Multimedia Tools and Applications (2021) 80:26273–26296
https://doi.org/10.1007/s11042-021-10932-x

An efficient CNN based encrypted Iris recognition approach in cognitive-IoT system

Ahmed Sabry Shalaby[1] · Ramadan Gad[1] · Ezz El-Din Hemdan[1] · Nawal El-Fishawy[1]

Received: 13 August 2020 / Revised: 25 January 2021 / Accepted: 13 April 2021 /
Published online: 30 April 2021

Abstract
Recently, biometric-based security plays a vital role in the success of the Cognitive Internet of Things (C-IoT) based security framework. The iris trait solves a lot of security issues, especially in smart IoT-based applications. It increases the resistance of these systems against severe authentication attacks. In this paper, an efficient iris recognition model based on chaotic encryption and deep Convolutional Neural Networks (CNNs) is proposed for C-IoT applications. CNN is used to extract the deep iris features from the left and right eyes, which will be used as input features to a fully connected neural network with a Softmax classifier. CASIA V4 Interval dataset and Phoenix dataset are used to train the CNN model; to get the best tuning of network parameters. In this paper, the effect of adding different kinds of noise to iris images, due to noise interference related to sensing IoT devices, bad acquisition of iris images by system users, or other system assaults, is discussed. This strategy of noisy encrypted iris images is evaluated over the internet environment. Chaotic encryption is utilized to secure the transmission of iris templates in the proposed model. The results showed that the proposed approach attains supreme accuracy compared to the existing approaches, it is obtained up to 99.24% and 100% with CASIA V4 and Phoenix datasets, respectively. The proposed model achieves satisfied and competitive results regard accuracy, and robustness among existing methods. Regards to recognition accuracy rate, this methodology shows low degradation of recognition accuracy rates in the case of using noised iris images. Likewise, the proposed method has a relatively low training time, which is a useful parameter in critical IoT based uses such as Tele-Medicine application.

Keywords Biometrics · Iris recognition · Deep learning · Convolutional neural networks · Chaotic encryption · Cognitive IoT

✉ Ezz El-Din Hemdan
ezzvip@yahoo.com

Extended author information available on the last page of the article

1 Introduction

Currently, most modern advanced technologies such as cloud computing [15] and the Internet of Things [4, 15, 16] mostly depends on the use of the network and Internet services for multimedia communications. In the last years, most of our daily applications are based on IoT systems where several devices and sensors are connected. These applications produce a huge amount of data. The IoT applications are considered the source of the biggest kind of information on the internet, so identity verification becomes a very crucial and very challenging task when it has to be automated with high accuracy of recognition rates and low probability of break-ins in IoT systems [8]. The community has adopted several ways to verify the identity of a person through traditional ways [37], like physical possessions of special objects or having pieces of information that are supposed to be kept secret. There is a third way to verify the identity of a person using biometrics [22]. Iris is considered the most accurate trait available today; because of its desirable characteristics [9].

A biometric recognition problem is a special kind of pattern recognition or classification problem which has a very long history [26], in which we need to make a classifier to a set of classes of data. There is a need to extract the best features that represent the data, to facilitate the role of the classifier, and reduce its complexity. Designing handcrafted feature extractors for biometric data is a very complex and challenging task [7]. It takes a lot of time and it needs a great knowledge of the field that governs these data, and it is not guaranteed to achieve high accuracy of recognition rate. Deep learning [11, 20] came into the picture, especially Convolutional Neural Networks (CNNs) which can give us a very good understanding of image data without depending completely on any domain knowledge and handcrafted features.

Recently, the key challenge of researchers - in using the deep learning approach, especially CNNs in biometrics - is that they usually use a pre-trained model of CNNs. These models are trained on a very large number of data classes that exclude iris classes themselves and using these models as a black box. So, using these pre-trained models as they are also is not guaranteed to achieve high accuracy recognition rates because of the loss of the biometric information which was not used in the training stage of these models. It is very difficult to modify these huge pre-trained models to satisfy our needs. Building a new iris-based CNN model, as the proposed model in this paper, needs an intelligent selection of the number of kernels, the kernels' dimensions, input image dimensions, and other factors that affect the model recognition rate [11]. It also needs a huge number of experiments of training and testing to achieve the best architecture that has a high recognition accuracy rate with relatively low training time. Even with using iris biometric in critical C-IoT applications, the communication channels are still a risky point in the application and any penetration of these communication channels may fail the overall system.

In this paper, we propose an efficient iris recognition method based on chaotic encryption and convolutional neural networks for secure C-IoT applications as shown in Fig. 1. The encryption is used to secure the iris sample before sending it to the server. The server is responsible for the classification task. Then, the convolutional neural networks used for the task of feature extraction from both right and left iris images and a softmax classifier. The experimental study will be tested on two public datasets: the CASIA V4-interval [10], and the Phoenix [13, 14, 29] datasets. The main contribution of this work as follows:

- Provide an efficient method via utilizing both the right and left iris images for providing a strong iris-based authentication system with confirming the person through the right and

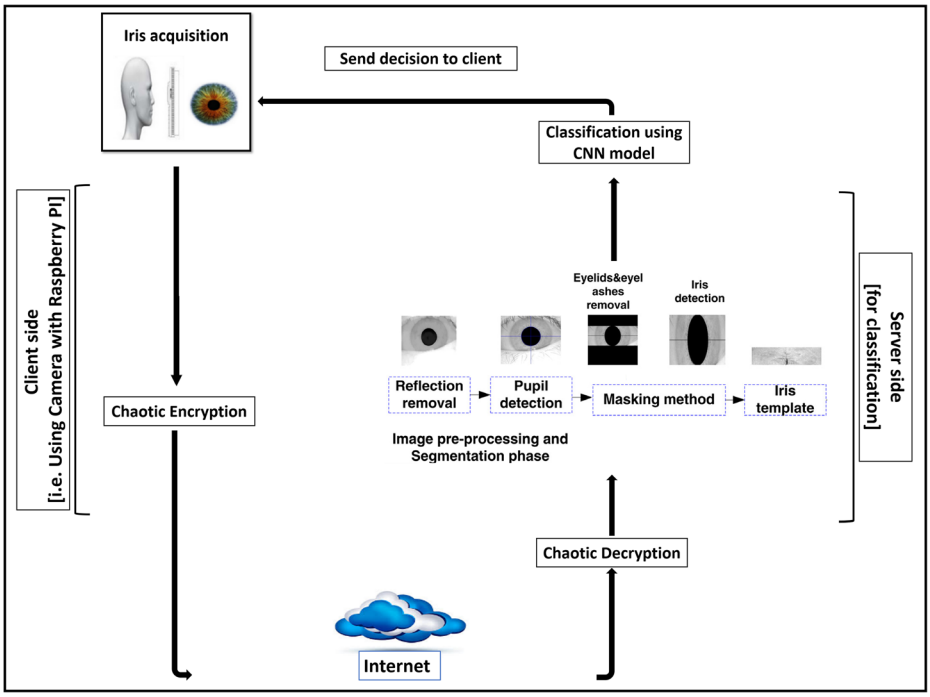

Fig. 1 Structure of the proposed model

left irises. It can be more reliable and favored than a lot of state-of-the-art methods that are used in building iris recognition systems.

- Present a proficient multi-level biometric security system for Cognitive-IoT applications with the following features:
- Secure iris samples using chaotic encryption for secure iris transfer over the Internet.
- Achieve high recognition accuracy rate and increase the security of digital systems due to the classification for both left and right irises.
- Conducting a systematic evaluation of the proposed system through different experiment consequences over two different datasets, as CASIA V4-interval and Phoenix, respectively. The results analysis proved that the proposed system provided that the proposed approach attains supreme accuracy compared to the existing methods.

The rest of this paper is organized as follows: Section 2 provides the related works while the proposed iris recognition system over C-IoT is presented in Section 3. The experimental study and results analysis are presented in Section 4. Finally, the paper conclusion is delivered in Section 5.

2 Related work

In past years, several works have been done in the domain of iris recognition. Mainly the researchers differ in the way of extracting features from iris images. A lot of them used handcrafted feature extractors to build their classification systems. Some works addressed the

use of CNN as a feature extractor. Using handcrafted feature extractors to extract iris features, as we mentioned requires a great knowledge of iris data and its characteristics which makes handcrafting feature extractors relatively hard work. A lot of researchers [1, 24, 25], who addressed the use of CNNs with iris traits, used a pre-trained model of CNNs like VGG-16 [40], ResNet50 [33], Inceptionv3 [21], and AlexNet [2]. These pre-trained models are trained on a very large number of data classes, that exclude iris classes themselves and using these models as a black box. So, using such pre-trained models as they are is not warranted to achieve high accuracy recognition rates; because of the biometric information loss which was not used in the training stage of these models.

