ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 5, No. 4, 130-143 (2020)
www.astesj.com
Special Issue on Multidisciplinary Innovation in Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Composition of Methods to Ensure Iris Liveness and Authenticity

Ali Al-Rashid*

Division of ICT, College of Science and Engineering, Hamad Bin Khalifa University, 00974, Doha-Qatar

ARTICLE INFO

Article history:
Received: 08 June, 2020
Accepted: 26 June, 2020
Online: 18 July, 2020

Keywords:
Authentication
Iris Spoofing Detection
Iris Recognition

ABSTRACT

In a biometric system technology, a person is authenticated based on processing the unique features of the human biometric signs. One of the well known biometric systems is iris recognition, this technique being considered as one of the most secure authentication solutions in the biometric field. However, several attacks do exist that are able to spoof iris. In this paper, we propose a novel approach for securing the iris recognition system by eye liveness detection technique. The proposed system detects the eye liveness, and recognises the iris. This process includes multiple steps. As per the first step, the person opens his eye and the system reads remotely the changes in pupil size as a result of the response to the ambient illumination. Then, the system starts matching the iris with a database. The second step: the person closes his eye and the system remotely detects the heartbeats signals under the skin of the eyelid. As per the third step, the person opens his eyes again and the system reads the pupil size again and compares the results of the pupil size, and then the system matches again the iris with the above database. For the iris recognition to be validated, all the above checks have to be passed. We have conducted several experiments with our proposed system, based on a brand new dataset comprised of 40 subjects. In addition, we also used public datasets: CASIA-Interval, CASIA-Twin and Ubiris.V1. The achieved results show the quality and viability of our proposal.

1 Introduction

Among all human physical biometrics, iris recognition systems are considered the most secure biometric systems that can be operated at a low false acceptance rate (FAR). The applications of iris recognition comprise personal identification cards, border controls, and other government applications [1]. Moreover, the distinct feature of the iris recognition system that makes it so popular in security is its uniqueness; even the iris patterns of twins are different.

However, iris is still subject to attacks. The most well known attacks are called spoofing—whose detection is still an open challenge. Iris recognition technology is considered as a robust authentication technology because of the difficulty of counterfeiting the human iris. But adversaries have found numerous manners by tricking the iris recognition systems through forging the iris [2]. So, researchers began to analyze the structure of the human eye to find effective countermeasures versus the adversary.

An attack technique is to utilize an artificial human iris to be placed in front of the camera sensor to grant authentication to the adversary as the legitimate person [3]. While a popular attack is by using a printed photo. The adversary captures a photo of the targeted user to impersonate him as an authorized user [4]. A countermeasure is liveness recognition, that is employed to identify whether the person is alive or not. One of the common approaches to recognize life signs is the signal of the heartbeats. When the heartbeats occurs, then we cannot ignore the assumption that alive human is facing the sensor. The existing work in recognizing the heartbeats is remote photoplethysmography (rPPG) [5]. The rPPG detects the signals of blood flooding underneath the human skin. Furthermore, various ways to detect rPPG— the widespread technique is probably by sensing remotely the signals of the heartbeats through the face.

The Author in [6] demonstrated the possibility to remotely acquire a heart pulse through one particular camera. The experiment of capturing rPPG is achieved by detecting a certain area of the face skin and calculating a liveness score in the region of interest (ROI) within a short period [6].

In [7], the remote capturing of heartbeats is based on the detection of the color variations in the face skin of the person and recognizes the irregular bio signs. If the indication of the heartbeats under the skin does not occur, it would indicate that the analyzed face is a fake.

Contribution We present in our work a new contribution to detect the eye-liveness, integrated with iris recognition. The proposed methodology is articulated over a series of steps: eye liveness, iris recognition, and again eye liveness and iris recognition. The eye-liveness detection depend on

*Ali Al-Rashid, Doha-Qatar & e-mail: alialrashid@mail.hbku.edu.qa

the reaction of pupil diameter size during the existence of the ambient light, integrated with the remote reading of the heartbeat of the eyelid; while iris recognition is based on matching the iris—with the one previously stored in a database—two times, in real-time.

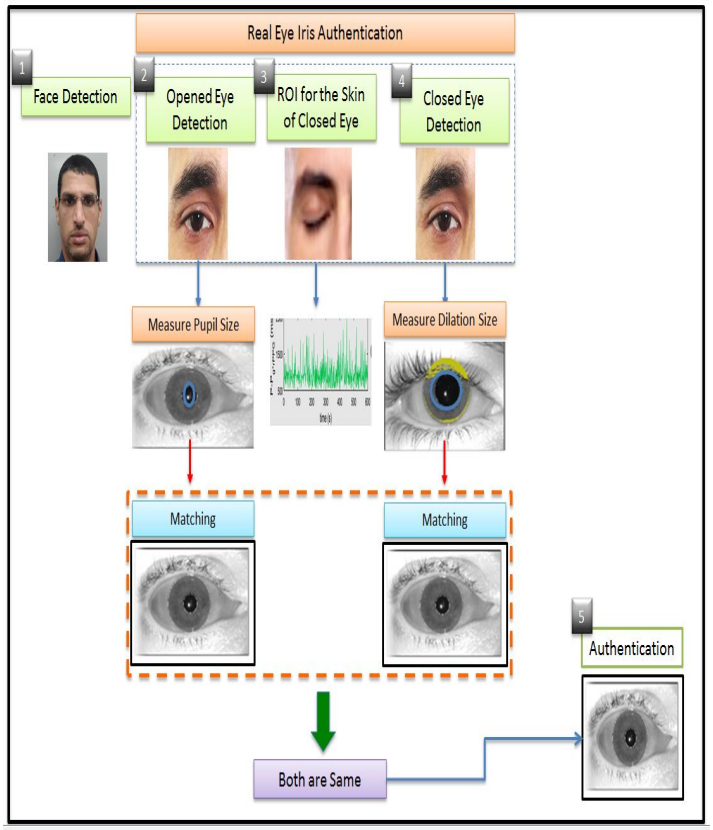


Figure 1: Proposed system

The system starts capturing the face of the supplicant, and runs a time counter. Next, the system recognizes the eye as opened during opening the eye and then reading the actual measurement of the size of pupil diameter. After that, the system initiates matching the person's iris with the database as the first match. Then, the user closes his eyes and the system identifies the eyes as closed and then starts detecting the signals of blood flowing under the eyelid skin as heart pulses. The user subsequently opens the eyes, and the system reads the diameter size of the pupil again to recognize the dilation. The system matches again the iris with the database as a second match. Consequently, if the iris first match is equivalent to the second match, the dilation of the pupil exists, the heartbeat is recognized, and the time counter of the face did not interrupt, then eye-liveness is validated and iris is authenticated.

Roadmap We have structured our proposal as follows: Section 2 reviews the prior art in the field. Section 3 introduces the adversary models and illustrates the methods of spoofing that the can be performed by the adversary. Section 4 presents our system and how to grant a secure authentication discriminating between an authentic and a spoofed eye. Section 5 is the iris recognition and explains the process of identifying the iris from the database. Section 6 illustrates the results of experiment. Section 7 is a discussion of the proposed system. Section 8 reports the limitations of our work, while conclusions are reported in Section 9.

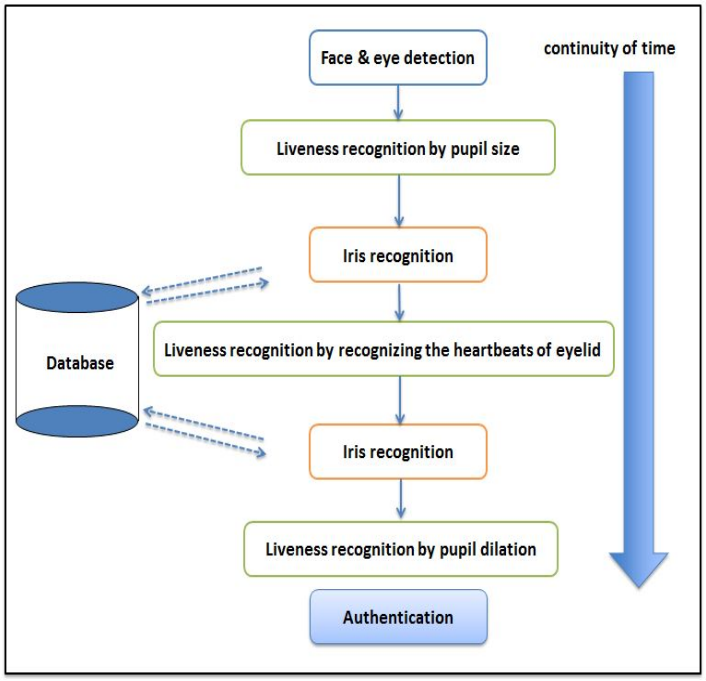


Figure 2: Flowchart for the proposed sytem

2 Related work

The concept of the iris recognition system started initially in 1987 by Flom and Safir [8]. This was demonstrated as a basic matching approach for the imaging system by using mathematical theories.

