JSCDM

http://penerbit.uthm.edu.my/ojs/index.php/jscdm

e-ISSN : 2716-621X

Journal of Soft Computing and Data Mining

Personal Authentication System Based Iris Recognition with Digital Signature Technology

Huda M Therar[1*], Ahmed J Ali[2]

[1]Department of Computer Engineering Technology,
Northern Technical University, Mosul, IRAQ

[2]Department of Power Engineering Technology,
Northern Technical University, Mosul, IRAQ

*Corresponding Author

DOI: https://doi.org/10.30880/jscdm.2023.04.01.002
Received 02 January 2023; Accepted 17 March 2023; Available online 25 May 2023

Abstract: Authentication based on biometrics is used to prevent physical access to high-security institutions. Due to the rapid rise of information system technologies, Biometrics is now being used in applications for accessing databases and commercial workflow systems. These applications need to implement measures to counter security threats. Many developers are exploring and developing novel authentication techniques to prevent these attacks. However, the most challenging problem is keeping biometric data while maintaining the functional performance of identity verification systems. This paper presents a biometrics-based personal authentication system combining a smart card, a Public Key Infrastructure (PKI), and iris verification technologies. Raspberry Pi 4 Model B+ is the core of hardware components with an IR Camera. Following that idea, we designed an optimal image processing algorithm in OpenCV/ Python, Keras, and sci-kit learn libraries for feature extraction and recognition chosen for application development in this project. The implemented system gives an accuracy of (97% and 100%) for the left and right (NTU) iris datasets, respectively, after training. Later, the person verification based on the iris feature is performed to verify the claimed identity and examine the system authentication. The time of essential generation, Signature, and Verification is 5.17sec,0.288, and 0.056 for the NTU iris dataset. This work offers a realistic architecture to implement identity-based cryptography with biometrics using the RSA algorithm.

Keywords: Multimodal iris recognition, Convolutional Neural Network (CNN), biometric signatures, RSA algorithm

1. Introduction

Unlike conventional methods, biometric techniques are rapidly developing technologies that can be utilized in automated systems to effectively and uniquely recognize and verify a person's identity without remembering or bringing anything. As the biometric identification process offers several advantages over conventional identification techniques, it has become widely accepted as the method for the user's unique identification. It becomes critically important for the biometric identification process to be safe from attacks in applications where security is of high importance, such as e-commerce [1]. Identity theft has been a major concern in the internet age, and uniquely identifying an individual is proved to be their best defense. This paper aims to design a multimodal biometric method depending upon the design of a deep learning model of a person's (right & left) irises image. At first, the Convolution

*Corresponding author: hudamm2014@gmail.com

Neural Networks –Support vector machine (CNN-SVM) model has been trained, and the efficiency of the system was examined on a dataset generated in the laboratory of Northern Technical University (NTU) by night vision camera.

Later the recent technique to digitally sign a message utilizing biometrics- combination with the digital signature key generation, so, merging the benefits of Public Key Infrastructure (PKI), through the utilization of the biometric-based digital signature generation that is secure, reliable, quickly comfortable, non-invasive, and clearly describes the transaction creator [2]. Managing the private keys has remained the main concern with PKI algorithms. They are vulnerable to attacks for information theft. Using biometrics for private key access can resolve this key management concern. A mechanism to secure the private key and prevent the risk of a breach is required. This will prevent the hackers from stealing the private key. These two techniques' results are provided as input to the Raspberry Pi 4 Model B. This model can contain personal information, cryptographic keys, and other information stored in a built-in and secure form. The major objective of this study can be summarized in the following aspects:

1. Design and implement a multi-biometric iris recognition system that can overcome world requirements of security challenges.
2. Implement an efficient iris localization model to detect the iris region.
3. Build a Convolutional Neural Network-Support Vector Machine (CNN-SVM) model to extract a set of unique features of the same person's right and left eyes and a classification stage.
4. Design a new method to generate digital signatures using biometrics (iris template) and has been denominated as Biometric Signature [3].
5. Allow multiple key generations using the same biometric template.

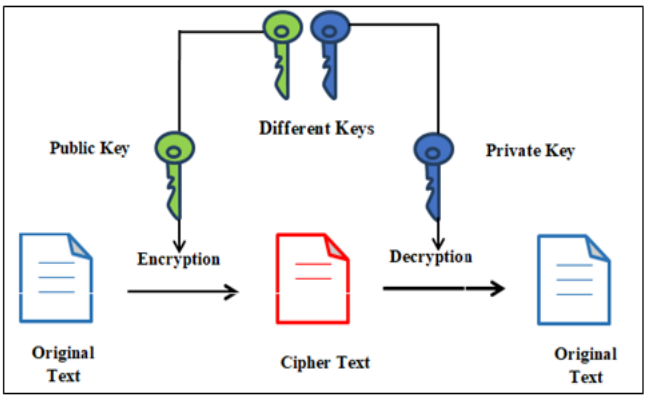


Fig. 1 - Encryption and decryption by RSA [3]

The remainder of the paper is organized as follows: Section 2 contains a review of the suggested methods. The achievement of the biometric digital signature system is defined in section 3. Section 4 discusses the results of the strategies implemented. The conclusion and future work are explained in Section 5.

2. Related Work

This study discusses biometric signature technique systems that depend on the biometric features produced by various authors based on their experiments. The most significant studies related to this research. The authors in [3] have suggested a new approach for generating digital signatures utilizing biometrics, named biometric signatures, and presented two methods for creating biometric signatures employing RSA and DSA. The work describes in detail the changes suggested in private key generation utilizing both approaches to facilitate certificate renewal. In addition, utilizing the RSA algorithm in this work presents a new approach for generating private keys for biometric signatures. The speed of biometric signatures utilizing improved iris recognition algorithms, as well as comparative key generation speeds for various biometrics, are demonstrated using JAVA implementations of both methods.

The authors in [4] have presented a biometric approach for producing key encryption utilizing iris recognition stored in a smart card using the author's signature. many measures were taken to ensure the safety and efficiency of the use of the private key. The employed iris recognition is based on a novel emerging technology based on the Flexible-ICA methodology, which contributes to the service's quality. In comparison to other approaches previously employed, this method has a lower Equal Error rate. In 2016, Sireesha and Reddy have been implemented two stages of combination in an iris and fingerprint pictures for biometric authentication [5]. Iris and fingerprint features are calculated by a feature extraction module that has updated the Local Derivative Pattern (LDP) and Gabor-dependent features. Two levels of combination are utilized, like Sensor Level Fusion (SLF) and Feature Level Fusion (FLF). In [7], Raja, Raghavendra, Venkatesh, and Busch were suggested a multi-patch deep features extraction using deep coarse filters to construct a robust smartphone iris authentication method utilizing the visible spectrum [6]. Also, they indicated that the features must be defined in a collaborative subspace to improve the classification performance by

increasing probability, even under a single test enrolment. This approach is tested on the Mobile Iris Challenge Evaluation (MICHE_I) database, where the researchers registered an Equal Error Rate (EER) lower than 2 %.

The authors in [7] have been presented the biometric cryptography of the iris primarily for key generation, cancellable biometrics, key binding, and integrating keys from the iris with public-key cryptographic schemes. The main biometric key generation approach can be divided into the enrolment phase and the verification phase. The enrolment stage checks in the user data and produces a verification string to be compared with the verification stage when a legitimate user wishes to sign in. This main type of biometric cryptography has been shown to be insecure enough as an unauthorized user can still gain access to the system. Therefore, the key binding method shows further how the security of the biometric iris can be enhanced through the use of a fuzzy vault system, which adds an extra layer of protection whenever a legitimate user wants to sign in. Various modules are used in this proposed approach to build a more secure cryptographic key from an iris image [8]. In the first step, iris images from the CASIA Dataset V1.0 are handled to determine the iris region, and this region is normalized into a dimensionally constant rectangular block utilizing Daugman's algorithm known as the rubber sheet technique. To match the rubber sheet models, principal component analysis is performed. Two unique prime numbers have been generated for the selected area of the rubber sheet design which is to be used for the data encryption and decryption operation. The creation of prime numbers underlies the use of most public-key cryptosystems, basically as a primitive required for the generation of RSA key pairs. The technique was used for 105 images of the CASIA dataset and iris segmentation is approximately 85.71%. In 2018, A.Ullah and Mahmood have been proposed a lightweight, shortened, complex digital signature mechanism to provide safe communication between smart devices in person-centered IoT [9]. They utilized less comprehensive operations to perform signature and verification operations, such as person beings signing legal documents and later checking as per witness. Results show that this approach is improving the security intensity to protect against an analysis of traffic.