An iris recognition system is proposed in [24], where the authors used the pre-trained model of Xception as a feature extractor. Then, they used the Pre-trained model DeepLabV3+ with MobileNet for classification. They tested their model against CASIA Thousand dataset. They achieved a 97.46% accuracy of recognition rate, which is considered a relatively good recognition rate, but it could be better without using these generic pre-trained models.

An iris recognition system is proposed in [25], where they used the pre-trained model of Visual Geometry Group at the University of Oxford (VGG-Net) as a feature extractor. Then, they used a multi-class Support Vector Machine (SVM) algorithm for classification. They tested their model against the CASIA-Iris-Thousand dataset. They achieved a 90% accuracy of recognition rate, which is considered a relatively moderate recognition rate due to using a pre-trained model and the loss of biometric information during training. The authors in [1], proposed an iris recognition system, where they used the pre-trained Alex-Net model as a feature extractor. Then, they used a multi-class SVM algorithm also for classification. They tested their model CASIA-Iris-Interval dataset. They achieved 89% accuracy of the recognition rate, which is considered also a relatively moderate recognition rate due to using a pre-trained model and the loss of biometric information during training.

An iris recognition system is proposed in [12], they applied a method used Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT), as a handcrafted method for extracting features and Euclidean Distance for classification. They tested their model against the Phoenix dataset. They have an average of 88.5% of recognition rate. And their pre-processing stage of their model does not include iris segmentation and normalization which affects their recognition rate. The iris recognition system proposed in [6], in which researchers used Radon transform and gradient-based isolation as a handcrafted method for extracting features and Euclidean distance for classification. They tested their model against the CASIA-iris-V3 dataset. The accuracy of the recognition rate is 84.17%, which is considered a relatively low recognition rate that will make the system not suitable for critical C-IoT applications.

The authors in [23], proposed an iris recognition system, where they used Haar wavelet and Daubechies wavelet for feature extraction. Then, they used a feedforward neural network as a classifier. They tested their model against the CASIA-Iris-V1 dataset. They achieved a 94.76% accuracy of the recognition rate, which is considered a relatively moderate recognition rate. The researchers in [36], proposed an iris recognition system, where they used Integer Wavelet Transform (IWT) for feature extraction. Then, they used normalized Hamming distance as a classifier. They tested their model against the UBIRIS.v2 [30] dataset. They achieved a 98.9% accuracy of the recognition rate, which is considered a good recognition rate but the UBIRIS.v2 dataset is based only on one eye, which makes it less suitable for critical C-IoT applications.

The authors in [35] proposed an iris recognition system where they used the intensity of iris images as a feature extraction method and Hamming Distance (HD), Feed Forward Neural Network, and SVM for classification. They tested their model against the CASIA-iris-V3

dataset. They have 76.8%, 87%, and 98.5%, respectively, as the accuracy of the recognition rate for each classification method in a relatively low number of dataset classes which was 40 classes. Some researchers [19], who applied iris biometric in IoT applications, do not apply any encryption technique for iris images before transmission, and this problem may put the system at risk of attacks. So, there is a lack of research work that has addressed the problem of building strong and efficient full authentication systems for IoT based applications based on both left and right irises, which includes safe protection methods against attacks on communication networks.

Also, most of the researchers [1, 12, 35, 36] who worked in iris recognition build their classification models based only on one human iris either for left or right iris. This limitation in real-life systems will decrease the system's reliability against attacks, which we resolve in the proposed model. The performance of the proposed system is evaluated with an accuracy metric for the recognition rate over the used two data sets and outperformed the previous work.

3 Proposed model

The proposed model considers enrollment and authentication processes over the C-IoT authentication server. The proposed iris recognition model uses a chaotic algorithm and CNNs approaches for encryption and recognition purposes, respectively. Figure 1 shows the overall structure of the model. The proposed model consists of two sides, client-side, and server-side. Client-side is practically implemented using a raspberry pi-2 kit [32], keyboard, mouse, screen, and a cable for internet connection. It is assumed that will be sensing devices to capture the iris images from model users. The server side is practically implemented using a laptop and a cable for internet connection as shown in Fig. 2.

The proposed model structure consists of the following key steps of the client-side: (i) Iris Acquisition; (ii) Iris Encryption; and (iii) Sending the encrypted iris to the enrollment and the

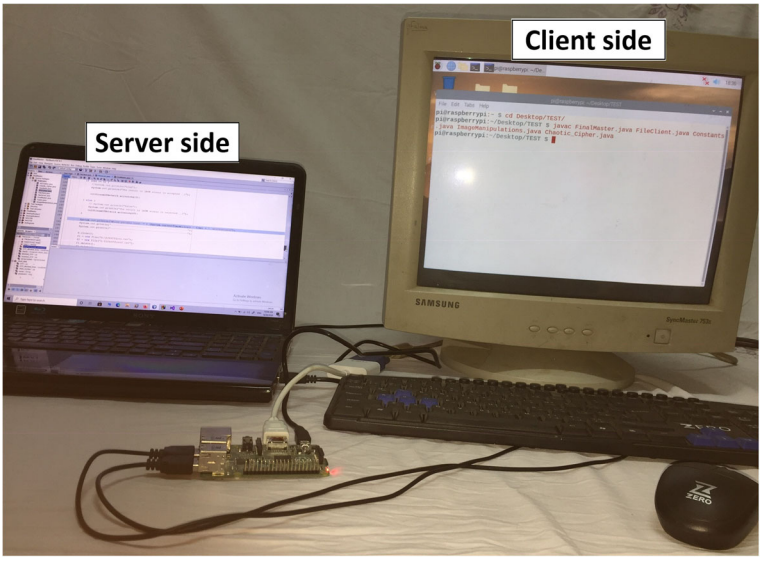

Fig. 2 The client and server sides from testing the proposed model

classification server over a communication channel. And it consists of the following key steps of the server-side: (i) Iris Decryption; (ii) Iris segmentation and normalization; (iii) Deep feature extraction using CNNs; and (iv) Classification using a fully connected neural network with a softmax layer.

The communication with the C-IoT proposed model follows the classical client-server network communication paradigm [38] as shown in Fig. 3. The communication steps are as follows:

1. The server and client create communication sockets.
2. The server binds its socket with any possessed IP address.
3. The server listens to any connection requests from clients.
4. When the server receives a request from a client, it accepts the request and forks a new process that handles that client.
5. A sequence of reading and writing data between them is done according to the needed task.
6. When the client ends the connection, by closing its socket, the server kills its forked process that served that client.

The iris images will be encrypted and sent to the server-side which decrypts them, performs iris pre-processing of segmentation and normalization. Then, the server makes the classification and sends back the result of classification to the client-side which makes the right actions based on these results. The next subsections discuss the detailed description of the proposed model.

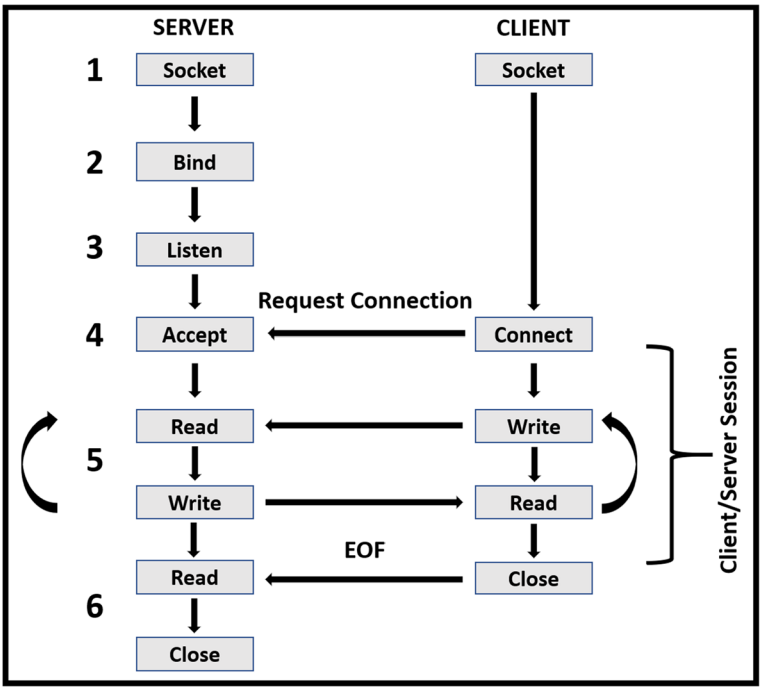

Fig. 3 The classical client/server model is used by C-IoT proposed model

3.1 Iris Acquisition

To achieve the best architecture for the proposed model; a lot of experiments are done with two publicly available datasets. These datasets are CASIA V4-interval [10] and Phoenix [13, 14, 29], as shown in Fig. 4. The iris images in these datasets are captured under different situations of pupil dilation, eyelids/eyelashes occlusion, the slight shadow of eyelids, specular reflection, etc.

