns

Using sample data for training, the CNN is able to perform feature extraction and classification. Including feature selection into the training process entails learning the weights responsible for feature extraction. The CNN can indeed, with little to no additional work, extract topological features from an input image. Moreover, the spatially structure of the input data is maintained while a limited degree of directionality is obtained. A portion of the CNN's robustness and resistance to deformations and transformations, as well as other 2D shape alterations, are incorporated as well. As the frequent pattern extractor is static, is developed separately from the adaptable classifier, and has not been integrated into the training process, the CNN is created to address these issues.

$$fr = S_{v+1} = \begin{cases} \frac{fr}{cs} \\ \sqrt{\frac{1-fr}{1-cs}} \\ \frac{fn\sqrt{(1-fr)}}{cs} * dl \end{cases} \qquad (1)$$

The feature representationsfr must be precisely defined in a classification systemcs that relies on machine learning. Unfortunately, deep learningdl approaches are guaranteed to be successful in situationsS_{v+1} where it is impossible or difficult to pre-define a feature representation of a given dataset$v+1$.This constraint of models for machine learning is overcome by deep learning approaches using equation (1), which can learn through the intrinsic properties of training data, with the learned information being stored as the network's weights.

$$dl_{sk} = \frac{1}{fr}\sum_{i=1}^{k} ap_i an_i \tag{2}$$

$$nw's = 1 - rn\sqrt{\frac{\sum_{i=1}^{k}(ap_i an_i - fr_{cs})}{(m^2 - sd^2)}} \tag{3}$$

Statistics that can be trusted must be checked This property, stated in equations (2) and (3), guarantees that the dl_{sk} will be available to authorisedpatterns$ap_i an_i$ in a random fashion for each resource that can be safely accessed by the proper nodes as quickly as possible with calculating the square of mean$m$ and standard deviationsd and it is given as$(m^2 - sd^2)$ and this can be used for the comparison of intrusion and authentication purposes.

In this paper, DL-PRM suggest a novel method of using a convolutional neural network (CNN) for real-time gender classification. The following are the major insights that resulted from this paper. It presents a fast and accurate 4-layer convolutional neural network (CNN) for pattern recognition in biometric images in real time.

3.2 Architecture of CNN for PRM

Several convolutional filters followed by subsampling filters and then fully linked layers make up a CNN, which is a feedforward network structure. Traditional CNNs are based on the design of the LeNet-5 CNN, shown in figure 2. The method is successfully implemented in a scenario requiring the recognition of input data. When counting the processing layers, CNN pooling comprises six layers, with an input layer that can handle images as large as 32 by 32 pixels.

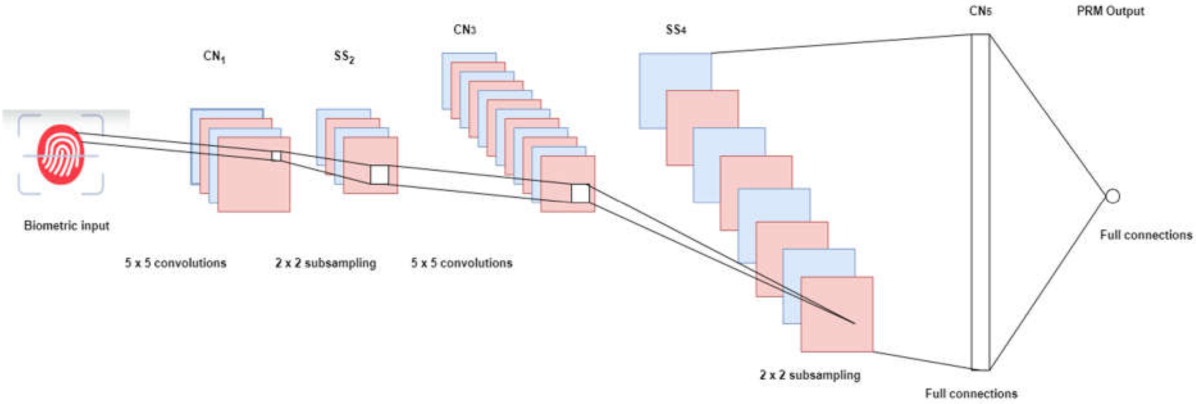


Fig. 2. Convolution and subsampling process in CNN

In the processing layers, the three convolutional layers (CN$_1$, CN$_3$, and CN$_5$), two subsampling levels (SS$_2$ and SS$_4$), and one output layer (PRM output). Feature maps are the horizontal sheets upon which the convolutional and resampling layers are stacked. Each layer in a convolutional layer receives information from a 5 x 5 receptive field in the layer below it. Neurons belonging to the same feature map all get inputs from a total of 5 x 5 independently weighted input areas, allowing the entire input plane to be examined and forms the kernel. On the other hand, distinct kernels are used by the many feature maps that make up the same layer. The extracted features are spatially down sampled in the convolution and pooling layers, which means the map size is decreased by a two-fold amount.

