Journal of Computer and Communications, 2016, 4, 22-32
Published Online January 2016 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2016.41003

Integrate Liveness Detection with Iris Verification to Construct Support Biometric System

Hanaa Mohsin Ahmad, Bushra Jabbar Abdulkareem

Computer Science, University of Technology, Baghdad, Iraq
Email: uot_info@uotechnology.edu.iq

Received 3 December 2015; accepted 21 January 2016; published 26 January 2016

Abstract

The probabilities for the technology to be spoofed are widely acknowledged in biometric verification system. Important efforts have been conducted to study such threats and to develop countermeasures to direct attacks to the biometric verification system to ensure the security of these systems against spoof attacks and reduce this risk, by using another module that is added to the biometric verification system called the "liveness detection" which uses different anatomical properties to distinguish between real and fake traits. Thus, the robustness of the system against direct attacks can be improved through increasing the security level offered to the final user. This paper is an attempt to construct support biometric security system to protect the iris biometric verification system from spoof attacks, through integrating the iris verification system with addition module called liveness detection which composed of two sub-modules (static and dynamic). A test has been performed, for iris verification phase performed on two types of database (MMU DB) for 180 samples and (CASIA DB) for 90 samples, and gave accuracy (99.44%) with FAR of (0.0277) and FRR (0.0055) for MMU DB, and accuracy (97.77%) with FAR of (0.0333) and FRR (0.0222) for CASIA DB.

Keywords

Liveness Detection, Iris Verification, Countermeasures, Direct Attacks, Fingerprint Verification

1. Introduction

The biometric based verification system is essentially a pattern-recognition system that recognizes a person based on a feature vector extracted from physical or behavioral traits. This type of systems has evolved to play a

How to cite this paper: Ahmad, H.M. and Abdulkareem, B.J. (2016) Integrate Liveness Detection with Iris Verification to Construct Support Biometric System. *Journal of Computer and Communications*, **4**, 22-32.
http://dx.doi.org/10.4236/jcc.2016.41003

critical role in personal, national and global security [1], which includes a variety of applications that require reliable verification techniques, such as passports, border control, and used in computer systems, cellular phones, medical records management, banking. The systems are also used in important and sensitive government departments, which include the traffic offices.

The probabilities for the technology to be spoofed are widely acknowledged. Absolute security does not really exist, but many researchers study such threats and develop countermeasures to direct attacks to the biometric system attempted to ensure the security of these systems against spoof attacks and reduce this risk [2]: one of the main points focused on it by researchers is the way in which another module is added to the biometric verification system called the "liveness detection" which uses different anatomical properties to distinguish between real and fake traits. Thus, improve the robustness of the system against direct attacks through increasing the security level offered to the final user [3] [4]. These methods for liveness assessment represent a challenging problem because they have to satisfy certain requirements [5]:

- Non-invasive: the technique should in no case penetrate the body or present and excessive contact with the user,
- 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,
- User-friendly: people should not be reluctant to use it,
- Low cost: a wide use cannot be expected if the cost is very high,
- Performance: it should not degrade the recognition performance of the biometric system.

On the other hand, Iris is an important feature of the human body and very stable throughout a lifetime of a person. Iris is used as a biometric trait and offers many advantages over other human biometric features. It is only an internal human body organ that is visible from the outside and is well protected from external modifiers. For example, voice patterns may be altered due to vocal diseases, a fingerprint may suffer transformations due to harm or aging. The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye [6].

Iris's image is characterized with richness of its texture details such as cornea, crypts, filaments, flecks, radial furrows, stripes, arching ligaments, etc. Therefore, the iris region in the eye image of an individual contains completely independent patterns, and minute details of the iris are so randomly distributed patterns, which make the human iris be one of the most important biometric characteristics [7].

This paper is an attempt to address the biometric security issue through integrating the iris verification system with addition module called liveness detection which composed of two sub-modules (static and dynamic) to protect the iris biometric system from spoof attacks, the system consists of two basic phases: liveness detection phase and iris verification phase and will be implemented successively.

