Journal of Scientific & Industrial Research
Vol. 82, January 2023, pp. 151-157
DOI: 10.56042/jsir.v82i1.70253

A Hybrid Classification Approach for Iris Recognition System for Security of Industrial Applications

P Jyothi[1*], D Krishna Reddy[2] & P Naveen Kumar[1]

[1]Dept. of Electronics and Communication Engg., University College of Engineering, Osmania University, Hyderabad 500 007, India

[2]Dept. of Electronics & Communication Engg., Chaithanya Bharathi Institute of Technology, Osmania University, Hyderabad 500 075, India

Received 30 May 2022; revised 24 September 2022; accepted 07 October 2022

The biometric authentication system is demanded to identify a particular person from the set of persons. Even though many biometric authentication methods are available such as fingerprint, palm, face, and iris, the iris-based recognition system is effective due to its simplified process. This article proposes an iris recognition system using a hybrid classification approach for security applications. The proposed method includes three modules: preprocessing, augmentation, and classifier. The preprocessing module converts the color iris images into grey scale images and also resizes the image into 256 × 256. The preprocessed iris images are now data augmented to construct the larger dataset. The data augmented images are classified into either genuine or imposter images using a hybrid classification approach. The hybrid classification approach functions in two modes as training and testing. In this article, the Convolutional Neural Networks (CNN) is integrated with the Adaptive Neuro-Fuzzy Inference System (ANFIS) classifier to enhance the recognition rate of the iris recognition system. The performance analysis of the proposed approach is shown in terms of sensitivity, accuracy, recognition rate, specificity, false-positive rate, and false-negative rate. The experimental results of the proposed iris recognition system stated in this article significantly outweigh other design methods.

Keywords: ANFIS, CNN, Data augmentation, Feature map, Genuine, Imposter

Introduction

A biometric authentication system is used to identify persons using biometrics methods such as fingerprint, palm, facial expression, and iris. Among these biometric authentication systems, Iris Recognition (IR) is one biometric authentication method for identifying a particular person among the set of persons in a region. This biometric authentication uses iris images that are captured by Charge Coupled Camera (CCC) or mobile phone. The iris-based recognition system uses ring-shaped patterns of iris images to identify individual persons.[1-5] Scanners or scanning devices are most important for the iris-based person identification system. In this modern era, high-resolution scanning devices are used to capture iris images without damaging the internal tissues of the human eye. The iris recognition system is complex compared with other biometric recognition systems such as the face, fingerprint (Fig. 1-(a)), and palm print (Fig. 1-(b)). These conventional biometric authentication systems use a large portion of the human part. Hence, it is easy to recognize the image for authentication purposes. In the case of the iris recognition system (Fig.1-(c)), only a small portion of the human eye is involved in the recognition process, which makes the recognition system more complex.[6–10]

This article uses soft computing techniques to overcome the limitations produced by convolutional methods. Two soft computing techniques are deep learning and machine learning. This paper integrates a deep learning algorithm with the machine learning algorithm to enhance the iris recognition rate.

Literature Survey

Ghosh *et al.*[11] used machine learning algorithms such as a linear classifier to recognize individual iris images. The authors obtained 94.7% of Sensitivity (Se), 90.6% of Specificity (Sp), 91.9% of Accuracy (Acc), 12.8% of False Positive Rate (FPR), and 8.7%

Fig. 1 — (a) Fingerprint image, (b) Palm image, (c) Iris image

*Author for Correspondence
E-mail: jyothi.doj@gmail.com

of False Negative Rate (FNR). Also, this method consumed 7.67 ms of time for identifying the iris images for authentication. Jayanthi *et al.*[12] proposed an iris-based biometric authentication system for determining individual iris images using deep learning algorithms. The authors computed the interior features from each layer, which were then integrated into the feature map. This feature map was classified by the dense layers of the deep learning architecture, which produced the identification results, such as authenticated or imposter images. Galla *et al.*[13] owned an SVM (Support Vector Machine) classifier for differentiating particular iris images from the imposter iris images. This iris recognition system used multi-kernel patterns for a multi-class object classification process. These multi-kernel functions were used to differentiate the iris images for the biometric authentication system. The authors obtained 92.8% of Se, 89.9% of Sp, 90.7% of Acc, 11.8% of FPR, and 8.5% of FNR. Also, this method consumed 7.98 ms of time for identifying the iris images for authentication.