$$size_k = (fr_i)RS^{sk} + (fr_i - 1)acc^{sk-1} + \cdots . + (fr) \qquad (4)$$

Using statistical methods to calculate$(fr_i)$for each user, our paper concludes with a genuine statistic$size_k$ value that the programme does not incur substantial costs for convolutional process. When compared to the neural network model in equation (4), the accuracy of user classification acc^{sk-1}appears to have increased significantly.

$$nnf(pc) = \frac{\sum_{i=1}^{k}(e_{sk1} - \overline{fr_1})}{\sqrt{\sum_{i=1}^{k}(e_{sk2} - \overline{fr_1})^2}} \frac{(d_{sk2} - \overline{fr})}{\sqrt{\sum_{i=1}^{k}(d_{sk1} - \overline{fr})^2}} \qquad (5)$$

Although regular neural network's functionnnf admirably when it comes to picture classification(pc), having complete connectivity in every layer would require a massive number of parameters and would lead to overfitting$\frac{\sum_{i=1}^{k}(e_{sk1}-\overline{fr_1})}{\sqrt{\sum_{i=1}^{k}(e_{sk2}-\overline{fr_1})^2}}$, making the computations too expensive are easily done by applying equation (5).

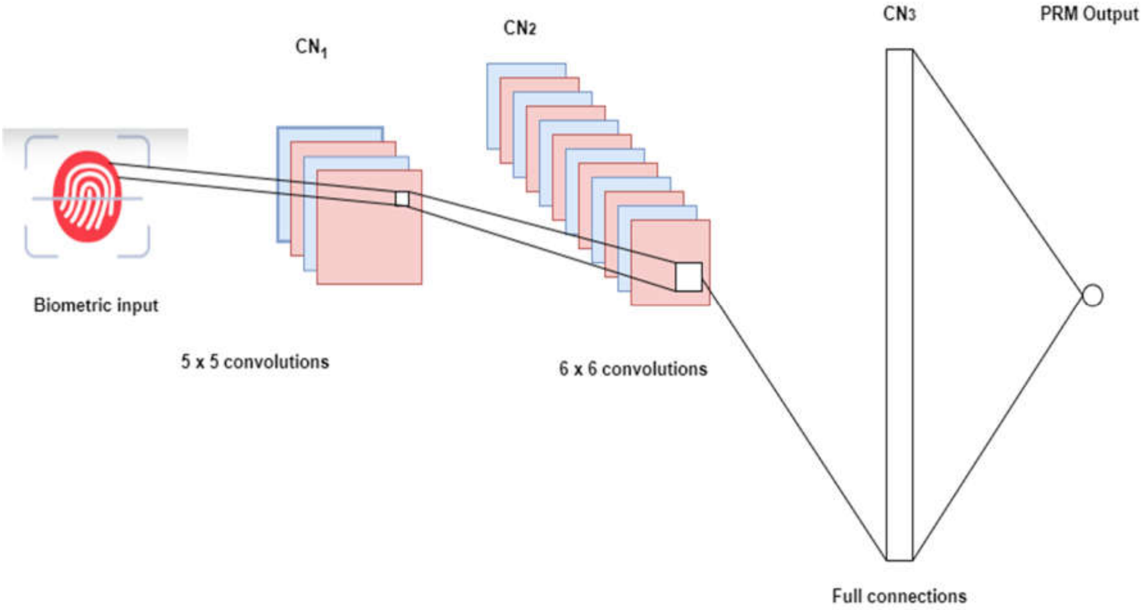


Fig. 3. CNNs process with PRM output

Using the partial-connection approach depicted in figure 3, here provided with the link the feature maps from layer CN1 to those of layer CN2. Due to the incomplete nature of this link, each filter is effectively compelled to use the same image representation to learn new information, there is no break between layers CN2 and CN3. All 16 of CN2's feature maps are coupled to each of CN3's neurons through 5x5 regions illustrated in table 1 below. In a spatial array, neurons with similar kernel values and local receptive regions form an architecture similar to hypothetical biological vision systems. This tactic has a number of positive side effects.