3.2 Image encryption and decryption

The encryption is used to increase the security of the proposed model while transmitting iris images over the internet. Iris image encryption of the proposed model is done at the grayscale mode. The algorithm used for this task is based on a chaotic key sequence generated by the sequence of the logistic map and sequence of states of Linear Feedback Shift Register (LFSR) as in [34]. This algorithm consists of two main steps: the generation of the encryption key sequence and encryption of the iris image with the generated key.

The encryption key sequence (K_Seq) is generated by XORing two sequences called ($K1$) and ($K2$). ($K1$) a sequence is generated by the logistic map Eq. (1), as shown in Fig. 5.

$$X_{n+1} = r*X_n*(1-X_n) \tag{1}$$

Where (r) is a parameter in the range of the closed interval [2, 4], X_{n+1} is in the range of [0,1], with high values of (r) like ($r = 3.99$), the generated sequence will be chaotic and completely unpredictable. The length of that sequence must be of the same length as the iris image sequence, it will equal ($w * l$), where w and l are the widths and the length of the iris image that will be encrypted. Then we round all values of ($K1$) sequence by multiplying it by 255 to make sequence values in the range of grayscale mode.

($K2$) a sequence is generated by a sequence of states of an 8-bit Linear Feedback Shift Register shown in Fig. 6. This sequence is defined inductively by the recurrence relation in Eq. (2) with an initial term $K2_1$, called the seed value, equals an integer in the range of [0,255], then perform XOR binary operation on bits of that seed, shift left it with the output of XOR operation and the result will be the second element of the ($K2$) sequence and other sequence elements will be generated inductively in the same way. The length of ($K2$) the sequence must be of the same length as ($K1$) sequence.

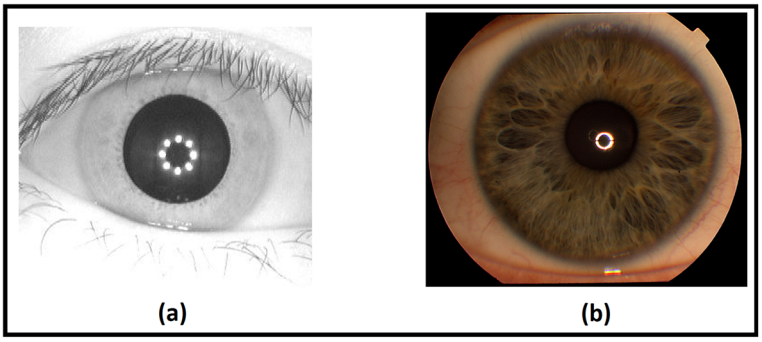

Fig. 4 Samples from used datasets. (**a**) CASIA V4-interval dataset, (**b**) Phoenix dataset

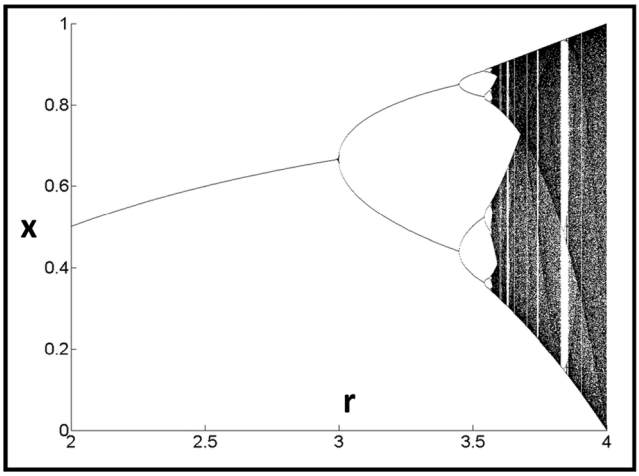

Fig. 5 Bifurcation diagram for Logistic map [28]

$$K2_{n+1} = K2_n \gg (\oplus K2_n) \qquad \forall n(\ 1 \le n \le w*l-1) \tag{2}$$

Where $\gg(x)$ denotes shift left operation with the value of x bit, and $\oplus$ denotes the XORing operation of all bits of a term of a sequence.

Now (K_Seq) can be obtained directly from $(K1)$ and $(K2)$ sequences by XORing them as shown in Eq. (3)

$$K\_Seq_n = K1_n \oplus K2_n \qquad \forall n(\ 1 \le n \le w*l) \tag{3}$$

Now, after the encryption sequence key is obtained, encryption of the iris image will be done by XORing each pixel of an iris image with its corresponding element in the key sequence. The decryption operation is simply the reverse order of this method. As in [34], this LFSR method provides cryptographically better results as compared to the methods that encrypt using a logistic map scheme alone, it provides a high degree of secrecy and security. The original iris image and the encrypted image are highly uncorrelated and perceptually different. For these reasons, our proposed model incorporates this algorithm; to add secure iris transmission for critical C-IoT applications.

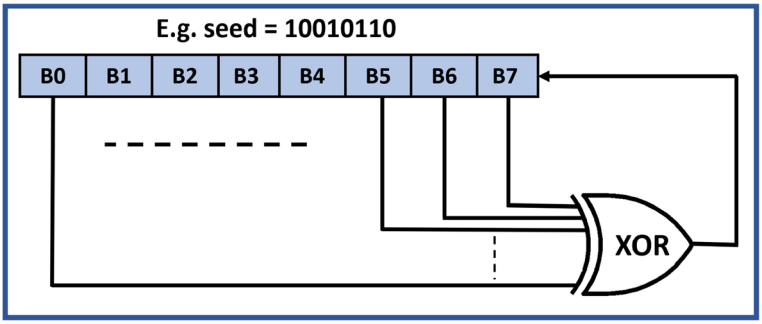

Fig. 6 Linear feedback shift register

3.3 Iris segmentation and normalization

In the case of the CASIA V4-interval dataset, the segmentation step, as the more critical in the recognition operation, is proposed. In this subsection, we will illustrate the suggested method to generate an iris template stored in the IoT server in detail. The decrypted iris image A (x, y) is the original iris image in this stage.

3.3.1 Reflection removal and pupil detection

In [18], a sequence of morphological operations was proposed; to remove the corneal and specular reflections in iris images. Regarding pupil detection, the Adaptive Local Threshold (ALT) algorithm depending on the mean filter is used to filter bright pixels in the iris image $A\ (x, y)$. Regards the result binary image, shown in Fig. 7, let *Rmatrix* is the summation matrix for each row, and *Cmatrix* is the summation matrix for each column. The row-centroid (R_C) = *Index* (*max*| *Rmatrix*|), and column-centroid (C_c) =*Index* (*max*| *Cmatrix*|). The '*Index*' parameter is the position (coordinate) of the pixel in the image along the x-axis and y-axis. The sign '| . |' means the absolute value. The pupil center point ($P_C(x, y)$) is the intersection point of R_C and C_c The pupil radius (R_p) calculated as:

$$R_p = max\left(R_{p1}, R_{p2}, R_{p3}, R_{p4}\right) \tag{4}$$

$$R_{p1} = |Index\ (P_1(x,y))–Index\ (P_C(x,y))| \tag{5}$$

$$R_{p2} = |Index\ (P_2(x,y))–Index\ (P_C(x,y))| \tag{6}$$

$$R_{p3} = |Index\ (P_3(x,y))–Index\ (P_C(x,y))| \tag{7}$$

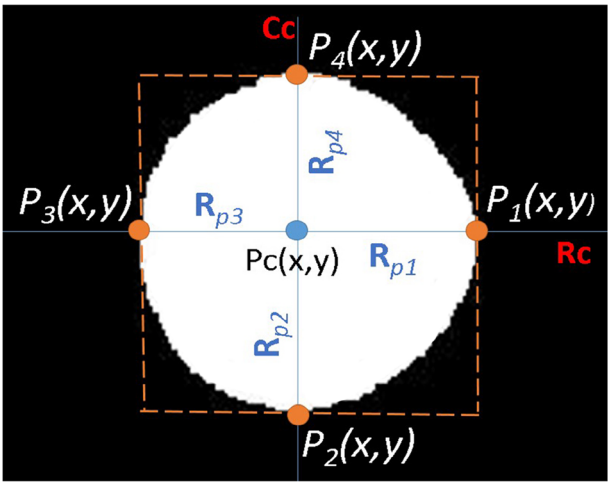

Fig. 7 Pupil parameter detection (pupil center $P_c(x,y)$ and pupil radius R_p)

$$R_{p4} = |Index\ (P_4(x,y))–Index\ (P_C(x,y))| \tag{8}$$

Each of the points P_1, P_2, P_3 and P_4 has the index of the first zero-value pixel along the radius axis in the four directions. Pupil detection steps with the results are illustrated in Fig. 8, in sequence. The pupil region mask ($M_p(x,y)$) (Fig. 8-d) identified by the center ($P_C(x,y)$)and the radius (R_p) is multiplied again in the original image $A(x,y)$; to isolate the iris region $I(x,y)$ free of artifacts without deformation. The pupil border is shown in Fig. 8-f.

3.3.2 Masking technique (MT)

With the aid of the pupil detection parameters (P_1, P_2, P_3 and P_4) and the pupil region mask ($M_p(x,y)$), the iris mask could be declared and detect. First, the mask to isolate the eyelashes and eyelids part calculated ($M_e(x,y)$). Then, multiply this mask as a binary matrix to the pupil mask generated ($M_p(x,y)$) . This multiplication will generate the final iris mask ($M_o(x,y)$) pixels that could multiply in the original image to localize the iris region free of pupil, eyelashes, and eyelids.

Let iris image $I(x,y)$ has $m \times n$ pixels, $\forall\, y\ 1 \le y \le n$, the eyelashes/eyelids removing a mask ($M_e(x,y)$) identified as:

$$M_e(x,y) = \begin{cases} 0: & 1 \le x \le Index(P_4(x,y)), Index(P_2(x,y)) \le x \le m \\ 1: & Index(P_4(x,y)) < x < Index(P_2(x,y)), \end{cases} \tag{9}$$

Here the mask has two binary values. Binary (0) declare each point of the eyelashes and eyelids up and down the pupil circle. And binary (1) represents the pupil and iris pixels between the eyelashes and eyelid parts.

The final mask ($M_o(x,y)$), is shown in Fig. 9-a, identified in a binary format as

$$M_o(x,y) = M_p(x,y) * M_e(x,y) \tag{10}$$

The concatenation of the two masks represent the output iris mask, that used to isolate the iris region by the multiplication process of ($M_o(x,y)$) and the original image $I(x,y)$.

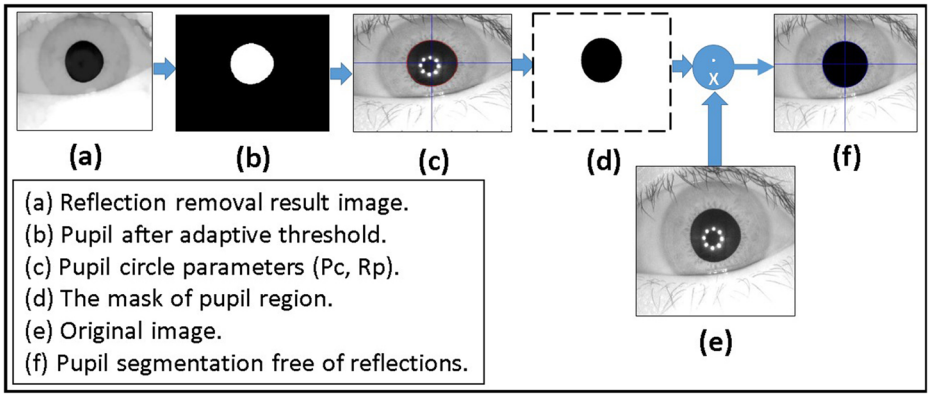

Fig. 8 Pupil detection steps

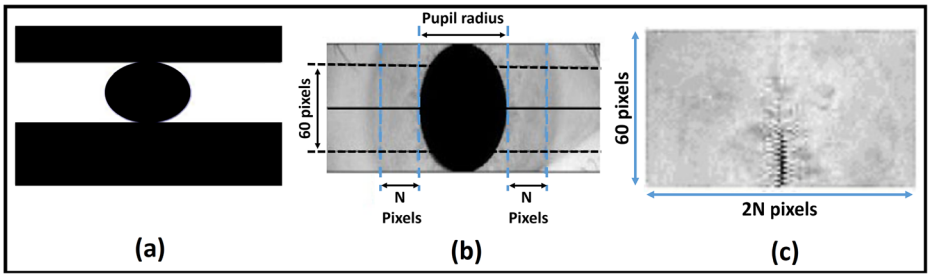

Fig. 9 MT processes illustration. (**a**) Iris mask $M_o(x, y)$ by the aid of pupil parameters and eyelashes mask. (**b**) Iris template parameter declaration. (**c**) Final iris template

In [17], a fixed template size (60 × 90 pixel) generated. This was unsuitable for some images in datasets, due to image sizes and resolution modifications were done over MT; the N pixels to the left and right of the localized pupil are concatenated. The iris template is created by mapping the selected pixels on a fixed size (60 × 2 N) matrix as shown in Fig. 9 (b-c).

In the case of the Phoenix dataset, the dataset is already segmented as shown in Fig. 10-a. The upper half and the lower half of iris images were separated, each of the dimensions of (350*100) pixels. Then, we concatenate them together, as shown in Fig. 10-b, 10-c, and 10-d. We use the final image of dimensions of (350*200) in the next stage of feature extraction. This solution does not consider the rotation of both the camera and the eye. Moreover, it is suitable for offline images only. More iris information is lost in the left and right collarette zones.

3.4 CNN-based deep feature extraction and classification

Different CNNs with different architectures, as it will be shown in experimental results, were used to extract the deep features from iris images for the dual iris. The goal is to find a more accurate architecture that increases the recognition accuracy rate. After these experiments, we propose a CNN model for both datasets. It consists of "3" convolutional layers, "3" max-pooling layers, "3" RELU activation layers, "2" fully connected layers, and "1" SoftMax layer as the architecture of the proposed model. It is illustrated in Table 1 and Fig. 11. Each CNN architecture tested; to maintain its recognition accuracy rate; to adjust the model configuration to achieve a higher recognition rate.

The overall practical steps of the experiments will be viewed before dealing with the experimental results of each step alone. First, the server-side which is responsible for the classification task is set up for listening to connection requests from clients. When the client requests a connection with the server, the server accepts it. After the client performs iris image acquisition, it performs iris decryption using a chaotic algorithm. The server receives the

Fig. 10 The proposed template generation for the Phoenix dataset

Table 1 The Proposed CNN architecture for both datasets

Layer name	No of filters	Filter size	Stride size	Padding
Conv1	100	3*3	1*1	Valid
RELU	n/a	n/a	n/a	n/a
Max pooling	1	2*2	2*2	Valid
Conv2	150	3*3	1*1	Valid
RELU	n/a	n/a	n/a	n/a
Max pooling	1	2*2	2*2	Valid
Conv3	200	3*3	1*1	Valid
RELU	n/a	n/a	n/a	n/a
Max pooling	1	2*2	2*2	Valid
Fully connected layer1	250 node	n/a	n/a	n/a
Fully connected layer2	150 node	n/a	n/a	n/a
Softmax layer	n/a	n/a	n/a	n/a

encrypted image and decrypts it to obtain the original one, then perform iris pre-processing operations and pass the iris image to the trained classifier. Then send the result of classification to the client whose C-IoT application access request will be accepted or rejected based on the classification result. These sequences of actions at the server and client sides are shown in Fig. 12-a and 12-b respectively.

