Iris Anti-spoofing: Static and Dynamic Technique

Dr. Hanaa M. Ahmed
Computer Science Department, University of Technoloigy/Baghdad
Bushra Jabbar Abdulkareem
Computer Science Department, University of Technoloigy/Baghdad
Email:bushraalkreem@yahoo.com

Received on:9/11/2015 & Accepted on:21/4/2016

ABSTRACT

The probabilityof the biometric system to be spoofed is widely acknowledged. Complete security does not really exist, butsignificant efforts have led to study such threats and to develop countermeasures to direct attacks to the biometric system in an attempt to ensure the security and to reduce this risk.

This paper presents two novel anti-spoofing techniques to protect iris biometric system from spoof attack, static and dynamic. Static technique is based on the principle of degree of sharpening of the input eye image.Dynamic technique is based on variation of the size of the pupil if the illumination is increased. This technique is tested on 15 folders of original MMU database (Multi Media University database) Each folder contains two eyes image sampleswhich represent live trail and 15 folders of (MMU database) eye images printed using scanner device and photographed using a specific camera are saved in computer to represent 15 attempts of spoof attack.

The evaluation tests of liveness detection phase for iris which is applied in iris database show that the detection of the liveness properties is very good as depicted in Table (1) and Table (2).

Keywords: Software liveness detection, Iris, Anti-spoofing, Static and dynamic technique, and direct attacks.

INTRODUCTION

Biometric systems as not based on a token but on the body itself for recognition and identity affirmation; therefore it is different from any other system for automatic human ID. Biometrics is the scientific discipline of measuring relevant attributes of living individuals to identify active properties or unique characteristics.IRIS recognition is one of the biometric systems whichhave acquired popularity due to a number of reasons, such as its quick, high accuracy, fast to compare, robustness, its non-contact acquisition method and the availability of low cost sensors due to improvements in technology. But there are numerous manufactured techniques evolved to cheat every IRIS biometric sensor.These techniques are called IRIS spoofing methods which include Printed IRIS Images and re-played video, photographic surfaces, fake glass/plastic eye and IRIS texture printed on contact lenses [1]. Liveness detection represents a common countermeasure to address Anti- spoofing by using different anatomical properties to distinguish between real and fake traits. Thus robustness of the system is improved against direct attacks through increasing the security level offered to the final user [2, 3]. There are certain requirements and should be satisfied by liveness detection technique, of these are [4]:

1. Non-invasive : “the technique should in no case penetrate the body or present and excessive contact with the user”,
2. Fast: “results should be produced in very few seconds as the user cannot be asked to interact with the sensor for a long period of time”,
3. User friendly: “people should not be reluctant to use it”,

4. Low cost: “a wide use cannot be expected if the cost is very high”, and
5. Performance: “it should not degrade the recognition performance of the biometric system”.

The existing techniques for liveness detection, depicted in Figure (1), can broadly be divided into two classes as follows [5, 6]:

1. Hardware-based techniques which:“exploit characteristics of vitality from the available biometrics at the acquisition stage, by adding extra device to the sensor in order to acquire live signs from the presented biometric sample such as the blood pressure, skin distortion, or the odor”, and
2. Software-based techniques: “in this case fake traits are detected once the sample has been acquired with a standard sensor during processing stage. (i.e., feature used to distinguish between real and fake trait), as is used in this proposed system”.

Software-based techniques have the advantage over the hardware-based ones of being less expensive (as no extra device in needed), and less intrusive for the user (very important characteristic for a practical liveness solution) [4].

Software-based approaches “can extract any one peculiarity of live signs from the acquired sample using static techniques (using single sample) (e.g., the finger is placed and lifted from the sensor one or more times), or dynamic techniques (using multiple samples) (e.g., the finger is placed on the sensor for a short time and a video sequence is captured and analyzed)” [5].

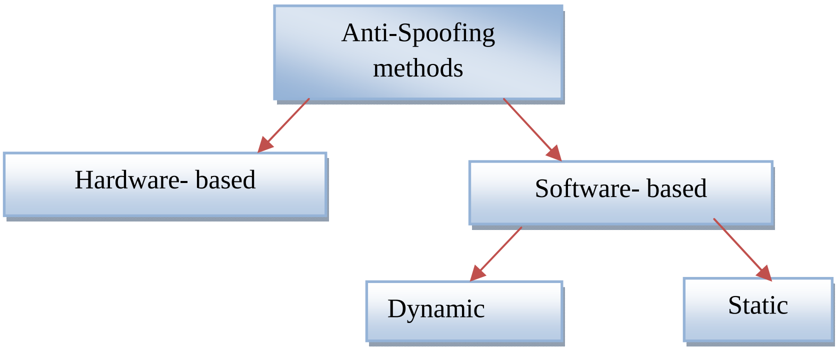


Figure (1): The existing anti-spoofing approaches [5].