The author in [10] has been studied a combination of iris templates with the main and commonly utilized digital signature algorithm RSA. The template size of 320 bits improves accuracy at the expense of higher execution and processing time. However, in today's environment, when correct user identification is of prime essential in critical applications such as online financial transactions, banking, and user authentication, precise user identification is critical. With the advancement in system processing power, it is now possible to use template sizes of 512 bit and 1024 bit, and their use can be commonly accepted in critical applications where accuracy is a top priority. The authors in [11] have been provided the first feasible architecture for using the RSA algorithm to implement identity-based cryptography with biometrics. The solution offered in this paper is able to provide a certificate-less digital signature mechanism to the users where public and private keys are produced on the fly. The author has developed a practical solution for integrating biometrics with ID-PKS, which offers complete certificate-less technology for executing digital signatures.

The authors in [12] have been developed a special concept of digital signature named fuzzy signature, which is a signature strategy that utilizes a noisy string like biometric data as a private key but does not involve user-specific auxiliary data (also known as a helper string in the context of fuzzy extractors) for signature generation. They also describe how to implement a biometric-based PKI that employs biometric data as a cryptographic key, which we refer to as the public biometric infrastructure (PBI). In 2020, V. Carmel, and D. Akila have been given a critical review of how biometrics can be effectively implemented to remove one problem of cloud protection, identity theft [13]. A broad range of biometric authentication method protocols and cloud-based applications, particularly to combat identity theft have been previously proposed.

3. Proposed System

This section offers a summary of the proposed method is provided that used two techniques: iris recognition-based deep neural network and digital signature based on RSA algorithm as shown below:

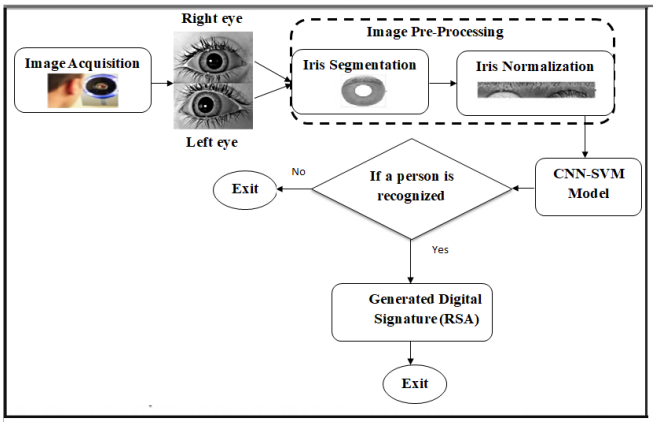


Fig. 2 - Flowchart of the implemented system

3.1 Iris Recognition System Based on Deep Neural Network

1. Image Acquisition: This is an important stage in this system since all the next stages highly depend on the output of this stage. At the first, the iris dataset has been utilized to test the system [1]. After several attempts, images can be directly taken from the camera and entered the port of Raspberry Pi 4 Model B successfully, offering a complete authentication system. Northern Technical University Iris Dataset (NTU) has been collected from 30 persons with 10 iris images from each person by camera infrared [15]. These images are taken under various situations of pupil expansion, eyelids & eyelashes occlusion, and a slight shadow.

2. Iris Segmentation Technique: The inner edge of the iris area is identified before the outer edge, since the pupil is the darkest area in the eye image, and can be easily detected [16]. The pupil localization is performed by converting the grayscale eye image into a binary image utilizing the threshold procedure. In this procedure, all pixels with values greater than the upper threshold are represented as edge points. Moreover, all the adjacent pixels to these edge points with values greater than the lower threshold, are represented as edge points as shown in Figure 3(b). The Canny edge detection technique is used to produce the edge map given the fact that the Canny operator beats other edge detection techniques of detection of iris edges, as shown in Figure 3(c). The pupil is successfully identified by using the CHT to determine the center coordinates and radius of the pupil circle. The pupil area in the binary image is almost completely detected. Figure 3 (d) illustrates the inner boundary of the iris region that has been identified.

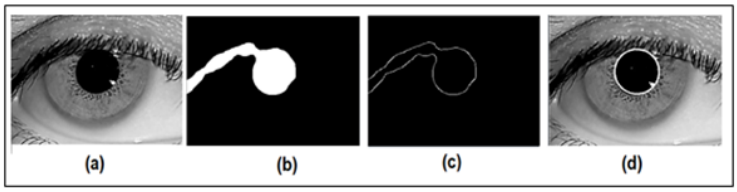


Fig. 3 - Pupil localization (a) the input image; (b) threshold method, (c) output of the canny edge detector; (d) the localized pupil boundary

The most difficult step of the iris localization is locating the outer border of the iris, because of the low difference in intensity between the iris and sclera, therefore is no defined border between them. Moreover, in several cases, the upper portion of the iris is completely hidden by the upper eyelid and eyelashes. The isolated ROI is used in this study to extract the significant features of the iris for its efficient representation, as shown in Figure 4 (b). The 2D Gaussian filter is also used to smooth the photo of the eye and decrease noise, as seen in Figure 4 (c). Then, an edge map of the eye image is created by implementing the Canny edge detector as can be shown in Figure 4 (d). After this, the coordinates of the center and radius of the iris circle are found by performing the CCHT, as seen in Figure 4 (e).

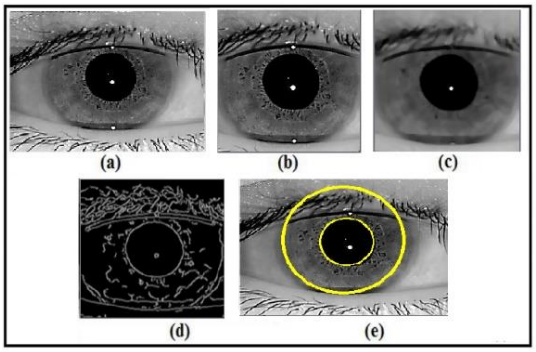


Fig. 4 - Iris localization stages: (a) input image; (b) ROI; (c) the 2D Gaussian Filter; (d) canny edge detector; (e) the final detected iris boundaries

The Gaussian filter is a low pass filter, the 2D parameters of which are determined as follows [17]:

$$G(I) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{I^2}{2\sigma^2}} \quad (1)$$

Where I, is the input image and σ = 0.8 is the default deviation of the Gaussian. Gaussian filter removed the noise and unnecessary detail and enhanced the quality of the image. Then, a Canny edge detector is utilized to create the edge map [18].

3. Normalization: When the iris boundaries have been located, iris normalization is executed to generate a vector of a fixed dimension feature that helps two different iris images to be compared. The iris normalization method is implemented using Daugman's Rubber Sheet mapping to convert the iris image from cartesian coordinates to polar coordinates. The rubber sheet algorithm remaps every point in the segmented iris region in the cartesian (x,y) coordinates[19], to the polar coordinates (r,θ) Where r is at the [0,1] interval, and where (θ) is at the [0,2π] angle. As shown in Figure 5.

$$I\big(x(r,\theta), y(r,\theta)\big) \rightarrow \mathrm{I}(\mathrm{r},\theta) \quad (2)$$

$$x(r,\theta) = (1-\mathrm{r})x_p(\theta) r x_I(\theta) \quad (3)$$

$$y(r,\theta) = (1-r)y_p(\theta) \mathrm{r} y_i(\theta) \quad (4)$$

In which I(x,y) is the region of the iris, (x,y) is the main Cartesian, coordinates, r_p and r_i are the pupil and iris radius respectively, (r,θ) is the conformable polar coordinates x_p, y_p & x_i, y_i are the pupil & iris region coordinates along θ the direction[20].