The rest sections of the paper are structured as follows. Section 2 presents a collection of previous studies related to the paper theme. Section 3 explains algorithm for proposed system and results and discussion are done in Section 4, and Section 5 deals with the conclusions.

2. Literature Survey

Many researchers and designers of biometric systems studied the possibility of exposure these systems to attempts to attack it by attackers, these attempts affected on data security through alteration in order to the system becomes inactive. In spite of the human iris considered as one of the most important biometric characteristics. There are many fake techniques evolved to cheat the security of these systems, here is a collection of previous studies related to the paper theme:

In 2002, Daouk *et al.* [8] present a new technique to create the new biometric system for iris recognition. Canny edge detection and circular Hough transform used to detect iris region from input eye image by detect inner boundary and the outer boundary of the iris, And then using the Haar Wavelets to extract the Patterns of an iris in the form of a feature vector. In the last step, the matching score has been produced using Hamming Distance operator as a method to compare feature vector for submitted iris with the feature vector stored in a database (template) to find the similarity between two irises. Finally, the decision that the person is genuine or imposter has been made according to the similarity degree. This work results in successfully and simple and not cost Biometric Recognition system used iris trait. The ratio of error in the accuracy of this system can be easily overcome by the use of constant equipment.

In 2012, Amel Saeed Tuama [9] presented a typical iris recognition method which performed by: first, eye image capturing, second, iris segmentation through pupil localization by dividing eye image into 8 × 8 regions and compute the mean intensity for each region, lowest mean used as threshold to detect pupil region, and then iris localized by detect the outer boundary from horizontal line starting from the pupil to iris boundary, then normalize the detected iris region from Cartesian to polar, the third step is feature extracted, by filtering the normalized iris region by convolution with a pair of Gabor filters, finally using Hamming distance approach to producing the similarity between two irises to decide whether these two eye images belong to the same person or not. This algorithm enhances the performance of iris recognition system by detected and segment the iris region in a fast and effective manner and use statistical features for iris recognition and using Hamming distance to perform the comparison of two iris patterns.

In 2011, Shashi Kumar D R, *et al.* [7] New algorithm for iris Recognition has been proposed. In this algorithm using a morphological process to remove the noise is caused by eyelids and eyelashes from upper and lower portion of the iris. Forty-five pixels to left and right of the pupil boundary detected as iris template, and then enhanced the image using Histogram Equalization to get high contrast. Discrete Wavelet Transform (DWT) is applied on histogram equalized iris template to get DWT coefficients. And then extract the features from the DWT coefficients using Principal Component Analysis (PCA). In matching module, multiple classifiers are used such as K-Nearest Neighbors (KNN), Random forest RF and SVM. The proposed algorithm has better performance parameters compared to existing algorithm. And the success rate is better in the case of KNN classifier compared to RF and SVM.

In 2012, Ashish kumar, and Majid Ahmad [10] developed an iris recognition system to verify the uniqueness of the human iris through used it as a biometric. The iris recognition starting with automatic iris segmentation, here use circular Hough transform technique to determine the parameters of circles(radius and centre coordinates of the pupil and iris regions) and then, remapping of the iris region from Cartesian coordinates to the polar coordinates to get rectangular block representation with constant dimensions to account for imaging inconsistencies. Feature vector has extracted using Log-Gabor filter. Finally, for matching, the Hamming distance was chosen as a metric for recognition. The performance of the system has been perfect and produces good recognition results.

In 2012 Gil Santos, Edmundo Hoyle [11] The recognition techniques used in this work performed by five steps: first, iris boundary detection, by following procedure: construct binary for the iris information, A contour is extracted from the white region of binary image, Hough transform is applied to obtain the circle for the iris region. Convert the eye image to grayscale and enhance it using Canny edge detection which applied inside the circular region finally, a Hough transform is used on the resulting to obtain the circle of the pupil. The second step is Iris normalization, then the third step feature extracted through five recognition techniques: Scale-Invariant Feature Transform, Local Binary Patterns, 1-D Wavelet Zero-Crossing, 2-D Dyadic Wavelet Zero-Crossing, Comparison Maps. In the fourth step is matching performed by five techniques: Distance-Ratio Based Scheme, Euclidean Distance, Dissimilarity Using Correlation Coefficient, Dissimilarity Using Correlation Coefficient, and Spatial and Frequency Analysis; The Decision is taken in the last step. In this system several different autonomous approaches were tested; the performances of each individual were evaluated in identification and verification modes and then the methods were fused and caused to improved accuracy, and showed that combining features extracted from the iris region with particular information improve the performance in both recognition modalities.