Lin *et al.*[14] proposed an iris recognition system using HAAR like feature set and Adaboost classification algorithm. The HAAR-like feature set was computed from the human iris image, and these HAAR features were trained and classified using the Adaboost classifier. The internal nodes in this Adaboost classifier were fixed, which improved the iris recognition rate more significantly. The authors obtained 91.7% of Se, 89.6% of Sp, 91.7% of Acc, 11.5% of FPR, and 8.9% of FNR. Also, this method consumed 8.38 ms of time for identifying the iris images for authentication. Chaturvedi *et al.*[15] used Daugman's Algorithm for segmenting the iris region from the entire eye image, and then the segmented iris images were recognized by the Artificial Neural Networks (ANN) for biometric authentication purposes. The iris image was segmented from an eye image using Hough transformation, and the segmented portion was normalized using Daugman's Algorithm. Then the non-linear computational features were computed from this iris image, and these features were classified into either genuine or imposter images using the ANN classifier in this work. The authors obtained 90.5% of Se, 89.9% of Sp, 90.4% of Acc, 12.6% of FPR, and 8.6% of FNR. Also, this method consumed 9.10 ms of time for identifying the iris images for authentication.

Materials and Methods

Materials

This article uses the Multimedia University (MMU) iris image dataset (https://www.kaggle.com/datasets/naureenmohammad/mmu-iris-dataset) for the proposed iris image authentication system. The iris images in this dataset are fully open access; hence, it does not require any license. The iris images in this dataset are obtained from the students who studied at Multimedia University. The iris images in this dataset are used worldwide for biometric attendance and authentication systems. This dataset is constructed by scanning the left iris and right iris images of 46 persons. Therefore, 460 iris images are available in this dataset. The iris image size is about 256 × 256 pixels as image width and height, and these images are stored in the dataset as BMP files.

Methods

This article proposes an iris recognition system using a hybrid classification approach for security applications. The proposed method comprises three modules; preprocessing, augmentation, and classifier. The preprocessing module converts the color iris images into grayscale images and also resizes the image into 256 × 256. The preprocessed iris images are now data augmented to construct the larger dataset. The data augmented images are classified into either genuine or imposter images using a hybrid classification approach. This approach functions in 2 modes: training mode and testing mode. The training mode of the proposed method is illustrated in Fig. 2-(a), and the testing mode of the

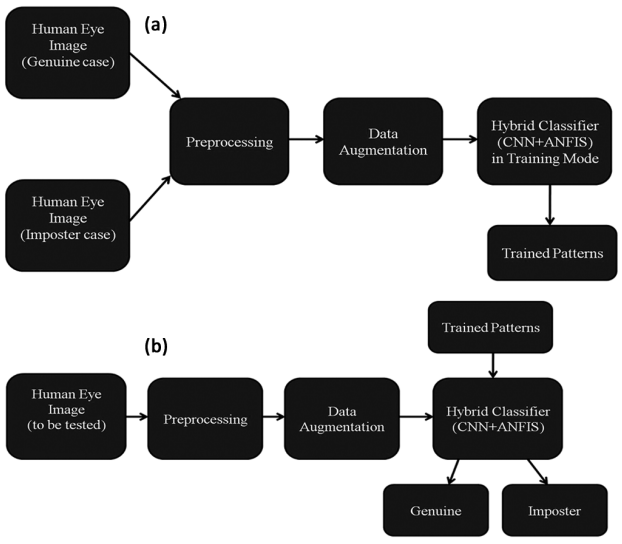

Fig. 2 — Proposed iris recognition system using hybrid classifier: (a) in training mode, (b) in testing mode

proposed hybrid classification approach is shown in Fig. 2(b), respectively.

Preprocessing and Data Augmentation

Preprocessing is used to convert the color iris images into grayscale images to improve the processing time for the iris recognition system. Further, the grey scale iris image is resized into 256 × 256 pixels as image width and height, respectively. The CNN classifier requires a more significant number of iris images for both training and testing the classifier. Hence, the data augmentation process is used in this article to increase the number of iris images. Right with left shift functions and left shearing and right shearing functions are used in this article as the data augmentation functions. Each data augmentation function produces a single iris image; hence, four iris images are produced after applying all data augmentation functions. Therefore, the 460 iris images from the MMU iris dataset are data augmented into 1840 iris images. These data augmented iris images are used for training and testing the classifiers for the iris recognition system.