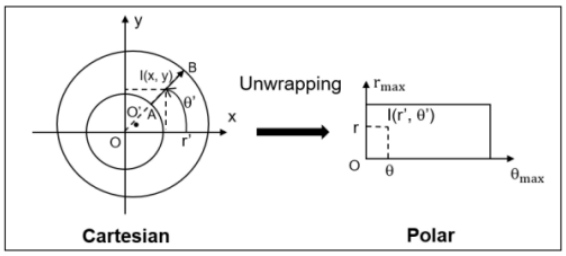


Fig. 5 - Daugman's Rubber Sheet algorithm

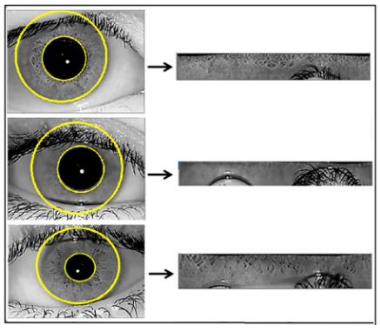


Fig. 6 - Examples of normalization process

3.2 Feature Extraction

This study implements feature extraction and classification using a deep learning method. Two models have been suggested for iris recognition; the first is a CNN model and the second is a hybrid CNN-SVM model. Through this study, the experiments have been performed utilizing (80%) manually selected samples for training, while the remaining (20%) for testing provided a specific set of sample data.

3.3 CNN-SVM Model

Also termed as ConvNet or CNN is a deep learning method that consists of multiple layers. CNN's can be used for various functions such as segmentation, object detection, and recognition. In comparison to other neural network models, the number of parameters in CNN models has been greatly reduced by utilizing share weights and biases [21]. The CNN architecture is made up of several types of layers, like an input layer, a convolution layer, a pooling layer, a fully connected hidden layer, and a softmax layer [22] as shown in Fig.7.

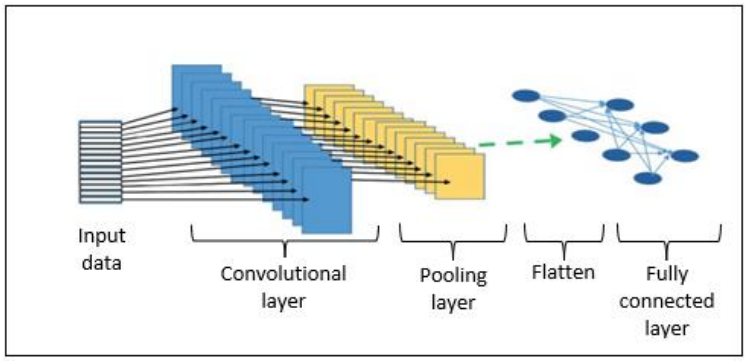


Fig. 7 - CNN architecture [22]

- **Input Layer:** The neural network's input is represented by the input layer, which defines all matrix pixels in the input image. A grayscale or RGB image can be used as the input layer.

- **Convolutional Layer:** Convolution layers is essential in deep convolution neural networks. The convolution layer's goal is to extract the main feature maps by performing a convolution operation (*) around the image. The factor involved with the execution of the convolution operation in the convolution layer is known as Kernel or Filter, and it is a square matrix smaller than an image. The equation of the convolution operation is shown in Eq. (5) [23].

$$y^i = \sum_j (b^{ij} + w^{ij} * x^j) \qquad (5)$$

Where x^j is an input image of the previous layer, w^{ij} represents is the filter's weight across the x^j & y^i while b^{ij} is a filter's bias via the input channel and the output channel, y^i is a neuron in the i output.

- **The rectified linear unit (ReLU)** In the CNN model, the rectified linear unit (ReLU) has been utilized after each convolution layer and fully connected layer. Eq. (6) represents the ReLU activation function [24].

$$f(x) \_ max(0; x) \qquad (6)$$

- **Pooling Layer:** The pooling layer is accountable for lowering the size of the input data [25].

- **Flatten Layer:** Flatten layer is used to convert the multi-dimension input to the one-dimension, typically used in the conversion from the convolution layer to the fully connected layer.
  Fully Connected Layer: In a convolutional network, the fully connected layers are effectively a multilayer perceptron (usually a two or three-layer MLP) that attempts to map the m1(l−1) ×m2(l−1) ×m3(l−1) activation volume from the set of previous various layers into a class probability distribution [26].

- **The softmax** activation function computes the event's probability distribution over a set of n events. This function calculates the probabilities of every target class across all potential target classes. The probabilities obtained later will be useful in evaluating the target class for the provided inputs [27].

$$f(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{K} e^{x_j}} \qquad (7)$$

After the normalization process is finished, the CNN model will be ready to recognize each person. The architecture of the proposed CNN model is shown in Figure 8. CNN model consists of seven layers. CNN takes an input image with a fixed size. Therefore, all training images are resized to 64x360 pixels. CNN layers are partitioned into 2 sections, the first four layers are used for the extraction of features, and the following three hidden layers are liable for the classification of features.

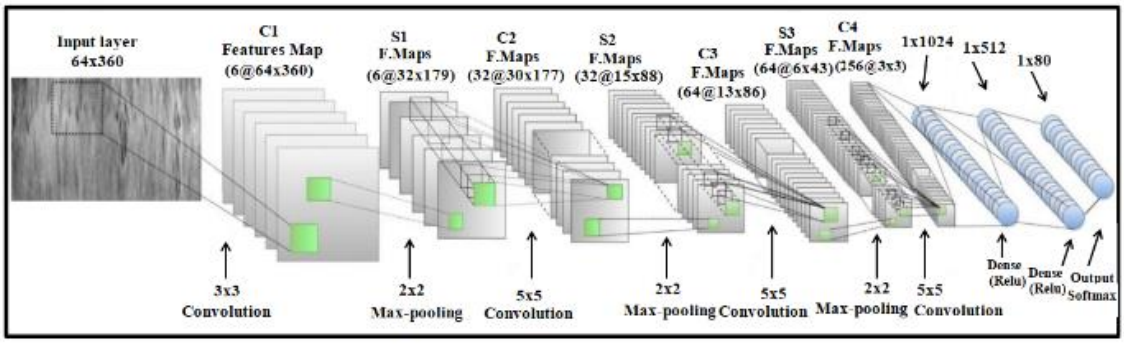


Fig. 8 - CNN model [29]

The system implemented has been programmed to utilize ADAM optimizer with (β=0.9), and (β=0.999), (0.0001) learning rate, 0.0005 Weight decay, and 32 batch size. The detailed definition of CNN layers is shown in Table 1.

Table 1 - The architecture parameters of CNN layers

Layer (type)	Kernel	Kernel Size	Output Shape	Parameter
conv2d_1 (Conv2D)	6	3x3	(64,360,6)	60
maxpooling2d_1 MaxPooling2	-	2x2	(32,179,6)	0
conv2d_2 (Conv2D)	32	3x3	(30,177,32)	1760
max_pooling2d_2 MaxPooling2	-	2x2	(15,88,32)	0
conv2d_3 (Conv2D)	64	3x3	(13,86,64)	18496
max_pooling2d_3 MaxPooling2	-	2x2	(6,43,64)	0
conv2d_4 (Conv2D)	256	3x3	(4,41,256)	147712
flatten_1 (Flatten)	-	-	(41984)	0
dense_1 (Dense)	-	-	(1024)	42992640
dense_2 (Dense)	-	-	(512)	524800
dense_3 (Dense)	-	-	(30)	15390
Output(Softmax)	-	-	(30)	0

2. CNN-SVM Model: The Support Vector Machine (SVM) is a machine learning supervised technique. Because it is exceptionally accurate, able to detect and process high-dimensional information, and flexible in modeling multiple information sources, the SVM classifier is widely used in bioinformatics (and other disciplines) [28]. The CNN-SVM model was created by swapping the last two hidden layers of the pre-training CNN with SVM to improve the efficiency of the CNN model. This model used Pre-training CNN as a feature extractor, and SVM as a classifier. Figure 9 displays the architecture of the proposed hybrid CNN-SVM model. The CNN-SVM model has been trained in two steps. The

training dataset images were supplied into the pre-training CNN model to extract the features in the first stage. The features were then fed into the SVM classifier for training, and the step was repeated on the testing dataset to test the model.