3. The Main Approach of Proposed Algorithm

This algorithm represents new try to construct a biometric system using iris trait and integrates this system by adding another module called liveness detection to protect it from spoof attack. The architecture of the proposed algorithm composed of two main phases' liveness detection phase and iris verification phase. The liveness detection performance by two sub-modules: (static sub-module and dynamic sub-module). And then iris verification phase is performed to produce matching scores for iris biometric. Finally, the decision is taken if a person is declared as genuine or an imposter as following:

3.1. Iris Liveness Detection

The existing techniques for liveness detection, depicted in **Figure 1**, can broadly be divided into two classes:

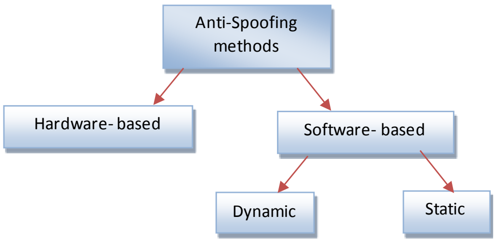

Figure 1. The existing anti-spoofing approaches.

[12] [13]:

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

Software-based approaches can extract any one peculiarity of live signs from the acquired sample using static techniques (using single sample), or dynamic techniques (using multiple samples) as showed in **Figure 1** [12].

Iris liveness detection module aims to ensure that an input eye image is from a live subject instead of a counterfeited eye image. In this proposed system focused on the establishment of countermeasure to iris photograph spoof attack, by using static and dynamic techniques as in subsection.

3.1.1. Static Technique

Considering the degree of focus property in 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 less than in 3D image, as in **Figure 2**, also defocus primarily suppresses high spatial frequencies which reduce the sharpening of the image, so that, the focus of a fake iris will differ from that of a genuine sample [4].

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

$$\begin{bmatrix} G_x \\ G_y \end{bmatrix} = \begin{bmatrix} \dfrac{\mathrm{d}f}{\mathrm{d}x} \\ \dfrac{\mathrm{d}f}{\mathrm{d}y} \end{bmatrix}. \tag{1}$$

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

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

$$G\left[f(x,y)\right] = \left|G_x\right| + \left|G_y\right|. \tag{3}$$

3.1.2. Dynamic Technique

Conceding Pupil variation in size with change in illumination, by comparing the size of pupils of two eye image samples of the same person acquired in different illumination, the difference in size of two pupils is measured (**Figure 3**). If a variation is in the range of 5% - 15%, then it is considered as real eye image, else fake eye image [14]. The percentage variation in size can be computed by this formula [15]:

$$\left|\frac{\text{First size} - \text{Second size}}{\text{First siz} + \text{Second size}/2}\right| \times 100\%. \tag{4}$$

3.2. Iris Verification Phase

This phase executed after liveness detection phase and if the output from this phase detected that the eye image

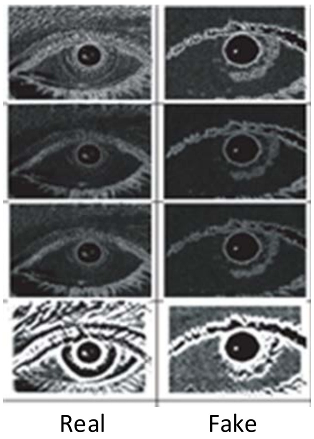

Figure 2. Different in focus quality features for a real and fake iris [4].

