AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Spoofed Iris Recognition: Synthesis of Gabor and LBP descriptor using SPPC

[1]M. Malathy and [2]Dr.J. Arputha Vijaya Selvi

[1]*Associate Professor, Department of Information Technology, Kings College of Engineering, Pudukkottai, Tamil Nadu, India*
[2]*Dean, Department of Electronics and Communication Engineering, Kings College of Engineering, Pudukkottai, Tamil Nadu, India*

ARTICLE INFO

Article history:
Received 2 March 2014
Received in revised form
13 May 2014
Accepted 28 May 2014
Available online 13 June 2014

Keywords:
Biometric, Iris recognition, Spoof iris image, Multi-scale local binary pattern (MLBP), Gabor wavelet, Local binary pattern (LBP), Spatial point pattern classifier.

ABSTRACT

Background: With the growing requirement of safety in everyday activities, identity management has quickly become an eminent concern. Biometrics using iris recognition systems are employed to scrutinizing an individual from a digital image or video source. In the proposed work, the robustness of iris recognition with spoofing attack is expounded. The dataset images are improved using image enhancement techniques. Multi-scale Local Binary Pattern (MLBP) algorithm is established for extracting the effective features to symbolize the images. This algorithm is a combination of Gabor wavelet followed by Local Binary Pattern (LBP) descriptor. The magnitude coefficients (real part) are isolated from Gabor wavelets and considered as an input for LBP which extracts the features of the given input image in various directional scales. Here, a supervised learning classifier especially spatial point pattern classifier is employed to check the verification process. Both dataset iris images and synthetically spoofed iris images are evaluated by the algorithm in order to increase a genuine acceptance ratio (GAR). The experimental result exhibits high efficiency and evaluates the better performance of the proposed approach. **Objective:** Spoofed Iris Recognition: Synthesis of Gabor and LBP descriptor using SPPC. **Results:** This section presents the result analysis for proposed work in which the spoofed iris image is detected by using the normalization method and feature extraction method. The classification accuracy and timing analysis of the algorithm are given in table I. In the presence of uncertainty, true positive rate or sensitivity is used to test the robustness of the results of a proposed system. **Conclusion:** In this paper, the robustness of iris recognition system with spoofing attack is explained. The dataset images are enhanced using image enhancement techniques. It is later subjected to multi-scale local binary pattern (MLBP) algorithm for extracting the efficient features to represent the images. This algorithm is a combination of Gabor wavelet followed by local binary pattern description (LBP) where the magnitude coefficient from Gabor wavelets takes as its input. A spatial point pattern classifier is used to check the verification process. Both dataset iris images and synthetically spoofed iris images are evaluated by the algorithm in order to increase a genuine acceptance ratio (GAR).

To Cite This Article: M. Malathy and Dr.J. Arputha Vijaya Selvi., Spoofed Iris Recognition: Synthesis of Gabor and LBP descriptor using SPPC. ***Aust. J. Basic & Appl. Sci.,*** *8(9): 433-442, 2014*

INTRODUCTION

Biometric authentication refers to the recognition of humans by their individuality or characters. Biometricis used in computer science as a form of detection and access control. It is also used to recognize persons in groups that are under observation. Biometrics using fingerprint, face, voice, iris, and more based recognition systems is to identify an individual, has been accepted as an identification verification technology. A facial recognition system (O'Connor, B. and K. Roy, 2013; Robson Schwartz, W., *et al.*, 2011) is used for identifying a person from an image or video automatically. This is mainly for security purpose which can then compare with biometrics such as fingerprint or iris detection process. The process of identifying image or video by comparing with extracted features placed in a database.

Iris recognition is a computerized technique of biometric detection which uses mathematical pattern-recognition methods on video pictures of the iridesof a singular eye which can be detected from several distances. Iris is a skinny, round composition in the eye, answerable for controlling the diameter and size of the pupil and thus the quantity of light arriving the retina. The pigment of the iris is frequentlyconsidered as "eye color." In visualexpressions, the pupil is considered as the eye's aperture whereas the iris is regarded as the aperture stop.