Table 1 Convolution .mapping table

	L1									
L2	1	2	3	4	5	6	7	8	9	10
	0	m		m		m			m	
	1						m	m		m
	2	m		m		m				
	3			m			m			m
	4		M						m	m
	5			m		m		m		

The suggested CNN has fewer layers because of the integration of a convolutional and sub-sampling layer into a single one in our proposed system DL-PRM. The work presented here consists of a reliable convolutional layer with strides of 2 in place of a series of convolutional and subsampling layers are characterized using below equations.

$$fr_i = \frac{1/fr}{fr_{max}} \frac{fr_{min}}{fr_{min}} * CNi * SSi \qquad (6)$$

When the inputs are feed, our proposed model CNN input batches of 64, 128, and 256 squares from the cropped centres of each test picture with the calculation of $fr_i = \frac{1/fr}{fr_{max}} \frac{fr_{min}}{fr_{min}}$.Data is fed into a convolution layer shown in equation (6), where it is processed by a series of layers. Then, the information will be fed into pooling layers.The primary goal of pooling layers is to minimise feature dimension, computation, and training-process overfitting.

$$Pl = \sqrt{CN_1(fr_2 - fr_1)^2 + CN(fr_2 - fr_1)^2} \qquad (7)$$

The first step in accessing a dataset record is checking the private key to determine if it is similar to the one on file. Pooling layersPl with the radius squared values$(fr_2 - fr_1)$it must be same in order for data to be transferred between two CN values as$\sqrt{CN_1(fr_2 - fr_1)^2 + CN(fr_2 - fr_1)^2}$, as shown in the equation (7) by transfer learning with square root of $softmax$ values.

3.3 Transfer learning for DL-PRM

Pooling follows convolution as the next step in a convolutional neural network. As an aid to gaining a reduced component depiction that is resistant to interpreted in different ways in object scale, posture, and translation in a picture, the pooling procedure is useful depicted in figure 4. Maximum pooling and average pooling are the most common types of pooling operations for detecting any malicious activities. Using max pooling, the most numerous candidates for that role is found and used. Since it can be quickly calculated and allows for effective simplification of the image, it is the most used form.

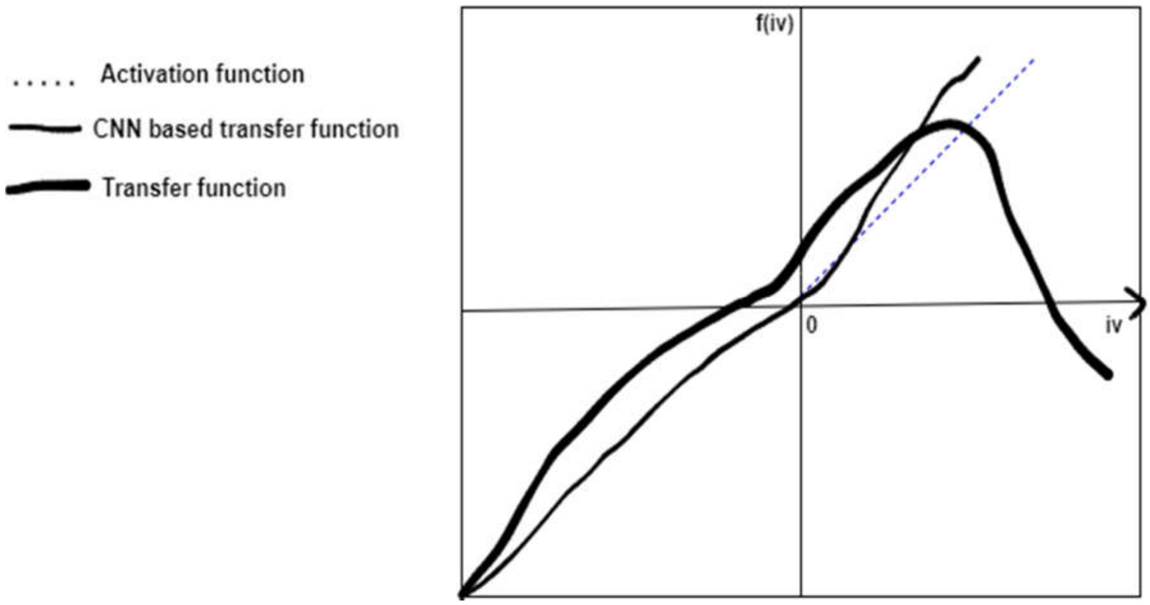


Fig. 4. Transfer learning process

$$f(y;\theta) = x * \frac{1/fr}{fr_{max}} \frac{fr_{min}}{fr_{min}} \tag{8}$$

As shown in equation (8), where θ denotes the set of variables, y indicates M-dimensional feature vectors, and x signifies scalar values. Thus, the features of the scoring system are the input features y and the model parameters θ.