Classifications

This article uses two classifiers such as machine learning (ANFIS classifier) and deep learning (CNN classifier) classifiers for iris recognition systems. The CNN classifier is integrated with the ANFIS classifier to improve the iris recognition system. In this article, the CNN classifier is used to create the feature maps, and the ANFIS classifier is used to classify the future maps. The proposed CNN architecture is shown in Fig. 3 to constructing feature maps for the iris recognition system. The proposed CNN architecture is designed with 2 number of Convolutional layers along with 2 no. of pooling layers with two numbers of dense layers. Convolutional layer 1 is constructed with 256 Convolutional filters with the kernel size of 11 × 11. The data augmented iris image is convoluted by Convolutional layer 1, which produces significant feature metrics. A feature map can be derived from Eq. (1).

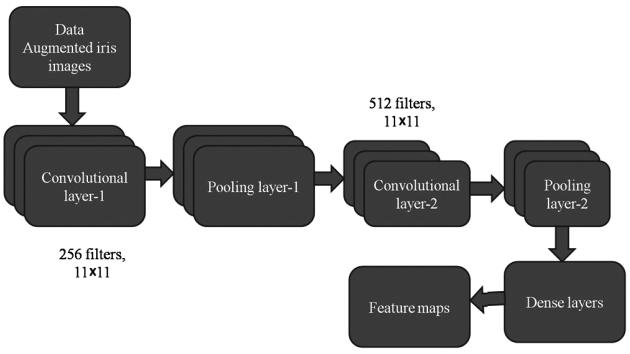

Fig. 3 —Proposed CNN architecture for constructing feature maps for iris recognition system

$$Featuremap = \sum I * k \quad \ldots (1)$$

where, I represent the data augmented iris image, k is the kernel of the Convolutional filter in the convolutional layer, and '$*$' denotes the convolution operator.

The size of this feature metric is significant due to the Convolution process in Convolutional layer 1. Therefore, it is necessary to reduce the size of these feature metrics generated through Convolutional layer 1. The number of layers in pooling layer 1 is equal to the number of filters in Convolutional layer 1. Two types of Pooling layers are used in the iris recognition system: Average pooling and Max pooling. The reconstruction error rate of the Max pooling function is low when compared with the reconstruction error rate of the Average pooling function. Therefore, this proposed CNN architecture uses the Max pooling function to decrease the reconstruction error rate significantly. The feature maps from the Convolutional layer may contain negative values also. Hence, the Linear Rectification Unit (ReLU) is included between the Convolutional layer and Pooling layer to eliminate negative values in generated feature maps. The action of ReLU is described in Eq. (2).

$$ReLU_{outpout} = \begin{cases} x; if\, x \geq 0 \\ 0; else \end{cases} \quad \ldots (2)$$

X = feature map, that is generated by the Convolutional layer.

The feature maps 1 by pooling layer 1 are fed to the kernels of Convolutional layer 2. Convolutional layer 2 is constructed with 512 Convolutional filters with the kernel size of 11 × 11. Feature maps 1 are convoluted by Convolutional layer 2 to create feature maps 2. Then feature maps 2 is fed to the pooling layer 2 to decrease the size of feature maps 2. Finally, feature maps 2 are passed through the two dense layers, where the dense layer 1 is designed with 4096 neurons, and the dense layer 2 is designed with 2048 neurons. Final feature maps are generated by integrating feature maps 2 with the dense layer feature maps.

The proposed CNN architecture generates the feature maps for both genuine case iris images and

imposter case iris images. The generated feature maps are now classified by the ANFIS classifier as depicted in Fig. 4. The generated feature map of the genuine case iris images is fed into 'x,' and the generated feature map of the imposter case iris images is fed into 'y' of the ANFIS architecture. During the training mode of this classifier, both feature maps from genuine and imposter case iris images are trained by ANFIS architecture which is depicted in Fig. 4, and thus produces the trained patterns 'f' during training mode.

During the testing mode of this classifier, the feature maps from the unknown or test iris image are fed with 'x' of the ANFIS architecture, and the trained patterns which are generated by the training mode of ANFIS architecture is fed with 'y' of the ANFIS architecture. The final response is produced as 'f', which is a binary value. The following constraint is used in this article to identify the genuine case iris image from the imposter case iris image. From equation (3), it is a Genuine case if f = 0 and Imposter case if the f value is not zero.

$$Iris_{image} = \begin{cases} genuinecase; iff = 0 \\ impostercase; else \end{cases} \quad \ldots (3)$$

Simulation results can be found in Fig. 5, Fig. 5 (a) is the actual case iris recognition system simulation screenshot, and Fig. 5 (b) is the imposter case iris recognition system simulation screenshot. The genuine and imposter case iris images used in this article from the MMU dataset are given in Fig. 5 (c) and Fig. 5 (d) respectively.