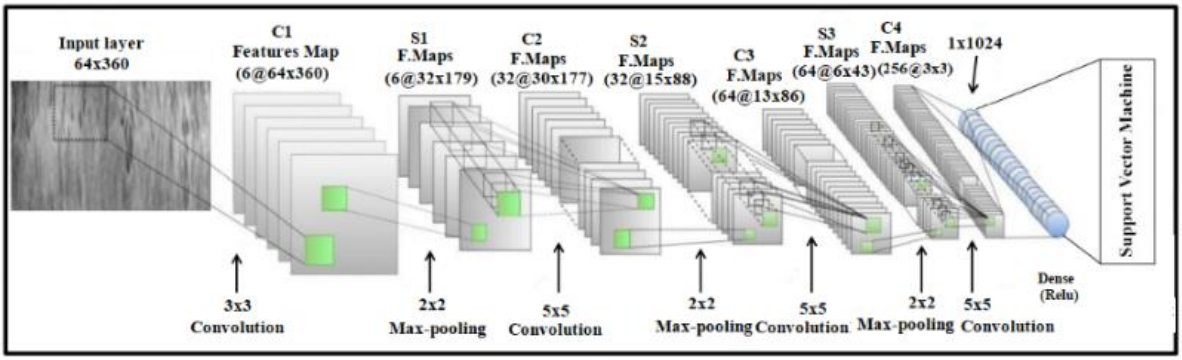


Fig. 9 - CNN-SVM model

3.4 Training Strategies

1. DAM Optimizer: Adaptive Moment Estimation is one of the most popular gradient descent optimization techniques discovered by Kingma and Ba, that measures adaptive learning rates for every parameter and solves the issues with other optimization techniques like learning rate decay, high update variance, and low convergence. The formulae are as follows [30].

$$\left\{\begin{array}{l} m_t = \beta_1 m_{t-1} + (1-\beta_1) g_t \\ v_t = \beta_2 v_{t-1} + (1-\beta_2) g_t^2 \\ \hat{m}_t = \frac{m_t}{1-\beta_1^t} \\ \hat{v}_t = \frac{v_t}{1-\beta_2^t} \\ \theta_{t+1} = \theta_t - \mu . \frac{\hat{m}_t}{\sqrt{\hat{v}_t + \epsilon}} \end{array}\right\} \quad (8)$$

Here β_1 and β_2 are rates of exponential decay, m_t and v_t are estimates of the first and second moment of the gradients, m_t and v_t are variants that have corrected the m_t and v_t bias through the initial iterations to 0 according to the initialization values of m_t and v_t to 0's [31].

2. Data Augmentation: Deep Neural Networks require to be trained on a big number of training samples to accomplish effective prediction and avoid overfitting [32]. In an attempt to increase the dataset artificially for the training of the large model, data augmentation could extend each dataset "by factors of 16x, 32x, 64x, or more" It was achieved by using simple functions such as rotations, cropping, flipping, scaling, translations, and shearing to create several copies from a single image. These techniques could be applied individually/combined to produce more flipped and cropped images [32].

3.5 Digital Signature Based on RSA Algorithm

Biometric Signature-based RSA algorithm is the first public-key cryptography method which is commonly utilized for secure information transfer [33], which ensures both confidentiality and protection. RSA algorithm is utilized with a 2048-bit iris template to produce a private key by determining the nearest number to the biometric template that is relatively prime with the Euler totient equation ø(n) by utilizing it as a decryption exponent, d (maintained secret). The size of p and q have been selected to be 1024 bit; therefore, the size of the modulus is 2048 bit.

1. Transmitter (key and signature generation)

a) Key generation:

1. Creat two prime numbers p, q each1024bit.
2. Find modulus n = p×q then ∅(n) = (p-1) (q-1).
3. Create decryption key, d from the 2048-bit iris template by increasing it to the nearest relatively primary number to ∅ (n). [Private key = (d, n)].
4. Calculate the exponent of encryption (e) as its multiplicative inverse of the (d) modulus ∅ (n), termed:

$$e = d^{-1} mod(\emptyset\ (n)) \quad (9)$$

[Public key = (e, n)] [33].

b) Signature Generation:

1. Calculate messages hash H (m) utilizing SHA1 in which (m) is the message to be signed digitally. Encrypt H (m) with d and n by the equation (11):

$$S = (H(m))^d mod\ n \quad (10)$$

Here S is the signature [33].

1. Encrypt message and signature (m + S) through each previously accepted private key scheme and transmit that to the recipient.

2. Recipient (signature verification)

1. Decrypt the obtained encrypted message utilizing a previously agreed private key mechanism to decrypt the original message and the signature (m + S).

2. Calculate H'(m) from the message, m utilizing the same hash function as the transmitter [34]. Decrypt the signature to extract H (m) utilizing:

$$H(m) = S^e\ modn \quad (11)$$

3. Compare H (m) to H'(m) and check the biometric signature. If a template itself (without incrementing) is relatively prime to ø (n) then utilize the template here as a private key. Because the private key is never transferred, there is also no possibility of the recipient end being misused for the iris templates.

3. Generation Keys from Iris

The iris image's features have been converted to a binary template termed IrisCode (the iris image after processing and encoding) [35]. The features obtained by the CNN is arranged to the feature vector, and then the threshold value is applied, then the feature vector is flattened to 1D.

A private key is denoted in the RSA algorithm as {d, n}, where d is the private part, and as such d here is the private key = iris template. Increase the decryption exponent (d) obtained from SHA1 of the 2048-bit iris template to get the nearest relatively primary number with (n), by choosing an integer d such that GCD [Φ(N), d] = 1. [(d, n) = private key]. Determine the encryption exponent (e) as the multiplicative inverse of the (d) modulus ∅ (n), which is denoted as $e = d^{-1} mod(\emptyset(n))$,[Public key = (e, n)].

4. The Designed Prototype for Biometric Signature Technology

This section describes the overall design of the system explains all the equipment required to establish the system, which is consisting of a Raspberry Pi 4 Model B, Raspberry Pi infrared camera (placed inside a box and having a hole to position the eye on it), CSI camera port of the Raspberry Pi has been used to connect a Raspberry Pi camera, Ethernet cable has been used for attaching the Raspberry Pi to PC laptop through Gigabit Ethernet port, then the Raspberry Pi could be programmed by the keyboard as shown in Fig. 10.

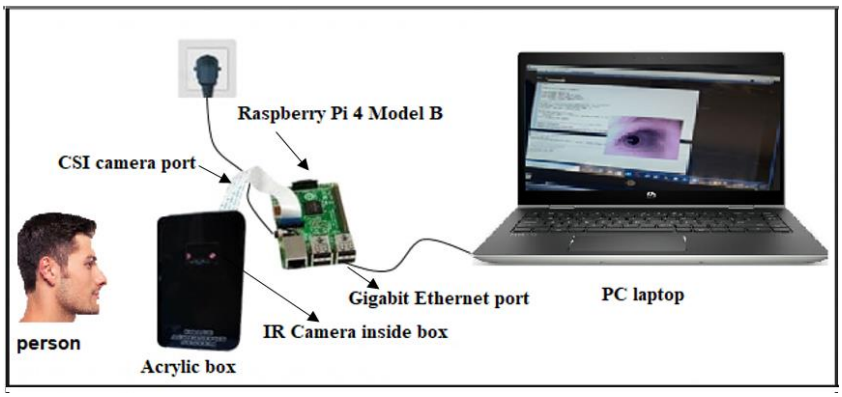


Fig. 10 - Proposed prototype

1. Raspberry Pi 4 Model B: Raspberry Pi is a credit card machine developed in February 2012 by the Raspberry Pi Foundation, which can execute small to medium tasks that can be done by a conventional desktop computer. It provides major improvements in processor speed, multimedia performance, memory, and connectivity compared with the prior-

version “Raspberry Pi 4 Model B” while maintaining drawbacks as the consumption of power. The “Raspberry Pi 4 Model B” specifications are mentioned below and shown in Figure 11:

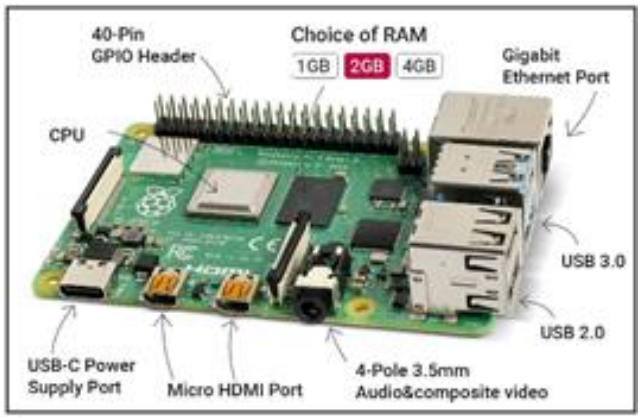


Fig. 11 - Raspberry Pi 4 model B [36]

The Raspberry Pi arrives without an operating system. An operating system (OS) should be installed on a micro Secure Digital (SD) card to use the Raspberry Pi. The most suitable OS that can be used essentially with Raspberry Pi is a Raspbian operating system. This OS is focused on Linux designed for the Raspberry Pi. Raspbian is backed formally by the Raspberry Pi Foundation for OS.