Corresponding Author: M. Malathy, Associate Professor, Department of Information Technology, Kings College of Engineering, Pudukkottai, Tamil Nadu, India.

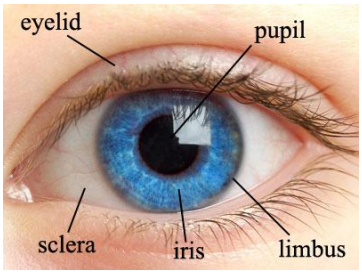

Fig. 1: Human Iris.

Blue region of a human eye in the fig.1is the iris. Remaining visible black part in the center is the pupil and the white part which is surrounding the iris is sclera.Scanning of the retinal region leads to many mistakes while taking a picture, to overcome this iris recognition playing a major role for better authentication. The following is the advantage of iris recognition:

- Stable
- Uniqueness
- Flexible
- Reliable
- Non-Invasive

A spoofing attackis a state in which one person effectively masquerades as another by faking data and thereby gaining an unauthorizedbenefit.This paper investigates the robustness of iris recognition with spoofing attacks. The dataset images are enhanced using image enhancement techniques. It is later subjected to multi-scale local binary pattern (MLBP) algorithm to extract efficient features to represent the images. This algorithm is a combination of Gabor wavelet followed by local binary pattern description (LBP) where the magnitude coefficient from Gabor wavelets takes as its input. A spatial point pattern classifier is used to check the verification process. Both dataset iris images and synthetically spoofed iris images are evaluated by the algorithm in order to increase a genuine acceptance ratio (GAR).

The rest of the paper is systematized as follows. Section II briefly overview the related happening in the spoof iris recognition technique. Section III involves the detailed explanation about the proposed method. Section IV describes the implementation details. Section V summarizes with a brief conclusive remark and discussion on future works.

Related Work:

Han et al proposed a local mean decomposition (LMD) techniquewhich was used for extracting iris attribute and also for recognition based on iris image database. In this, an initial process was to assess the quality of iris image, then follows iris image preprocessing, attribute extraction and finally matching process decided whether the unknown attributes came from an authenticated person. This technique was considered as an excellent technique for iris recognition and also for attribute extraction (Han, W.Y., *et al.,* 2014). *Akhtar et al* investigated the security issues in a real spoof attack samples beneath distinct situations. It mainly focused on the behavior of permanent and trained score fusion rules. This enhanced the security against spoof attacks and also avoided multimodal system by the actual spoofing of the individual biometrics which examines the behavior of the score fusion rules (Akhtar, Z., *et al.*, 2011). *Bodade et al* presented a new process of precise iris segmentation for fake iris detection. Iris was segmented by capturing two images of distinct intensities. It was more robust and useful against fake iris based spoofing technologies (Bodade, R. and S. Talba, 2010).

Radu et al proposed an iris recognition technique where the multiple classifier systems (MCS) were introduced for noisy color iris images. The major advantage behind this approach was that eye color was employed as soft biometric and also simple to consider for an individual image. MCS works on database-free and provides accurate results over color iris (Radu, P., *et al.*, 2013). *Rathgeb et al* proposed various improvements to iris-based template protection and comparators. It enhances the security and accuracy for iris templates without re-enlistment of registered topics (Rathgeb, C., 2013). *O'Connor et al* applied modified local binary pattern (MLBP) for enhancing the performance of facial textures. Random forest was introduced to decrease the feature vectors without affecting the accuracy of face recognition systems. This system also useful for speeding up the classification process (O'Connor, B. and K. Roy, 2013).*Venugopalan et al* discussed the formation of artificial iris texture. Based on the iris bit code, to bypassing a system alternate iris texture (spoof) was produced. Spoofed texture was compared to the original iris texture and if matches occur it provides the same score. Daugman style systemswere introduced for iris matching scheme (Venugopalan, S. and M. Savvides, 2011).

