The Visual Computer (2023) 39:1571–1581
https://doi.org/10.1007/s00371-022-02429-x

ORIGINAL ARTICLE

Multi-instance cancelable iris authentication system using triplet loss for deep learning models

Mulagala Sandhya[1] · Mahesh Kumar Morampudi[2] · Indragante Pruthweraaj[1] · Pranay Sai Garepally[1]

Accepted: 25 January 2022 / Published online: 22 February 2022

Abstract
Many government and commercial organizations are using biometric authentication systems instead of a password or token-based authentication systems. They are computationally expensive if more users are involved. To overcome this problem, a biometric system can be created and deployed in the cloud which then can be used as a biometric authentication service. Privacy is the major concern with cloud-based authentication services as biometric is irrevocable. Many biometric authentication systems based on cancelable biometrics are developed to solve the privacy concern in the past few years. But the existing methods fail to maintain the trade-off between speed, security, and accuracy. To overcome this, we present a multi-instance cancelable iris system (MICBTDL). MICBTDL uses a convolutional neural network trained using triplet loss for feature extraction and stores the feature vector as a cancelable template. Our system uses an artificial neural network as the comparator module instead of the similarity measures. Experiments are carried on IITD and MMU iris databases to check the effectiveness of MICBTDL. Experimental results demonstrate that MICBTDL accomplishes fair performance when compared to other existing works.

Keywords Cancelable biometrics · Privacy-preserving · Triplet loss · Convolutional neural network · Artificial neural network

1 Introduction

Nowadays, the use of passwords is becoming obsolete for important tasks in many organizations and they have been moving to biometric authentication. According to a report given by Verizon [1], it has been observed that passwords are responsible for 81% of the data breaches. This can be eliminated by using biometric systems. Biometric authentication is more secure because it is harder to recreate or forge due to their distinctive features and they are unique for each person [2,3].

Biometric traits are body measurements and calculations associated with human characteristics. The physical traits such as iris, fingerprint, finger vein, etc, can be used to identify an individual and distinguish them from others [2,3]. Iris is considered as the widely accepted biometric trait due to features like uniqueness and stability [4,5]. Enrollment and verification are the two phases involved in a biometric system. In the enrollment phase, the reference biometric is captured and the features are extracted from it by a feature extractor. A reference template is generated from these features using the template generator and stored in a template database. During the authentication phase, the features are extracted from the query biometric using the feature extractor, and a query template is generated. The comparator module compares the query template with the templates stored in the database. Then the comparator returns the verification decision. The comparator returns the accept decision if the query template and reference template belongs to the same user otherwise it returns the reject decision. The feature extractor should be good at extracting the features from

✉ Mahesh Kumar Morampudi
morampudimahesh@gmail.com
https://srmap.edu.in/faculty/dr-m-mahesh-kumar/

Mulagala Sandhya
msandhya@nitw.ac.in

Indragante Pruthweraaj
indragantipruthviraj@gmail.com

Pranay Sai Garepally
pranaysai27@gmail.com

[1] Department of Computer Science and Engineering, National Institute of Technology, Warangal, Telangana 506004, India

[2] Department of Computer Science and Engineering, School of Engineering and Applied Sciences, SRM University - AP, Neerukonda-Kurugallu Village, Mangalagiri Mandal 522 502, Andhra Pradesh, India

the biometric data so that it can accurately differentiate the genuine and imposter user. Feature extractor plays a crucial role in a biometric system and the accuracy of the biometric system depends very much on the feature extractor.

The use of multiple instances of biometric information to recognize and authenticate an individual is known as multi-instance biometrics. Multi-instance biometric systems are more secure because it is harder for the attacker to manipulate multi-instance biometrics [2]. Deep learning-based models are widely explored in many fields of computer science nowadays. Their ability to learn patterns, extract features from given data is essential for day-to-day problems. Training a stable and robust deep learning-based model requires enough training examples, which may be impractical in many real-world scenarios [6]. A convolutional neural network inspired by AlexNet is used for feature extraction in our system to avoid the mentioned limitation.

Cloud computing has been getting very popular in recent years due to its large computing power, data storage, and scalability. Fraudulent activities can be reduced by performing biometric authentication on the cloud. Cloud was already used for biometric authentication in mobile phones [7]. But, biometric authentication on the cloud has problems like the privacy of the biometric template on the cloud [8]. Indeed, it has been shown that iris images can be reconstructed from templates [9,10]. Therefore, biometric template protection schemes such as cancelable biometrics [11], bio-cryptosystems [12] and homomorphic encryption (HE) [13] are introduced and has been applied successfully in recent years to achieve the required template protection. However, HE schemes suffer from considerable computational requirements [13]. In the literature, several works are proposed in the biometric field to provide the privacy of templates using cancelable biometrics [14–18]. But they fail to maintain the trade-off between speed, security, and accuracy.

As a contribution to the aforementioned challenges, this paper proposes a cancelable iris authentication system (MICBTDL), which uses a convolutional neural network (CNN) trained using triplet loss for feature extraction. The artificial neural network (ANN) is used as a comparator module to compare the reference template and query template. MICBTDL uses both random projection and random crossfolding to achieve the irreversibility requirement of the biometric template protection scheme. As a result, our system is more secure when compared to the state-of-the-art approaches. In addition, our proposed system does not use any tool kits like the University of Salzburg Tool Kit [19] to extract the features of an iris image. So, our method can be applied to any other biometric trait also. MICBTDL is evaluated on MMU and IITD iris databases to check its efficiency. MICBTDL can solve attacks like modify template and intercept channel of biometric authentication system.

The rest of this article is structured as follows: Sect. 2 presents about the state-of-the-art approaches. Section 3 describes our proposed system. Subsequently, the experimental evaluation and its results are presented in Sects. 4 and 5 offers our conclusion.