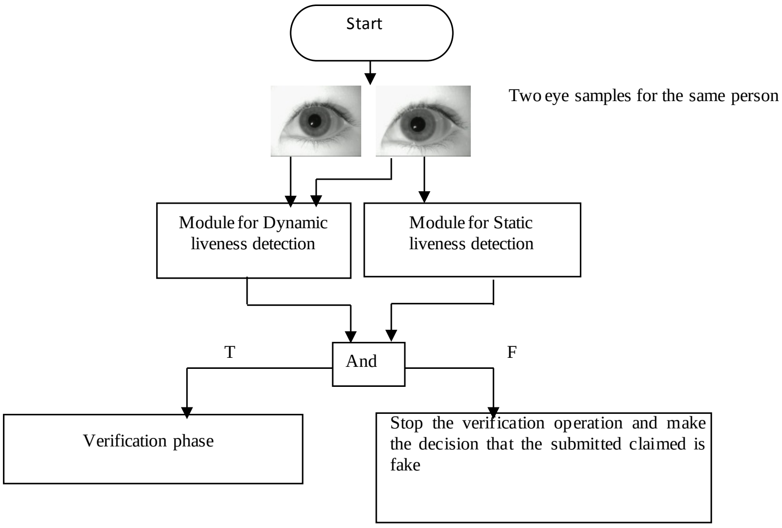
Start
Two eye samples for the same person
Module for Dynamic liveness detection
Module for Static liveness detection
T
And
F
Verification phase
Stop the verification operation and make the decision that the submitted claimed is fake

Figure 3. The flowchart of liveness detection phase algorithm.

samples is not spoofed. This phase contains two stage, Enrolled (training) stage and Verification (testing) stage:

- Enrolled stage: This stage deals with how to create reference set (template) for iris biometric system which composed of feature vector of iris biometric traits and an identifier (ID) for each authorized individual based on his input samples and stored in DBs to be used in matching operation in the verification (testing) module.
- Verification (testing) stage: In this stage Person submits the requested biometric traits to the sensors, and claims the identity of a client. This sample detected if it is fake or real sample by liveness detection module, and then pass through sequins of steps to extract feature vector and comparing this submitted feature vector with previously enrolled (template) for this claimed person, using a matching function. The output is matching scores for iris sample. The threshold used to accept the testing sample for the submitted person is (85%).

Iris Verification Steps

The iris verification phase composed of four steps performed in sequential mode, these are: Initialization, Iris Segmentation, Feature Extraction and Matching. As described below and depicted in Figure 4:

Step-1: Initialization: Input the eye image to extract iris feature set from it. The eye dataset used in this proposed system (MMU database and CASIA database) is grayscale eye images; therefore there is no need to convert from RGB to gray image

Step-2: Iris Segmentation: The main objective here is to isolate iris region from other regions of the eye image, by detecting papillary (inner) and limbic (outer) boundaries. It is the most important step in iris recognition

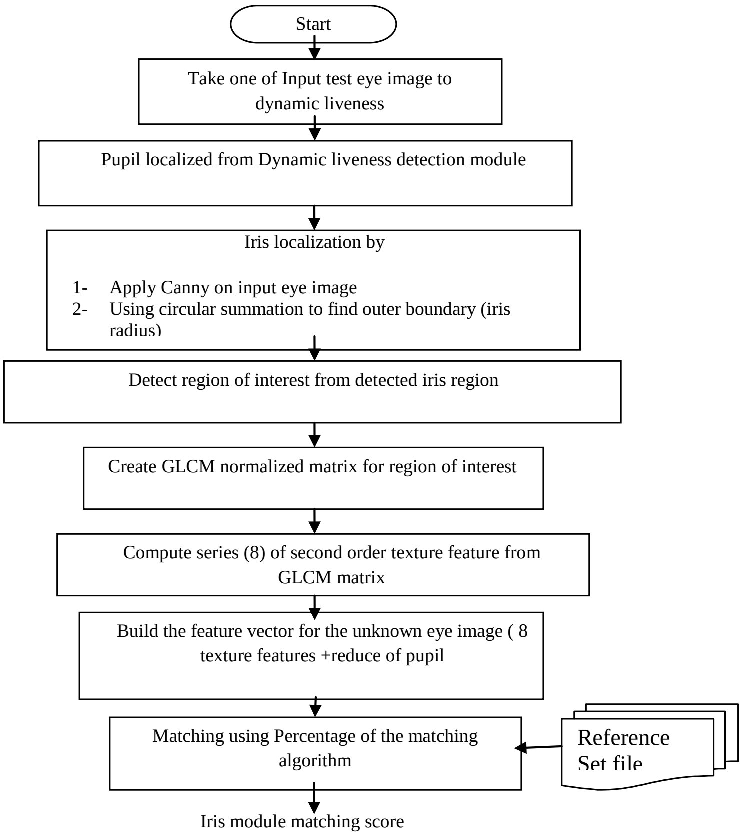
Start
Take one of Input test eye image to dynamic liveness
Pupil localized from Dynamic liveness detection module
Iris localization by
1- Apply Canny on input eye image
2- Using circular summation to find outer boundary (iris radius)
Detect region of interest from detected iris region
Create GLCM normalized matrix for region of interest
Compute series (8) of second order texture feature from GLCM matrix
Build the feature vector for the unknown eye image (8 texture features +reduce of pupil
Matching using Percentage of the matching algorithm
Reference Set file
Iris module matching score