Results and Discussion

In this paper, simulation software, MATLAB R2018b, is used for simulating the proposed iris recognition system using a hybrid classifier. The iris images in the MMU iris dataset are split into 300 numbers of genuine case images and 160 numbers of Imposter case images. The iris images in each case are divided into training and testing to verify the effectiveness of the proposed iris recognition system. The 30:70 ratio is used in this article for training and testing split up. In this article, 300 genuine case images are split into 90 iris images belonging to the training category and 210 iris images belonging to the testing category. In this article, 160 imposter case images are divided into 48 iris images belonging to the training category and 112 iris images, belonging to the testing category. Therefore, 138 iris images are trained, and the proposed iris recognition system tests the remaining 322 iris images.

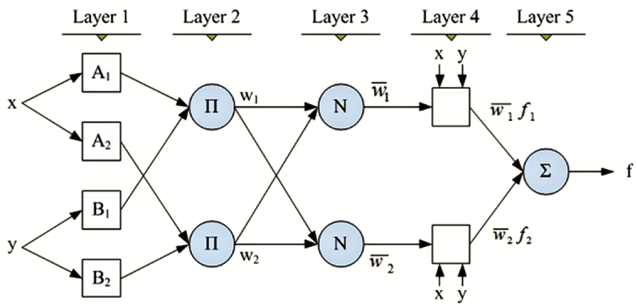

Fig. 4 — ANFIS architecture for iris recognition system[16]

The accuracy of the presenting system is corroborated through Eqs (4) & (5). The Genuine Recognition Rate (GRR) is the parameter equal to the ratio between correctly identified genuine case images to the total no. of genuine case images. The Imposter Recognition Rate (IRR) is the parameter equal to the ratio between correctly identified imposter case images to the total number of imposter case images. Both the parameters GRR and IRR are measured in percent.

$$GRR = \left(\frac{Correctly\ identified\ genuine\ case\ images}{Total\ number\ of\ genuine\ case\ images}\right) \times 100\% \quad \ldots (4)$$

$$IRR = \left(\frac{Correctly\ identified\ imposter\ case\ images}{Total\ number\ of\ imposter\ case\ images}\right) \times 100\% \quad \ldots (5)$$

In this article, the value of GRR is 96.6% by correctly identifying 203 genuine case iris images over 210 genuine case images. Also, the value of IRR is 94.6% by correctly identifying 106 imposter case iris images over 112 imposter case images. Therefore, the Average Iris Recognition Rate (AIRR) is computed by averaging the value of GRR and IRR. Hence, the AIRR value is about 95.6%. The computation of the Recognition rate of the proposed system is shown in Table 1, for both genuine and imposter cases.

The recognition rate of the proposed system is described in Table 2, which shows the performance analysis of the presented method weighed up with various classifiers SVM, NN, and Adaboost with the proposed method hybrid classifiers. This article analyzes the proposed method by applying different classifiers to the MMU iris dataset to validate accuracy. The proposed iris recognition system using