4 Experimental study and results analysis

4.1 Iris datasets

In this work, to evaluate the proposed approach, we used two datasets called CASIA V4-interval and Phoenix respectively as the following:

- CASIA V4-interval dataset is the latest dataset captured by CASIA self-developed close-up iris camera, all iris images are 8-bit Gray-level (. JPEG) files, collected under near-infrared (NIR) illumination. It consists of 2641 iris images taken from 249 subjects. Its iris images with resolution (320*280) pixel. This dataset has two problems. The first problem

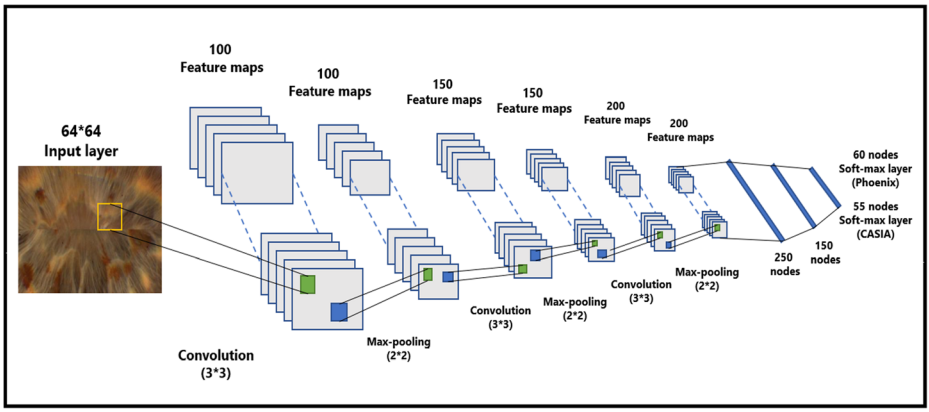

Fig. 11 The proposed CNN model structure of both datasets

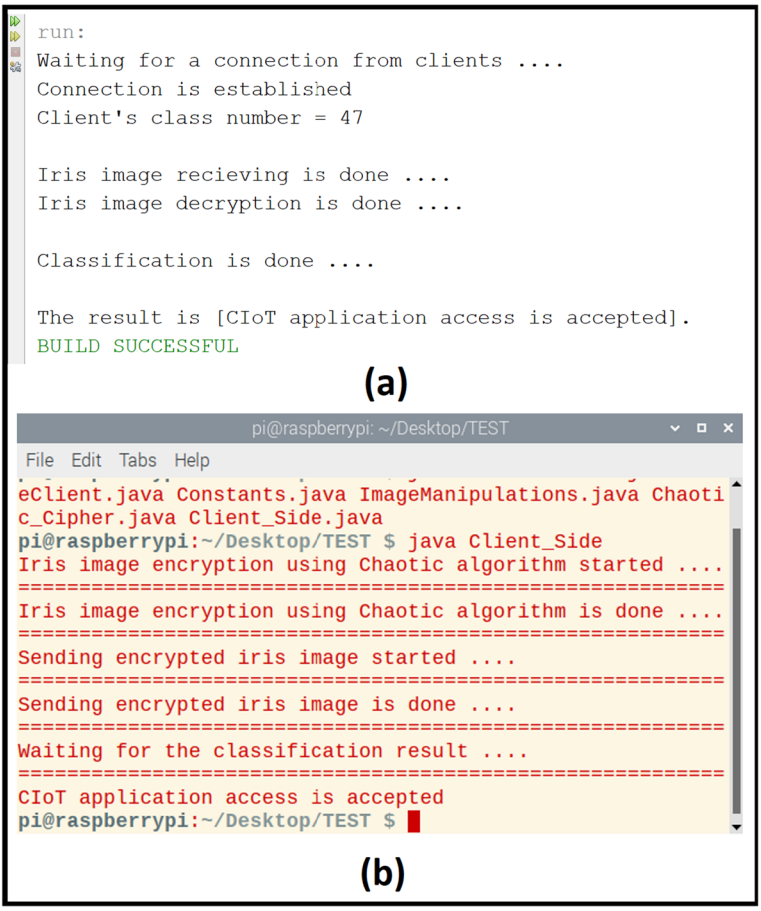

Fig. 12 The connection actions sequence (**a**) Server-side. (**b**) Client-side

is that there are a lot of subjects without any iris image for either left or right iris, the second problem is that there are a lot of subjects that have a very small number of iris images for either left or right iris. These problems limited our choice of subjects used in the proposed model.

- Phoenix dataset consists of 384 irises Image taken from 64 subjects, 192 for the left iris and 192 for the right iris, the iris images are 24-bit RGB of (. PNG) file format. Its iris is

Table 2 Description Summary of the used datasets

	CASIA V4 interval	*Phoenix*
Description	2641 iris image taken from 249 subjects	384 iris Images taken from 64 subjects
Images resolution	320*280 pixels	576*768 pixels
Image format	JPEG	PNG
Subjects used in localization	ALL	ALL
Subjects used in classification	55	60
Samples per subject	not regular	3 right and 3 left

imaged with a resolution of 576 × 768 pixels. The irises were taken by TOPCON TRC50IA optical device connected to SONY DXC-950P 3CCD camera. The summary of the configuration of these two datasets is shown in Table 2.

4.2 Iris encryption and decryption

In all experiments on both dataset images, the values of the parameters needed to generate K_Seq, $K1$, and $K2$ sequences are chosen as shown in assignments Eq. (11)

$$r = 3.99 \quad \& \quad X_1 = 0.1 \quad \& \quad K2_1 = (0100101)_2 \tag{11}$$

Figure 13 shows the results of the chaotic encryption algorithm implemented in the proposed model on both datasets.

4.3 Iris segmentation and normalization

In MT, the mask size (n) controls the iris region. In Table 3, the accuracy changed according to the value of the (n) parameter. The specular reflect in the pupil is one circular white spot; our algorithm hardly detects a pupil with such environmental nature. The range of (30–45) for mask size (n) in MT achieves the best accuracy. When ($n < 30$) the final iris mask expanded, including sclera pixels gradually. For ($n > 45$), the mask loses more information from the iris circle.

4.4 Training and classification using CNNs

To achieve the proposed model architecture previously shown in Table 1; a large number of experiments are done to achieve the best tuning parameters. To evaluate the performance of the proposed model; two metrics were measured. The first is the recognition accuracy rate (ARR %) which is the fraction of correctly iris classifications, and the other metric is the training time of the CNN model.

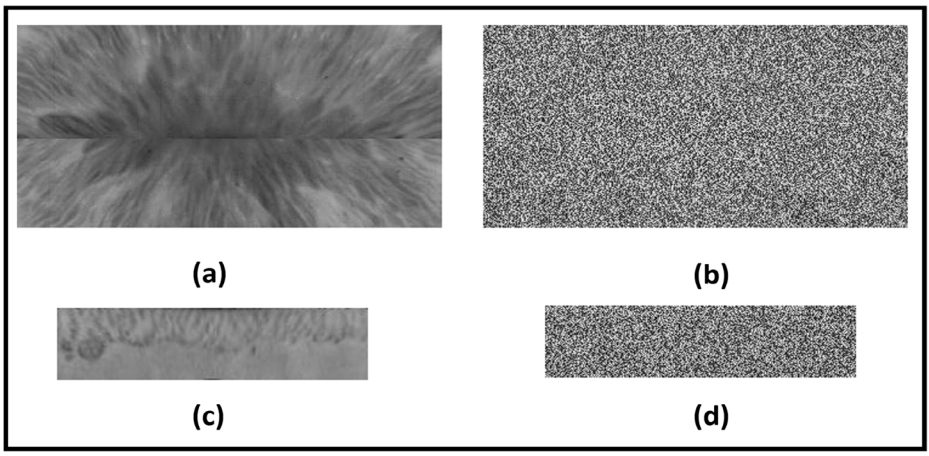

Fig. 13 Results of Chaotic encryption and decryption. (**a**) Original image from the phoenix dataset. (**b**) Encrypted image of the original image from the phoenix dataset. (**c**) Original image from the CASIA V4 dataset. (**d**) The Encrypted image of the original image from the CASIA V4 dataset

Table 3 The segmentation success rate for every n pixels in MT

Mask Size(n) (pixel)	Success Rate (%)
60	95.724
55	96.998
50	98.271
45	99.545
40	99.545
35	99.545
30	99.545

$$\text{ARR}\ (\%) = \frac{\boldsymbol{C_c}}{\boldsymbol{T_c}} * 100 \tag{12}$$

Where ($\boldsymbol{C_c}$) represents the number of correct iris classifications and ($\boldsymbol{T_c}$) represents the total number of classified irises. We clustered each data set into subsets. The first for training CNN to get the best tuning parameters and the second is for testing this CNN configuration to have a recognition accuracy rate. The aim is to adjust its configuration to achieve a higher recognition rate.