Figure 4. Block diagram for the eye verification using second order texture feature from GLCM, AndPercentage of the matching algorithm.

systems because all the subsequent steps depend on its accuracy. And detect the region of interest to extract a feature from it. This step is performed in three stages:

Stage 1: Pupil localization: The assumption that the Pupil is considered as the darkest region in an eye image. And the pupil considers a very compact and connected region, that the difference between standard deviations for the coordinates (x) and (y) of the pixel inside of the pupil region tends to be the minimum value in eye image. On this basis, a new method for the pupil localization, which is based on the morphology of the binary image, constructed from the original eye image as following: the region with lowest gray scale take white color other regions take black color. The morphology operation was performed by using structuring element which represented by a disk of radius 2.5 shown in Figure 5. And then computes the difference between standard deviation for the coordinate of white region of binary image result from the morphological process (Sdt_{Diff}).

$$Sdt_{Diff} = \left|Std_x - Std_y\right|. \tag{5}$$

$$Std_x = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_i - \overline{x}\right)^2}. \tag{6}$$

$$Std_y = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(y_i - \overline{y}\right)^2}.$$

$$\overline{y} = \frac{\sum_{i=1}^{n}\left(y_i\right)}{n}. \tag{7}$$

$$\overline{x} = \frac{\sum_{i=1}^{n}\left(x_i\right)}{n}.$$

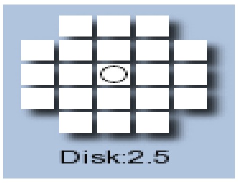

Figure 5. Structure element used in morphological operation.

After detecting the true pupil, next step is to find its radius R_p and center coordinates (C_{px}, C_{py}). Using this equation:

$$R_p = \frac{(y_{\max} - y_{\min})}{2}. \tag{8}$$

$$C_{py} = \frac{(y_{\max} + y_{\min})}{2}. \tag{9}$$

$$C_{px} = x_{\max} - R_p. \tag{10}$$

Stage 2: Iris localization

The outer boundary of an iris (the boundary between the sclera and the iris) has been found based on Intensity variation between iris and sclera. This operation can be conducted by using the canny operator with default two threshold values which have detected by the training data, to obtain the gradient image. And exploit the center coordinate and radius of the pupil which have been detected in the pupil localization stage and apply a Circular summation which consists of summing the intensities over all circles, pass over all possible radii starting from pupil's radius +15 to the pupil's radius +50 and center coordinates of the pupil. The circle with the highest summation corresponds to the outer boundary.

Stage 3: Detect the Region Of Interest (ROI): In the proposed system the conventional methods by using Daugman's rubber sheet model for iris normalization, is avoided as number of researchers do so, such as Debnath *et al.* [16] who Extracting a 8 × 12 Iris Pattern from Edge Detected IRIS Image, and Shashi Kumar D R, *et al.* [7] who select the iris regions to the left and right of the pupil From the localized image. Here, the region of interest is detected by selecting the part of iris region to the left and right and to the bottom of the pupil and then make all gray level values in pupil region equal to zero to isolate it from detected region to extract features from this detected region as templates. Selection of the region in this way reduces the dimension as the non-useful information is cropped out.