$$k_j = \sum_{t=\Gamma_j}^{\Gamma_j+1-1} \log\big(q(w_t|w_{t-1})q(y_t|w_t)\big) \tag{9}$$

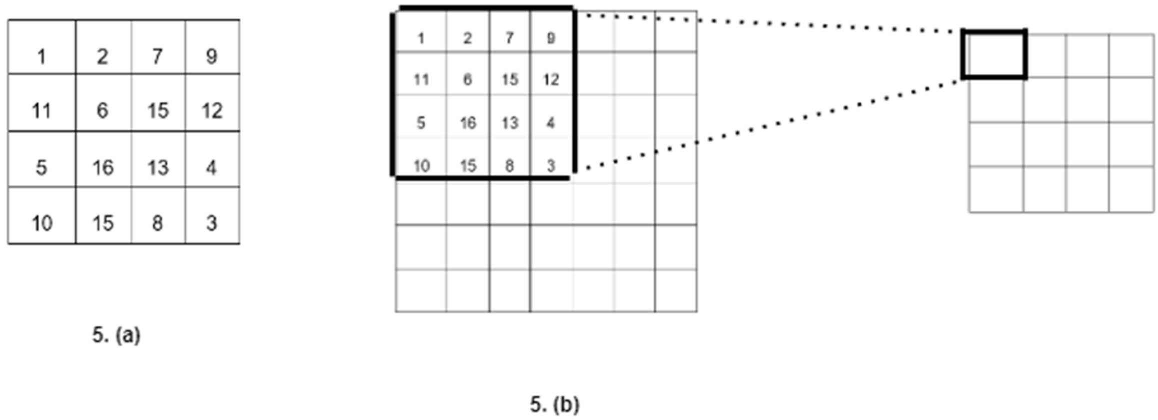
As inferred from equation (9), where $y_t$and w_t are observation vectors and the model's state at time t, correspondingly. $q(w_t|w_{t-1})$ indicates the transition probability. $q(y_t|w_t)$ indicates the output likelihood dissemination of the state w_t. For every frame respective to the jth segments of the phonemes p_j, the frame-based posterior likelihood $q(p_j|y_t)$ of the phonemes p_j is computed,

$$q(p_j|y_t) = \frac{q(y_t|p_j)q(p_t)}{\sum_{p-1}^{N} q(y_t|p)q(p)} \tag{10}$$

If a picture input value is more than the filter weight value, it is helpful in calculating the pixel number. An activation function, denoted by deep learning, the transfer learning from machine learning techniques is commonly utilised. It does this by applying above equation (10) illustrated in figure 4 where $\sum_{p-1}^{N} q(y_t|p)\, q(p)$ is the output of the convolutional layer, and replacing negative values with 0.

This indicates the current observation's probability density, and sum on the denominators are the overall sum of text-independents phoneme $p = 1, \ldots N$. Like the probability log scores, the frame-based posteriors likelihood log scores are acquired by collecting every frame in jth segments.

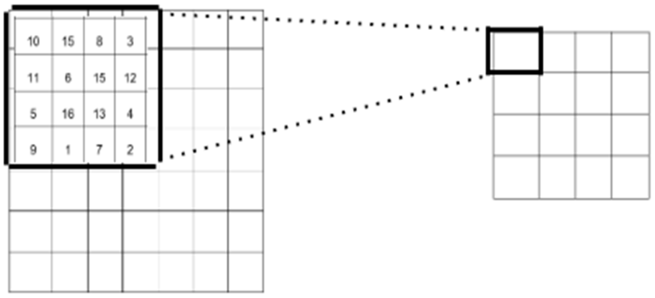
3.4 Anomaly Detection in Biometric Images



1	2	7	9
11	6	15	12
5	16	13	4
10	15	8	3

5. (a)

5. (b)



5.(c)

Fig. 5. 5 (a), 5(b), and 5(c) Pooling process

Maximum pooling and average pooling are the most common types of pooling operations. Using max pooling, the most numerous candidates for that role is found and used. Since it can be quickly calculated and allows for effective simplification of the image, it is the most used form. The average of the group is determined by performing the steps in figure 5 for the pooling average.