One of the famous methods for matching iris is the Daugman method. Daugman proposed an automatic segmentation approach, processes for normalization and 2D Gabor filter feature extraction, and match the data to get iris matching [9]. Where [10] made a comparison by comparing the iris recognition algorithm between Principal Component Analysis (PCA), Independent Component (ICA) and Gabor Wavelet for getting iris code.

As countermeasures for spoofing attacks, the previous proposals concentrated on liveness detection. The principle of the liveness is to guarantee that the iris of the eye has a life sign by examining the biometric characteristics of the eye [1]. Basically, illumination technique is one of the popular techniques in forged iris detection, where the eye obtains illumination by focusing light to the eye. So, the pupil reacts with the light by expanding or contraction. The change in the size of pupil confirms the eye is real.

The contributions that depend on checking the pupil radius after centering the illumination have certain restrictions. For instance, if the room is lightened by strong light, then the pupil response could be not satisfactory. Park [2] demonstrated a mechanism utilizing a texture feature to determine the countrified the human iris, by the pupillary light response.

Besides, the illumination method has the ability to identify the corneal whether as alive or fake. The corneal usually

reflects when directly illuminated, and creates a red circle in the center of the pupil. By examining the color that occurs in the corneal [6], an alive eye is recognized. Therefore, the attention concentrated on the reaction of the eye to the light, to discriminate between the alive eye and spoofed eye [11]. The author in [4] proposed Pupil Centre Corneal Reflection (PCCR) method relied on gaze estimation to discriminate between the signals of live and spoof eye. In addition, the vein of the sclera used to identify the liveness of the eye. The sclera is the white region inside the eye and the pattern can be extracted and compare it with the pre-stored database, such as in [8].

Regarding the rPPG, the earlier works were focused on analyzing the face skin of the human [6]. The used method is called a color-based method, it measures the heartbeat from the reflection of the colors that occur on the skin— those colors are the blood streaming under the skin [7]. This method is one of the cornerstone for detecting spoofing attacks.

The work in [12] presented a contactless heart pulse system to detect the fabricated mask of the victim. This approach has been achieved by measuring the heart pulse of the face. Therefore, when the heart pulse of the face is detected, then the face is considered alive.

Finally, the authors in [13] proposed to preventing 3D mask PAD (presentation attack detection) by using rPPG pulse detection.

3 Adversary models

The adversary relies on spoofing to obtain the identity of the legitimate user. In this section, we introduce the techniques of spoofing that have been used to tamper iris recognition systems.

In general, the iris system captures the iris of the person and then matches it with stored images. The major purpose of the adversary is to fool iris recognition systems by using forged iris models of the targeted user in iris recognition devices to grant an authentication. The iris spoofing attacks can be classified as follows:

- Photo Attack;
- Video Attack;
- Contact Lens Attack; and,
- Artificial Attack.

Photo Attack: This type of attack is one of the popular attacks in iris recognition systems due to its simplicity. The attacker uses printed photo one a piece of paper to impersonate a victim. Also, the attacker can use a stored photo in the smartphone to implement the same attack [14].

Video Attack: It is a recorded short video of the victim's eye that encompasses all the parts of the eye such as: iris and pupil. The attacker strives to make the video very clear to view the iris in the screen looks real by the adjusting graphics and the resolution.

Contact lens attack: This attack is considered a development of a photo attack. The adversary prints the iris drawing of the victim on the contact lens in a special manner. After that, he wears a fake lens to authenticate himself and bypass the system. Normally, contact lens attack is not easy to be detected, unless the attacker shows unusual behavior in front of the iris camera.

Artificial Eye: The adversary uses plastic or glass to fabricate a spoofed eye. After that, the attacker place this artificial eye in iris systems to get authentication.

4 Proposed Method

This section details the framework of our system. The system authenticates the eye of the user and identifies spoofing attacks by recognizing a real eye from a fake eye. The proposed system in Figure 1 depicts the liveness of eye recognition. As shown in Figure 1, our system is structured over several stages, described in the following.

1. The system detects the face and starts a timer (the face must be presented facing the camera sensor and the timer will be stopped in case any interruption in the detection of the face.
2. The person opens his eyes and the system identifies the opened eye. Next, begin capturing the pupil diameter and it must be small (because of surrounding illumination) and then matches the iris with the database.
3. The person closes his eyes and the system identifies a closed eye. After that, the system extracts the vein of the eyelid skin.
4. Detecting the heart signals of the eyelid skin.
5. The person opens his eyes again and pupil size will be dilated. Then, the system immediately identifies the dilated pupil and matches the iris again with the database.

Furthermore, the process should be implemented while maintaining its continuity. If any step of the process is stopped or interrupted, then the system detects this abnormal behavior as a spoofing attack. Therefore, when the pupil size is changed before and after closing the eye and the signals are recognized as a heartbeat of the eyelid, and at the same time the iris is matched twice, the system recognizes the eye as real and then iris matching process will initiate.

4.1 Pupil Diameter Detection with Heartbeat Signals Recognition from the Eyelid

As an initial step, the system captures the user's face and a temporal window will set with length T [15]. The window can be configured to execute time-dependent analysis.

Subsequently, pupil diameter detection and rPPG of the eyelid will be performed into various phases, as follows: face and eye detection, pupil diameter size readings, and Region of Interest (ROI)detection with rPPG readings recognition.

4.1.1 Face Detection

Capturing the face precisely is necessary to capture the eye in clear view and to determine good quality candidate regions of the eye. Consequently, the false positive rate will be reduced and also the computation time. The Haar-like feature

is typically the used approach for detecting the face due to its fast processing and accuracy [16].

4.1.2 Eye Detection

The eye-detection implemented by using Haar-like features and a cascade classifiers algorithm. As explained in the previous section, if face detection is performed accurately, the efficiency of detecting the eye will be raised as well [16].

4.1.3 Pupil Detection

Pupil detection is implemented by using the Hough transform algorithm [17]. There is a pre-processing step that must be achieved before implementing the Hough transform [17]. First, we have transformed the image into a grayscale. Next, we got the major data of the eye contour. To implement this stage, we used the 'Prewitt filter' to obtain the contour image [18]. It gives two types of edges Gx and Gy on the image, where Gx detects edges in horizontal direction and Gy detects edges in vertical direction as demonstrated below:

$$Gx = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 1 & 0 & -1 \end{bmatrix} \; Gy = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 1 & 0 & -1 \end{bmatrix}$$

And the contour image as shown in Figure 3:

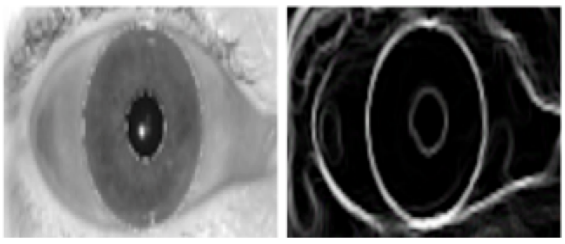


Figure 3: Prewitt filter to get the contour of the eye image

When the circle is detected on the image, the pattern of the pupil is extracted and stored. To get the circle of the pupil after this stage, we apply Hough Transform.

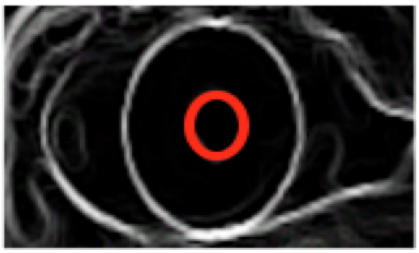


Figure 4: Hough circle

4.1.4 Region of Interest (ROI) Selection

The ROI is a significant element in the captured image of the eye. It locates the skin portion of the eye [19, 20]. Furthermore,the ROI determines the external layer of the eyelid which includes the vein (inside the vein is the blood flowing, used for the detection of the heart pulses).

4.1.5 rPPG Extraction

Once the ROI of the eyelid is determined in the image, we begin measuring the rPPG based on the average of the pixels which are located inside the eyelid skin [6, 7]. The measurements are accomplished independently, over three separate colored channels: Red, Green, and Blue (RGB). Accordingly, rPPG measurements appear on RGB image at every frame and the output appears on the temporal window [7].