2 Related works

In recent years, deep learning models have been showing very promising results in improving the accuracy of many biometric authentication systems. Specifically, convolutional neural networks (CNNs) are the most successful and widely used architecture in the deep learning community.

Sibai et al. [20] designed an iris recognition system by using feed-forward artificial neural network. Authors conducted several experiments by varying the input format, number of hidden layers, and the number of neurons in the hidden layer to find the optimal parameters. Khedkar and Ladhake [21] proposed an iris recognition system using neural network techniques such as radial basis function (RBF), support vector machines (SVM), & multi-layer perceptron (MLP). Two feature extraction techniques, namely Haar wavelet decomposition & 1D Log Gabor wavelet used in a method proposed by Rai et al [22]. The iris patterns are identified with Hamming distance and SVM. Srivastava et al. [23] implemented an approach for iris recognition by combining functional modular neural networks and evolutionary fuzzy clustering. Saminathan et al. [24] introduced a method for iris authentication by using kernel-based multi-class SVM. Marsico et al. [25] presented a survey of machine learning techniques ranging from neural networks to deep learning for iris recognition. Ahmadi et al. [26] suggested a recognition system which used MLP and particle swarm optimization to increase generalization performance. Later to reduce the computational complexity, Ahmadi et al. used a genetic algorithm with RBF. Fahim et al. [27] proved the feasibility of machine learning techniques to recognize a person with iris modality even if an eye image is captured through a smartphone.

Ahmadi et al. [28] designed a biometric system by using MLP-imperialist competitive algorithm (MLP-ICA) as a classifier. The authors used a Gray-level difference matrix to obtain the features from the iris. The softmax classifier and convolutional neural network (CNN) are used to obtain the features from the iris image and classify the user into any of the N classes by Waisy et al. [29]. When compared to state-of-the-art works, the performance is better for this method. Arsalan et al. [30] proposed a method by using deep learning to determine the true iris region without pre-processing the eye image. Zhao and Ajay [31] suggested a framework to accurately detect, segment the iris images by using the fully convolutional network. Zhao and Ajay [31] introduced an

“Extended Triplet Loss (ETL)” function to learn the spatially corresponding features of an iris image. A cross-spectral iris recognition system is designed by Wang et al. [32]. The features are extracted by using CNN and supervised discrete hashing (SDH) is used for compression and classification. Admovic et al. [33] proposed an approach for iris recognition by using stylometric features and random forest machine learning methods. The hybrid-based particle swarm optimization (PSO) is used as a classifier and proposed an iris recognition system by Gale et al. [34]. Hybrid-based PSO is a combination of a weighted directed acyclic graph (DAG) SVM and spiking neural networks (SNN). The classification task is achieved by weighted DAG SVM and evaluation is achieved by SNN. Sudhakar et al. [35] proposed a cancelable biometric system using a feature extractor based on deep learning for extracting iris features and then used a random projection technique to convert the extracted features into a cancelable template. Later in 2020, they suggested a cancelable biometric system [36] based on the cloud which has the server on the cloud and a client is connected to the server for authentication. El-Hameed et al. presented a scheme to preserve the privacy of fingerprint templates using the advanced chaotic maps [14]. Abdellatef et al. [15] proposed a cancelable multi-biometric face recognition method using bio-convolving encryption. A novel cancelable multi-modal biometric system in which iris and fingerprint are fused using the projection-based approach is proposed by Gupta et al. [16] The feature points are projected onto a random plane obtained using a user-specific key to generate the cancelable template. Mahesh et al. [37] proposed a novel privacy-preserving iris authentication using fully homomorphic encryption.

The state-of-the-art works fail to maintain the trade-off between accuracy, speed, and security. Therefore, MICBTDL is proposed to achieve high accuracy and provide confidentiality to the iris templates.

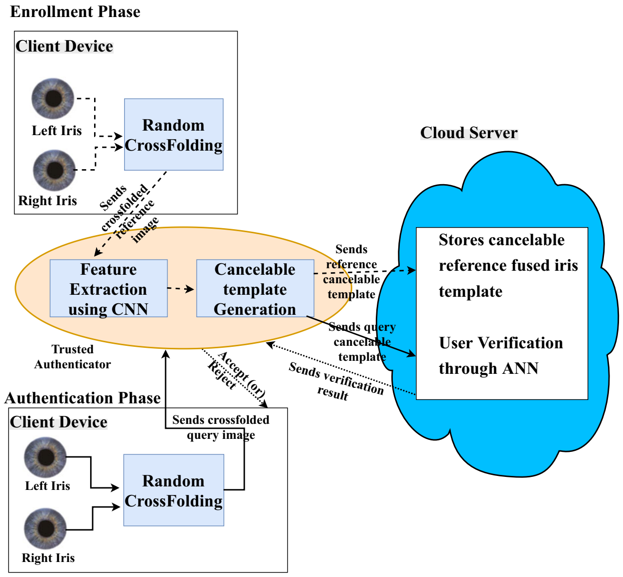

Enrollment Phase
Client Device
Left Iris
Right Iris
Random CrossFolding
Sends crossfolded reference image
Feature Extraction using CNN
Cancelable template Generation
Trusted Authenticator
Sends reference cancelable template
Cloud Server
Stores cancelable reference fused iris template
User Verification through ANN
Sends query cancelable template
Sends verification result
Accept (or) Reject
Authentication Phase
Client Device
Left Iris
Right Iris
Random CrossFolding
Sends crossfolded query image

Fig. 1 Block diagram of MICBTDL. The steps during the enrollment, authentication and after the authentication phases are indicated with dashed, solid and dotted lines