Puhan et al proposed a novel iris liveness detection approach which was used to identify semi-transparent contact lens based spoofing. It helps to compute the textural difference between localized iris sub-images.It won't show any changes in textural and then it would return in extremely low values of the standardized

hamming distances (Puhan, N., *et al.*, 2011). *Schwartz et al*described an anti-spoofing solution based on a complete depiction of the facial region. It was described for differencing the live and spoof images and videos using partial least square regression. The results were obtained by the datasets based on only one feature of images and videos (Robson Schwartz, W., *et al.*, 2011). *Kathikeyan et al*presented multi-modality human identification system, which combines the iris and electroencephalogram (EEG). It also checks the liveness of the system. This integrated model was used to simplify the design and also ease in fusion (Kathikeyan, T. and B. Sabarigiri, 2012).

Galballyet al presented a new liveness detection method based on quality associated measures. It was used to detect the fake data by choosing the subgroup of parameters which adapts to the anti-spoofing. It helps to prevent the direct attack and also provides better security (Galbally, J., *et al.*, 2012). *Al-khassaweneh et al*suggested a fusion system of fingerprint and iris recognition. For iris recognition, iris were extracted by using segmentation method. For fingerprint recognition, initial image was converted into grayscale and enhanced the image which further improve the overall matching score. This system provides high security and performance (Al-khassaweneh, M., *et al.*, 2012).

*Hughes et al*proposed a novel iris recognition spoof mechanism using cosmetic contact lens. It was used to provide speedy, precise, and automatic detection.The stereo imaging was introduced to require a second camera in iris sensor which simplifies the overall process.This system minimizes the specular inter-reflectionsand its range was sensitive to reflections on the iris (Hughes, K. and K.W. Bowyer, 2013). *George et al*discussed various iris recognition systems which provide high accuracy and also analyzed without false error rate. Each system consists of benefits and limitations, where the result for accuracy was improved by all techniques (George, A.M. and C. Anand Deva Durai, 2013). *Connell et al*described a novel structured light projection process for detecting fake iris. This method was used to make contour changes in a stripe pattern. It improves security and also calculated end-to-end performance and crosstalk with the integrated iris recognition systems (Connell, J., *et al.*, 2013).

Godara et al proposed cascade forward and learning vector quantization neural network structures. The result of these structures was compared and finally LVQ has the better time consuming (Godara, S. and R. Gupta, 2013). *Bonnen et al*presented a framework for component based representation in face recognition. This system provides robust to changes and potential for high accuracy. This also overcomes the difficulties in extracting individual facial components (Bonnen, K., *et al.*, 2013). *Martino et al*discussed a countermeasure against face spoofing attacks using the local binary patterns from three orthogonal planes (LBP-TOP) descriptor joining both space and time information into a single descriptor. This system showed an immense potential against face spoofing in distinct kind of attack situations (De Martino, J.M., *et al.*, 2012). *Bodade et al*proposed a composite method which provides a robust iris recognition system with fake iris detection module. To extract the accurate image, image segmentation and active method were introduced. For better results and higher efficiency passive method using the wavelength reflection coefficient method was suggested (Bodade, R. and S. Talbar, 2011). *Moghadam et al*proposed a feed forward neural network (FFNN)which improves the accuracy for iris localization. To reduce the error in neural network cascaded FFNN was introduced. This provides better results with minimum error (Moghadam, F.M., *et al.*, 2013).

Proposed Work:

This section presents the detailed explanation about the iris recognition and spoofing attacksagainst an eye iris image. Iris recognition is a computerized method of biometric detection that adoptsa mathematical pattern-recognition procedure on video, pictures of the irises of singular eyes. It intends to precise, robust, quick, safe and easy to useverification of individualcharacteristics by the acquisition, processing, analysis and comparison of iris patterns. It involves a complicated process to produce the digital uniquenessinstruction from physical eyeballs. The flow diagram of a typical iris recognition method is diagrammatically shown in Fig. 2. The overall iris recognition method mainly includes three modules in which each basic module of iris recognition with some related concerns is concisely described as follows:

- Iris Image Enrollment
- Iris Image Verification
- Iris Image Spoofing

An initial module of iris recognition system takes an input from the respective dataset.Fig.3. (a) and (b) depicts the images of both left and right eye's irises. It determines the communication between the user and the iris recognition process.