With the CASIA V4-interval dataset, we divided the dataset such that for each person 80% of iris images were used in training and 20% of iris images were used in testing. With the Phoenix dataset, we divided the dataset such that for each person 66% of iris images were used in training and 33% of iris images were used in testing.

We used different CNNs with different configurations in their number of convolutional, max pooling, RELU, and fully connected layers. Each trained with different training parameters like learning rate, number of epochs, patch sizes, and dimensions of input iris images.

All experiments were done on a lab top, which is used as the server-side of the model, with Core i5 CPU and 6 GB of RAM, and the codes were written in MATLAB, Java, and Python languages. And raspberry pi 2 for the client-side of the model and its scripts are written in Java language.

Table 4 Accuracy of recognition rates obtained for different CNN architectures using the input image size of (256 × 64) pixels

	Phoenix		CASIA V4	
Configuration	left	right	right	Left
[20 80,120] *	93.333	90.000	96.969	96.969
[5 50,100]	93.333	81.666	93.939	93.939
[5 50,120]	91.666	90.000	98.484	95.454
[5 40,120]	90.000	88.333	89.393	86.363
[120120120]	85.000	88.333	98.484	96.969
[20 70,160]	91.666	90.000	95.454	92.424
[120,100 80]	88.333	86.666	93.939	87.878
[120 80 50]	90.000	90.000	100	95.454
[20 80,140,256]	81.666	88.333	80.303	83.333
[5 50,100 150]	85.000	93.333	83.333	84.848
[10 80,120 180]	91.666	93.333	92.424	86.363
[20 70,160 200]	88.333	78.333	89.393	87.878

**Where in the pattern of [× 1 × 2 × 3] × 1, × 2, and × 3 indicates the number of kernels in each convolutional layer*

Table 5 Accuracy of recognition rates obtained for different CNN architectures using the input image size of (128 × 64) pixels

	Phoenix		CASIA V4	
Configuration	left	right	right	Left
[6 50,150]	93.333	98.333	95.454	93.939
[100150200]	91.666	90.000	98.484	90.909
[10 50,250]	95.000	91.666	95.454	93.939
[10100200]	93.333	88.333	96.969	90.909
[120120120]	96.666	85.000	95.454	92.424
[100200300]	93.333	86.666	95.454	90.909
[20 70,160]	96.666	98.333	98.484	93.939
[120 80 50]	93.333	93.333	93.939	93.939
[10 40 80]	96.666	93.333	93.939	92.424
[10 50,100 200]	90.000	91.666	92.424	90.909
[50,100 150 250]	90.000	90.000	89.393	87.878
[100,150,200 250]	93.333	91.666	92.424	92.424

The best architecture for both datasets together, as shown in Table 6, was found when the dimensions of the input image were (64*64) pixels, and its configuration is previously described in Table 1.

Tables 4, 5, 6, and 7 show a side of the experiments done on the model until reaching the best architecture that gives the largest recognition rate. With the CASIA V4 interval dataset, we trained our model with 265 iris images for 55 classes of data in the case of each iris left and right and tested it against 66 iris images. The model correctly classified 65 iris images with the left eye and 66 images with the right eye. The accuracy of the recognition rate of 98.48% and 100% for left and right iris respectively, as shown in Table 6. So, the model has an accuracy of 99.24% of the overall CASIA V4-interval dataset. With the Phoenix dataset, we trained our model with 120 iris images for 60 classes of data in the case of each iris left and right and tested it against 60 iris images. The model correctly classified all iris images for both left and

Table 6 Accuracy of recognition rates obtained for different CNN architectures using the input image size of (64 × 64) pixels

	Phoenix		CASIA V4	
Configuration	left	right	right	left
[10 50,100]	95.000	96.666	98.484	98.484
[10 40 80]	98.333	98.333	96.960	98.484
[10100150]	98.333	95.000	95.454	96.969
[20 70,160]	96.333	95.000	98.484	95.454
[120120120]	95.000	95.000	96.960	98.484
[100150200]	100	100	98.484	100
[20 60,120,180]	90.000	96.666	92.424	95.454
[10 50,100 150]	93.333	95.000	95.454	92.424
[50,100 150 200]	95.000	96.666	96.960	93.939
[100,150,200 250]	95.000	95.000	95.454	92.424
[10 50,100]	95.000	96.666	98.484	98.484
[10 40 80]	98.333	98.333	96.960	98.484

Table 7 Accuracy of recognition rates obtained for different CNN architectures using the input image size of (128 × 128) pixels for Phoenix dataset only

Configuration	*Phoenix* left eye	*Phoenix* right eye
[20 80,120]	83.333	90.000
[5 50,100]	95.000	93.333
[5 50,120]	86.666	91.666
[5 40,120]	88.333	96.666
[120 80 50]	93.333	88.333
[5 50,100 150]	93.333	88.333
[10 80,120 180]	95.000	90.000
[20 70,160 200]	90.000	90.000

right irises with an accuracy of recognition rate of 100% for left and right iris as shown in Table 6. So, it has an accuracy of 100% of the overall Phoenix dataset.

Concerning training time, after a lot of experiments until reaching the proposed architecture, it is found that the number of epochs needed for training which gives us the best accuracy of recognition rate was 60 with a patch size of 40. With this configuration, the training time of the CASIA V4 interval dataset was about 25 min for each right and left iris sub-sets. And the

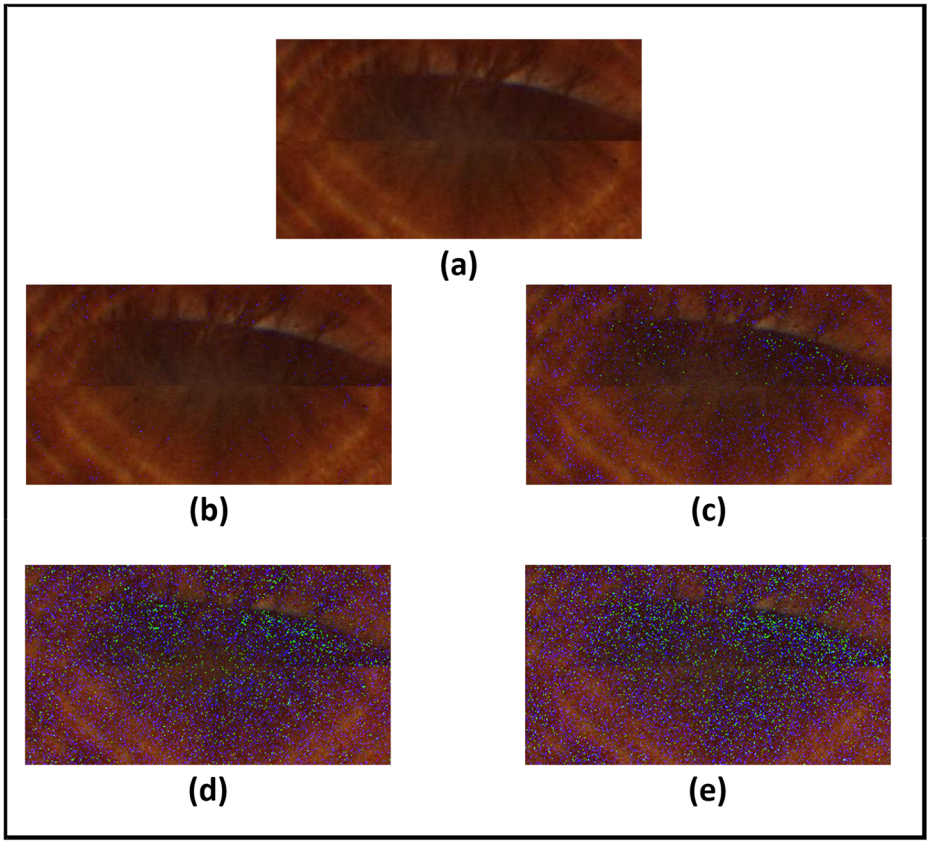

Fig. 14 Results of adding Gaussian noise with different standard deviations. (**a**) Original image. (**b**) Standard deviation = 5 (**c**) standard deviation = 10 (**d**) standard deviation = 15 (**e**) standard deviation = 20

training time of the Phoenix dataset was about 17 min for each right and left sub-sets. This training time is considered relatively low concerning other researchers, like [3], who addressed the use of deep learning in iris recognition and their training time exceeds 6 h.