3 Multi-instance cancelable iris authentication using triplet loss for deep learning models (MICBTDL)

MICBTDL is the first multi-instance cancelable iris authentication system using triplet loss as a loss function during the training phase of deep learning models. Triplet loss [38] is a loss function that is used for training machine learning models by comparing an anchor image to a positive and a negative image [39,40]. The models trained using triplet loss are generally good at distinguishing between images of the same class and images of different classes [39]. For some cases like biometric authentication, triplet loss is better for training the network compared to the Softmax cross-entropy loss which contains a fixed number of classes and trains the classification model. In biometric recognition, we need to be able to compare two unknown biometrics and be able to declare whether the biometrics are of the same person or not. The models are trained such that the outputs of the positive image and anchor image are close and at the same time outputs of the negative image and anchor image are far away. In MICBTDL, a convolutional neural network inspired by AlexNet is used for feature extraction which is the most crucial part of biometric authentication. For user authentication, a Multi-layer Perceptron network which is a fully connected network of neurons is used after which Euclidean distance is used to compare the distance between outputs of template image and test image.

Figure 1 depicts the flow diagram of MICBTDL. It consists of three entities namely, the client device, the cloud server, and the trusted authenticator. MICBTDL consists of two phases, enrollment and authentication phases. The steps during the enrollment phase are given as below:

1. The client device acquires the reference right and left iris images.
2. The client device applies the random crossfolding and transforms the cross folded images to the trusted authenticator.
3. The trusted authenticator extracts the features using CNN.
4. The trusted authenticator generates the reference cancelable template and sends to the cloud server.

The steps during the authentication phase are given as below:

1. The client device acquires the probe left and right iris images.
2. The client device applies the random crossfolding and transforms the cross folded images to the trusted authenticator.
3. The trusted authenticator extracts the features using CNN.
4. The trusted authenticator generates the reference cancelable template and sends to the cloud server.
5. The cloud server performs the verification through ANN and sends the verification result to the trusted authenticator.
6. The trusted authenticator compares the verification result with threshold and transmits the reject/accept decision to the client device.

3.1 Assumptions

MICBTDL assume the following

1. The client device has limited computational & memory resources. It is a trusted entity during the authentication and enrollment phases.
2. The cloud server performs the computations honestly but curious to view the data.
3. The trusted authenticator is a semi-trusted entity.

3.2 Image capture and random crossfolding

In this phase, the right and left iris images are captured from the user and random crossfolding is applied. First, both the images are resized to 192 x 192 pixels, and then a random matrix of the same size is generated. The generated random matrix is converted to the binary matrix which is then multiplied to the left iris image and its complement is multiplied to the right iris image. In this way, we generate a random cross folded image in which half of the pixels are of the left iris and the other half are of the right iris. The illustration of random crossfolding can be seen in Fig. 2.

The generated random crossfold ensures the safety of the original biometric. Even if the random crossfold is compromised, the original biometric is safe because the random crossfold contains half pixels of the left iris and the other half pixels are of the right iris. So, when the user feels the random crossfold is compromised, the user can just change the user key just as how he changes a password, and then a new random matrix is generated from the new user key which then generates a new random crossfolded template which is different from the previous one because the random matrix has changed. Now, the user will be authenticated using the new user key. The crossfolded images are given as an input to CNN for feature extraction.

3.3 Feature extraction through deep learning

Feature extractor is the most crucial component in a biometric system that decides its performance of it. In this biometric system, a convolutional neural network performs feature extraction from the crossfolded images. First, the crossfolded images (192x192px) are normalized using greyscale normalization. The CNN architecture can be visualized in Fig. 3.

Conv1 is a pair of convolution layers with 16 filters. Conv2 is a pair of convolution layers with 32 filters. Conv3 is a pair of convolution layers with 64 filters. Convolution is done by parsing the kernel filter over the entire image. Every convolution layer is followed by the max pool layer and dropout layer. Max pool layer is used for dimensionality reduction of the output of convolution layers. Max pool layers reduce computation cost and also prevent over-fitting The dropout layer is used for regularization, i.e., it ignores weights randomly making the CNN model learn in a regularized way. In the proposed model, the ReLU activation function is used to increase the nonlinearity in the images. Finally, a flatten layer is used after 3 convolution layers which are followed by a dense layer containing 256 neurons. Triplet loss is a loss function that is used for training machine learning models by comparing an anchor image to a positive and a negative image. The models trained using triplet loss are generally good at distinguishing between images of the same class and images of different classes.

For training a model using triplet loss, we need the input data to be in the form of triplets. Each triplet has an Anchor image at index 0, a Positive image at index 1, and a Negative image at index 2. We generate the database of triplets as follows, first, we select a random class and pick an anchor image from it randomly and then a positive image from the same class randomly (other than anchor). Later a different class is chosen and pick a random image (as a negative image) from it.

A triplet loss layer is added at the end of our CNN model. The architecture of triplet loss is shown in Fig. 4. Each triplet is fed into the CNN model and then the triplet loss layer modifies weights in the CNN model such that the outputs of the positive image and anchor image are close and at the same time outputs of the negative image and anchor image are far away. In this way, the CNN model is trained, and then the triplet loss layer is removed from the model to extract outputs of size 256×1 from the final dense layer.