2. Raspberry Pi Camera: Raspberry Pi Camera Board is an official device night vision adjustable focus lens (5MP) with the acrylic box holding by stand carrier. Support all updates of the Raspberry Pi, 5 megapixels OV5647 sensor. Support the relation of flash LEDs and/or infrared LEDs. It also offers a power output of 3.3V, with the best resolution sensor 1080p. Includes 15cm Pi zero camera cable, and dimensions: 72.60 x 24mm (including cable connector) as shown in Figure 12.

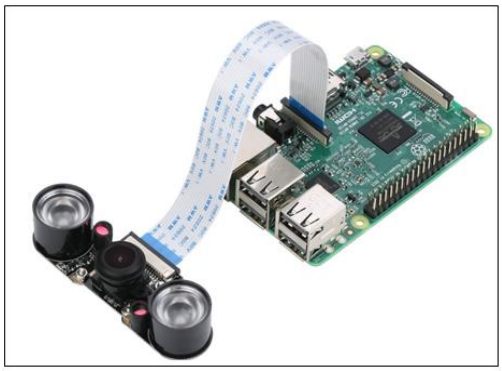


Fig. 12 - Camera setup directly with the camera port on Raspberry Pi 4 [37]

3. NTU Dataset: Northern Technical University (NTU) iris dataset, after many trials on different cameras, it became clear that the Camera Near - Infrared (NIR) Board mentioned in Appendix A2, with night vision enabled and placed inside a box and having a hole to position the eye on it, can be a successful way to capture the image as seen in Figure 13. The specifications of these datasets are described in Table 2.

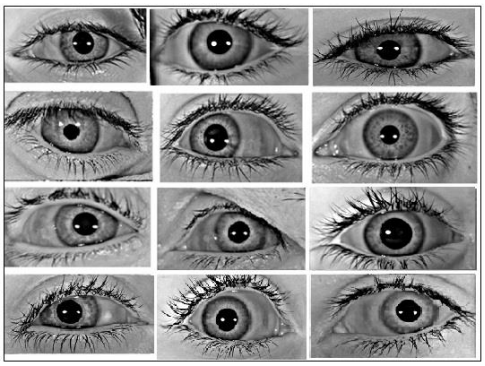


Fig. 13 - Samples of NTU iris database collected by night vision camera [15]

Table 2 - The specifications of NTU iris datasets

Property	NTU
No. of Classes	30
Samples/ Subject	5 right 5 left
No. of Images	150 left 150 right
Image Size	(1024x768) pixel
Image Format	JPG

The Near-Infrared (NIR) wavelengths distributing by the camera detect rich and complex features including black irises. Also, the size of the pupil may change due to the variation of the light, and the associated elastic deformations in the iris texture may interfere with the results of pattern matching. After many trials, images can be taken directly from the camera and successfully entered the port on Raspberry Pi, providing a complete authentication system. Iris images have been obtained from 30 volunteers with 10 iris images from each person. The images were saved in the format of "JPG" with an image size of pixels (1024x768).

4. Personal Computer: The experiments of the Biometric Signature system have been carried out on a Laptop PC (64-bit operating system, x64-based CPU, (8) GB RAM, Core i5--3210 processor, 2.40GHz) using python libraries and Jupyter notebook environment.

5. Results and Discussion

Several experimental tests are presented in this section to evaluate the efficiency of the implemented iris localize, deep learning technique for iris recognition, and biometric digital signature-based RSA algorithm with provided a comparison of key generation speeds.

The major measurement criteria for measuring performance in deep learning and machine learning are accuracy. Accuracy is the number of data points correctly classified from all data points. Equation12 define the accuracy [38]:

$$\text{Accuracy} = \frac{Number\ of\ correct\ classifications}{Total\ number\ of\ classifications}\ x\ 100\% \qquad (12)$$

The dataset then moved through several phases, like resizing the image, dividing the dataset into training and testing, the next phase is loaded into the CNN training dataset to extract its features and verify the trained network and check the accuracy of recognition. Table 3 shows the recognition accuracy of the selected iris image datasets with running time and number of the epoch.

Table 3 - The recognition accuracy of The NTU iris datasets

Dataset	No. of Epoch	Accuracy (%) Train CNN Model	Time (m)	Accuracy (%) CNN-SVM Model	Time (m)
NTUID left	500	96.67%	29m	97%	31.7m
NTUID right	500	100%	38m	100%	38m

The implemented system gets an accuracy of (97% and 100%) for both left & right for the left and right (NTU) iris datasets respectively, after training as described in Figures 14.

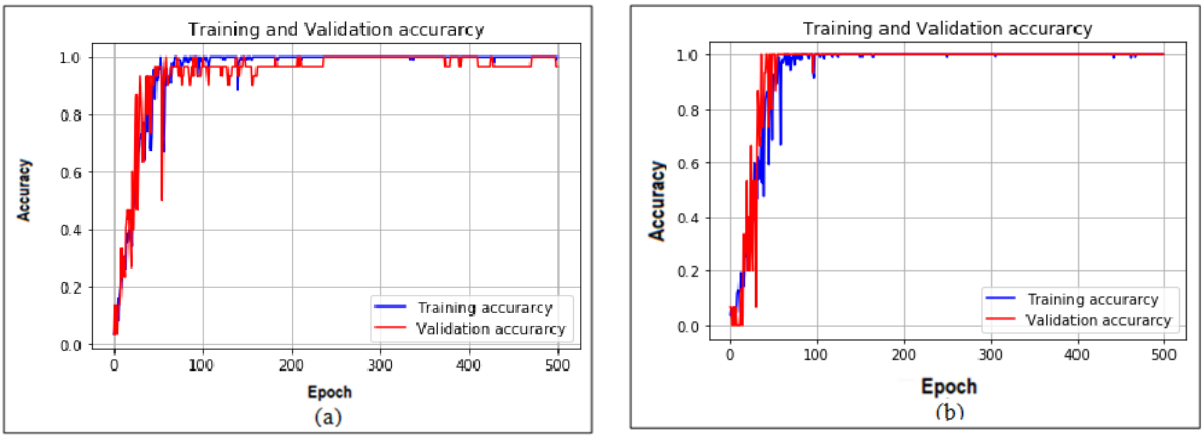


Fig. 14 - Accuracy of training and validation of the CNN model (a) left NTU dataset; (b) right NTU dataset

Figure 14 shows that the accuracy of the training and validation process rises with each epoch as the model has been trained and the model is trained without overfitting problems between the training samples and validation samples. The amount of loss at the end of epochs is shown in Figure 15. It can be seen that a very small loss was 0.004 and 0.00023 obtained for the left and right iris, respectively.