Iris liveness detection aims to ensure that an input sequence of eye image is from a live subject instead of a counterfeited eye image. This proposed system focuses on the establishment of countermeasure to iris photograph spoof attack, by using static technique and dynamic technique.

Literature Survey

This section presents methods employed for iris liveness detection as an overview of the representative work in this area.

In 2012 Javier Galbally et al. [3], in their works showed“a new parameterization based on quality related measures which is used in a global software-based solution for iris liveness detection. This novel strategy has the clear advantage because it needs just one iris image (i.e., the same iris image used for access) to extract the necessary features in order to determine if the eye presented to the sensor is real or fake”. These facts shorten the acquisition process and reduce the inconvenience for the final user. “The presented method is tested on an iris database which comprises 1,600 real and fake (high quality printed images) samples where it has proven its high potential as a countermeasure to prevent spoofing attacks. The results presented in this work have been obtained for a specific type of synthetic traits (i.e., high quality iris printed images), this proposed method can also be used to detect other types of fake data (e.g., printed lenses) by selecting the subset of parameters that better adapt to the new anti-spoofing problem. Liveness detection solutions such as the one presented in this work are of greatimportance in the biometric field as they help to prevent direct attacks (those carried out with synthetic traits, and as very difficult to detect)".

In 2013 Oleg V. Komogortsev and Alex Karpov [7]in their works perform liveness detection for biometric modalities that use eye movement signal for person identification through investigating counterfeit resistance capabilities of the eye movement-driven biometric traits. Specifically, it investigates liveness detection capabilities afforded by the Oculomotor Plant Characteristics (OPC), internal non-visible anatomical structure of an individual human eye represented by the extra ocular muscles, tissues surrounding the eye globe, and the eye globe itself. The threat model considers spoofing attacks where an accurate mechanical replica of the human eye is presented to the sensor. Such replica performs the eye movements similar to that of a human.This paper outlined and explored liveness detection capabilities afforded by the movements of the eye. The approach is based on extracting (OPC) - internal non-visible anatomical structure of an individual human eye and making a decision about the liveness of the signal based on the variability of those characteristics. Spoof attacks were conducted by the mechanical replicas simulated via three different mathematical models representing human eye. The replicas varied from relatively simple ones that over simplify the anatomical complexity of the Oculomotor plant to more anatomically accurate ones. Two strategies were employed for the creation of the replicas.

In 2014, B. Sabarigiri and D. Suganyadevi [1] published a paper which provides "the valuable input to IRIS direct attacks and Spoofing. Electroencephalogram (EEG) is a Novel Modalities used for liveness detection achieving authentication with someone iris well as supplementary Biometric Modality to improve hiding your own pupil behind it. The performance of the IRIS Authentication system,to protect our system from direct attacks uses Fake IRIS images the integrated Multi modal biometric systems using two individual modalities, like IRIS and Electronic ephalogram (EEG) is fused**.** The assessment of the vulnerabilities to direct attacks of IRIS-Based Verification systems has been offered, using data base of fake images from 32 people's right eyes. The results showed that the system is highly vulnerable to the two evaluated attacks. Liveness Detection Procedures are possible countermeasures against direct attacks. Here Electronic ephalogram (EEG) is Novel Modality used for liveness detection as well as additional Biometric Modality to the system".

In 2014,R. Raghavendra and Christoph Busch [8], presented a novels Presentation of Attack Detection (PAD) algorithm that forms a generic solution to reduce the attacks on both face and iris biometrics. The proposed method explores both microtexture variation using Binarized Statistical Image Features (BSIF) and micro-frequency variations using 2D Cepstrum. Then these two features are combined before obtaining the decision using linear SVM. Extensive experiments was carried out on the available databases of face and iris biometrics,andother experiment results that show the performance of the proposed PAD algorithm with various camera resolutions. These experiments with various camera resolutions especially on the face biometrics show the sensitivity of the camera interoperability on the presentation attack detection. Further, experimental results also revealed that, the proposed PAD algorithm emerged as the best scheme.

Iris Liveness Detection System

Iris liveness detection operation is used to assign input eye image into one of two classes: real or fake, therefore; it can be seen as a two class classification problem. The main purpose of this process is to find a set of discriminate characteristic which allows building a classifier which gives the probability of the image vitality. In this work two modules for liveness detection (dynamic and static)which have been proposed, the theoretical part of these two modulesis presented below:

Static Technique:

Considering the degree of sharpening property in an acquired eye image, the real eye image is 3D volume object, while fake eye image (printed eye image), is a 2D surface. Thus, the focus in 2D isless than on 3D image, as in Figure (2), also defocus primarily suppresses high spatial frequencies which reduce the sharpening of the image, so that, “the sharpening of a fake iris will differ from that of a genuine sample” [3].