4.2 Feature Extraction

4.2.1 rPPG signal pre-processing

The signals generated from the rPPG contain the light variations from the heart-beats and the light surrounding the environment [12]. So, signals of the rPPG are affected by the light of the environment, and compounded with the noise from other sources. Hence, a pre-processing step is important to be performed before getting the rPPG signals. The step consists of three stages as follows [6, 7, 12, 13]:

- Detrending filter: it operates as a temporal filter that is utilized to reduce the static part of the signals that produced from the rPPG. For instance: reducing the signals that are not part of the expected heartbeats and removing the interference of light environment.
- Moving-average filter: this type of filter used to remove the random noise of rPPG signals. This random noise could occur due to incorrect parameters which are gained during the image capturing.
- Band-pass filter: commonly, the human heart rate ranges between 40-240 bpm (beats per minute), which is equivalent to a frequency between 0.6 and 4 Hz. Therefore, the frequency outside this range will be be removed (because they are not heart pulses).

4.2.2 Transformation of the eyelid skin to frequency

This phase has a special input signal, which is, filtered rPPG signals. The filtered rPPG is the extracted signals from the estimation of the changes in eyelid skin tone caused by the blood streaming under the eyelid skin. Now, the extracted signals will be converted to the frequency domain by using fast Fourier transform (FFT) [6, 13].

4.2.3 Extracting the heart pulse

The extracted domain after the pre-processing step shows a range of frequencies; the highest frequency peaks are the heart pulses. In our state, we need to detect the heart-beat to identify the real eye or fake eye.

The method applied to the features is called transformation. The signals are converted from the domain to the frequency by applying fast Fourier transforms (FFT), and later its power spectral density (PSD) distribution is computed [12]. The patterns of PSD present the discrimination of the eye—whether it is a real or a spoofed one. An alive eye has an obvious peak in the PSD, while a spoofed eye has random noise peaks in PSD [21].

Subsequently, we extracted for every color channel two features for detecting the real eyelid.

In the feature extraction stage, PSD is visible and its maximum power response is specified as first feature P. The frequency range (expected between 0.6 - 4Hz), is the second feature R which is the ratio of P to the total power. The pair of features (P, R) are the outcome of three channels of RGB video [21].

5 Iris Recognition

This section explains the stages of processing the iris image and then matching the database.

5.1 Segmentation

The segmentation method is used to get the contours of iris precisely, which is an inner boundary comprising the pupil with the iris and an external boundary comprises the iris with the sclera.

These boundaries are used to discriminate the pixels whether there is the iris. So, this outcome produces a binary mask that consists of on-pixels (belong to the iris) and off-pixels (do not belong to the iris) [22]. Subsequently, the Hough Transform Circle is used to determine the circular iris area. The segmentation step generates two contours (iris and pupil) that will be used in the next step which is the normalization, as depicted in Figure 5.

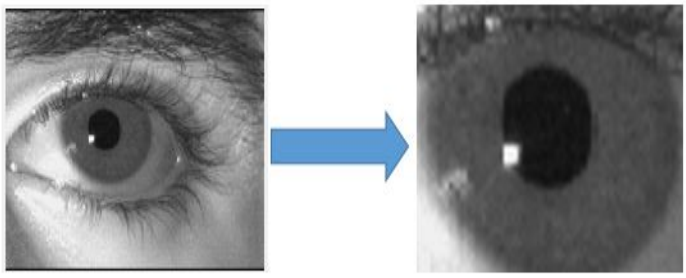


Figure 5: The left image is the original eye for a subject and the right image is the eye after segmentation

5.2 Normalization

The normalization converts the area of iris into a straight strip by using the Daugman's rubber-sheet technique, as depicted in Figure 7.

Daugman's rubber-sheet manner is a popular technique for iris normalization which transform the circle of iris area to a rectangular block with a fixed size [22].

$$I[x(r,\theta), y(r,\theta)] \rightarrow I \tag{1}$$

Based on equation (1), the equation converts the pixels in the circle of the iris into an equivalent location on the polar axes (r, θ), where r is the radial distance and θ is the rotated angle at the corresponding radius.

5.3 Encoding

With encoding, the iris texture will be extracted through filtering the normalized image by using a Gabor filter method, as shown in Figure 8. The Gabor filter has the ability to generate an optimum conjoint representation of a signal in space and spatial frequency. [23] Moreover, a Gabor filter is structured by modulating a sine/cosine wave with a Gaussian.

So, using the Daugman method we can later use the 2D Gabor filter to encode the iris data. The equation of the 2D Gabor filter over the image domain as (2):

$$G(x,y) = e^{-\pi[(x-x0)^2/a^2+(y-y0)^2/\beta^2]} e^{-2\pi[\mu(x-x0)/v0(y-y0)^2]} \tag{2}$$

where, $(x0, y0)$ determines the position on the image, (α, β) determines the actual width and length, and $(u0, v0)$ determines the modulation, which has spatial frequency t $(u0^2 + v0^2)$.

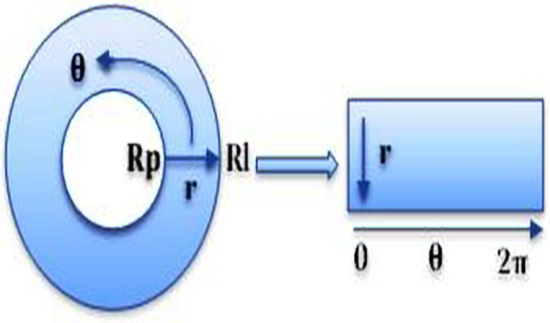


Figure 6: Daugman's model used for iris normalization.

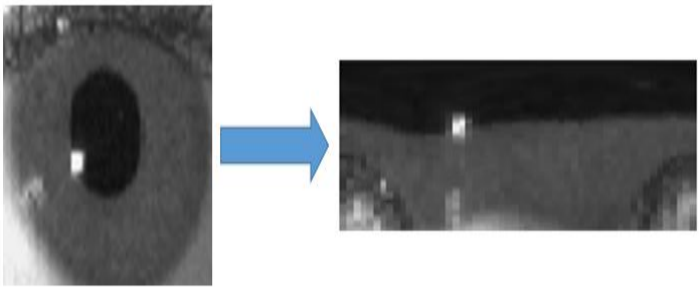


Figure 7: The subject's iris converted to strip by using normalization method.

5.4 Matching

The matching section is the final stage. It compares two iris codes using the Hamming distance (HD) between the binary codes corresponding to the selected points within the iris templates.

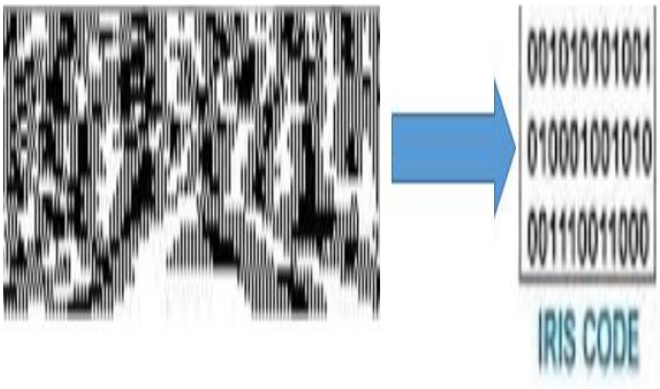
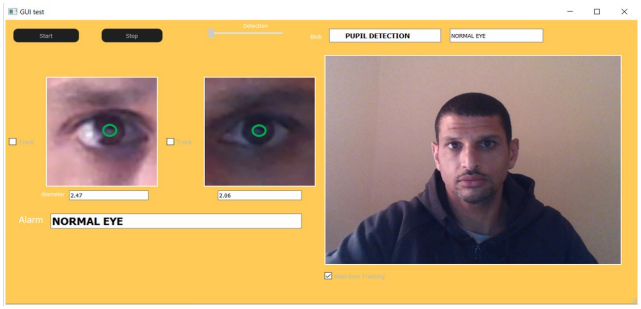
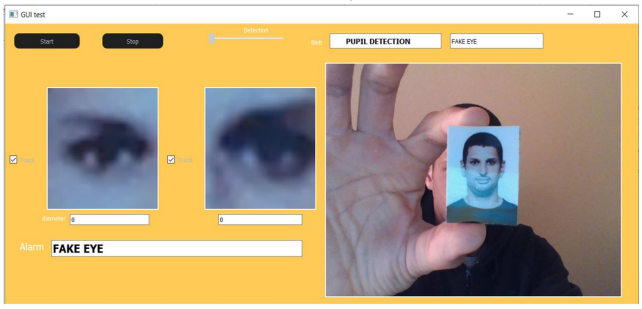


Figure 8: Encoding stage by converting the normalized iris to iris code

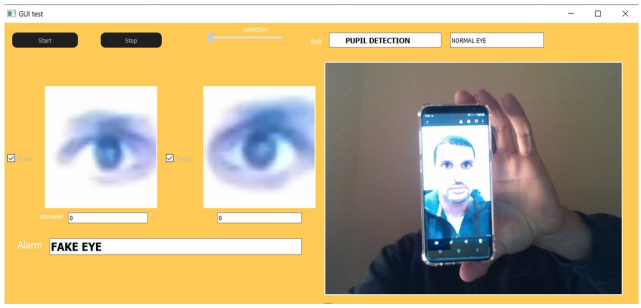
Indeed, if two patterns are derived from the same iris, the HD between them will be close to 0. In this stage, we match the iris two times to make sure the same user is physically present in front of the sensor. The first check, when the user opens his eye, and the second check when the user finishes from measuring the heartbeats through the eyelid while closing the eye and then open again his eye.