The probabilities attained by passing the outputs of these fully-connected layers on to the next layer are what are needed to facilitate the classification operation. The output y is computed by the equation (10), where x is the scaled version of the sample data and w represents the weight vector, while the $softmax$ function uses equation (9) where m is the class and n are the maximum number of classes' number to accomplish this. A score vector is the result of a $softmax$ classifier, and it is a set of chances that are weighted differently for each class.Popular smartphone biometric identification methods include iris scanners and fingerprint readers.

$$FRR(th) = \frac{number\ of\ acceptance\ ratio}{number\ of\ fake\ accesses} \qquad (11)$$

$$FAR(th) = \frac{number\ of\ rejection\ ratio}{number\ of\ fake\ accesses} \tag{12}$$

It's possible for the system to commit either false acceptance rate (FAR) or false rejection rate (FRR) depending on the value of threshold(th).The FAR and FRR curves as a proportion of threshold are obtained by empirically tracing this function from a training set and normalising it based on the total number of fake and client accesses, respectively to calculate error rate using equations (11) and (12).

By allowing for the improvement of existing methods and the creation of new ones, CNNs can enhance sensor-based approaches to biometric authentication. A fresh method of biometric authentication based on the recognition of inertial motion in the biometric pattern. The proposed model DL-PRM created makes use of information gathered from an accelerometer and an analyser. A CNN is then fed the resulting gait signals from these values.

4. Experimental Methods

To process high-dimensional inputs and large-scale datasets, a DL-PRM architecture is developed that can extract useful features from raw biometric data using dataset from link [28]. The final proposed model DL-PRM architecture is trained on Google Cloud, which has access to powerful CPUs and GPUs, using the Python TensorFlow implementation for a total of 90 epochs across all datasets. Moreover, the library of OpenCV is used to perform some preliminary processing. The level of a dataset is determined using a series of tests; this threshold is then used to differentiate a genuine from a fake version of a specific fingerprint. This system's resilience against spoofing attacks can be guaranteed with the help of the estimated threshold are compared and given below using tables and graphs.

4.1 Comparison of DL-PRM with Various Datasets

The popularity of biometrics has led to an explosion of related materials, such as software and data sets for training systems to recognize faces. In this paper, the results of widely-used face recognition datasets on which DL-PRM is tested the performance of several hopeful deep learning-based biometric models, and compared these results to those obtained with several hopeful traditional biometric modeling techniques are given in below table 2. In addition, the outcomes of two widely-cited classical biometric research gives this model trained with deep learning algorithms outperform those trained with more traditional methods by applying on above equations (11) and (12).

Table 2 Comparison of DL-PRM datasets

Datasets	Accuracy	FAR	FRR	Error rate (%)	Lower and upper limits
Crossmatch 2020	79.1%	0.089	0.091	1.089	0.92
Italdata 2020	80.7%	0.095	0.085	0.095	0.88
Swipe 2020	84.9%	0.067	0.077	2.067	0.81
Biometrika 2021	89.8%	0.059	0.069	1.059	0.77
Greenbit 2022	90.7%	0.039	0.049	0.039	0.67
DL-PRM dataset	91.4%	0.015	0.025	0.015	0.54

4.2 Authentication comparison of DL-PRM

Using a person's unique set of behavioural and physiological traits, biometric authentication (BA) ensures that the claimed identity belongs to the individual making the claim. Biometric authentication offers advantages in that it cannot be stolen or forgotten, unlike more conventional types of authentications like keys and personal identification number (PIN) digits can be obtained using equations (2) and (3). The authentication process of our proposed model DL-PRM is obtained by comparing with traditional methods MFCC, CMI-CNN, CI-DLt, DL-As, and MmBIS are illustrated in below table 3. Integrating many biometric methods can improve its accuracy and efficiency. Here, our proposed model demonstrates how a novel margin-based confidence metric can enhance modal or intramodal fusion biometric systems.

Table 3 Comparison with traditional methods

Number of Epochs	Techniques					
	MFCC	CMI-CNN	CI-DLt	DL-As	MmBIS	DL-PRM
10	45.6	56.5	62.4	60.8	77.4	88.3
20	43.4	59.8	58.7	75.5	64.9	89.6
30	50.2	48.6	65.5	67.4	73.8	91.8
40	49.4	51.8	63.9	78.6	66.2	94.7
50	41.7	54.7	54.6	73.2	71.5	93.4
60	52.5	62.1	69.3	71.8	73.6	95.8
70	63.8	74.8	64.6	74.6	71.4	92.8
80	75.9	79.2	75.1	69.8	79.9	91.2

90	72.1	82.6	80.2	79.6	78.2	93.6
100	81.6	86.5	83.3	82.6	83.6	97.6

4.3 Reliability comparison of DL-PRM

The use of biometrics, or identification based on unique phenotypes, has the possibility to become integral to all modern means of verification. It has been difficult to solve the recognition challenges in the past, and the amount of work required to accomplish this has been appreciated using equation (6). From a system's point of view, both privacy and security are open challenges with no obvious, adequate remedies in range. While the focus of this work is on the unresolved basic issues in biometrics, that does not mean that the state of the art is not useful are compared from figure 6.