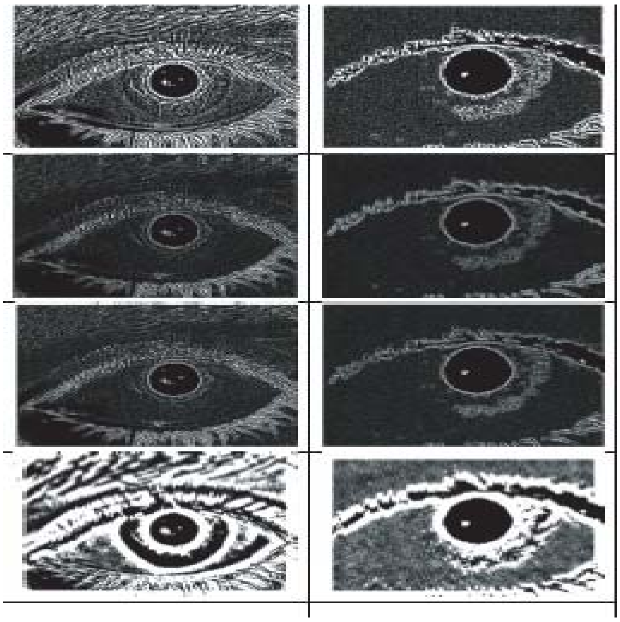
In this work high pass filter is used for this purpose, which is accomplished by using a kernel containing a mixture of positive and negative coefficients, such as (Sobel filter), to compute gradient of the image which represents the change in intensity level. Since an image $f(x,y)$ is a two-dimensional function, its gradient is a vector:

$$\begin{bmatrix} G_x \\ G_y \end{bmatrix} = \begin{bmatrix} \frac{df}{dx} \\ \frac{df}{dy} \end{bmatrix} \quad \ldots..(1)$$

The magnitude of the gradient may be computed by any of these two ways[9]:

$$G[f(x,y)] = \sqrt{G_x^2 + G_y^2} \quad \ldots.(2)$$

$$G[f(x,y)] = |G_x| + |G_y| \quad \ldots.(3)$$



a: Real iris b: Fake iris

Figure (2): Difference in focus quality features [3]

Dynamic Technique:

Conceding pupil variation in size with change in illumination is mad, by comparing the size of pupils of two eye image samples of the same person is acquired in different illumination, the difference in size of two pupils is measured. If percentage variation in size of first pupil and second is confined within the limits of 5-15%, then it is considered as real eye image, else fake eye image. [10]

The percentage variation in size can be computed by this formula [11]:

$$\left|\frac{Firstsize - Secondsize}{(Firstsiz + Secondsize)/2}\right| \times 100 \qquad \text{….. (4)}$$

Main Diagram of Iris Liveness Detection

Two modules for eye liveness detection are used: dynamic and static, then a decision is made according to the output from two modules, depends on two input samples of eye images for the same claimed person taken under different illumination, as in, follows:

- **Dynamic module:** This module takes an input these two samples of eye images which are acquired in different illumination, and compares the size of pupils for these two images, the percentage difference in magnitude of two pupils is measured. If percentage difference is (5–15) % then the decision is true (real eye), else the decision is false, (Fake eye).Algorithm (1)as represented in Figure (3),illustrates the main steps for dynamic liveness detection for eye image.

```
Algorithm (1): Dynamic liveness detection for eye image
Input: two eye images of the same person acquired in different illumination
Output: Live or  Fake
Begin:
Step1: Read the first eye image
Step2: Localize the pupil to get the radius of the pupil ($R_p$) and its center($C_{px}$,$C_{py}$).
Step3: Convert the region that contain pupil to the binary as follows:
For i = $C_{px} – (R_p + 5)$ To $C_{px} + (R_p + 5)$
For j = $C_{py} - (R_p + 3)$ To $C_{py} + (R_p + 5)$
    -   Compute (threshold) for this region using Otsu's thresholding method
    -   Convert this region to the binary.
    -   Pupil takes white color otherwise takes black color
Step4:Summation of the number of pixels with white color and put it in the parameter (sump1).
Step5:Repeat the steps (one to four) on the second eye image to compute the number of pixels with white color which represent pupil in the second eye image and put it in the parameter (sump2).
Step 6:Compute the percentage difference in magnitude of two pupils by formula below. If difference is (5–15) %, then the output from procedure is true (real eye), else false (fake eye).
$P.\text{difference} = \frac{|sump2 - sump1 |}{(sump2 + sump1)/_{2}} \times 100$
End
```