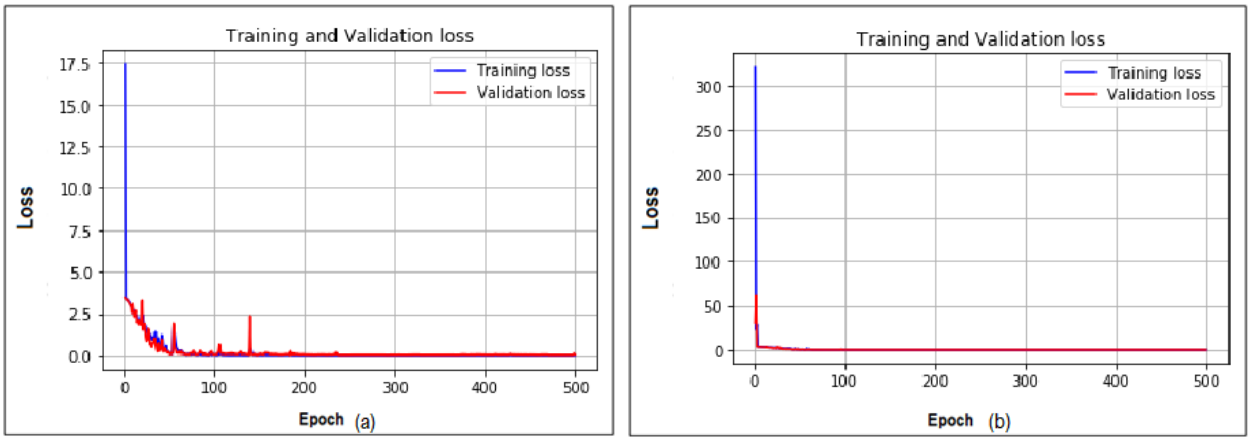


Fig. 15 - Loss function of the CNN model after training process (a) left NTU dataset; (b) right NTU dataset

5.1 Matching and Decision

The template that is produced by the feature extraction module is matched with all the previously saved templates in the system's database to calculate decisions. So that the decision can be taken with high confidence as to whether the two templates are from the same iris or two various irises. The decision is the last stage of the biometric system in which the person is identified or a claimed identity is either accepted (authorizing the person) or rejected (not authorizing the person). The error rate is the rate that divides the number of misclassified samples by the total number of samples. The error rate is determined by the equation below [38]:

$$Error\ rate = \frac{Number\ of\ misclassifications}{Total\ number\ of\ classifications} \quad (13)$$

$$Accuracy + Error\ rate = 1 \quad (14)$$

1. Prediction on One Image with Threshold Value: In this case, a comparison is made by matching the feature vector of the present input with the saved feature vectors within the template. The basic threshold definition for iris classification will read and define the intensity values of every data element is true if the value is above the threshold and false if the value is less than the threshold. To calculate the prediction threshold that decides what the predicted class is, the classification threshold operator depends on the probabilities that the model generates.

$$\text{Classification} = \begin{cases} inclass, & \text{Confidence value} \geq \text{Threshold} \\ outclass, & \text{Confidence value} < \text{Threshold} \end{cases}$$

Here the threshold value is equal to 0.97, and this value has been chosen after reading all the data and finding the lowest true value. The major limitation of threshold methods is that they are often absent for accurate classification.

2. Prediction on One Image with Claim Verification: The authentication system tries to verify the claimed identity of an individual in the matching operation by comparing a verified sample to previously-stored templates and trying to answer the question? What is the claim of this person? Which class no.? In this case, a user claims his identity. So, similar processes of biometric acquisition, pre-processing and feature extraction are performed. Then, with the same claimed identity vector, the resulting feature vector will be matched. This module is referred to as one-to-one matching. At last, the decision on identity is to accept the claim or reject it.

3. Prediction on All Dataset: The model has been loaded to make final predictions for all datasets. The result shows the false prediction of the data predicted false, and the minimum true confidence value is mentioned in Table 4.

Table 4 - CNN predictions (all datasets)

Dataset	Prediction all Dataset	Confidence value
NTU	0.003	0.98

4. Prediction on the Train Dataset: The result of predictions in the training dataset shows the false predictions of the dataset and the minimum true confidence value is mentioned in Table 5.

Table 5 - CNN predictions (train datasets)

Dataset	Prediction Train Dataset Right /Left Iris		Confidence value Right /Left Iris	
NTU	0.0	0.0	0.99	0.98

5. Prediction on the Test Dataset: The result of the predictions of the test dataset shows the false predictions of the data predicted false, and the minimum true confidence value.

Table 6 - CNN predictions (test datasets)

Dataset	Prediction Test Dataset Right /Left Iris		Confidence value Right /Left Iris	
NTU	0.0	0.34	0.99	0.98

5.2 Confusion Matrix

A confusion matrix has been employed to determine the performance in the classification issues. The confusion matrix is C x C matrix (C: here represents the number of classes). It is used to identify the number of samples that are properly classified, and the number of the samples that are wrongly classified. When C=2 (two classes) [39].

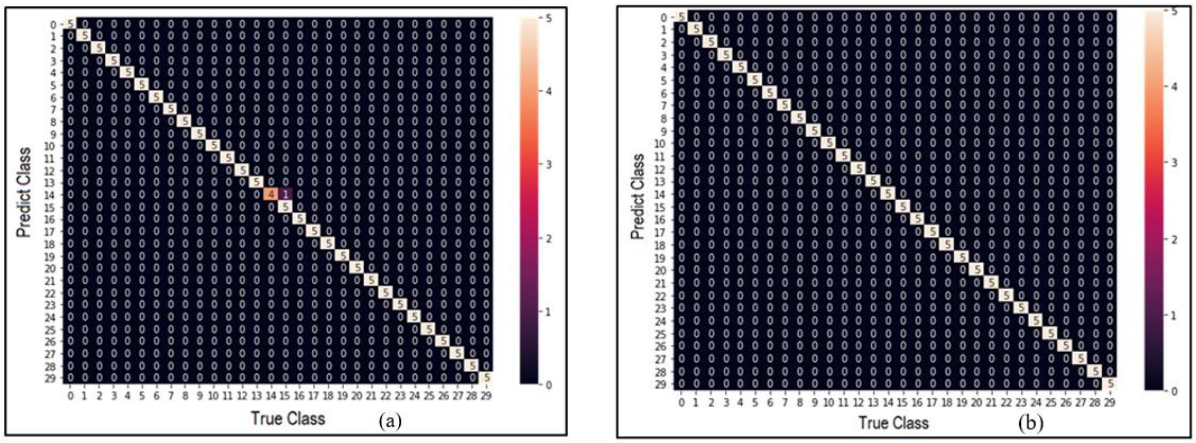


Fig. 15 - Confusion matrix of the model (a) left NTU dataset; (b) right NTU dataset

5.3 Results of Biometric Signatures Using RSA Algorithm

The digital signatures system was designed with the biometric features of the iris to improve the security of the required system. The principal steps of the signing process after obtaining the iris template for the classified person are:

1. Calculate the public and private keys for the classified person.
2. Load the public and private keys from the disk.
3. Input person class no. to load the keys for sending the message.
4. Answer the question? from the left (l) or the right (r) eyes.
5. Input person class no. to load the keys for receiving the message.
6. Answer the question? from the left (l) or the right (r) eyes.
7. Enter the message.
8. Cipher message is.
9. Sender's signature is.
10. Decrypted message is.
11. Verify Successfully (sign by the person no.).

The result of implementing the (Biometric Signature utilizing RSA algorithm) is calculated and a comparison of key generation speeds has been provided. Table 7 shows the average time taken for biometric signature utilizing RSA for various modulus lengths and iris recognition (template size = 2048 bits). SHA1 was used the one-way function to convert the template to (120 & 240) bit of hash by concatenating the results acquired by utilizing (6 & 12) various keys for modulus sizes of (1024 & 2048) bits respectively.

The key generation (calculating n, d, and e) time has been raised for the modulus of 2048 bits because of a more considerable key length included. The time of signature and verification is extremely short.

Table 7 - Biometric signature using RSA speeds for different modulus lengths and template size of 2048 bits (NTU) dataset

	1024 bits (in a sec)	**2048 bits (in a sec)**
Key generation (n,d,e)	2.77	5.17
Signature S	0.158	0.288
Verification	0.022	0.056
Note: SHA1 is used as the hash function to produce message-digest		

The time required for Biometric Signature for various key lengths is shown in Table 7. The key generation (calculating d and e from a provided 2048bit template) time is considered large due to the key length involved, while the time of the signature and verification is too short.

The comparison speed of signature key generation for the different iris templates has been described in Figure 17.

Biometric signature utilizing RSA can be applied with any biometric without limiting template size because the verification time is very shorter, the validity of the private key produced could be tested locally in a short time (in a millisecond).