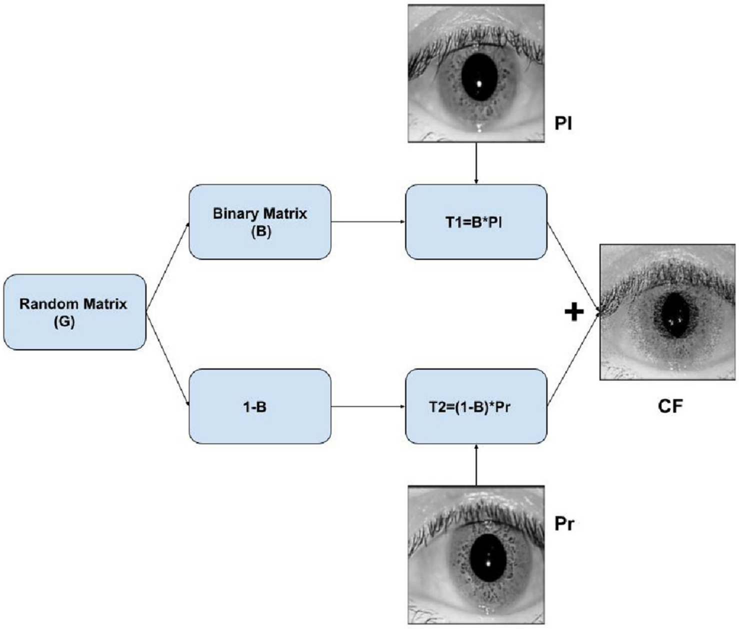


Fig. 2 Illustration of Random Crossfolding

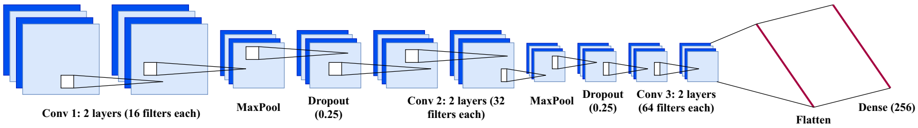

Conv 1: 2 layers (16 filters each)
MaxPool
Dropout (0.25)
Conv 2: 2 layers (32 filters each)
MaxPool
Dropout (0.25)
Conv 3: 2 layers (64 filters each)
Flatten
Dense (256)

Fig. 3 Schematic representation of Convolutional Neural Network

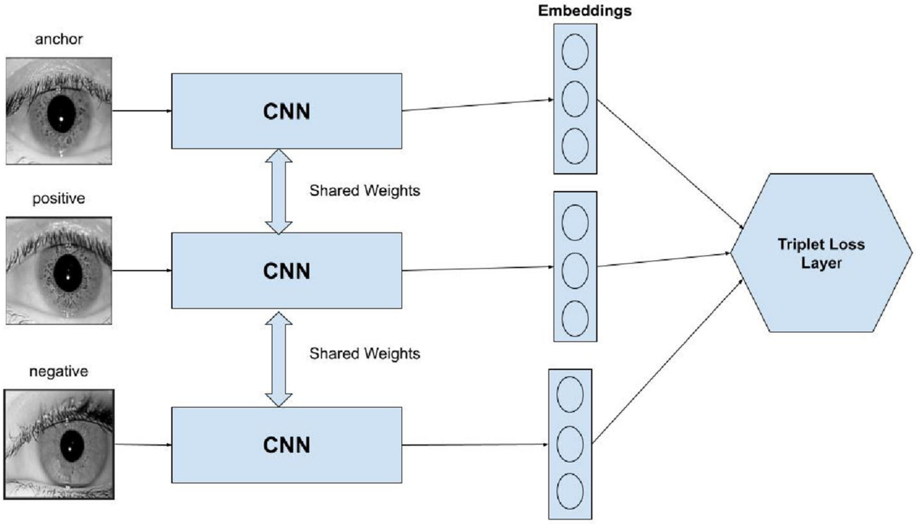


Fig. 4 Triplet loss Architecture

3.4 Cancelable template generation

Random projection is used in this phase to store the biometric template. Cancelable biometrics is achieved in this system by transformations such as random crossfolding and random projection. Random orthogonal matrices are generated using user keys which are then multiplied by the feature vectors to generate the cancelable templates. So, the original biometrics are not stored on the cloud and even if this cancelable biometric template is compromised, the user can change his/her user key just as he changes his/her password to generate a new template.

3.5 User verification through artificial neural network

An artificial neural network (ANN) is a fully connected network of neurons in which the input is passed forward layer by layer. The input to this ANN model is the feature vectors extracted from the CNN model. The schematic representa-

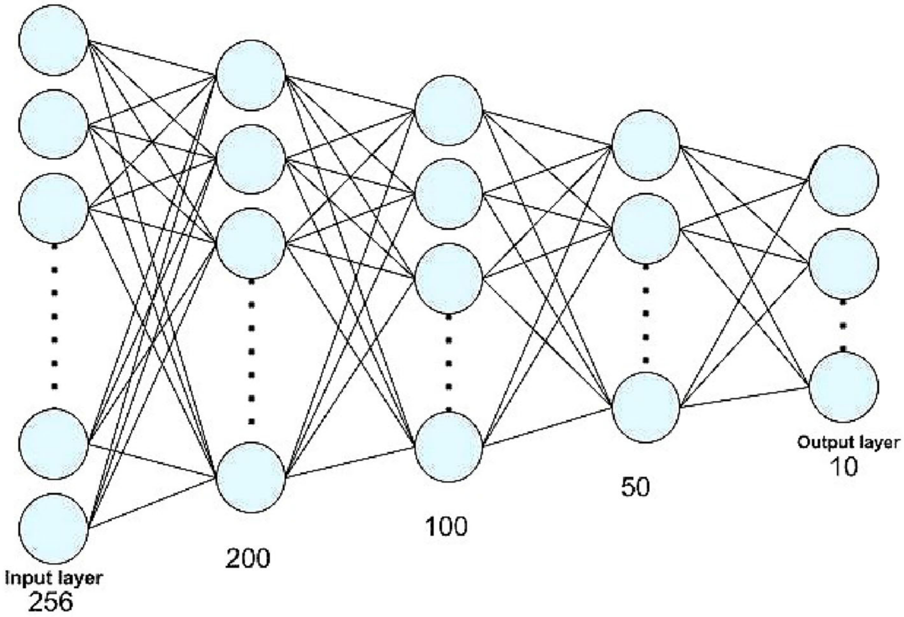


Fig. 5 Schematic Representation of Artificial Neural Network

tion of the ANN model is shown in Fig. 5. The ANN model consists of dense layers with 256, 200, 100, 50, 10 neurons at each layer, respectively. L2 normalization is done on the output layer. The ANN model is trained using triplet loss in the same way as the CNN model. Triplets are created from feature vectors. Euclidean distance between the reference random projected feature vector and the query random projected feature vector is computed and used for the verification decision. If the distance exceeds the threshold, the user is an imposter otherwise he/she is genuine.