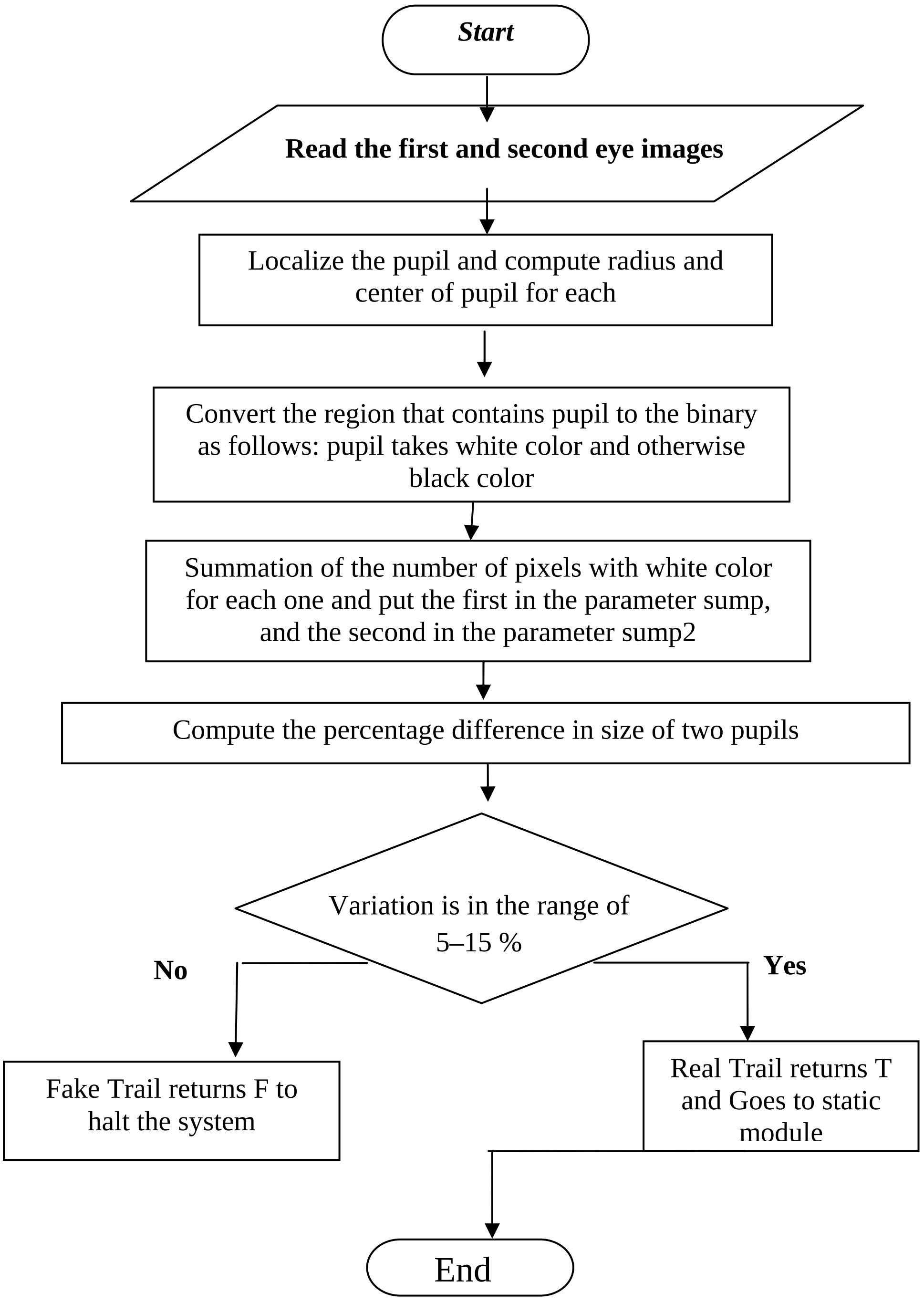

Start
Read the first and second eye images
Localize the pupil and compute radius and center of pupil for each
Convert the region that contains pupil to the binary as follows: pupil takes white color and otherwise black color
Summation of the number of pixels with white color for each one and put the first in the parameter sump, and the second in the parameter sump2
Compute the percentage difference in size of two pupils
Variation is in the range of 5–15 %
No
Yes
Fake Trail returns F to halt the system
Real Trail returns T and Goes to static module
End

Figure (3):Block Diagram illustrating dynamic eye liveness detection

- **Static module**: This module takes as input one sample of eye images, and then one measures of the high frequency content in the whole image is used to compute the sharpening of the image to make decision according specific threshold whether the input eye image comes from real or fake image. The classic 3×3 high pass filter (Sobel operator) is used to for this purpose. Algorithm (2) is the main steps for Static liveness detection for eye image. Figure (4) depicts Algorithm (2).