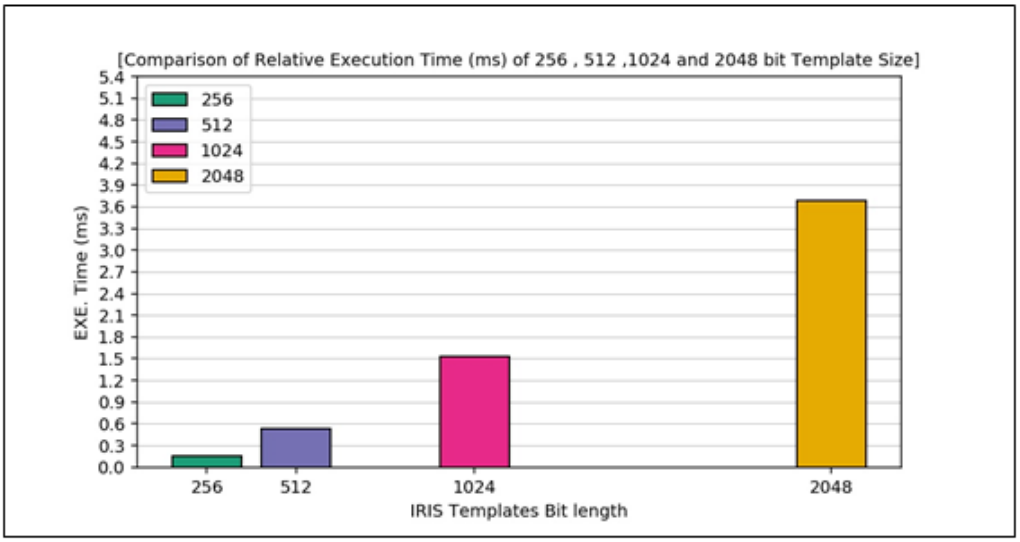
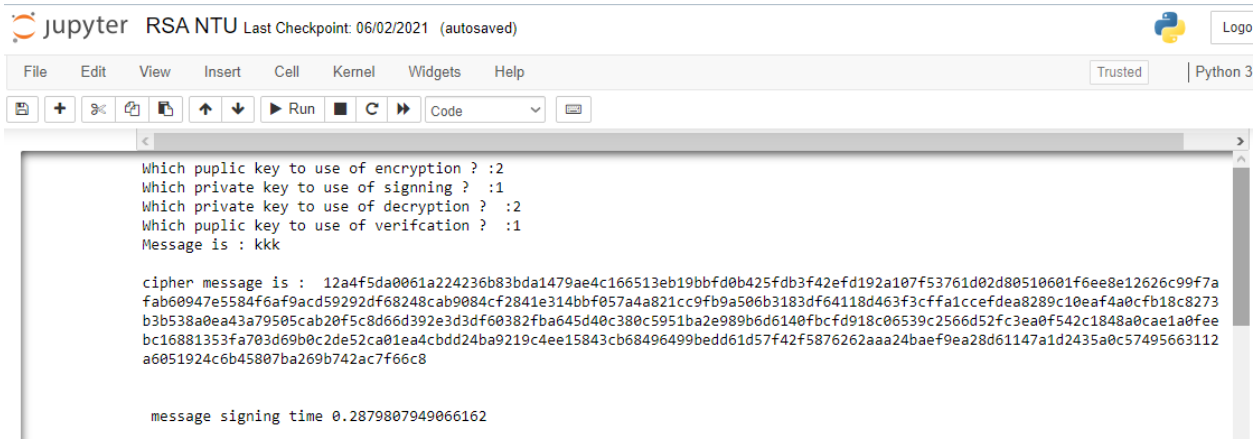


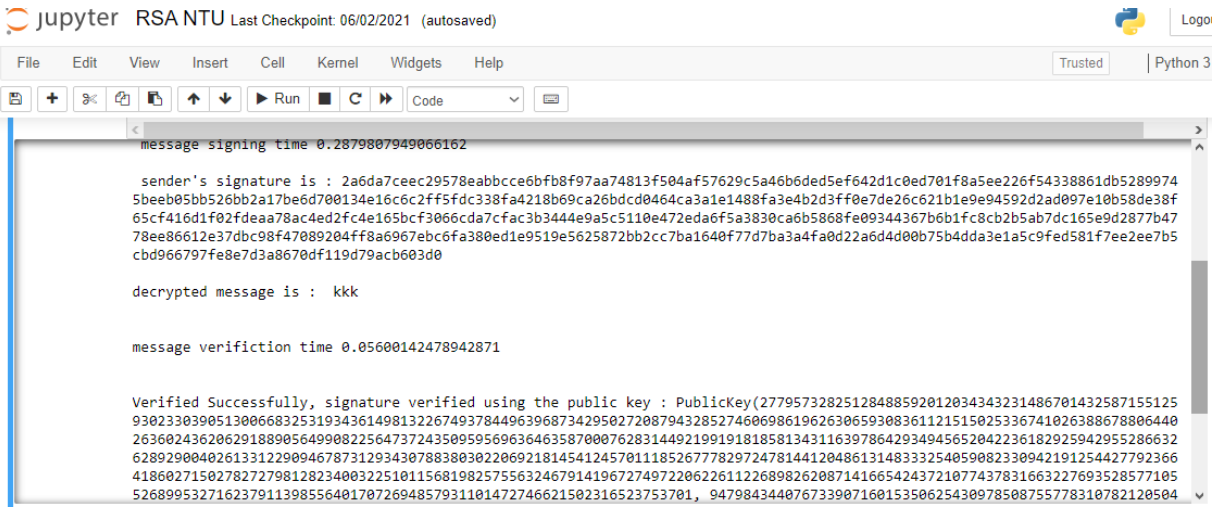
Fig. 17 - Comparison of Execution Time of Different Template Size (NTU Dataset)

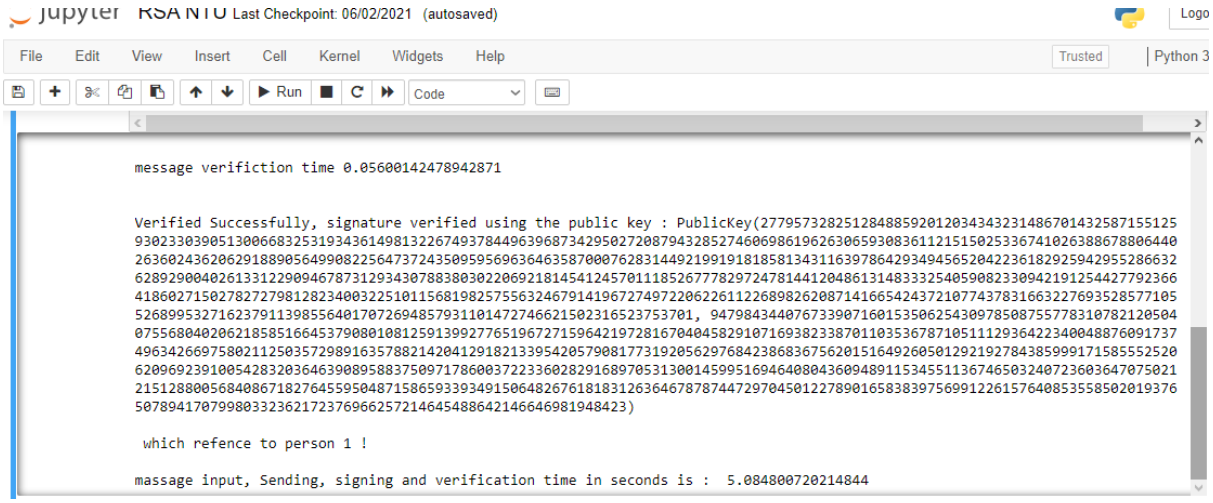
6. Conclusion

In this work, iris recognition for Security applications with the microcomputer Raspberry Pi 4 Model B has been implemented. The powerful and efficient multimodal biometric system has been implemented to determine the person's identity by building a deep learning-dependent approach of the same person's right and left irises. The current system includes image acquisition stage using IR camera, segmentation using CHT algorithm, normalize image by a rubber sheet model, features extraction and classification stage depending on the Convolutional Neural Network (CNN) with a multi_class SVM algorithm to improve the accuracy of the CNN model and the matching of iris templates for biometric identification and verification. The system gets an accuracy of (97% and 100%) for both left and right (NTU) iris datasets respectively after training. The experiments have been expanded to examine the authentication system aims to verify the claimed identity of an individual by comparing a verified sample to previously-stored templates and the decision on identity is to accept the claim or reject it. Based on the results of the iris classification, a new system to create digital signatures using biometrics has been implemented and named biometric signatures. The iris templates are used to be combined with the PKI for digitally signing messages. This method is used to produce a private key based on any size of the biometric template and the RSA algorithm. The Speed of Biometric Signatures based on iris image and comparison key generation speeds for different biometrics are provided. Biometric signatures can ensure long-term stability and high accuracy without limiting the size of the template. The implemented system confirms that it is possible to create a public / private key pair in less than a minute. Private keys may be easily updated periodically or on request. Furthermore, it explains the time of key generation, signature, and verification is 5.17sec,0.288, and 0.056 respectively for the NTU iris dataset. As future work, this design could be modified to use colored iris images, which may provide additional details that can improve the accuracy of identifying iris boundaries. The performance of the current IrisConvNet model could be examined in solving the challenge of heterogeneous iris detection. The use of biometric could be modified to use DNA as the best biometric to be combined with a digital signature that will aid to improve the system performance.