(a) Real eye



(b) Photo attack



(c) Video attack

Figure 9: (a) Real eye. (b) Photo attack. (c) Video attack.

The principle of matching the iris two times with running a timer is to make sure that it is the same user present in front of the sensor, otherwise the attacker could first pass the liveness process, and then fool the system by using counterfeit iris.

6 Experiment and Results

6.1 Experiment Setup

The experiments were conducted with the resources reported in the following.
The hardware: 1. PC with OS Win10 ; and, 2. two cameras sensors: one infrared camera type DingDangSmart 2MP 1080P OV2710 Mini IR Webcam and one cameras type Logitec C930e. We fix the two cameras on one stand. The first camera (infrered camera) was used for detecting the pupil diameter size and iris of the eye and the second camera (logitec C930e) for detecting the eyelid.

The application software: we designed GUI (Graphical User Interface) by using QT program, C++ for pupil diameter detection and iris matching and python for heart pulse detection through the eyelid. The first GUI is configured to camera 1 and captures the pupil from a 1-meter distance and shows on the screen the actual diameter size of the pupil depicts as in Figure 10 and matches the iris with stored database as in Figure 11. Furthermore, it determines the difference between the closed and opened eye through displaying a message.

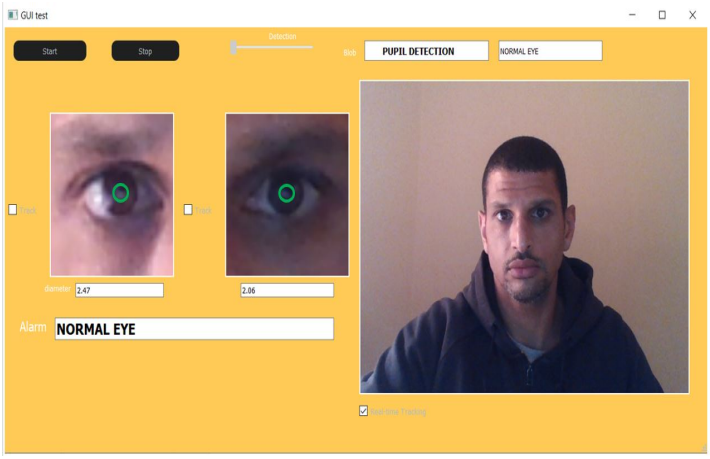


Figure 10: Pupil size recognition

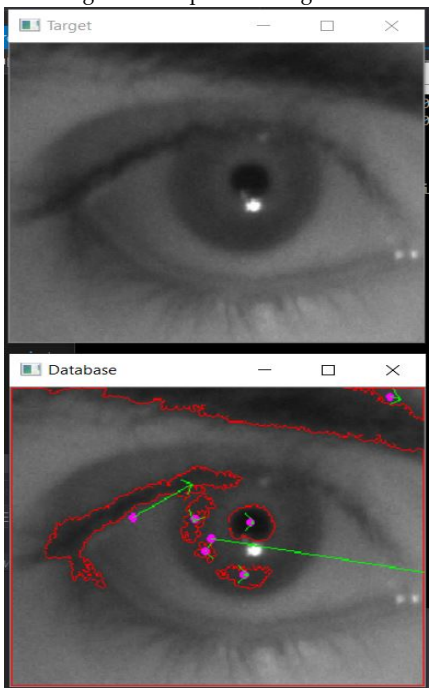


Figure 11: The first image is the scanned eye from the proposed system and the second image is recognized eye with the database.

Also, camera 1 is configured for scanning the iris and matching it with the Database. To detect the heart pulses of the eyelid, we designed another software and configured to camera 2 and measures remotely the user heart pulses of the eyelid as shown in Figure 12. The SW also displays in

Table 1: The pupil size values for 40 subjects

(a) The values of the initial state, dilation, and final state of the pupil sizes for first 20 subjects

Subjects	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Initial State of Pupil Size	2.88	2.34	2.06	2.04	2.55	2.88	2.47	2.53	2.62	2.11	2.06	2.67	2.33	2.26	2.72	2.06	2.42	2.57	2.57	2.31
Pupil Dilation	3.29	2.67	2.88	2.56	3.29	3.31	3.09	3.29	2.77	2.96	2.88	3.19	2.68	2,57	2.88	3.09	2.67	3.29	3.11	2.56
Final State of Pupil Size	2.88	2.34	2.06	2.04	2.55	2.88	2.47	2.53	2.62	2.11	2.06	2.67	2.33	2.26	2.72	2.06	2.42	2.57	2.57	2.31

(b) The values of the initial state, dilation, and final state of the pupil sizes for second 20 subjects

Subjects	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Initial State of Pupil Size	2.87	2.13	2.26	2.72	2.06	2.42	2.57	2.06	2.04	2.55	2.88	2.47	2.53	2.62	2.11	2.06	2.77	2.38	2.46	2.31
Pupil Dilation	3.47	2.67	2.67	3.09	3.91	2.67	3.11	2.67	2.47	3.11	3.21	3.09	3.09	2.88	2.22	2.67	3.67	2.79	3.07	2.56
Final State of Pupil Size	2.87	2.13	2.26	2.72	2.06	2.42	2.57	2.06	2.04	2.55	2.88	2.47	2.53	2.62	2.11	2.06	2.77	2.38	2.46	2.31

real-time the heart pulse on the screen as in Figure 13. In addition, we used certified medical oximeter device type TATRIX Medical fingertip pulse oximeter device for comparing the heartbeats signals with our system.

Figure 12: Eyelid detection

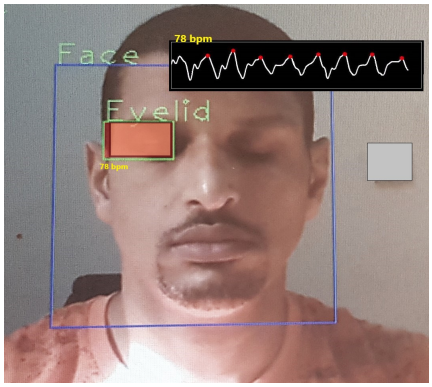
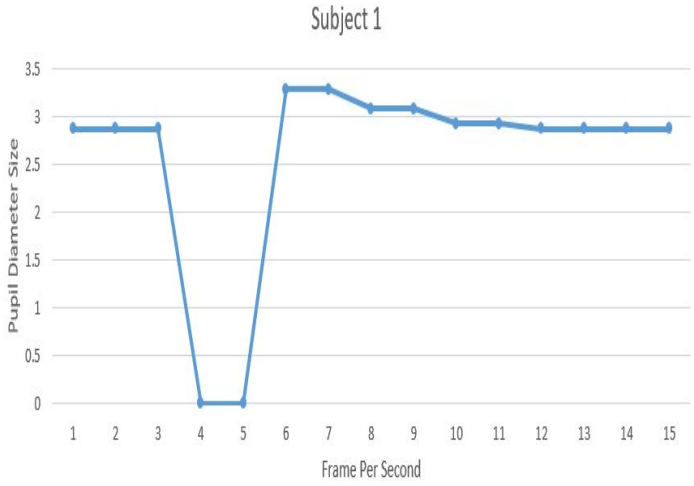


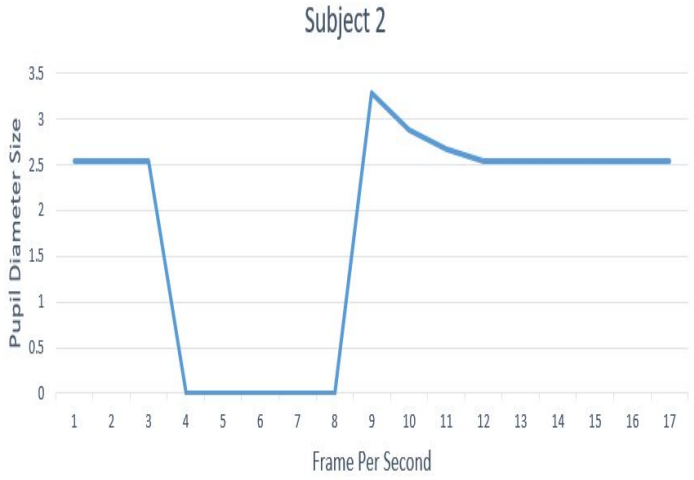
Figure 13: Heart pulse detection by eyelid

6.2 Data

Since, to the best of our knowledge, there is no available dataset for heartbeats signals of eyelid and pupil diameter size changes before and after closing the eye, we have created three data-sets composed of 40 subjects. The first data set is the diameter size of the eye pupil.