4.5 Evaluating the proposed model against noised iris images

In the proposed model, we assume that iris images may get some external noise at the first stage of iris acquisition. This external noise is due to several reasons like system attacks, interference noise on iris sensing devices, inaccurate iris acquisition due to system users, etc. We assume two kinds of noise will be added. The first kind is a noise that is generated randomly from a Gaussian distribution, with a mean value equals to zero and several standard deviations, to test how the accuracy of the recognition rate of the proposed model would be affected. The other type of noise is generated from a uniform distribution. The noise is added for each pixel of iris images. Figures 14 and 15, Tables 8 and 9 show the obtained results with both CASIA V4 and Phoenix datasets for the added noise from Gaussian distribution and the uniform distribution, respectively. These results are based on our final network architecture that gives the best recognition rate in the ideal case of iris images without any added noise as shown previously in Fig. 11.

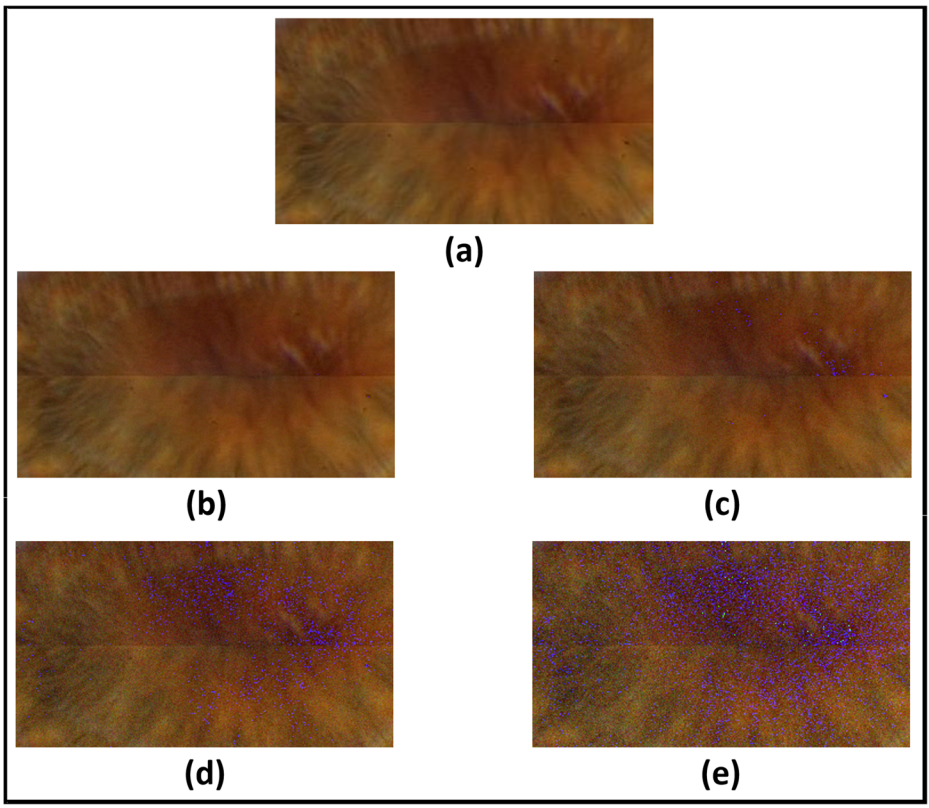

Fig. 15 Results of adding uniform noise within different intervals. (**a**) Original image. (**b**) Within interval of [−5, +5] (**c**) within interval of [−10, +10] (**d**) within interval of [−15, +15] (**e**) within interval of [−20, +20]

Table 8 The model recognition rate against noised iris images (Gaussian noise)

Standard deviation	CASIA V4		*Phoenix*	
	Left iris	Right iris	Left iris	Right iris
5	100	98.484	100	100
10	96.969	95.454	96.666	100
15	92.424	93.939	88.333	96.666
20	86.363	87.878	80.000	88.333

These results show how well our proposed model deals with noised iris images from different noise distributions. Table 10 shows that the proposed CNNs model has admirable and competitive results compared to state-of-the-art methods in terms of recognition accuracy. Table 10 compares the proposed model with the current literature that differs in the datasets used, the feature extraction methodology, or the classification methodology.

5 Conclusion

In this paper, an efficient iris recognition model based on chaotic encryption and deep Convolutional Neural Networks in Cognitive IoT applications is proposed. A chaotic encryption algorithm based on a key sequence, generated by a sequence of logistic maps and sequences of states of (LFSR), is used to secure iris template transmission over the internet. CNN is used to extract the deep iris features from both irises which will feed a fully connected neural network with a Softmax classifier. Two publicly available datasets, namely CASIA V4-Interval and Phoenix, are used during experiments for training and testing the proposed model. The proposed model shows satisfied and competitive results regard reliability, the accuracy of recognition rate, training time, and robustness among a lot of state-of-the-art methods. Likewise, it showed a low degradation of recognition accuracy rates in the case of noised iris images. It is robust against noise interference due to sensing devices, bad iris acquisition; due to system user interactions, or other client-end system attacks. Using the dual iris increases the security level of the proposed model. The accuracy of the recognition rate of the proposed model is 99.24% and 100% with CASIA V4 and Phoenix datasets, respectively. The training time of the proposed model was 25 and 17 min with both datasets. The results of the proposed model highly recommend it to be a solution for the security issues of many C-IoT systems, especially in the era in which IoT applications are considered the source of the biggest kind of information on the internet. In the future, we will evaluate the performance of the proposed

Table 9 The model recognition rate against noised iris images (uniform noise)

Interval	CASIA V4		*Phoenix*	
	Left iris	Right iris	Left iris	Right iris
[−5,+5]	100	98.484	100	100
[−10,+10]	100	98.484	100	100
[−15,+15]	96.969	95.454	96.666	96.666
[−20,+20]	89.393	92.424	83.333	85.000

Table 10 Comparison of the proposed model with other works

Approach	Dataset	Feature extraction	Classification	Recognition accuracy %
Ghanapriya Singha et al. (2020) [36]	UBIRIS.V2	Integer Wavelet Transform (IWT)	Normalized Hamming distance	98.9
Ruqaiya Khanam et al. (2019) [23]	CASIA-Iris-V1	Haar wavelet and Daubechies wavelet	Feedforward neural network	94.76
Peter Peer et al. (2019) [24]	***CASIA Thousand***	Pre-trained Xception	Pre-trained DeepLabV3+ with MobileNet	97.46
HK Rana et al. (2019) [31]	CASIA-Iris-V4	PCA and DWT	SVM	95.40
Maram and Lamiaa (2018) [1]	CASIA-Iris-Interval	pre-trained Alex-Net model	Multi-Class SVM	89
Alaa Al-Waisy et al. (2018) [3]	CASIA-Iris-V3	Convolutional Neural Network	Softmax classifier + fusion	100
Minaee et al. (2016) [25]	CASIA-Iris-Thousand	pre-trained VGG-Net	Multi-Class SVM	90
Umer et al. (2016) [39]	IIT Delhi Iris Database	TCM with ordered PB	SVM+Fusion	99.52
Nalla and Chalavadi (2015) [27]	IIT Delhi Iris Database	Log-Gabor wavelet	Online Dictionary Learning	86
Saminathan et al. (2015) [35]	CASIA-Iris-V3-interval	Intensity image	Least square method of quadratic SVM	98.50
S. S. Dhage et al. (2015) [12]	***Phoenix***	Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT)	Euclidean distance	88.50
Bharath et al. (2014) [6]	CASIA-Iris-V3	Radon transform and gradient-based isolation	Euclidean distance	84.17
Baqar et al. (2011) [5]	MMU	Dual boundary contour vector	Multilayer feedforward neural network	99
The proposed System	CASIA-Iris-V4	Convolutional Neural Network	Softmax classifier	99.24
	Phoenix			100

model using different iris datasets and apply it in real-life C-IoT applications such as ATMs in banks and travelers' authentication at airports.