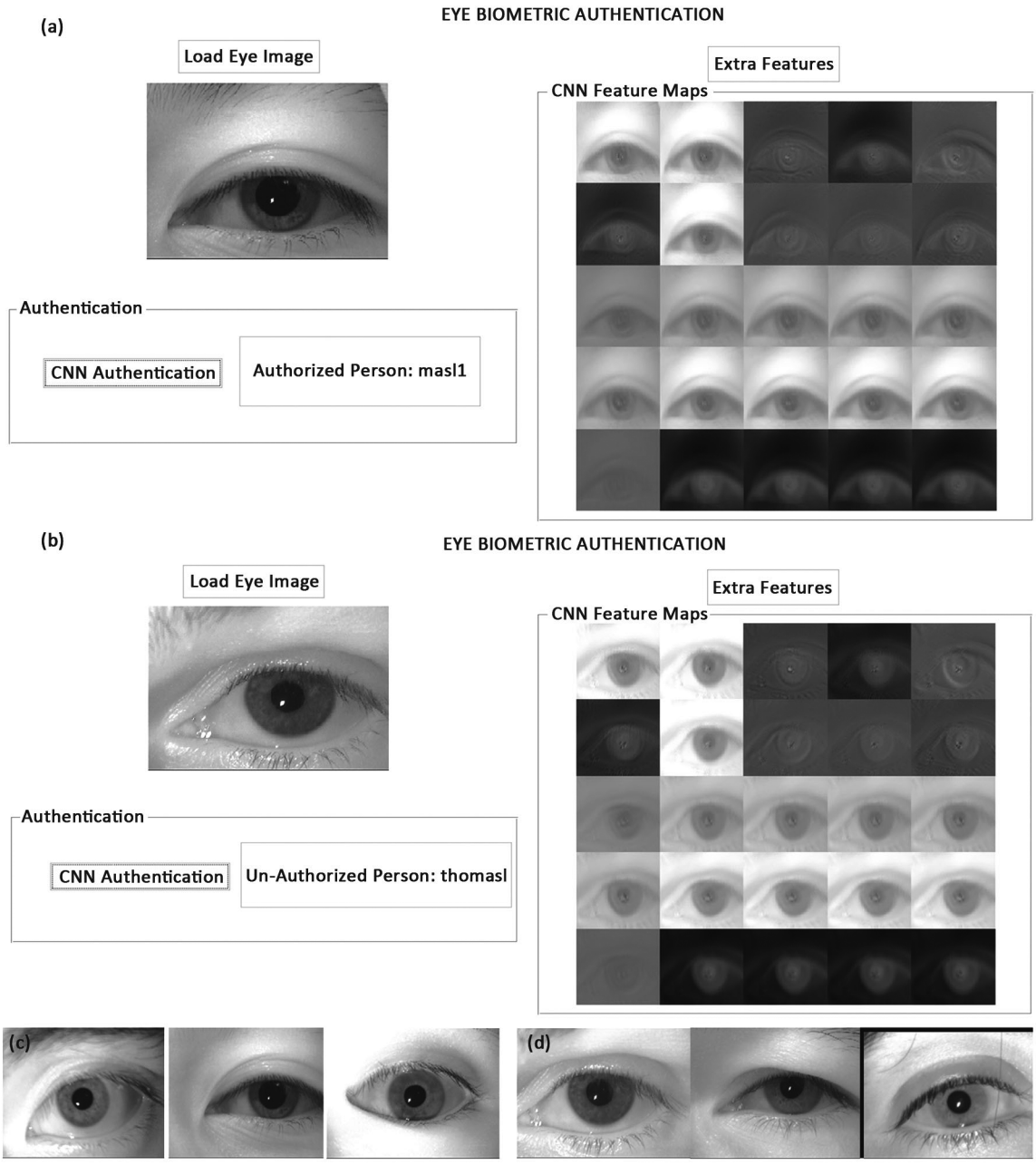

Fig. 5 — Simulation screenshot for (a) Genuine case (Authorized), (b) Imposter case, (Un-Authorized), (c) Genuine case iris images, (d) Imposter case iris images

a hybrid classifier obtained 95.6% of AIRR. In contrast, the iris recognition system using the SVM classifier got 90.3% of AIRR, the iris recognition system using the NN classifier obtained 91.7% of AIRR and the iris recognition system using Adaboost classifier obtained 91.4% of AIRR. The implemented iris recognition system using a hybrid classification algorithm is shown in Table 2, provides a higher AIRR value than the conventional classification approaches.

Further, the performance of the proposed iris recognition system is evaluated with respect to the following parameters by Eqs (6–10).

$$Sensitivity(Se) = \frac{TP}{TP+FN} \quad \ldots (6)$$

$$Specificity(Sp) = \frac{TN}{FP+TN} \quad \ldots (7)$$

$$Accuracy(Acc) = \frac{TP+TN}{TP+TN+FP+FN} \quad \ldots (8)$$

Table 1 — Computation of Recognition rate of the proposed iris recognition system

Parameters	Values
Number of genuine case iris images tested	210
Number of genuine iris images identified correctly	203
GRR	96.6%
Number of imposter case iris images tested	112
Number of imposter iris images identified correctly	106
IRR	94.6%