(a) Pupil diameter size changes for user 1



(b) Pupil diameter size changes for user 2

Figure 14: Pupil diameter size changes

The second one stores the heartbeats parameters of the eyelid. The third dataset is the iris dataset. In addition, we used external datasets from Chinese Academy of Sciences Institute

of Automation (CASIA): CASIA-IrisV3-Interval contains 2655 samples with 320*280 image size , CASIA-IrisV3-Twins contains 3183 samples with 640*480 image size and UBIRIS.V1 contains 1214 samples 200*150 image size to evaluate the performance for the iris recognition [24].

Algorithm 1: The proposed system for eye liveness detection

Input :Capture the face
While the same face on the screen **do**
Run the continuation timer
Begin Stage 1
The system asks to open the eye for 3 seconds
Detect the face
Detect the eye
End of Stage 1
Begin Stage 2
if *The eye is opened* **then**
Detect the pupil and measure its diameter size;
Match the iris with the database
else
Termination in case the eye is closed;
end
End of stage 2
Begin Stage 3
The system asks to close the eye for 3 seconds...
if *The eye is closed* **then**
Detect the eyelid;
Extract the vein of the eyelid
else
Termination in case the eye is opened;
end
End of Stage 3
Begin Stage 4
if *The vein is detected and the blood streaming detected* **then**
Read the heart pulse signals that come through the eyelid
else
Termination in case not detected
end
End of Stage 4
Stage 5 (Last Stage)
The systems asks to open the eye again
if *The eye is still closed* **then**
Termination
else
Detect the pupil and measure the changes in diameter size
Pupil size must be dilated and starts to shrink gradually until it becomes smaller like the first time in step 2
if *The pupil size is different* **then**
Match the iris with the database
Output: The eye is real and the iris authentication is triggered
end
end

6.3 Methods

We have divided the proposed method into 3 stages: stage 1 for opening the eye, stage 2 for closing the eye and stage 3 for opening the eye again. We created dataset for pupil diameter sizes and iris of every subject. The system captures the pupil diameter with the iris during opening the eye in stage 1 and 3. In the meanwhile the system compares the changes in pupil diameter size and matches the iris two times .

The concept behind the two matches of the iris during the stages is to confirm the physical presence of the subject. In case the iris matched just one time, it means an error occurred in the system or the attacker tried to bypass the camera sensor by forging the iris. As per stage 2, we created a dataset for the heartbeats of the eyelid and measured it for the same 40 subjects. We let the subjects to look at camera sensor (which is dedicated for measuring the heartbeats signals) for 20 seconds. Next, the system detects and stored the heartbeats of the eyelid in database1. Furthermore, we used certified oximeter device to gather the parameters of heartbeats of the 40 subjects and stored them in database2.

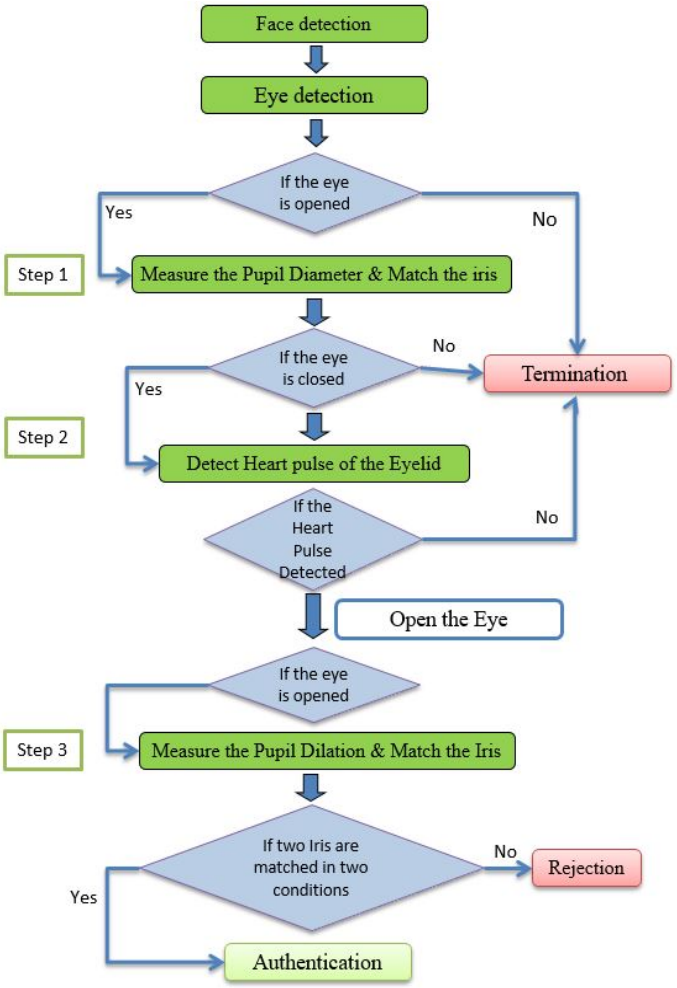


Figure 15: Proposed system

6.4 Results

In this section, we report the evaluation of the results for our proposal.

Pupil diameter detection

We calculated the pupil diameter size while the subject's eye was opened and the diameter size was smaller than while the eye was closed for a short time and then opened again. As shown in Figures 14a and 14b, we observe the curve of the pupil in a static state while the eye is opened. After that, the

curve moves toward "0" during closing the eye and then the curve increased higher than the static state. Then, the curve returns to the static state again because of the response to the surrounding light.

Moreover, we measured the average of the initial state of the pupil diameter size (when the user looks to the camera), dilation state of the pupil diameter size, and the final state of pupil diameter size (when the user closes and opens his eye again) for all the 40 subjects, as depicted in tables 1a and 1b.

Iris recognition In this stage we have examined 40 subjects by matching their irises two times: one before and one after closing the eye. The result of matching the same iris two times—using our algorithm—resulted in a 100% accuracy rate.

Moreover, we used outsource datasets CASIA and UBIRS to evaluate the recognition performance. In table 2 we report the parameters for evaluating the proposed system which checks the same person two times, namely: Correct Recognition Rate (CRR), false accept rate (FAR)—it calculates the probability of the user being incorrectly recognized as another user—, false reject rate (FRR)—it calculates the probability of registered users not being recognized, and Equal Error Rate (EER)—it is the value where FAR and FRR cross. Decision Threshold: when the hamming distance (HD) of two irises is lower than the threshold, then we consider the two iris the same (authorized user). However, if HD of two irises is bigger than the threshold, we consider them as different (unauthorized user). The ROC (receiver-operating characteristic) shows the relationship between the FRR and FAR.

Eyelid signals

We conducted a comparison between the eyelid dataset (database1) and the medical oximeter dataset (database2). Each subject was scanned for 20 seconds by our proposed system along with a medical oximeter device which was attached physically on subject's finger.

The results that we found from database1 were very near to database2 as demonstrated in Figures 16 and 17.

According to the Figures 16 and 17, the curves depict that the parameters are close to each other. We observe that the curve of of the eyelid's heartbeat is very close to the one related to the oximeter, till some variance appears between 13 to 16 seconds because of some delay in the proposed system during the capture of the heartbeats of the eyelid. This delay considers regular because the size of the vein is small which is exists inside in the eyelid and difficult to capture this vein. Besides, the vein of the eyelid differs from subject to subject. However, the delay occurs for few seconds only (not more than 3 seconds). Overall, the parameters of the proposed system are almost the same as the certified oximeter device.

Table 2: Evaluation of our dataset, CASIA-interval, CASIA-twin and UBIRIS.v1

Database	FAR %	FRR %	CRR	ERR
Our dataset (40 irises)	1 0.1 0.01	0.06 3.14 5.67	99.25%	0.74
CASIA-Interval	1 0.1 0.01	1.27 4.27 12.34	98.85%	1.15
CASIA-twin	1 0.1 0.01	1.76 4.32 8.76	98.25	1.75
UBIRIS.V1	1 0.1 0.01	3.67 9.67 19.4	97.57%	2.43

Moreover, with reference to the heart pulse parameters, we measured the mean, the median, and the standard deviation for all the subjects, as shown in tables 3a and 3b.