Iris Image Preprocessing:

The main purpose of iris image preprocessing or segmentation includes the discovery of the iris existence, the decision of the iris liveness, the evaluation of image quality, development of the iris image, the confinement of the internal and external iris borders, the detection and exclusion of noise and the standardization of image dimension and distortion. Fig.4 depicts the eye iris image segmentation for the given input images. It requires

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 433-442

performing automatic preprocessing of the eye iris image and also it isolate noise areas such as occluding eyelids and eyelashes.

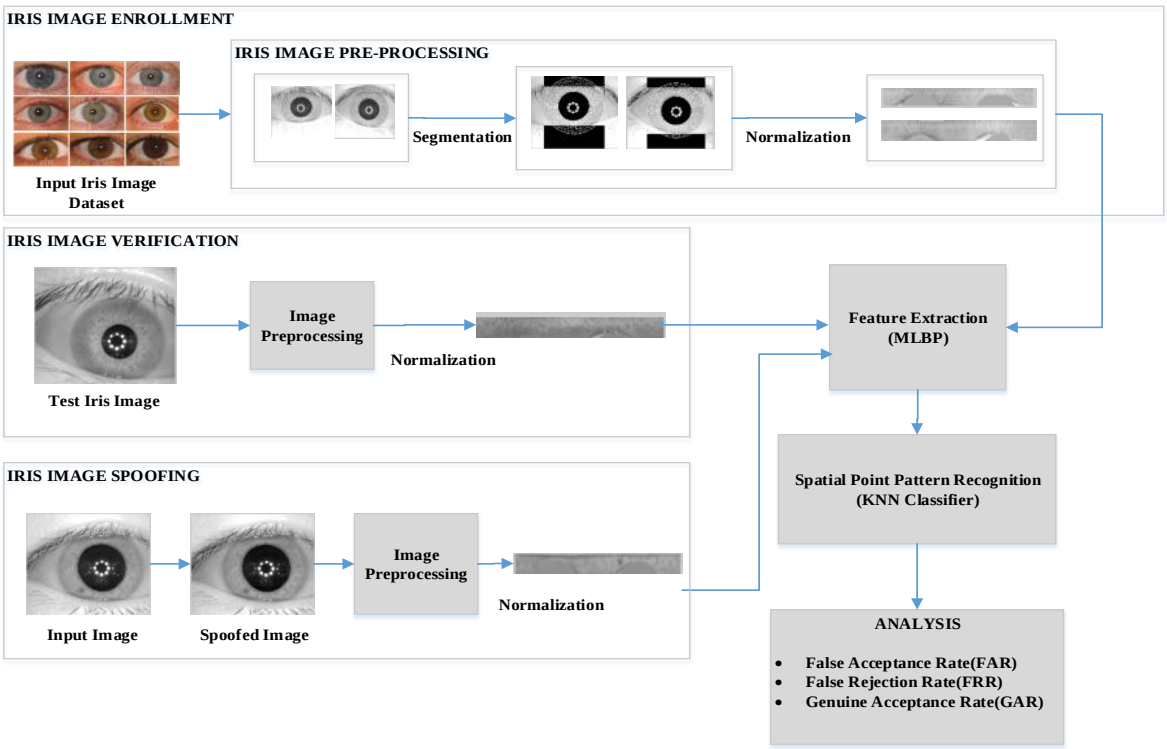

Fig. 2: Flow diagram of the proposed iris recognition scheme.