The training data turned out to be that radius of the pupil of the MMU database ranges from 20 to 30. The region that will be taken is 84 horizontally and 65 vertically around the Centre of the pupil.

Step-3: Feature Extraction: Once the segmentation has been performed and the region of interest (ROI) has been detected. The next step is to extract the feature from it to create the reference template. This operation performed by two stages:

Stage 1: Create a GLCM Normalized matrix for the detected interest region. The Grey Level Co-occurrence Matrix (GLCM) is a matrix fill with how many times different neighbor combinations of pixel's values occur in an image.

Stage 2: Find a series of "second order" texture as features. These texture measures consider the relationship between groups of two neighboring pixels in the original image, these (8) feature calculated from normalized GLCM matrix result from the previous stage and adding to them a radius of the pupil to represent feature vector consist of (9) features.

Step-4: Matching: this operation carry out by comparing the submitted feature vector with the template feature vector for the claimed person stored in the database using a matching algorithm, in order to compute a similarity degree between these two feature vectors, this similarity degree represented by a value called (matching score).

Many algorithms have been proposed to match two biometric trait representations such as Euclidean distance, City block distance, Hamming distance. However, it is still trying to design a matching algorithm suitable of satisfying the right requirements of many real applications in terms of verification errors. The (Percentage of the matching) is metric used in proposed system for measuring the matching score between two feature vectors and is performed by the (algebraic sum of the percentages of the matching achieved by each element in the test vector set with the corresponding element in the template vector set). Finally, the decision has been taken if the submitted biometric trait belongs to the genuine or impostor person.

4. Results

4.1. Iris Liveness Detection Results

Database that is set up to test the robustness of the proposed algorithm through iris liveness detection process through static and dynamic modules consists of 15 folders of original (MMU database) each folder contain tow eye images sample represent live tries. And 15 folders of(MMU database) eye images printed using the scanner as a devise and recapture using a specific camera and resaved in the computer to represent 15 attempted spoof attack against the system each folder contained two samples of fake eye image. **Table 1** shows experiment results for dynamic iris liveness module and **Table 2** show the results of static iris liveness module.

4.2. Iris Verification Experimental Results

Two types of iris database used to training and testing the proposed system: MMU Iris database and CASIA-IrisV1database. The training of iris verification algorithm consists of three experiments as follows:

The first experiment conducted to test the proposed iris verification algorithm by applied on 180 eye image of (MMU database) for 30 persons for left and right eyes three samples for the left eye and three sample for the right eye for each person. The second experiment testing of the proposed iris verification algorithm phase by applied on 90 images of (CASIA-IrisV1 database) for 30 people's three samples of eye image for each person. In the third experiment, the eye images database collected for testing the proposed biometric verification algorithm as completed system. Started from liveness detection phase and ending with verification phase consists of 15

Table 1. The experiment results for dynamic iris liveness module of 15 real tries and 15 fake tries.

Person No.	Results by appling on original eye images			Results by appling on recaptured eye images		
	No. of pixel in pupil for two samples with different eliminations	Percentage difference in pupil size	Decision	No. of pixel in pupil for two samples with different eliminations	Percentage difference in pupil size	Decision
1	291210 325125	11.005	Live	694620 695895	0.183	Fake
2	482460 540090	11.272	=	682380 691050	1.613	Fake
3	457980 525300	13.693	=	1418310 1419330	0.072	Fake
4	330735 372300	11.824	=	961605 974355	1.317	=
5	699210 759900	8.319	=	512295 772395	40.492	=
6	410550 474300	14.409	=	930495 759900	20.184	=
7	408000 431460	5.589	=	1266075 1327530	4.739	=
8	337875 368220	8.595	=	542640 548760	1.121	=
9	248625 288150	11.116	=	482715 685695	34.745	=
10	514845 566355	9.528	=	675750 907800	29.308	=
11	585735 627555	6.894	=	1564425 1195695	26.718	=
12	469455 536010	13.239	=	828750 562785	38.226	=
13	439110 469710	6.734	=	1036065 1171980	12.311	Faulty live
14	336345 336345	5.529	=	818805 842265	2.825	Fake
15	719865 762450	5.746	=	1002915 860880	15.241	Fake

Table 2. Show the experiment results of applying static module on original eye images and recaptured eye images for 15 person enter to the system.