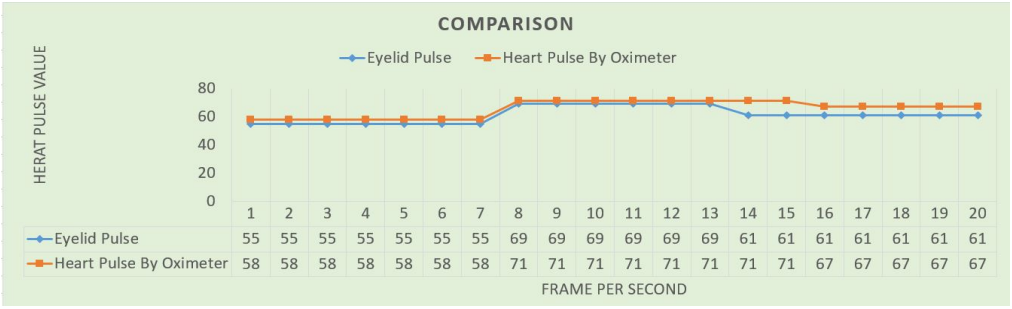


Figure 16: Comparison between heart pulse by eyelid and oximeter for user 1

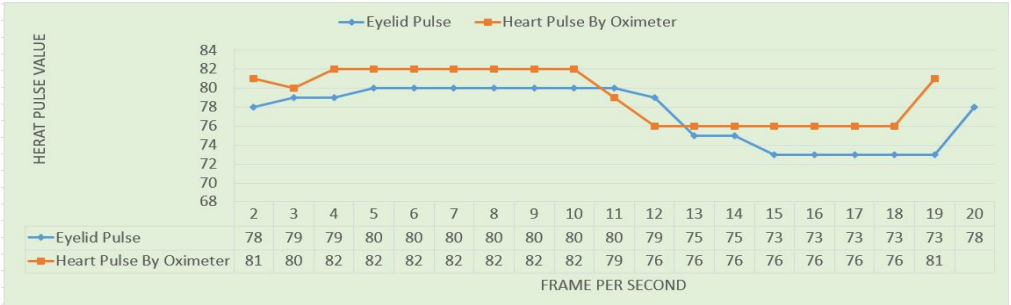


Figure 17: Comparison between heartbeats signals of eyelid and oximeter for user 2

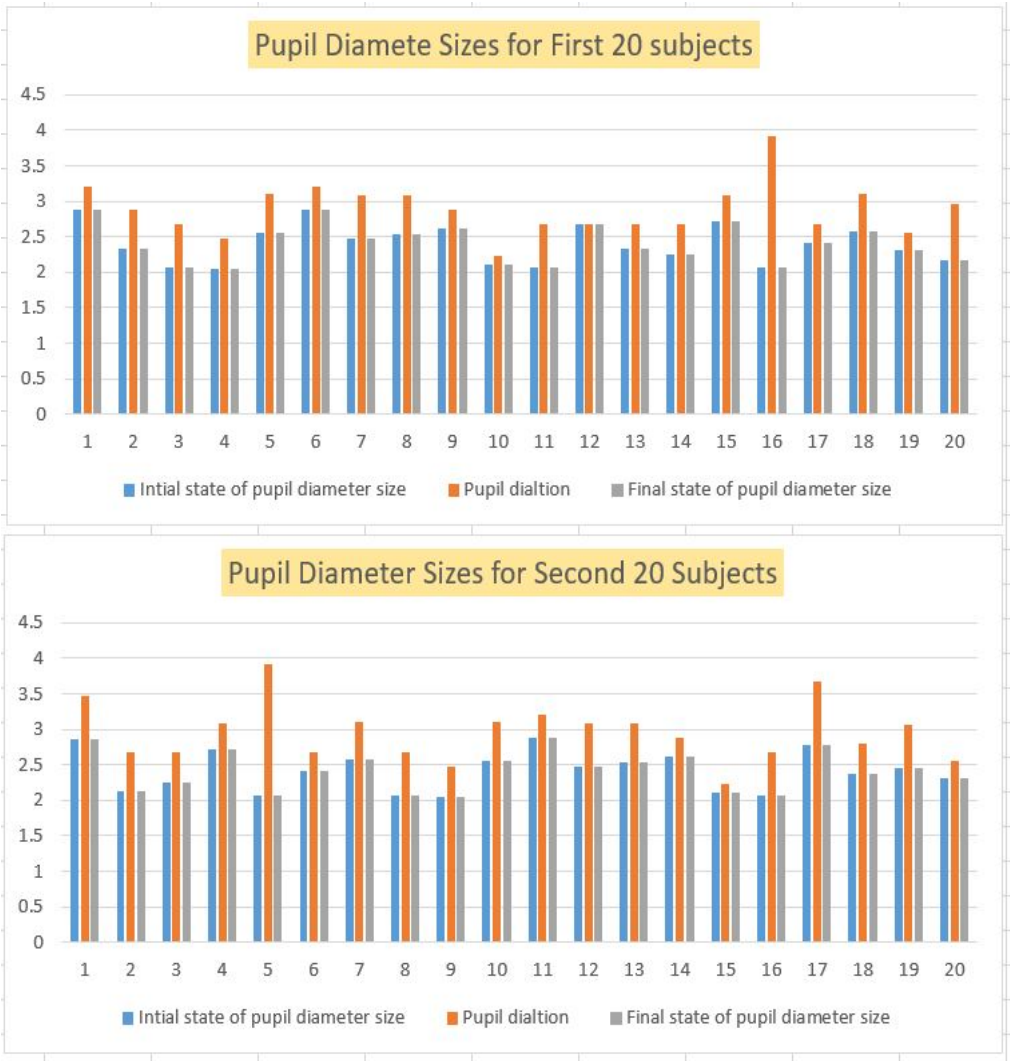


Figure 18: All subjects are grouped, and their pupil diameter sizes is reported to highlight the differentiation between the initial state and dilation state of the pupil diameter size changes.

Table 3: The heart beats parameters for 40 subjects

(a) Mean, median, and standard deviation heart pulse values for all subjects

Subjects	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Mean	55	65	55	70	71	78	55	60	78	55	53	60	59	62	57	61	59	58	72	78
Median	55	65	55	69	71	78	56	60	78	56	53	58	59	63	57	60	60	58	71	78
Standard Deviation	1	1	2	2	2	1	1	1	1	1	1	2	1	2	1	2	5	1	2	1

(b) Mean, median, and standard deviation heart pulse values for all subjects

Subjects	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Mean	55	60	78	70	55	53	60	59	53	60	59	62	59	57	61	59	58	72	65	55
Median	56	60	78	56	53	58	59	53	58	59	63	57	60	60	58	71	65	55	69	71
Standard Deviation	1	1	1	1	1	1	1	1	2	1	2	1	2	5	1	2	1	2	2	2

6.5 Alarms

According to our experiments, we got the average of the pupil diameter change as follows:
- The size of pupil diameter in the initial state (before closing the eye) is **2.4mm**.
- The size of pupil diameter in dilation is **2.9mm**.
- The size of pupil diameter in the final state is **2.4mm**.

Therefore, if the sizes detected at run time are not the same as the above sizes, then an exception is raised an the test would fail—that is, we detected either a spoofing attack or a system error.

The curves in Figures 19a and 19b demonstrate how the fake eyes shape differs from the expected curve. For the first fake eye in Figure 19a, we notice that the curve is in a straight line without any changes in pupil diameter.

As per the second fake eye in Figure 19b, there is no dilatation in the curve after closing the eye. While for the Figures 19c and 19d, we notice that the curve is lower than the initial state, which can be considered as an error, due to incorrect positioning of the user during the scan of the eye.

7 Discussion

In the following, we will discuss the significance of our proposal. Our proposed system is designed to recognize the iris and at the same time the liveness of different parts of the eye: the pupil and the eyelid.

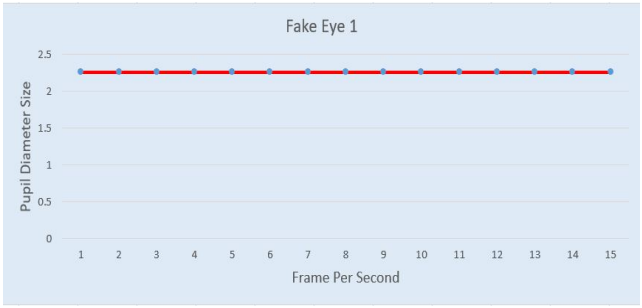
7.1 Pupil analysis detection

As demonstrated in the previous section, we are concentrating on the response of the pupil to the surrounding light without using LED flashlight to decrease the pupil diameter size. The physiological characteristics of the eye make the pupil dilates and shrinks, according to on the surrounding illumination. Therefore, with just ambient illumination, we are able to capture the diameter size of the pupil during all process of our proposal.