Table 2 — Average Recognition rate by various classifiers

Classifiers	Average iris recognition rate (AIRR) in %
Hybrid Classifier (Current article)	95.6
Support Vector Machine (SVM)[13]	90.3
Adaboost classifier[14]	91.4
Neural Networks (NN)[15]	91.7

Cases	Actual Positive	Actual Negative
Predicted Positive	TP	FP
Predicted Negative	FN	TN

Fig. 6 — Confusion Matrix

$$FalsePositiveRate(FPR) = \frac{FP}{TN+FP} \quad \ldots (9)$$

$$FalseNegativeRate(FPR) = \frac{FN}{TP+FN} \quad \ldots (10)$$

where, TP = True Positive; TN= True Negative; FP= False Positive; FN= False Negative

The sensitivity, specificity, and accuracy value should be high for the best iris recognition system. Also, the value of FPR and FNR should be low for the best iris recognition system. All these performance measuring parameters are in percentage.

In this article, TP is the correctly identified genuine case iris images, TN is the correctly identified imposter case iris images, FP is the wrongly identified genuine case iris images, and FN is the wrongly identified imposter case iris images. In this article, TP is 203, TN is 106, FP is 07, and FN is 06. The relation between each computational parameter is depicted by the Confusion Matrix (CM), which is given in Fig. 6. The experimental results of the proposed iris recognition system are shown in Table 3, in terms of sensitivity, specificity, accuracy, false-positive rate, and false-negative rate.

From Table 4, it is observed that the comparisons of iris recognition systems of the proposed approach with other conventional methods Ghosh *et al.*[14], Jayanthi *et al.*[15], Galla *et al.*[11], Lin *et al.*[13] and Chaturvedi *et al.*[12] This article's proposed iris recognition system obtained 97% of Se, 93.8% of Sp, 95.9% of Acc, 6.1% of FPR, and 2.8% of FNR. It is

Table 3 — Experimental results by the proposed iris recognition system

Parameters	Experimental results in %
Sensitivity (Se)	97
Specificity (Sp)	93.8
Accuracy (Acc)	95.9
False Positive Rate (FPR)	6.1
False Negative Rate (FNR)	2.8

Table 4 — Comparisons of iris recognition systems

Methodologies	Experimental results in %				
	Se	Sp	Acc	FPR	FNR
Proposed work	**97**	**93.8**	**95.9**	**6.1**	**2.8**
Ghosh *et al.*[11]	94.7	90.6	91.9	12.8	8.7
Jayanthi *et al.*[12]	93.2	90.7	91.3	10.7	7.9
Galla *et al.*[13]	92.8	89.9	90.7	11.8	8.5
Lin *et al.*[14]	91.7	89.6	91.7	11.5	8.9
Chaturvedi *et al.*[15]	90.5	89.9	90.4	12.6	8.6

Table 5 — Performance analysis of iris recognition system in terms of detection time using various classifiers

Classifiers	Detection time (ms)
Hybrid Classifier (current article)	**1.38**
Support Vector Machine (SVM)[13]	4.83
Adaboost classifier[14]	4.29
Neural Networks (NN)[15]	3.27

Table 6 — Comparisons of iris recognition systems in terms of detection time

Methodologies	Detection time (ms)
Proposed work	1.38
Ghosh *et al.*[11]	7.67
Jayanthi *et al.*[12]	8.14
Galla*et al.*[13]	7.98
Lin et al.[14]	8.38
Chaturvedi *et al.*[15]	9.10

clear from Table 4, that the proposed iris recognition system using a hybrid classifier obtains higher performance than the other conventional methods in terms of Se, Sp, Acc, FPR, and FNR.

Detection time is another performance evaluation parameter that is used to estimate the execution time for identifying the genuine case or imposter case iris image. It is measured in milliseconds. The detection time should be low as possible. The system's performance is high if the detection time of the iris recognition system is inadequate. The performance analysis of the iris recognition system in terms of detection time using various classifiers is given in Table 5. It can be seen that the implemented iris recognition system using a hybrid classifier consumed less detection time than the other classifiers, SVM, NN, and Adaboost. The detection time (ms) of the implemented iris recognition system with other conventional methods are illustrated in Table 6

Conclusions

The hybrid classification approach is proposed in this work for biometric authentication. This proposed work integrates deep learning and machine learning algorithms to improve iris recognition rates. The ANFIS classifier classifies the feature maps generated by the CNN classifier. In this article, the value of GRR is 96.6% by correctly identifying 203 genuine case iris images over 210 genuine case images. Also, the value of IRR is 94.6% by correctly identifying 106 imposter case iris images over 112 imposter case images. Therefore, the AIRR is computed by averaging the value of GRR and IRR. Hence, the AIRR value is about 95.6%. This article's proposed iris recognition system obtained 97% of Se, 93.8% of Sp, 95.9% of Acc, 6.1% of FPR, and 2.8% of FNR. The algorithms proposed in this work can be extended to recognize the real-time iris images directly captured by the mobile phone.