Person No.	Results by appling static module on original eye images		Results by appling static module on recaptured eye images	
	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	45.867 38.969	Live =	28.808 32.486	Fake =
2	36..203 58.622	Live =	29.355 39.577	Fake Faulty Live
3	42.561 37.927	Live =	34.55 30.977	Faulty Live Fake
4	35.306 35.998	Live	29.382 28.72	Fake =
5	55.638 49.592	Live =	32.273 32.884	= =
6	36.935 41.593	Live =	26.155 28.721	= =
7	36.489 36.454	Live	27.464 29.281	= =
8	35.789 45.489	Live	26.947 32.051	= =
9	35.49 35.186	Live =	26.22 25.554	= =
10	35.511 34.5	Live =	27.708 23.303	= =
11	35.122 35.052	Live =	25.392 28.361	= =
12	39.363 37.276	Live =	28.55 28.323	= =
13	36.702 38.173	Live =	23.235 28.416	= =
14	34.363 35.389	Live =	23.112 27.843	= =
15	35.55 33.55	Live =	26.295 24.792	= =

folders of (MMU database) for 15 persons each folder contained four samples for left eye image. Table 3 clarify the results of testing operation for verification phase of iris model and the accuracy computed and The False Accepted Rate (FAR) and False Rejected Rate (FRR) which computed by following equations:

$$\text{FAR} = \frac{\text{Number of times different member matching} \times 100}{\text{Number of comparison between difference members}}. \tag{11}$$

$$\text{FRR} = \frac{\text{Number of times same member rejected} \times 100}{\text{Number of comparison between same members}}. \tag{12}$$

5. Conclusions

By extensive and hard work in the design of the proposed system which is represented by iris verification to improve the security and accuracy of it through adding another module (liveness detection) to it, we reach to a number of conclusions.

- The dynamic method which used to detect liveness is more effective, more accuracy and more successful

Table 3. Experiment results of the iris verification phase.

Eye image database	No. of people	No. of samples	No of samples successfully verification	No. of samples faulty accepted	No. of samples faulty rejected	Tame of verification	Time for matching	FRR %	FAR%	Average accuracy
MMU DB	30	180	179	5	1	20 second	0.8 second	0.0055	0.0277	99.44%
MMU DB	15	60	59	2	1	20 second	0.8 second	0.0166	0.0333	98.33%
CASIA (Version 1.0)	30	90	88	3	2	24 second	0.8 second	0.0222	0.0333	97.77%

than static method, as shown in **Table 1** for iris dynamic liveness detection. The Static method needs to detect fixed threshold, and is extracted from original properties of the biometric trait to accept image sample as the real sample. Choosing this threshold will be influenced by the variance of these original properties from person to another, such as the degree of sharpening of original eye image and the way used to collect the original image database and manufacture spoof database, which causes the ratio of error in liveness decision.

- The sequence of morphological operations has been followed to isolate a pupil object from eye images and the limitation used to extract the region of interest from detected iris region is not fixed for all types of eye images database with any conditions. That means the sequence applied in (MMU database) is closing first and then opening. In CASIA database, different sequence of morphological operations is applied, and the radius of the pupil in MMU DB which it is in range (20 to 30) is different from radius in CASIA DB which it is in the range (30 to 45)
- For matching module of this proposed system, there is a specific percentage rate for similarity between each element in test feature vector with the corresponding element in template feature vector allowed to it to enter into the comparison process to produce the final matching score. If the percentage rate of similarity for any element in the feature vector is less than the specific percentage rate, it will be not take part in the matching process to avoid FAR in this system.
- Due to the richness of the texture details in the iris, we find that the calculating texture features from the normalized GLCM (series of second order texture features) is the most convenient and very successful method and satisfies good accuracy in calculating the features of this region.