4 Results and observations

4.1 Experimental design

MICBTDL is experimented on MMU[1] and IITD [19] iris database. The details of the database are listed in Table 1. The IITD iris database consists of 225 subjects. Since 208 subjects from the IITD database contains both left and right iris images with a minimum of 5 samples each. Therefore, we consider 208 subjects to conduct our experiments and exclude other subjects. The experiments of MICBTDL are trained on a GPU workstation (SuperMicro 7039, Dual Intel Xeon Silver processor 4110, CUDA enabled NVIDIA GPU card Geforce GTX1080Ti, 2 GPU). Further, the Tensor Flow and Keras were applied.

4.2 Performance analysis

We carried out experiments on IITD and MMU databases. IITD database has 2080 images (208 subjects-five right and five left iris images of each subject). MMU database has 450 images (45 subjects - five left and five right iris images of each subject). The metrics like false accept rate (FAR), false reject rate (FRR), genuine accept rate (GAR), and equal error rate (EER) are considered to check the performance of MICBTDL.

The baseline comparison of MICBTDL is shown in Table 2. We can infer from Table 2 that the fusion of left and right iris images using random crossfolding increases the performance. Even though there is a slight degradation in the performance after applying the random crossfolding and random projection, the privacy of the iris template is preserved. Figures 6a, 7a shows loss and Figs. 6b, 7b shows accuracy for each epoch during the training of CNN on MMU and IITD iris databases. Figure 8 shows the Receiver Operating Characteristic (ROC) curve of CNN and ANN on the MMU and IITD iris database. The FAR and FRR distributions of MICBTDL on MMU and IITD databases are shown in Fig. 9. We fine tune the important parameters of CNN such as Margin for Triplet loss, iterations, dropout and ANN such as Margin for Triplet loss, iterations. We can infer that when the epoch increases, loss decreases, and the accuracy increases when the epoch increases. At some point, even with the increase in epoch, there is no change in the accuracy. The margin for triplet loss and the number of iterations plays an important role. The parameters of CNN and ANN considered in MICBTDL are shown in Tables 3 and 4. It is observed that

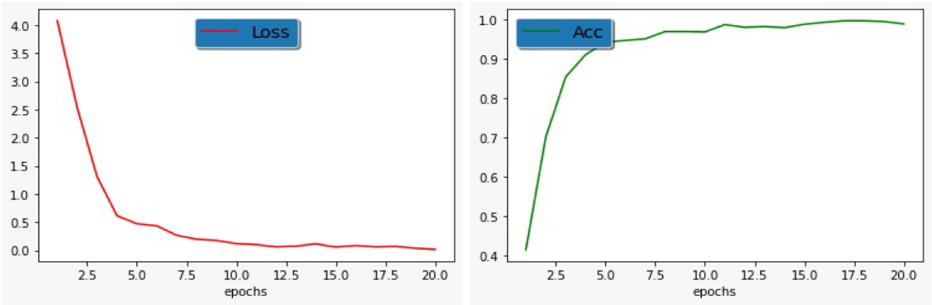
[1] http://pesonna.mmu.edu.my/ccteo/.

Table 1 Description of the database

Database	Number of subjects	Number of left iris samples	Number of right iris samples
MMU	45	225	225
IITD	208	1040	1040

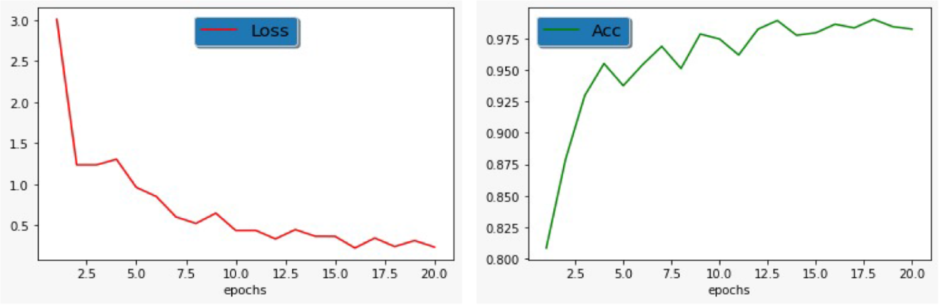
Table 2 Baseline Comparison of MICBTDL

Database	Template type	EER (in %)
IITD	Only left iris (without random crossfolding and random projection)	0.1295
	Only right iris (without random crossfolding and random projection)	0.1248
	With Random Crossfolding, without Random Projection	0.05
	With Random Crossfolding and random projection	0.06
MMU	Only left iris (without random crossfolding and random projection)	0.0965
	Only right iris (without random crossfolding and random projection)	0.094
	With Random Crossfolding, without Random Projection	0.04
	With Random Crossfolding and random projection	0.03