Appendix A: Screenshots of Encryption and Generated Signatures







Appendix B: Components of The Proposed System

(a) The system (b) IR Camera (c) Camera

References

[1] Therar, H. M., Mohammed, L. D. E. A., & Ali, A. J. (2021, June). Multibiometric system for iris recognition based convolutional neural network and transfer learning. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1105, No. 1, p. 012032). IOP Publishing.

[2] Therar, H. M., Mohammed, E. A., & Ali, A. J. (2020, December). Biometric signature based public key security system. In *2020 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 1-6). IEEE.

[3] Khan, A. G., Basharat, S., & Riaz, M. U. (2018). Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange. *Int. J. Sci. Eng. Res*, *9*(11), 992-999.

[4] Janbandhu, P. K., & Siyal, M. Y. (2001). Novel biometric digital signatures for Internet-based applications. *Information Management & Computer Security*, *9*(5), 205-212.

[5] Boukhari, A., Chitroub, S., & Bouraoui, I. (2011). Biometric Signature of Private Key by Reliable Iris Recognition Based on Flexible-ICA Algorithm. *Int'l J. of Communications, Network and System Sciences*, *4*(12), 778.

[6] Sireesha, V., & Reddy, S. R. K. (2016). Two levels fusion based multimodal biometric authentication using iris and fingerprint modalities. *International Journal of Intelligent Engineering and Systems*, *9*(3), 21-35.

[7] Raja, K. B., Raghavendra, R., Venkatesh, S., & Busch, C. (2017). Multi-patch deep sparse histograms for iris recognition in visible spectrum using collaborative subspace for robust verification. *Pattern Recognition Letters*, *91*, 27-36.

[8] Alsulami, A., Teo, D., & He, W. Combining Iris Biometric System and Cryptography Provide a Strong Security Authentication.

[9] Kallolimath, P., & Patavardhan, P. P. (2018). Study and Analysis of RSA Algorithm using Iris for Data Security. *Int. J. Res. Appl. Sci. Eng. Technol*, *6*(5), 2213-2222.

[10] Mughal, M. A., Luo, X., Ullah, A., Ullah, S., & Mahmood, Z. (2018). A lightweight digital signature based security scheme for human-centered Internet of Things. *IEEE access*, *6*, 31630-31643.

[11] Jain, P. (2019). Biometric Encrypted Key Security and Digital Signature, 21(6) 759–769.

[12] Dhir, S., & KA, S. D. (2019). Certificateless Digital Signature Technology for e-Governance Solutions. *Computer Science*, *20*(4).
[13] Takahashi, K., Matsuda, T., Murakami, T., Hanaoka, G., & Nishigaki, M. (2019). Signature schemes with a fuzzy private key. *International Journal of Information Security*, *18*, 581-617.
[14] Carmel, V. V., & Akila, D. (2020). A survey on biometric authentication systems in cloud to combat identity theft. *Journal of Critical Reviews*, *7*(03), 540-547.
[15] NTU Database. Available from: https://drive.google.com/file/d/16H7y1VNunJ-RuKgwZvUsVfUX_bTgwawE/view?usp=sharing
[16] Al-Waisy, A. S., Qahwaji, R., Ipson, S., & Al-Fahdawi, S. (2015, October). A fast and accurate iris localization technique for healthcare security system. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing;* Pervasive Intelligence and Computing (pp. 1028-1034). IEEE.
[17] Kowsalya, S., & Periasamy, P. S. (2019). Recognition of Tamil handwritten character using modified neural network with aid of elephant herding optimization. *Multimedia Tools and Applications*, *78*, 25043-25061.
[18] Kaur, S., & Singh, I. (2016). Comparison between edge detection techniques. *International Journal of Computer Applications*, *145*(15), 15-18.
[19] Daugman, J. (2007). New methods in iris recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *37*(5), 1167-1175.
[20] Choraś, R. S. (2009). Iris recognition. *Computer Recognition Systems 3*, 593-600.
[21] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.
[22] Lin, G., & Shen, W. (2018). Research on convolutional neural network based on improved Relu piecewise activation function. *Procedia computer science*, *131*, 977-984.
[23] Wang, K., & Kumar, A. (2019). Cross-spectral iris recognition using CNN and supervised discrete hashing. *Pattern Recognition*, *86*, 85-98.
[24] Zeiler, M. D., Ranzato, M., Monga, R., Mao, M., Yang, K., Le, Q. V., & Hinton, G. E. (2013). On rectified linear units for speech recognition. In *Proceedings ICASSP*.
[25] Hijazi, S., Kumar, R., & Rowen, C. (2015). Using convolutional neural networks for image recognition. *Cadence Design Systems Inc.: San Jose, CA, USA*, *9*, 1.
[26] Basha, S. S., Dubey, S. R., Pulabaigari, V., & Mukherjee, S. (2020). Impact of fully connected layers on performance of convolutional neural networks for image classification. Neurocomputing, 378, 112-119.
[27] Belay, B. H., Habtegebrial, T. A., & Stricker, D. (2018, October). Amharic character image recognition. In 2018 IEEE 18th International Conference on Communication Technology (ICCT) (pp. 1179-1182). IEEE.
[28] Diab, M. S., & Hamaydeh, M. N. K. (2019). Optimizing Support Vector Machine Classification Based on Semantic-Text Knowledge Enrichment. المجلة الفلسطينية للتكنولوجيا والعلوم التطبيقية, (2).
[29] Al-Waisy, A. S., Qahwaji, R., Ipson, S., & Al-Fahdawi, S. (2018). A multimodal deep learning framework using local feature representations for face recognition. Machine Vision and Applications, 29, 35-54.
[30] Block, S., Goppold, J., & Weiß, M. (2018). An improvement of the convergence proof of the ADAM-Optimizer. *arXiv preprint arXiv:1804.10587*.
[31] Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*.
[32] Umer, S., Sardar, A., Dhara, B. C., Rout, R. K., & Pandey, H. M. (2020). Person identification using fusion of iris and periocular deep features. *Neural Networks*, *122*, 407-419.
[33] Daugman, J. (2000). *Biometric decision landscapes* (No. UCAM-CL-TR-482). University of Cambridge, Computer Laboratory.
[34] Bellovin, S., & Housley, R. (2005). *Guidelines for cryptographic key management* (No. rfc4107).
[35] Boukhari, A., Chitroub, S., & Bouraoui, I. (2011). Biometric Signature of Private Key by Reliable Iris Recognition Based on Flexible-ICA Algorithm. *Int'l J. of Communications, Network and System Sciences*, *4*(12), 778.
[36] Gouillart, E., Nunez-Iglesias, J., & Van Der Walt, S. (2016). Analyzing microtomography data with Python and the scikit-image library. *Advanced structural and chemical imaging*, *2*(1), 1-11.
[37] Dan Aldred et al., Raspberry Pi Camera Guide. 2020. Available:https://www.amazon.com/Makerfocus-Raspberry-Camera Adjustable-Focus-Raspberry-pi.
[38] Alla, S., & Adari, S. K. (2019). *Beginning anomaly detection using python-based deep learning*. New Jersey: Apress.
[39] Al-Nima, R. R. O., Dlay, S. S., Woo, W. L., & Chambers, J. A. (2016, May). A novel biometric approach to generate ROC curve from the Probabilistic Neural Network. In *2016 24th Signal Processing and Communication Application Conference (SIU)* (pp. 141-144). IEEE.