Algorithm (2): Static liveness detection for eye image

Input: one sample of eye images

Output: Live or Fake

```
Begin
Step 1: Read eye image
Step 2: Define (3*3) window for convolution with Sobel filter:
For i = 1 To eye image. Width - 2
   For j = 1 To eye image. Height - 2,
p1 = eye image (i- 1, j- 1):p2 = eye image (i- 1, j): p3 = eye image (i- 1, j + 1):   p4 = eye image (i, j - 1): p5 = eye image (i, j): p6 = eye image (i,j + 1)
p7 = eye image (i+ 1, j - 1): p8 = eye image (i + 1, j):p9 = eye image (i +1, j +1)
//compute Gradients of x and y by convoluted with two sobel kernels
$G_x$ = (p7 + (p8 + p8) + p9 -p1 - (p2 + p2) - p3)
$G_y$ = (p3 + (p6 + p6) + p9 - p1 - (p4 + p4) - p7)
Compute (gradient magnitude)and sum of the gradient
gradient(i,j) = Sqrt(($G_x$ ^2)+ ($G_y$^ 2))
Sum gradient=Sum gradient +  gradient (i, j)
                c = c + 1
  Next   for j
  Next for i
Step3: Take decision by  computing  mean gradient magnitude
             Mean grad= Sum gradient/c
If mean grad>= threshold
the output decision (True) real image
Else
the output decision (False) fake image
End
```

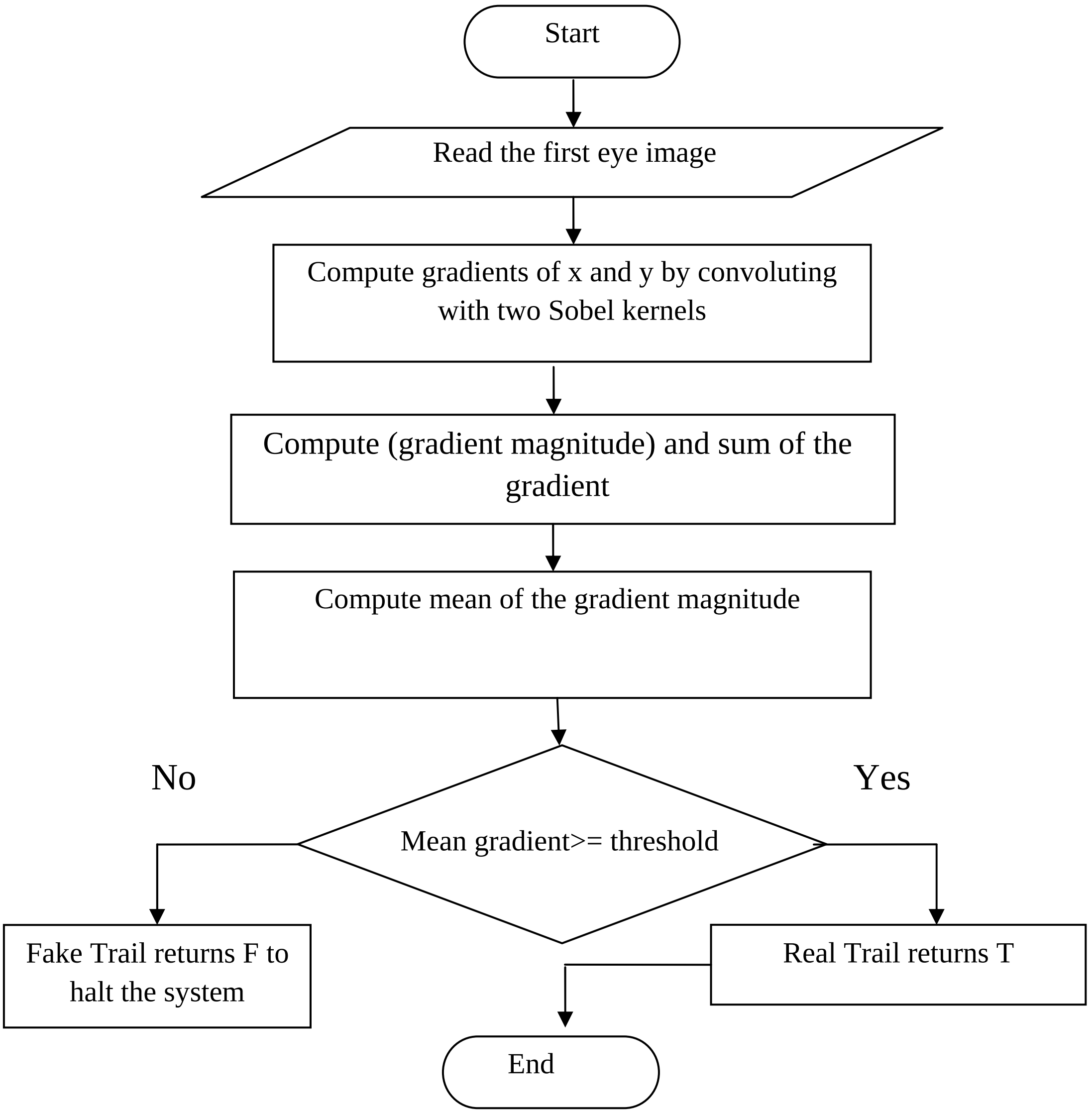

Start
Read the first eye image
Compute gradients of x and y by convoluting with two Sobel kernels
Compute (gradient magnitude) and sum of the gradient
Compute mean of the gradient magnitude
No
Yes
Mean gradient>= threshold
Fake Trail returns F to halt the system
Real Trail returns T
End