According to the Figures 14a and 14b of the experiment, we notice that the curve for the pupil of the subjects was stable when the eye was opened and changed to 'zero' during closing the eye. Next, with opening the eye again the curve raised and then it stabilizes at around the same level of when the eye was initially opened. This experiment proves the pupil's response to surrounding light.

7.2 Iris recognition

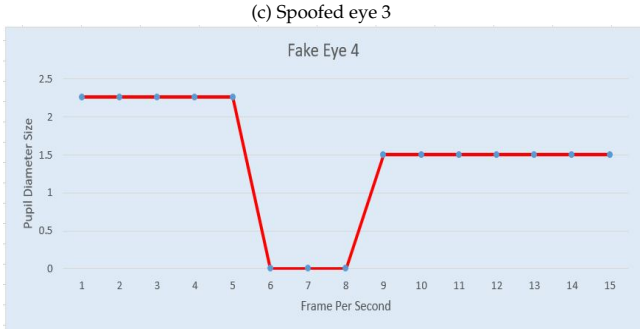
We have conducted numbers of experiments to optimize the performance quality of the iris recognition system. These experiments were focused on finding the best parameters for the Gabor filter in order to raise the performance of the proposed system. As depicted in Figures 20a, 20b, 20c, and 20d, we evaluated FAR and FRR of 4 datasets: our dataset (40 irises), CASIA interval, CASIA-Twin and UBiris.V1. In our dataset, as mentioned, we matched the iris of every subject two times: before and after closing the eye. The two irises that are matched two times must be similar to each other. consequently, we enhanced the recognition accuracy in every time and obtained better results as per the FAR and the FRR, as shown in 20a.
The external datasets (CASIA-Interval, CASIA-Twin, Ubiris.V1) show different results due to their huge datasets compared with our dataset and their image quality and noise as shown in Figures 20b, 20c, and 20d.



(a) Spoofed eye 1

(b) Spoofed eye 2

(c) Spoofed eye 3



(d) Spoofed eye 4

Figure 19: (a) Straight line. (b) The curve in the initial state is equal to dilation state . (c) The curve remains static line without any changes after the initial state. (d) The curve does not raise after closing.

7.3 Eyelid analysis detection

As per eyelid analysis, we provide a novel contribution by measuring the heartbeats of the eyelid. This technique implements liveness recognition of the human eye. Indeed, our

system detects the vein which is located inside the eyelid skin and then our system begins reading the signals of heart pulse.

In the experiment for the eyelid heartbeat, we have matched the results gathered by the proposed system with the results gathered from a certified oximeter machine. Subsequently, the results obtained shown to be very close to each other, while scanning for 20 seconds every subject by both systems, as depicted in Figures 16 and 17.

7.4 Assessment of the proposed work

In this section we show our proposed solution thwarts the previously identified attacker capabilities.

- *Pupil detection:* With the proposed method in pupil detection, the attackers will likely fail in bypassing the checks. For example: if the attacker makes a 3D model of the victim's eye, the pupil size will not change by expanding or contracting as a live eye and, subsequently, the proposed system will detect this 3D model as a fake eye. Note that the attackers could attempt to fake the pupil motion by presenting filmed video. However, these efforts will not succeed. The proposed system captures the diameter size of the pupil and its actual size changes in relation to the period of opening and closing the user's eye.

- *Eyelid detection:* By detecting the heart pulse of the eyelid, the attackers will be faced with another challenge to discover a method to create a fake heart pulse.

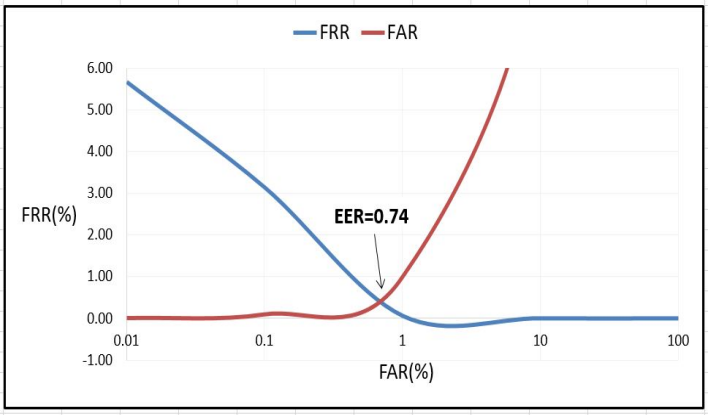
Thus, merging eyelid heart-beat and pupil identification into our solution will enhance the security of iris recognition. As an outcome, we have compared in table 4 our work with prior works in terms of spoofing detection capabilities.

8 Limitations of the proposed system

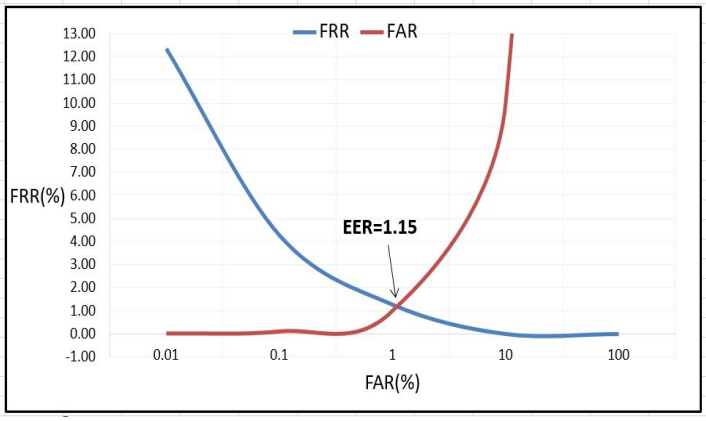
One possibility for an attacker to overcome our solution would be to adopt a new approach in spoofing attacks: eye robot. The attack could be deployed as illustrated in the following.

- *Pupil detection:*
  If the adversary designs an eye robot—including a synthetic pupil—, the robot eye can be configured to have the pupil of normal size, similar to a real pupil, and after a period the pupil size of the robot eye may dilate and contract as a normal pupil. So, there is a probability for the adversary to bypass the proposed system.

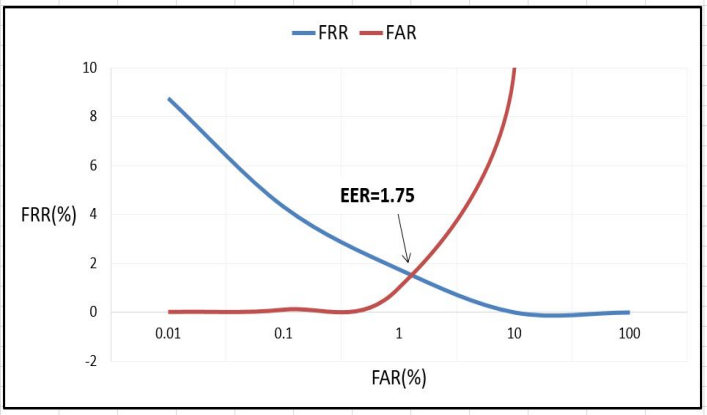
- *Eyelid detection:*
  The eye robot could also have synthetic eyelid and the adversary can add a particular fluid inside the synthetic skin that could mimic the bloodstream—with support of a pump system. Therefore, the proposed system could be triggered into identifying the spoofed pumped-fluid as a real bloodstream.



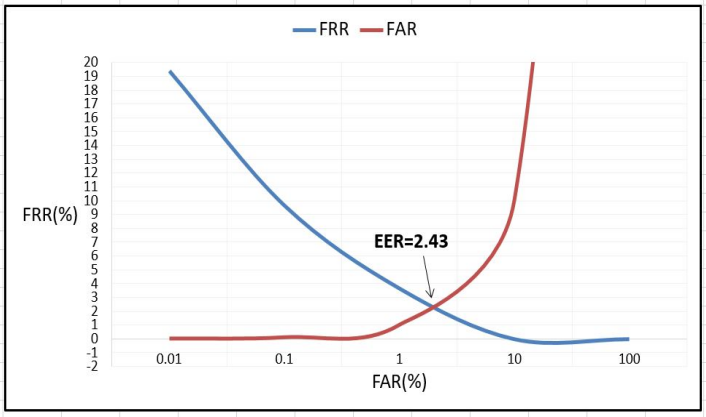
(a) Our dataset



(b) CASIA-interval



(c) UBIRIS



(d) CASIA-twin

Figure 20: The evaluation results of FAR and FRR.