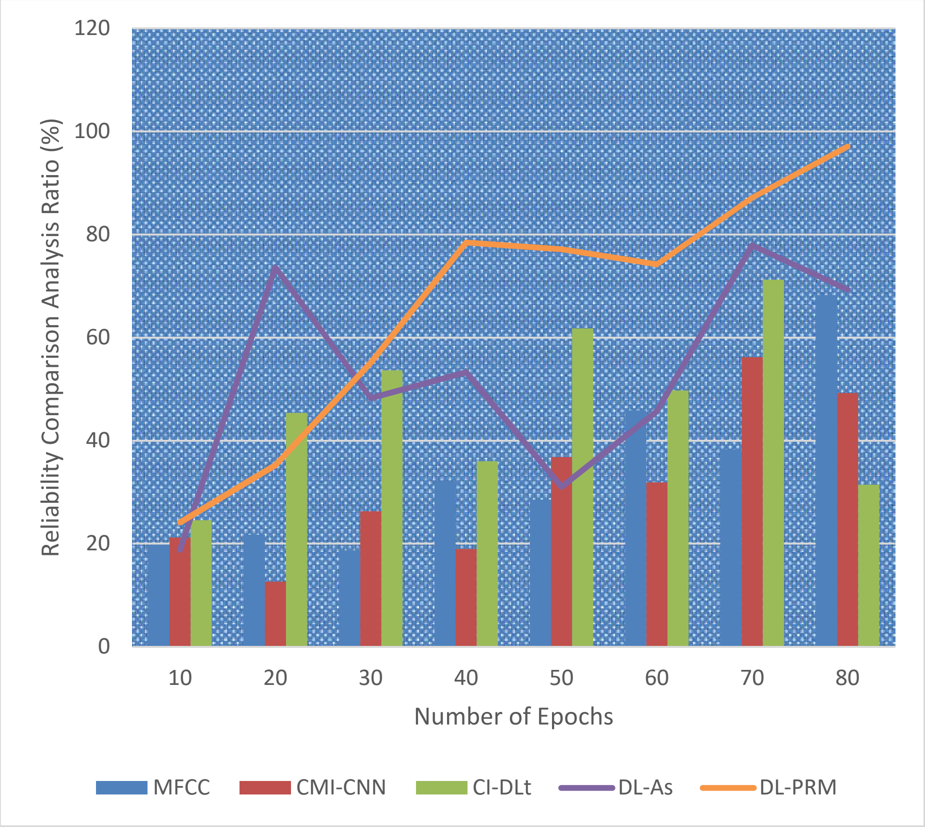


Fig. 6. Reliability comparison of DL-PRM

4.4 Malicious activity analyzing in DL-PRM

Compared to the typical dataset, this number is now off. As a data science application, anomaly detection makes use of techniques including cluster analysis, linear regression, and classifiers. One of the aforementioned methods is used to find the dataset's anomaly. Researchers additionally face a difficult problem when tasked with detecting anomalies in a biometric dataset. Certain major situations, technical faults, or variations in user actions might cause anomalies are neglected using equation (8). The various comparisons of analysing malicious activity are shown in below figure 7.