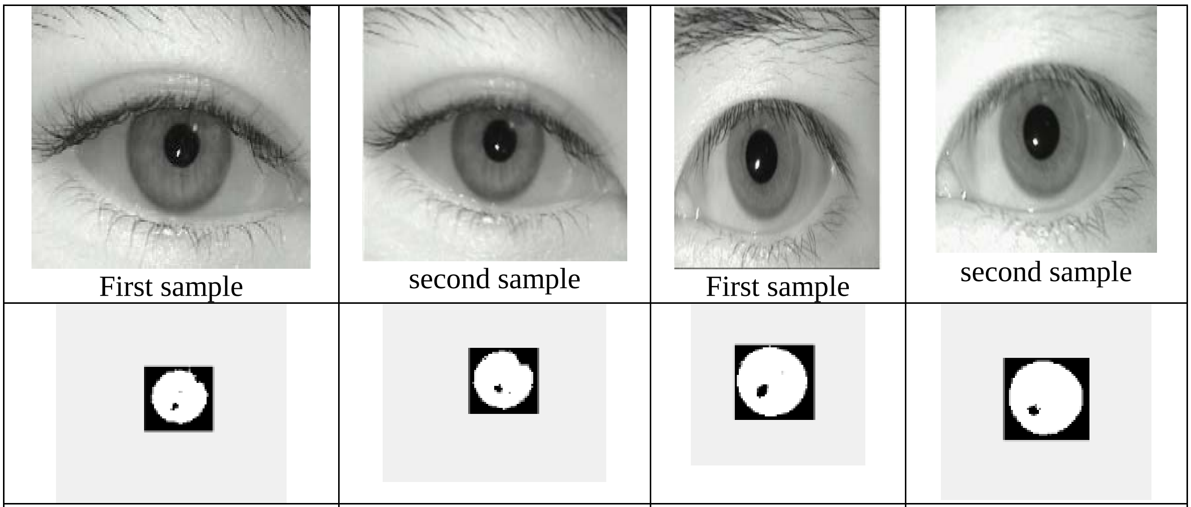
Figure (4):Block Diagram illustrating static eye liveness detection

- **Decision:** If the output decisions from dynamic module and static module of eye liveness detection are (True) then decision is that the acquired eye image is Real eye else the decision is that the acquired eye image is fake and halts the system.

Iris Liveness Detection Results

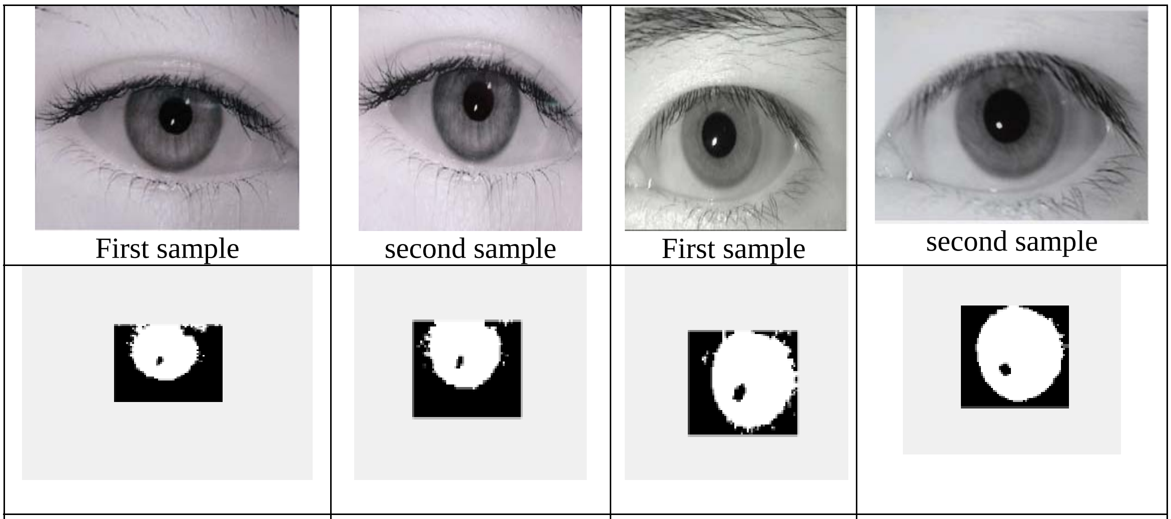
Database that is set up to test the robustness of the proposed algorithm through iris liveness detection process consists of 15 folders oforiginal (***MMU database) each*** folder contains two eye image sampleswhere represent live tries,and 15 folders of(***MMU database)*** eye images are printed using scanner devise and recaptured by using specific camera and resaved in computer to represent 15 attempted spoof attacks against the system.Each folder contains two samples of fake eye image. The results of this system are illustrated below:

Dynamic Module: The threshold that is used to detect livenessis: the difference in size of the pupil for two eye images must be confined within the limits of 5-15% to decide that the acquired eye image is live, else the decision is false (fake eye),Table (1) shows experiments result of this module. Example is applied on original MMU data base which represents real samples shownin Figure (5).Examples applied recapture MMU data base which represents fake samplesshown in Figure (6).



First sample	second sample	First sample	second sample
291210	325125	482460	540090
Percentage Difference = 11.005		Percentage Difference = 11.272	

Figure (5) Two real tries to enter to the dynamic liveness module by two persons



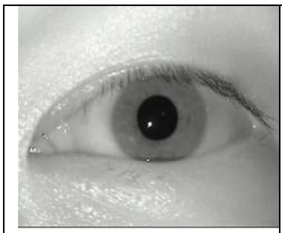
First sample	second sample	First sample	second sample
367965	384285	682380	691050
Percentage Difference = 4.93		Percentage Difference =1.613	

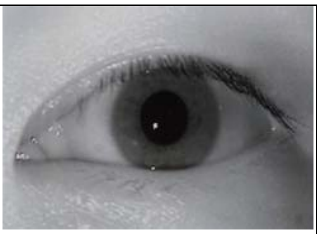
Figure (6) Two fake tries to enter to the dynamic liveness module by two persons

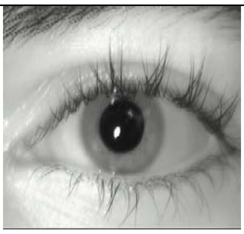
Table (1):The experimental results of Dynamic iris liveness module

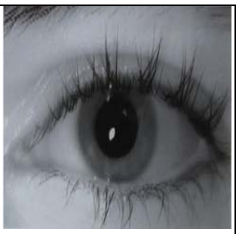
	Results of applyingto original eye images			Results of applyingto recaptured eye images		
Person No	No of pixels in pupil for two samples with different eliminations	Percentage ofdifference in pupil size	Decision	No of pixels in pupil for two samples with different eliminations	Percentage ofdifference in pupil size	Decision
1	451860 523770	14.741	Live	479400 456960	4.793	Fake
2	291210 325125	11.005	Live	502095 695895	32.354	Fake
3	482460 540090	11.272	=	682380 691050	1.613	Fake
4	457980 525300	13.693	=	546720 442680	21.031	Fake
5	330735 372300	11.824	=	961605 983535	2.255	=
6	699210 759900	8.319	=	556665 562785	1.093	=
7	410550 474300	14.409	=	558960 548760	1.842	=
8	408000 431460	5.589	=	577320 555135	3.918	=
9	388620 409785	5.302	=	407235 402135	1.26	=
10	368220 337875	8.595	=	662490 675750	1.982	=
11	288150 252450	13.208	=	254745 260100	2.08	=
12	514845 566355	9.528	=	690030 818805	17.069	=
13	585735 627555	6.894	=	860880 840735	2.368	=
14	735420 668355	9.555	=	668100 557685	18.015	Fake
15	536010 469455	13.239	=	696915 695130	0.256	Fake

Static Module: Threshold that is decided according spoof dataset generated by recapturing original (MMU dataset) is (34) (if the mean of gradients of eye images less than 34 then the input image sample is fake else it is live). Table (2) shows the results of static iris liveness module and Figure (7) shows two examples of detect as liveness by static module


real eye


fake eye


real eye


fake eye

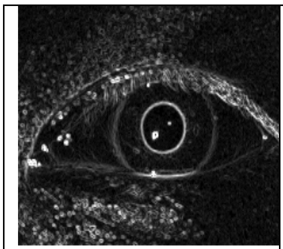
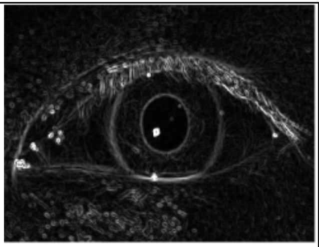
 gradient image	 gradient image	 gradient image	 gradient image
Mean for gradient = 36.935	Mean for gradient = 26.155	Mean for gradient = 49.592	Mean for gradient = 32.884