Table 4: Comparison of the proposed work with previous works in terms of detecting spoofing attacks

Author	Features and Methodology	Photo attack	Video attack	Artificial Eye	Contact Lens	Fake Eyelid
Czajka [25]	Pupil dynamics	Detected	Detected	Detected	Detected	N.A.
Raghavendra [26]	Pupil dynamics	Detected	Detected	Detected	Detected	N.A.
Zhang [27]	Fake iris detection by using LBP and statistical features	Detected	Detected	Detected	Detected	N.A.
The Proposed system	Pupil size detection with heart pulse recognition by eyelid	Detected	Detected	Detected	Detected	Detected

Moreover, the ambient illumination can impact the heart pulse signals of the eyelid. For example, the adversary concentrates LED light on the synthetic eye robot to make noise in the heart beats signals that are captured by the camera sensor for the eyelid. The noise will give wrong readings of the heart pulses to the Webcam. Hence, even if unlikely, the adversary has a potential chance to bypass the check.

9 Conclusion

In this paper, we have provided a solution to eye biometric spoofing. Our solution relies on multiple factors. First, we examine the pupil movements during opening and closing the eye with support of just ambient illumination. Later, we recognize whether the eye is closed, and then we start measuring remotely a heartbeat signals from the eyelid to validate the liveness feature. During these checks, we match the iris against a pre-loaded database two times: the first time before closing the eye, and the second time after closing the eye. A third contribution is a database composed of 40 subjects. The same 40 subjects have contributed to test the proposed methodology: by using a camera sensor with a software program that includes all the algorithms for liveness and iris recognition. The results have shown the quality and viability of our proposal. We believe that the proposed methodology, together with the experimental results reported in this paper, other than being interesting on their own, will also encourage researchers to conduct future research in this field.

References

[1] A. Al-Rashid, "A Three Steps Eye-Liveness Validation System," 2019 International Conference on Cyber Security for Emerging Technologies (CSET), Doha, Qatar, 2019, pp. 1-8, doi: 10.1109/CSET.2019.8904884.

[2] K.R. Park Robust Fake Iris Detection. In: Perales F.J., Fisher R.B. (eds) Articulated Motion and Deformable Objects. AMDO 2006. Lecture Notes in Computer Science, **4069**. Springer, Berlin, Heidelberg, 2006. doi.org/10.1007/11789239.2

[3] J. Connell, N. Ratha, J. Gentile and R. Bolle, "Fake iris detection using structured light," 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, 2013, pp. 8692-8696, doi: 10.1109/ICASSP.2013.6639363.

[4] Rigas, Ioannis, and Oleg V. Komogortsev. "Eye movement-driven defense against iris print-attacks." Pattern Recognition Letters. Elsevier, 2015. doi.org/10.1016/j.patrec.2015.06.011

[5] A. George and A. Routray, "Fast and accurate algorithm for eye localisation for gaze tracking in low-resolution images," in IET Computer Vision, **10**(7), pp. 660-669, 10, 2016. doi.org/10.1049/iet-cvi.2015.0316

[6] M. Poh, D. J. McDuff and R. W. Picard, "Advancements in Noncontact, Multiparameter Physiological Measurements Using a Webcam," in IEEE Transactions on Biomedical Engineering, **58**(1), pp. 7-11, Jan. 2011, doi: 10.1109/TBME.2010.2086456.

[7] M. P. Tarvainen, P. O. Ranta-aho and P. A. Karjalainen, "An advanced detrending method with application to HRV analysis," in IEEE Transactions on Biomedical Engineering, **49**(2), pp. 172-175, Feb. 2002, doi: 10.1109/10.979357.

[8] Wayman, James, Book review: Handbook of Iris Recognition. Biometrics, IET. 3. 41-43, 2014. DOI: 10.1049/iet-bmt.2014.0003.

[9] J. Daugman, "Biometric personal identification system based on iris analysis," U.S. Patent 5 291 560, Mar. 1, 1994.

[10] J. Shi and X. Gu, "The comparison of iris recognition using principal component analysis, independent component analysis and Gabor wavelets," 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, pp. 61-64, 2010. doi: 10.1109/ICCSIT.2010.5563947.

[11] J. Galbally and M. Gomez-Barrero, "A review of iris anti-spoofing," 2016 4th International Conference on Biometrics and Forensics (IWBF), Limassol, pp. 1-6, 2016. doi: 10.1109/IWBF.2016.7449676.

[12] X. Li, J. Komulainen, G. Zhao, Pong-Chi Yuen and M. Pietikäinen, "Generalized face anti-spoofing by detecting pulse from face videos," 2016 23rd International Conference on Pattern Recognition (ICPR), Cancun, pp. 4244-4249, 2016. doi: 10.1109/ICPR.2016.7900300.

[13] C. Wang, T. Pun, G.A. Chanel, "Comparative Survey of Methods for Remote Heart Rate Detection From Frontal Face Videos". Front Bioeng Biotechnol, **6**(33).doi: 10.3389/fbioe.2018.00033

[14] S. Thavalengal, T. Nedelcu, P. Bigioi and P. Corcoran, "Iris liveness detection for next generation smartphones," in IEEE Transactions on Consumer Electronics, **62**(2), pp. 95-102, May 2016, doi: 10.1109/TCE.2016.7514667.

[15] Królak, A., Strumiłło, P. Eye-blink detection system for human–computer interaction. Univ Access Inf Soc 11, 409–419, 2012. https://doi.org/10.1007/s10209-011-0256-6

[16] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001, Kauai, HI, USA, 2001. doi: 10.1109/CVPR.2001.990517.

[17] R. G. Bozomitu, A. Păsărică, V. Cehan, C. Rotariu and C. Barabaşa, "Pupil centre coordinates detection using the circular Hough transform technique," 2015 38th International Spring Seminar on Electronics Technology (ISSE), Eger, pp. 462-465, 2015. doi: 10.1109/ISSE.2015.7248041.

[18] A. R. Azar and F. Khalilzadeh, "Real time eye detection using edge detection and Euclidean distance," 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, pp. 43-48, 2015. doi: 10.1109/KBEI.2015.7436019.

[19] M. Heshmat, M. Girgis, W. M. Abd-Elhafiez and S. Elaw, "An efficient scheme for face detection based on contours and feature skin recognition," 2015 Tenth International Conference on Computer Engineering and Systems (ICCES), Cairo, pp. 255-260, 2015. doi: 10.1109/ICCES.2015.7393056.

[20] W. Wang, S. Stuijk and G. de Haan, "Exploiting Spatial Redundancy of Image Sensor for Motion Robust rPPG," in IEEE Transactions on Biomedical Engineering, **62**(2), pp. 415-425, Feb. 2015, doi: 10.1109/TBME.2014.2356291.

[21] J. Hernandez-Ortega, J. Fierrez, A. Morales and P. Tome, "Time Analysis of Pulse-Based Face Anti-Spoofing in Visible and NIR," 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Salt Lake City, UT, pp. 657-6578, 2018. doi: 10.1109/CVPRW.2018.00096.

[22] J. Daugman, "How iris recognition works. Proceedings of 2002 International Conference on Image Processing, **1**, 2002. doi: 10.1109/TCSVT.2003.818350

[23] O. Koç, L. Tosku, J. Hoxha, A. O. Topal, M. Ali and A. Uka, "Detailed Analysis of IRIS Recognition Performance," 2019 International Conference on Computing, Electronics and Communications Engineering (iCCECE), London, United Kingdom, pp. 253-258, 2019. doi: 10.1109/iCCECE46942.2019.8941784.

[24] CASIA-Iris, Chinese Academy of Sciences–Institute of Automation. http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp

[25] A. Czajka, "Pupil Dynamics for Iris Liveness Detection," in IEEE Transactions on Information Forensics and Security, **10**(4), pp. 726-735, April 2015, doi: 10.1109/TIFS.2015.2398815.

[26] R. Raghavendra and C. Busch, "Robust Scheme for Iris Presentation Attack Detection Using Multiscale Binarized Statistical Image Features," in IEEE Transactions on Information Forensics and Security, **10**(4), pp. 703-715, April 2015, doi: 10.1109/TIFS.2015.2400393.

[27] H. Zhang, Z. Sun, and T. Tan. Contact lens detection based on weighted lbp. In Proc. of ICPR, pages 4279–4282, 2010. doi: 10.1109/ICPR.2010.1040