References

1 Li X, Wang K, Shen J, Saru K, Fan W & Yonghua H,An enhanced biometrics-based user authentication scheme for multi-server environments in critical systems, *J Ambient Intell Humaniz Comput* **7** (2016) 427–443.

2 Srivastava V, Tripathi B K & Pathak V K, Biometric recognition by hybridization of evolutionary fuzzy clustering with functional neural networks, *J Ambient Intell Humaniz Comput*, **5(4)** (2014) 525–537.

3 Sallam A, Amery H A, Al-Qudasi S, Al-Ghorbani S, RassemT H & Makbol N M, Iris recognition system using convolutional neural network, *Int Conf Softw Eng Comput Syst 4th Int Conf Comput Sci Info Manag (ICSECS-ICOCSIM)* (Virtual mode) 24th – 26th Aug, 2021, 109–114.

4 Aro T, Jibrin M, Matiluko O, Abdulkadir I & Oluwaseyi I, Dual feature extraction techniques for iris recognition system, *Int J Softw Eng Comput Syst*, **5(1)** (2019) 1–15.

5 Minaee S, Abdolrashidiy A & Wang Y, An experimental study of deep convolutional features for iris recognition, *IEEE Signal Process Med Biol Symp (SPMB)* (2016) 1–6.

6 Zanlorensi L A, Luz E, Laroca R, Britto A S, Oliveira L S & Menotti D, The impact of preprocessing on deep representations for iris recognition on unconstrained environments, *31st SIBGRAPI Conf Graphics Patterns Images (SIBGRAPI)*(Parana, Brazil) 29th Oct – 1st Nov 2018, 289–296.

7 Nguyen K, Fookes C, Ross A & Sridharan S, Iris recognition with off-the-shelf CNN features: A deep learning perspective, *IEEE Access*, **6** (2017) 18848–18855.

8 Liu M, Zhou Z, Shang P & Xu D, Fuzzified image enhancement for deep learning in iris recognition, *IEEE Trans Fuzzy Syst* **28(1)** (2019) 92–99.

9 Chuang C W & Fan C P, Deep-learning based joint iris and sclera recognition with yolo network for identity identification, *J Adv Inf Technol*, **12(1)** (2021) 60–65.

10 Al-Shoukry S, Rassem T H & Makbol N M, Alzheimer's diseases detection by using deep learning algorithms: a mini-review, *IEEE Access*, **8** (2020) 77131–77141.

11 Ghosh U B, Sharma R & Kesharwani A, Symptoms-based biometric pattern detection and recognition, augmented intelligence in healthcare: A pragmatic and integrated analysis, in *Studies in Computational Intelligence* (Springer) 2022, 371–399.

12 Jayanthi J, Lydia E L, Krishnaraj N, Jayasankar T, Babu R L & Suji R, An effective deep learning features based integrated framework for iris detection and recognition. *J Ambient Intell Humaniz Comput*, **12** (2021) 3271–3281.

13 Galla D K K, Mukamalla B R & Chegireddy R P R, Support vector machine based feature extraction for gender recognition from objects using lasso classifier, *J Big Data*, **7(1)** (2020) 1–16.

14 Lin Y N, Hsieh T Y & Huang J J, Fast Iris localization using HAAR-like features and AdaBoost algorithm, *Multimed Tools Appl*, **79** (2020) 34339–34362.

15 Chaturvedi R & Thakur Y S, Iris Recognition using Daugman's Algorithm and ANN, *Int J Appl Eng Res*, **14(21)** (2019) 3987–3995.

16 Hassanzadeh Y, Jafari-Bavil-Olyaei A, Aalami M T & Kardan N, Experimental and numerical investigation of bridge pier scour estimation using ANFIS and teaching–learning-based optimization methods, *Eng Comput*, **35** (2019) 1103–1120.

17 https://www.kaggle.com/datasets/naureenmohammad/mmu-iris-dataset (13/03/2022)