Figure (7) Operation to detect liveness by static module for two persons

Table (2): Theexperiment results for Static iris liveness module

	Results of applying static module to original eye images		Results of applying static module to recaptured eye images	
Person No	Mean of gradient for input original MMU eye sample images	Decision	Mean of gradient for input recaptured MMU eye sample images(spoof image)	Decision
1	38.626 36.029	Live =	34.435 30.154	Faulty Live Fake
2	45.867 38.969	Live =	27.755 28.808	Fake =
3	58.622 36.203	Live =	42.832 29.355	Faulty Live Fake
4	42.561 37.927	Live	25.049 24.787	Fake =
5	35.306 35.998	Live =	23.839 28.72	= =
6	55.638 49.592	Live =	60.677 54.772	Faulty Live =
7	36.935 41.593	Live	27.299 28.721	= =
8	34.676 36.489	Live	23.765 23.661	= =
9	38.621 39.024	Live =	37.83 36.646	Faulty Live =
10	35.789 45.489	Live =	27.047 26.947	= =
11	34.752 36.181	Live =	34.93 34.677	Faulty Live =
12	29.648 35.511	Faulty Fake =	23.303 22.823	= =
13	31.122 35.052	Live =	20.221 20.376	= =
14	33.713 35.814	Live =	22.823 27.708	= =
15	39.363 37.276	Live =	22.417 22.293	= =

CONCLUSIONS

By extensive and hard work the designof irisbiometric system isprotected from spoof attack. The security of these types of system can be improvedthrough adding another module (liveness detection) to it; a number of conclusions are reached.

1-The dynamic method which is used to detect livenessis more effective, more accurate and successful than static method, as shown by the results in Table (1) for iris dynamic liveness detection. Static method needs to detect fixed threshold, extracted from original properties of the biometric trait to accept image sample as real sample. Choosing this threshold is influenced by the variance of these original properties from person to another, such as degree of sharpening of eye image,and the way that is used to make the original image database and spoof database which cause ratio of error in liveness decision.

2-Detect by pupil in this successful way is useful to help and facilitate liveness detection through dynamic module with high degree of accuracy. This method to detect liveness satisfies all requirements which must be satisfied in liveness detection operation (Non-invasive, fast,user friendly, low cost, performance).This way of liveness detection is improving the level of security which isprovided to the user.

3-In morphological operation, not any selected structure element has been suitable for extracting pupil from eye images.The correct selection of suitable structure element disk (2.5)has a direct impact on extracting pupil from eye images, by isolate the circle shape which is represented by pupil object, this decision is taken by training data.

4-The sharpening of the 3D volume object is more than 2D surface which isrepresented by printed eye images.Thus, the focus in 2D is less than in 3D image. Also defocus primarily suppresses high spatial frequencieswhich reduce the sharpening of the image,as in Figure (7) and from the result in Table (2).

REFERENCES

[1] B. Sabarigiri and D. Suganyadevi, "Counter Measures Against Iris Direct Attacks Using Fake Images and Liveness Detection Based on Electroencephalogram (EEG)", World Applied Sciences Journal, Vol. 29, 2014.

[2] EmanuelaMarasco,Arun Ross,"A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems",in JournalACM Computing Surveys(CSUR),Vol.47,No.2,Article A,September,2014.

[3]. Javier Galbally, Jaime Ortiz-Lopez, Julian Fierrez and Javier Ortega-Garcia, "Iris Liveness Detection Based on Quality Related Features", IEEE Browse Conference Publications,2012.

[4]. Javier GalballyHerrero, "Vulnerabilities and Attack Protection in Security Systems Based on Biometric Recognition", Thesis of Ph.D.,UniversidadAutonoma DE Madrid,November,2009.

[5]. YogendraNarain Singh,Sanjay Kumar Singh,"Vitality Detection from Biometrics: State-of-the-Art",IEEE World Congress on Information and Communication Technologies, Des, 2011.

[6]. Rattani, A.; Ross, A. Automatic adaptation of fingerprint liveness detector to new spoof materials. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB), Clearwater, FL, USA, 29 September–2 October 2014; pp. 1–8.

[7]. O. V. Komogortsev, A. Karpov, “Liveness Detection via Oculomotor Plant Characteristics: Attack of Mechanical Replicas”, In Proceedings of the IEEE/IARP International Conference on Biometrics (ICB), 2013, pp. 1-8.

[8]. R. Raghavendra and Christoph Busch, "Presentation Attack Detection Algorithm For Face and Iris Biometrics", IEEE, Signal Processing Conference (EUSIPCO), 2014 Proceedings of the 22nd European, Sept. 2014.

[9].ImageMagick v6 Examples – Convolution of Images. Abrufbarunter: http://www.imagemagick.org/Usage/convolve/. LetzterZugriff: 10. Juni 2013

[10]. Rajesh M.Bodade, Sanjay N.Talbar,"Iris Analysis for Biometric Recognition Systems",Springer, 2014.

[11]. Percentage Difference,https://www.mathsisfun.com/percentage-difference.html, 2014.