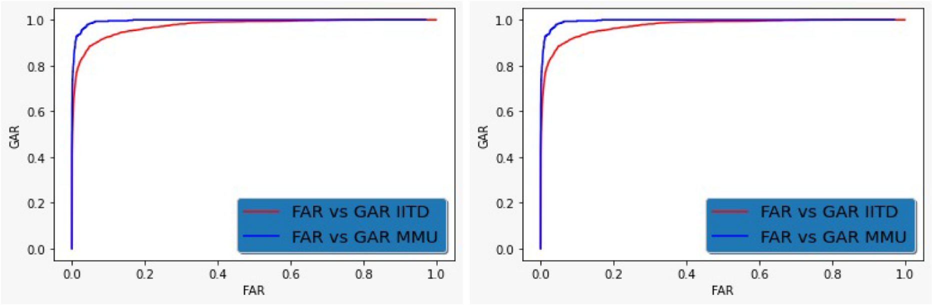
(a) (b)

Fig. 6 CNN training curves a) Loss vs Epochs b) Accuracy vs Epochs on MMU dataset



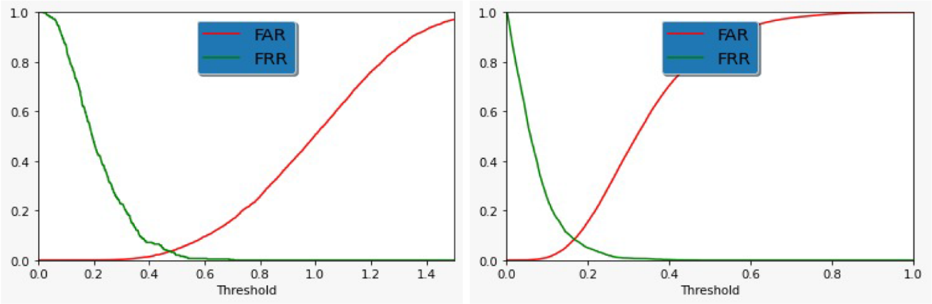
(a) (b)

Fig. 7 CNN training curves a) Loss vs Epochs b) Accuracy vs Epochs on IIT database



(a) (b)

Fig. 8 Performance evaluation. ROC curves of a) CNN b) ANN on MMU, IIT databases



(a)

(b)

Fig. 9 FAR and FRR distributions of proposed model on a) MMU b) IITD databases

Table 3 Parameters of CNN considered in MICBTDL

Database	Margin for Triplet loss	Iterations	Dropout	EER (in %)
IITD	0.15	45	0.25	0.18
	0.15	50	0.25	0.15
	0.2	45	0.25	0.11
	0.2	50	0.25	0.08
	0.2	55	0.25	0.08
MMU	0.15	45	0.25	0.13
	0.15	50	0.25	0.10
	0.2	45	0.25	0.08
	0.3	45	0.25	0.06
	0.3	50	0.25	0.03
	0.3	55	0.25	0.03

Table 4 Parameters of ANN considered in MICBTDL

Database	Margin for Triplet loss	Iterations	EER (in %)
IITD	0.15	45	0.21
	0.15	50	0.13
	0.2	45	0.10
	0.2	50	0.06
	0.2	55	0.06
MMU	0.15	45	0.13
	0.15	50	0.10
	0.2	45	0.08
	0.3	45	0.06
	0.3	50	0.03
	0.3	55	0.03

an optimal EER of **0.03**, **0.08** and **0.03**, **0.06** for CNN and ANN on MMU, IITD iris databases.

4.3 Security analysis

4.3.1 Irreversibitlity analysis

Cancelable iris templates are generated in MICBTDL by using two one-way transformations: 1) Random CrossFolding and 2) Random Projection. In random crossfolding, a random matrix (X) of size 128 × 128 is generated with the user key (U). A binary matrix (Y) of size 128 × 128is obtained by using X. An orthogonal matrix (G) is generated using the user key in random projection. The cancelable template (C) is formed by multiplying the crossfolded iris images with G.

The original iris images cannot be reconstructed by using the generated cancelable template & user key because:

1. It is infeasible to reconstruct X due to the possible combinations in the range of $10^{1}0^{128 \times 128}$. $2^{128 \times 128}$ combinations are required to construct Y.
2. Furthermore, it is very difficult to obtain G from C. The required number of combinations are in the order $10^{10^{256}}$, making it extremely difficult to achieve the same cross-folded feature image.

4.3.2 Revocability

The iris images cannot be generated from the cancelable template because of irreversibility. But, there is a possibility of compromising the cancelable template. In that scenario, the old cancelable iris template is replaced with a new cancelable iris template by changing the user key. A new random matrix is generated which is completely different from the previous one.

4.3.3 Diversity

Different cancelable iris templates are created from the original iris images by changing the user keys. There won't be any relationship between the generated cancelable templates.

4.4 Comparison analysis

From Table 5, we can see that the CNN in MICBTDL has a better EER for both IITD and MMU Dataset. The difference in EER is very significant for the MMU dataset because it has fewer users. The CNN in [36] needs more data for efficient feature extraction whereas the CNN in MICBTDL learns

Table 5 Comparison of MICBTDL with other feature extraction techniques (EER in %)

Dataset	Method	EER
MMU	5 × 5 Blocks of Avg Pixel Intensities [41]	0.86
	Log Gabor	0.42
	Raw Pixel Intensities [41]	0.76
	CNN in [36]	0.15
	CNN in MICBTDL	**0.03**
IITD	5 × 5 Blocks of Avg Pixel Intensities	0.62
	Log Gabor [42]	0.38
	Raw Pixel Intensities	0.50
	CNN in [36]	0.12
	CNN in MICBTDL	**0.08**

Table 6 Comparison of MICBTDL with existing works (EER in %)

Dataset	Method	EER
MMU	Sudhakar *et al*[36]	0.14
	MICBTDL	**0.03**
IITD	Rajasekhar et al [43]	0.46
	Gomez-Barrero *et al* [17]	0.7
	Sadhya and Raman [44]	1.4
	Mahesh *et al*[45]	0.88
	Mahesh *et al* [46]	0.88
	Sudhakar *et al* [36]	0.04
	MICBTDL	**0.06**

better even when the number of users is less. The reason to accomplish the fair performance is due to the triplet loss function.