References

1. Alaslani MG, Elrefaei LA (2018) Convolutional neural network based feature extraction for IRIS recognition. Int J Comput Sci Inf Technol 10(2):65–78
2. "AlexNet architecture." (2020) https://neurohive.io/en/popular-networks/alexnet-imagenet-classification-with-deep-convolutional-neural-networks/ (accessed Oct. 17, 2020).
3. Al-Waisy AS, Qahwaji R, Ipson S, Al-Fahdawi S, Nagem TAM (2018) A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal Appl 21:783–802
4. Atlam HF, El-Din Hemdan E, Alenezi A, Alassafi MO, Wills GB (2020) "Internet of things forensics: a review," Internet of Things
5. Baqar M, Azhar S, Iqbal Z, Shakeel I, Ahmed L, Moinuddin M (2011) "Efficient iris recognition system based on dual boundary detection using robust variable learning rate Multilayer Feed Forward neural network," in *Proceedings of the 7th International Conference on Information Assurance and Security, IAS*, pp. 326–330
6. Bharath BV, Vilas AS, Manikantan K, Ramachandran S (2014) "Iris recognition using radon transform thresholding based feature extraction with Gradient-based Isolation as a pre-processing technique," in *9th International Conference on Industrial and Information Systems (ICIIS)*, pp. 1–8
7. Bishop CM (2006) *Pattern Recognition and Machine Learning*, 1st ed. Springer-Verlag New York
8. Bolle RM, Connell JH, Pankanti S, Ratha NK, Senior AW (2004) *Guide to Biometrics*, 1st ed. Springer-Verlag New York
9. Bowyer KW, Burge MJ, Eds. (2013) *Handbook of Iris Recognition*, 1st ed. Springer-Verlag London
10. "CASIA iris dataset." (2021) http://www.cbsr.ia.ac.cn/china/Iris Databases CH.asp (accessed Jan. 23, 2021)
11. Courville A, Goodfellow I, Bengio Y (2016) *Deep Learning*, 1st ed. The MIT Press
12. Dhage SS, Hegde SS, Manikantan K, Ramachandran S (2015) Dwt-based feature extraction and radon transform based contrast enhancement for improved iris recognition. Procedia Comput Sci 45:256–265
13. Dobeš M, Machala L, Tichavský P, Pospíšil J (2004) Human eye iris recognition using the mutual information. Optik (Stuttg) 115(9):399–404
14. Dobeš M, Martinek J, Skoupil D, Dobešová Z, Pospíšil J (2006) Human eye localization using the modified Hough transform. Optik (Stuttg). 117(10):468–473
15. Ezz El-Din H, Manjaiah DH (2017) Internet of things in cloud computing. Internet of things: novel advances and envisioned applications. Springer, Cham:299–311
16. Ezz El-Din H, Manjaiah DH (2017) Internet of nano things and industrial internet of things. Internet of things: novel advances and envisioned applications. Springer, Cham:109–123
17. Gad R, Zorkany M, EL-Sayed A, EL-Fishawy N (2016) An efficient approach for simple Iris localization and normalization technique. Menoufia J Electron Eng Res 25(2):213–224
18. Gad R, Talha M, El-sayed A, EL-Fishawy N, Muhammad G, Zorkany M (2018) Iris recognition using multi-algorithmic approaches for cognitive internet of things (CIoT) framework. Futur Gener Comput Syst 89:178–191
19. Gad R, Abd El-Latif AA, Elseuofi S, Ibrahim HM, Elmezain M, Said W (2019) "IoT Security Based on Iris Verification Using Multi-Algorithm Feature Level Fusion Scheme," in *2nd International Conference on Computer Applications and Information Security,* ICCAIS 2019
20. Haykin S (2008) Neural Networks and Learning Machines 3rd ed. Pearson
21. "Inception V3 architecture." (2020) https://keras.io/api/applications/inceptionv3/ (accessed Oct. 17, 2020).
22. Jain AK, Ross AA, and Nandakumar K (2011) *Introduction to Biometrics*, 1st ed. Springer US
23. Khanam R, Haseen Z, Rahman N, Singh J (2019) Performance analysis of iris recognition system. Adv Intell Syst Comput 847:159–171
24. Lozej J, Stepec D, Struc V, Peer P (2019) "Influence of segmentation on deep iris recognition performance," in *7th International Workshop on Biometrics and Forensics, IWBF*
25. Minaee S, Abdolrashidiy A, Wang Y (2016) "An experimental study of deep convolutional features for iris recognition," in *IEEE Signal Processing in Medicine and Biology Symposium (SPMB)*, pp. 37–42
26. Mitchell TM (1997) *Machine Learning*, 1st ed. McGraw-Hill Education
27. Nalla PR, Chalavadi KM (2015) Iris classification based on sparse representations using on-line dictionary learning for large-scale de-duplication applications. Springerplus 4(1):1–10

28. Parker TS, Chua L (1989) *Practical Numerical Algorithms for Chaotic Systems*, 1st ed. Springer-Verlag New York
29. "Phoenix iris Dataset." (2019) http://phoenix.inf.upol.cz/iris/ (accessed Nov. 06, 2019).
30. Proença H, Alexandre LA (2005) "UBIRIS: A noisy iris image database," in *International Conference on Image Analysis and Processing*, pp. 970–977
31. Rana HK, Azam MS, Akhtar MR, Quinn JMW, and Moni MA (2019) "A fast iris recognition system through optimum feature extraction," *PeerJ Comput. Sci. 8 April*
32. "Raspberry Pi 2." (2020) https://www.raspberrypi.org/products/raspberry-pi-2-model-b/ (accessed Sep. 14, 2020).
33. "ResNet architecture." (2020) https://neurohive.io/en/popular-networks/resnet/ (accessed Oct. 17, 2020).
34. Rohith S, Bhat KNH, Sharma AN (2014) "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register," in *International Conference on Advances in Electronics, Computers and Communications (ICAECC) 10–11*.
35. Saminathan K, Chakravarthy T, Chithra Devi M (2015) Iris recognition based on kernels of Suppoet vector machine. ICTACT J Soft Comput 5(2):889–895
36. Singh G, Singh RK, Saha R, Agarwal N (2020) IWT based Iris recognition for image authentication. Procedia Comput. Sci. 171:1868–1876
37. Stallings W (2016) Cryptography and network security: principles and practices, 7th ed. Pearson Education, Inc
38. Stevens WR, Fenner B, Rudoff AM, Juszkiewicz K (2003) *Unix Network Programming Volume 1: The Sockets Networking API*, 3rd ed. Addison-Wesley Professional
39. Umer S, Dhara BC, Chanda B (2016) Texture code matrix-based multi-instance iris recognition. Pattern Anal. Appl. 19(1):283–295
40. "VGG16 architecture." (2020) https://neurohive.io/en/popular-networks/vgg16/ (accessed Oct. 17, 2020).

Ahmed Sabry has received his B.Sc. from the Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2017. His research focuses on machine learning and artificial intelligence.

Ramadan Gad received a Ph.D. degree in Computer Science & Engineering at the Faculty of Electronic Engineering, Menoufia University, Egypt. His research focuses on iris recognition and multi-biometrics. His research interests are in the areas of biometrics, FPGA, security, and digital signal/image processing. Besides, his interests include the Internet of Things (IoT), computer vision, machine learning, and data structures & algorithms. Currently, he is serving as an editorial board member and reviewer in various Journals and conferences.

Ezz El-Din Hemdan has received his B.Sc. from the Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2009. He received his M.Sc. From the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2013. He received his Ph.D. degree in the Department of Computer Science, Mangalore University, India in 2018. He has several publications in national/international conferences and journals. His research area of interest includes; Canacelable Biometric, Blockchain, Digital Twins, Image Processing, Virtualization, Cloud Computing, Internet of Things/Nano-Things, Cryptography, Data Hiding, Digital Forensics, Cloud Forensics, Big Data Forensics, Data Science and Big Data Analytics.

Nawal El-Fishawy received a Ph.D. degree in mobile communications, Faculty of Electronic Eng., Menoufia University, Menouf, Egypt, in collaboration with Southampton University in 1991. Her research interest includes computer communication networks with emphasis on protocol design, traffic modeling, and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms. She has served as a reviewer for many national and international journals and conferences.

Affiliations

Ahmed Sabry Shalaby[1] · Ramadan Gad[1] · Ezz El-Din Hemdan[1] · Nawal El-Fishawy[1]

Ahmed Sabry Shalaby
ahmed.sabry@el-eng.menofia.edu.eg

Ramadan Gad
ramadangad@el-eng.menofia.edu.eg

Nawal El-Fishawy
nelfishawy@hotmail.com

[1] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menof, Egypt