The experiment results show that the performance of the proposed system in MMU DB is better than performance in CASIA DB. This is shown from the results in **Table 3** which showed that the verification operation is faster in applying on MMU DB than in CASIA DB, and the accuracy in MMU DB is 99.44%, while in CASIA DB is 97.77%.

References

[1] Akhtar, Z. (2012) Security of Multimodal Biometric Systems against Spoof Attacks. Thesis of Ph.D. in Electronic and Computer Engineering, University of Cagliari, Cagliari.

[2] Galbally, J., Alonso-Fernandez, F., Fierrez, J. and Ortega-Garcia, J. (2009) Fingerprint Liveness Detection Based on Quality Measures. 2009 *International Conference on Biometrics*, *Identity and Security*, Tampa, 22-23 September 2009, 1-8. http://dx.doi.org/10.1109/bids.2009.5507534

[3] Marasco, E. and Ross, A. (2014) A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems. *Journal ACM Computing Surveys* (CSUR), **47**, Article A.

[4] Galbally, J., Alonso-Fernandez, F., Fierrez, J. and Ortega-Garcia, J. (2012) Iris Liveness Detection Based on Quality Related Features. 2012 5*th IAPR International Conference on Biometrics* (*ICB*), New Delhi, March 29 2012-April 1 2012, 271-276. http://dx.doi.org/10.1109/icb.2012.6199819

[5] Herrero, J.G. (2009) Vulnerabilities and Attack Protection in Security Systems Based on Biometric Recognition. Thesis of Ph.D., Universidad Autonoma de Madrid, Madrid.

[6] Patil, B.G. and Subbaraman, S. (2011) SVD-EBP Algorithm for Iris Patten Recognition. *International Journal of Advanced Computer Science and Applications*, **2**, 115-119.

[7] Shashi Kumar, D.R., Raja, K.B., Chhootaray, R.K. and Pattnaik, S. (2011) PCA Based Iris Recognition Using DWT. *International Journal of Computer Technology and Applications*, **2**, 884-893.

[8] Daouk, C.H., El-Esber, L.A., Kammoun, F.D. and Al Alaoui, M.A. (2002) Iris Recognition. *IEEE ISSPIT*, Marrakesh, 1.

[9] Tuama, A.S. (2012) Iris Image Segmentation and Recognition. *International Journal of Computer Science & Emerging*

Technologies, **3**, 60-65.

[10] Dewangan, A.K. and Siddhiqui, M.A. (2012) Human Identification and Verification Using Iris Recognition by Calculating Hamming Distance. *International Journal of Soft Computing and Engineering* (*IJSCE*), **2**, 334-338.

[11] Santos, G. and Hoyle, E. (2012) A Fusion Approach to Unconstrained Iris Recognition. *Pattern Recognition Letters*, **33**, 984-990. http://dx.doi.org/10.1016/j.patrec.2011.08.017

[12] Singh, Y.N. and Singh, S.K. (2011) Vitality Detection from Biometrics: State-of-the-Art. *IEEE World Congress on Information and Communication Technologies*, Mumbai, 11-14 December 2011, 106-111.

[13] Anonymous (2014) Fingerprint Liveness Detection Using Convolutional Networks. *IJCB*, *Confidential Review*, 1-2.

[14] Rajesh M. Bodade, Sanjay N. Talbar (2014) Iris Analysis for Biometric Recognition Systems. Springer, New Delhi, Heidelberg, New York, Dordrecht and London. http://dx.doi.org/10.1007/978-81-322-1853-1

[15] (2014) Percentage Difference. https://www.mathsisfun.com/percentage-difference.html

[16] Bhattacharyya, D., Das1, P., Bandyopadhyay, S.K. and Kim, T.-H. (2008) IRIS Texture Analysis and Feature Extraction for Biometric Pattern Recognition. *International Journal of Database Theory and Application*, **Vol.**, 53-60.