In the same way, from Table 6, we can observe that the MICBTDL achieves significantly fair performance than MLP in [36] for the MMU database and performs better than the other existing methods for the IITD database. The reason for the less performance in [36] is due to the fewer number of users. From the results, it is clear that MICBTDL is suitable for small datasets as well as large datasets.

5 Conclusion and future work

A multi-instance cancelable iris authentication system that uses a CNN trained using triplet loss for feature extraction and store the feature vector as a cancelable template is proposed in this paper. Later MICBTDL uses an ANN network as the matching module. MICBTDL uses triplet loss to train the neural networks so that the networks learn how to differentiate a positive image from a negative image by comparing it with the template(anchor) image. Cancelability of iris templates is ensured with two operations performed on the original iris images (1) Random crossfolding and (2) Random Projection. We experimented MICBTDL on IITD and MMU databases. From the experimental results, we can conclude that MICBTDL accomplishes fair performance when compared to other existing works.

In the future, MICBTDL can be applied to other biometric traits like finger-vein, fingerprint, etc. or a multi-modal system can be proposed as it does not require any preprocessing technique on the images that are specific to the iris. MICBTDL can also be used to safely process 2D images on cloud-based applications. So, this idea can also be extended to cloud-based 3D design.

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Jartelius, M.: The 2020 data breach investigations report-a cso's perspective. Netw. Secur. **2020**(7), 9–12 (2020)
2. Ross, A.A., Nandakumar, K., Jain, A.K.: Handbook of multibiometrics: human recognition systems, vol. 6. Springer (2006)
3. Jain, A.K., Flynn, P., Ross, A.A.: Handbook of biometrics. Springer, New York (2007)
4. Saini, R., Rana, N.: Comparison of various biometric methods. Int. J. Adv. Sci. Technol. **2**(1), 24–30 (2014)
5. Daugman, J.: How iris recognition works. IEEE Trans. Cir. Sys. Video Technol. **14**(1), 21–30 (2004). https://doi.org/10.1109/TCSVT.2003.818350
6. Zhang, G., Chen, K., Xu, S., Cho, P.C., Nan, Y., Zhou, X., Lv, C., Li, C., Xie, G.: Lesion synthesis to improve intracranial hemorrhage detection and classification for ct images. Comput. Med. Imag. Graph. **90**(101929), 1–14 (2021)
7. Zareen, F. J., Shakil, K. A., Alam, M., Jabin, S.: A cloud based mobile biometric authentication framework. CoRR (2016)
8. Prabhakar, S., Pankanti, S., Jain, A.K.: Biometric recognition: security and privacy concerns. IEEE Secur. Priv. **1**(2), 33–42 (2003)
9. Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., Ortega-Garcia, J.: Iris image reconstruction from binary templates: an efficient probabilistic approach based on genetic algorithms. Comput. Vis. Image Underst. **117**(10), 1512–1525 (2013)
10. Venugopalan, S., Savvides, M.: How to generate spoofed irises from an iris code template. IEEE Trans. Inf. Foren. Secur. **6**(2), 385–395 (2011)
11. Patel, V.M., Ratha, N.K., Chellappa, R.: Cancelable biometrics: a review. IEEE Signal Process. Mag. **32**(5), 54–65 (2015)
12. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. **1**, 1–25 (2011)
13. Acar, A., Aksu, H., Uluagac, A.S., Conti, M.: A survey on homomorphic encryption schemes: theory and implementation. ACM Comput. Surv. (CSUR) **51**(4), 1–35 (2018)
14. El-Hameed, H. A. A., Ramadan, N., El-Shafai, W., Khalaf, A.A., Ahmed, H. E. H., Elkhamy, S.E., El-Samie, F. E. A.: Cancelable biometric security system based on advanced chaotic maps. The Visual Computer pp 1–17 (2021)
15. Abdellatef, E., Ismail, N.A., Abd Elrahman, S.E.S., Ismail, K.N., Rihan, M., Abd El-Samie, F.E.: Cancelable multi-biometric recognition system based on deep learning. Vis. Comput. **36**(6), 1097–1109 (2020)