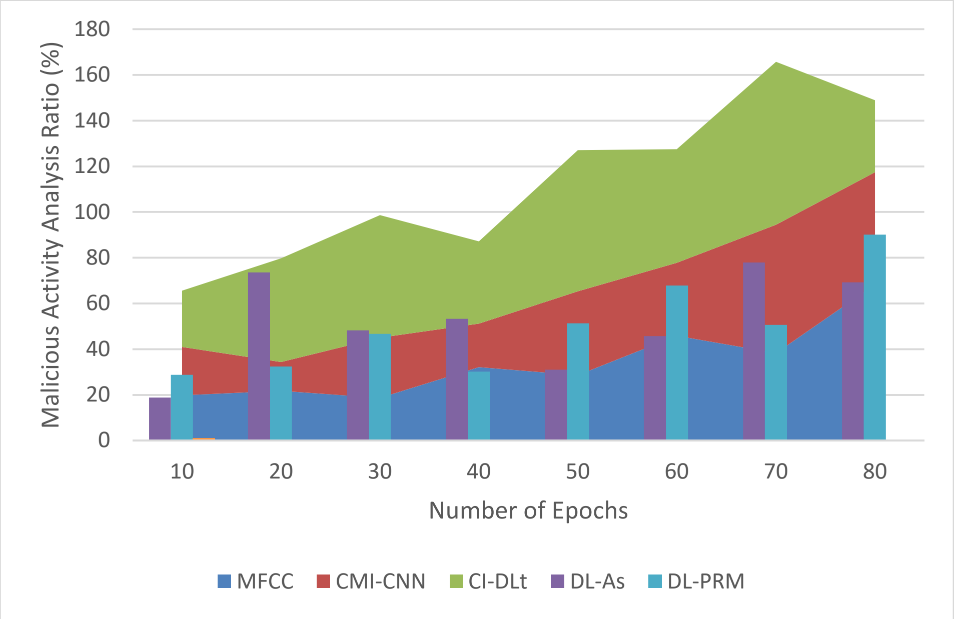


Fig. 7. Malicious activity comparison

4.5 Intrusion prevention comparison of DL-PRM

Adding biometrics to intrusion detection systems (IDSs) adds a new layer to the detection process. To detect the type of intrusion in which an attacker gains access to the resources and begins performing normal non-intrusive practices in our proposed system DL-PRM, such systems combine traditional intrusion detection systems, which focus on the deeds that the user takes, with biometrics, which focuses on the identity of the user is resolved using equation (1). If the attacker uses the operation phases and his access constraints, then differences in browsing activities cannot be identified; however, if the identification is predicated on biometrics information, then the attack can be uncovered is shown in below table 4

Table 4 Intrusion prevention comparison.

Number of Epochs	MFCC	CMI-CNN	CI-DLt	DL-As	DL-PRM
10	19.78	21.21	24.54	18.76	28.76
20	21.78	12.65	45.36	73.56	32.45
30	18.65	26.33	53.66	48.23	46.76
40	32.15	18.98	35.97	53.26	30.12
50	28.56	36.78	61.78	31.03	51.34
60	45.89	31.87	49.74	45.69	67.87
70	38.27	56.21	71.23	77.89	50.65
80	68.26	49.21	31.43	69.31	90.12

High-accuracy biometric pattern recognition is possible with DL-PRM, which can be put to use in many different settings, such as identification, authentication, and access control. The use of DL-PRM allows for the detection of anomalies in biometric data are obtained by comparing with other traditional methods MFCC, CMI-CNN, CI-DLt, DL-As, and MmBIS.

5. Conclusion

In this proposed method DL-PRM using CNN and anomaly identification to create multimodal secured biometric identification systems. Most of the recognition systems have shown their security strengths through the combination of modalities. During the design phase, the suggested model went through a number of iterations to identify the most suitable CNN model and the most relevant classifiers that can work with all multiple biometric modalities. In this proposed system, researches present a thorough overview of the state of the art in the subject of biometrics, covering such topics as identification by 92.3%, performance evaluation factor as 89.9%, authentication by 94.3% and existing methodologies like accuracy 91.4% and reliability of 95.7%. Their precision is analysed in comparison with each other and with other state-of-the-art frameworks. Second, histogram equalization contrast enhancement and CNN layer training are proposed for improved fingerprint identification. The large datasets are likely to be used in a more widespread application domain, such as government biometric data, therefore it makes sense to investigate how different dataset sizes affect system performance. Researching more machine learning methods for use with these biometric identifiers will be fascinating.

References

1. Serna, I., Morales, A., Fierrez, J., Cebrian, M., Obradovich, N., & Rahwan, I. (2019). Algorithmic discrimination: Formulation and exploration in deep learning-based face biometrics. arXiv preprint arXiv:1912.01842.
2. Medjahed, C., Rahmoun, A., Charrier, C., &Mezzoudj, F. (2022). A deep learning-based multimodal biometric system using score fusion. IAES International Journal of Artificial Intelligence, 11(1), 65.
3. BELLO, R. W., TALIB, A. Z. H., & MOHAMED, A. S. A. B. (2020). Deep learning-based Architectures for recognition of cow using cow nose image pattern. Gazi University Journal of Science, 33(3), 831-844.
4. Zhao, Z., & Kumar, A. (2019). A deep learning based unified framework to detect, segment and recognize irises using spatially corresponding features. Pattern Recognition, 93, 546-557.