16. Gupta, K., Walia, G.S., Sharma, K.: Novel approach for multimodal feature fusion to generate cancelable biometric. Vis. Comput. **37**(6), 1401–1413 (2021)
17. Gomez-Barrero, M., Rathgeb, C., Li, G., Ramachandra, R., Galbally, J., Busch, C.: Multi-biometric template protection based on bloom filters. Inform. Fus. **42**, 37–50 (2018)
18. Kumar, M.M., Prasad, M.V., Raju, U.: Iris template protection using discrete logarithm. In: proceedings of the 2018 2nd international conference on biometric engineering and applications, pp 43–49 (2018)
19. Rathgeb, C., Uhl, A., Wild, P., Hofbauer, H.: Design decisions for an iris recognition sdk. In: Handbook of iris recognition, Springer, pp 359–396 (2016)
20. Sibai, F.N., Hosani, H.I., Naqbi, R.M., Dhanhani, S., Shehhi, S.: Iris recognition using artificial neural networks. Exp. Syst. Appl. **38**(5), 5940–5946 (2011)
21. Khedkar, M.M., Ladhake, S.: Robust human iris pattern recognition system using neural network approach. In: 2013 international conference on information communication and embedded systems (ICICES), IEEE, pp 78–83 (2013)
22. Rai, H., Yadav, A.: Iris recognition using combined support vector machine and hamming distance approach. Exp. Syst. Appl. **41**(2), 588–593 (2014)
23. 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), 525–537 (2014)
24. Saminathan, K., Chakravarthy, T., Devi, M.C.: Iris recognition based on kernels of support vector machine. ICTACT J. Soft Comput. **5**(5), 889–895 (2015)
25. De Marsico, M., Petrosino, A., Ricciardi, S.: Iris recognition through machine learning techniques: a survey. Pattern Recogn. Lett. **82**, 106–115 (2016)
26. Ahmadi, N., Akbarizadeh, G.: Hybrid robust iris recognition approach using iris image pre-processing, two-dimensional gabor features and multi-layer perceptron neural network/pso. Iet Biomet. **7**(2), 153–162 (2017)
27. Khan, M.F.F., Akif, A., Haque, M.: Iris recognition using machine learning from smartphone captured images in visible light. In: 2017 IEEE international conference on telecommunications and photonics (ICTP), IEEE, pp 33–37 (2017)
28. Ahmadi, N., Akbarizadeh, G.: Iris tissue recognition based on gldm feature extraction and hybrid mlpnn-ica classifier. Neural Comput. Appl. **32**, 1–15 (2020)
29. Al-Waisy, A.S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., Nagem, T.A.: A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal. Appl. **21**(3), 783–802 (2018)
30. Arsalan, M., Kim, D.S., Lee, M.B., Owais, M., Park, K.R.: Fred-net: fully residual encoder-decoder network for accurate iris segmentation. Exp. Syst. Appl. **122**, 217–241 (2019)
31. Zhao, Z., Kumar, A.: A deep learning based unified framework to detect, segment and recognize irises using spatially corresponding features. Pattern Recogn. **93**, 546–557 (2019)
32. Wang, K., Kumar, A.: Cross-spectral iris recognition using cnn and supervised discrete hashing. Pattern Recogn. **86**, 85–98 (2019)
33. Adamović, S., Miškovic, V., Maček, N., Milosavljević, M., Šarac, M., Saračević, M., Gnjatović, M.: An efficient novel approach for iris recognition based on stylometric features and machine learning techniques. Futur. Gener. Comput. Syst. **107**, 144–157 (2020)
34. Gale, A., Salankar, S.: Analysis of iris identification system by using hybrid based pso classifier. In: ICDSMLA 2019, Springer, pp 117–130 (2020)
35. Sudhakar, T., Gavrilova, M.: Multi-instance cancelable biometric system using convolutional neural network. In: 2019 international conference on cyberworlds (CW), IEEE, pp 287–294 (2019)
36. Sudhakar, T., Gavrilova, M.: Cancelable biometrics using deep learning as a cloud service. IEEE Access **8**, 112932–112943 (2020)
37. Morampudi, M.K., Prasad, M.V., Raju, U.: Privacy-preserving iris authentication using fully homomorphic encryption. Multimed. Tools Appl. **79**(27/28), 19215–19237 (2020)
38. Schroff, F., Kalenichenko, D., Philbin, J.: Facenet: A unified embedding for face recognition and clustering. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 815–823 (2015)
39. Kertész, G.: Different triplet sampling techniques for lossless triplet loss on metric similarity learning. In: 2021 IEEE 19th world symposium on applied machine intelligence and informatics (SAMI), IEEE, pp 000449–000454 (2021)
40. Li, X., He, M., Li, H., Shen, H.: A combined loss-based multiscale fully convolutional network for high-resolution remote sensing image change detection. IEEE Geosci. Remote Sens. Lett. (2021). https://doi.org/10.1109/LGRS.2021.3098774
41. Zheng, A.: iris recognition. http://andyzeng.github.io/irisrecognition/, accessed: 10-04-2020 (2020)
42. Kumar, A., Passi, A.: Comparison and combination of iris matchers for reliable personal authentication. Pattern Recogn. **43**(3), 1016–1026 (2010)
43. Rajasekar, V., Premalatha, J., Sathya, K.: Cancelable iris template for secure authentication based on random projection and double random phase encoding. Peer-to-Peer Netw. Appl. **14**(2), 747–762 (2021)
44. Sadhya, D., Raman, B.: Generation of cancelable iris templates via randomized bit sampling. IEEE Trans. Inf. Foren. Secur. **14**(11), 2972–2986 (2019)
45. Morampudi, M.K., Prasad, M.V., Raju, U.: Privacy-preserving and verifiable multi-instance iris remote authentication using public auditor. Appl. Intell. (2021). https://doi.org/10.1007/s10489-021-02187-8
46. Kumar, M.M., Prasad, M.V., Raju, U.: Bmiae: blockchain-based multi-instance iris authentication using additive elgamal homomorphic encryption. IET Biomet. **9**(4), 165–177 (2020)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Mulagala Sandhya received PhD from School of Computer and Information Sciences, University of Hyderabad. Currently she is working as Assistant Professor in Department of Computer Science Engineering at National Institute of Technology Warangal. Her research interests include Biometrics, Image Processing, Pattern Recognition, and Machine Learning.

Mahesh Kumar Morampudi received Ph.D from NIT Warangal in 2020. Currently, he is working as an Assistant Professor at SRM University - AP, Andhra Pradesh, India. His current research interests include Biometrics, Cryptography and Privacy in Machine Learning. He is a life member of ISTE, CSI.

Indragante Pruthweraaj received the B.Tech (CSE) degree from National Institute of Technology Warangal. His research interests are biometrics, machine learning.

Pranay Sai Garepally received the B.Tech (CSE) degree from National Institute of Technology Warangal. His research interests are biometrics, machine learning.