5. Wang, X., Zhao, X., & Zhang, Y. (2021). Deep-learning-based reading eye-movement analysis for aiding biometric recognition. Neurocomputing, 444, 390-398.
6. Althabhawee, A. F. Y., &Alwawi, B. K. O. C. (2022). Fingerprint recognition based on collected images using deep learning technology. IAES International Journal of Artificial Intelligence, 11(1), 81.
7. Winston, J. J., Hemanth, D. J., Angelopoulou, A., &Kapetanios, E. (2022). Hybrid deep convolutional neural models for iris image recognition. Multimedia Tools and Applications, 1-23.
8. Zou, Q., Wang, Y., Wang, Q., Zhao, Y., & Li, Q. (2020). Deep learning-based gait recognition using smartphones in the wild. IEEE Transactions on Information Forensics and Security, 15, 3197-3212.
9. Fujiyoshi, H., Hirakawa, T., & Yamashita, T. (2019). Deep learning-based image recognition for autonomous driving. IATSS research, 43(4), 244-252.
10. Batra, R., Tran, H. D., Kim, C., Chapman, J., Chen, L., Chandrasekaran, A., & Ramprasad, R. (2019). General atomic neighborhood fingerprint for machine learning-based methods. The Journal of Physical Chemistry C, 123(25), 15859-15866.
11. Yang, W., Wang, S., Hu, J., Zheng, G., Yang, J., & Valli, C. (2019). Securing deep learning based edge finger vein biometrics with binary decision diagram. IEEE Transactions on Industrial Informatics, 15(7), 4244-4253.
12. Khan, S., Islam, N., Jan, Z., Din, I. U., & Rodrigues, J. J. C. (2019). A novel deep learning based framework for the detection and classification of breast cancer using transfer learning. Pattern Recognition Letters, 125, 1-6.
13. Chen, B., Chen, C., Hu, J., Sayeed, Z., Qi, J., Darwiche, H. F., ... & Palacio-Lascano, C. (2022). Computer Vision and Machine Learning-Based Gait Pattern Recognition for Flat Fall Prediction. Sensors, 22(20), 7960.
14. Kim, S. K., Yeun, C. Y., &Yoo, P. D. (2019). An enhanced machine learning-based biometric authentication system using RR-interval framed electrocardiograms. IEEE Access, 7, 168669-168674.
15. Guo, H., Wang, Z., Wang, B., Li, X., &Shila, D. M. (2020, May). Fooling a deep-learning based gait behavioral biometric system. In 2020 IEEE Security and Privacy Workshops (SPW) (pp. 221-227). IEEE.
16. Chuang, C. W., & Fan, C. P. (2021). Deep-learning based joint iris and sclera recognition with yolo network for identity identification. Journal of Advances in Information Technology, 12(1).

17. Peng, L., Zhang, J., Liu, M., & Hu, A. (2019). Deep learning based RF fingerprint identification using differential constellation trace figure. IEEE Transactions on Vehicular Technology, 69(1), 1091-1095.

18. Pannu, H. S., Ahuja, S., Dang, N., Soni, S., & Malhi, A. K. (2020). Deep learning based image classification for intestinal hemorrhage. Multimedia Tools and Applications, 79, 21941-21966.

19. Liu, M., Wang, L., Lee, K. A., Zhang, H., Zeng, C., & Dang, J. (2021). Exploring deep learning for joint audio-visual lip biometrics. arXiv preprint arXiv:2104.08510.

20. Tyagi, S., Chawla, B., Jain, R., & Srivastava, S. (2022). Multimodal biometric system using deep learning based on face and finger vein fusion. Journal of Intelligent & Fuzzy Systems, 42(2), 943-955.

21. Dayal, A., Paluru, N., Cenkeramaddi, L. R., &Yalavarthy, P. K. (2021). Design and implementation of deep learning based contactless authentication system using hand gestures. Electronics, 10(2), 182.

22. NOĞAY, H. (2021). Comparative experimental investigation of deep convolutional neural networks for latent fingerprint pattern classification. Traitement Du Signal, 38(5).

23. Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: A survey. Artificial Intelligence Review, 1-49.

24. Daas, S., Yahi, A., Bakir, T., Sedhane, M., Boughazi, M., &Bourennane, E. B. (2020). Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion. IET Image Processing, 14(15), 3859-3868.

25. Kamboj, A., Rani, R., & Nigam, A. (2022). A comprehensive survey and deep learning-based approach for human recognition using ear biometric. The Visual Computer, 38(7), 2383-2416.

26. Sameer, V. U., Naskar, R., Musthyala, N., &Kokkalla, K. (2017). Deep learning based counter–forensic image classification for camera model identification. In Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August 23-25, 2017, Proceedings 16 (pp. 52-64). Springer International Publishing.

27. Boles, A., & Rad, P. (2017, June). Voice biometrics: Deep learning-based voiceprint authentication system. In 2017 12th System of Systems Engineering Conference (SoSE) (pp. 1-6). IEEE.

28. https://dasl.datadescription.com/