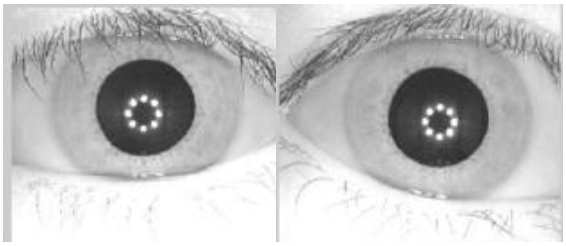

Fig. 3: (a) Left eye iris image (b) Right eye iris image.

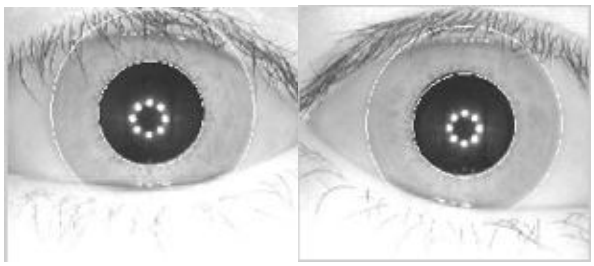

Fig. 4: (a) Left eye iris image segmentation (b) Right eye iris image segmentation.

Iris or Pupil Localization:

The iris is a skinny, round composition in the eye situated between the pupil (inner boundary) and the sclera (outer boundary). At first, the range of the pupil and radii of the iris is described. Canny edge detection is employed to get the edge map. By applying Hough transform the boundary of the iris is determined. From the Hough transform pupil boundary, top eyelid, bottom eyelid, line coordinates are findout. Then eliminate the eye lashes using the value of threshold. Next obtain the pixel coordinates for the circle around the iris and the pupil. Finally, find the polar coordinates by excluding the values at the pupil-iris boundary, and the iris-sclera boundary as these may not correspond to areas in the iris region and it will introduce noise. Thus calculate the

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 433-442

Cartesian location of each data point around the circular iris region. Intensity values are extracted into the normalized polar representation through interpolation.

Iris Normalization:

For normalizing the iris image following steps are described. At the start, the displacement of pupil center from the iris center is calculated and then radius around the iris is evaluated as a function of the angle. Exclude the boundary values of pupil-iris border and the iris-sclera border as these may not correspond to areas in the iris region and will introduce noise. The outside rings are neglected as it is not iris data. The Cartesian location of each data point around the circular iris region is determined and then intensity values are extracted into the normalized polar representation through interpolation. The polar coordinates for the circle around the iris are acquired and finally the rings overlaying an original iris image are recorded.

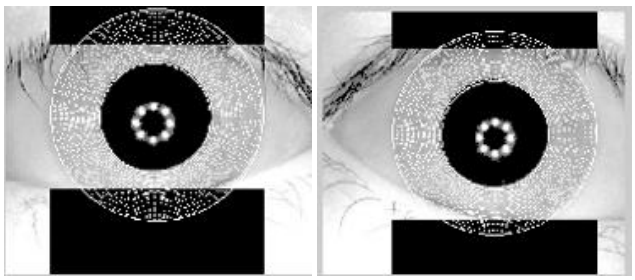

Fig. 5: (a) Left normalized iris (b) Right normalized iris.

Fig. 6: Polar coordinates of left and right iris image.

Fig. 5 depicts the normalized iris image in which the pupil-iris border and the iris-sclera border are excluded. The outer rings presented in the normalized iris imageare neglected and lastly the rings overlaying an original iris image are recorded as displayed in fig. 6.

Iris Synthesis:

Iris pattern of an anonymous person is embedded into the real iris image of person without disturbing the quality of the image. Iris is synthesized by using a least significant method which allows large amounts of data to be embedded without observable changes. The technique works by replacing some of the information in a given pixel with information from the data (iris pattern) in the image.

Aleast significant bit (LSB) is embedded directly into a pixel where assome information from the cover image is always lost. To carry this out, some of the cover's information must discard and hide the replaced information from the data. LSB algorithms have an option about how they embed that data to hide. It takes up less space for embeddinglossless data, preserving all information about the data, or the generalize data. In this, the seven most-significant bits are assigned to the cover and only the LSB contains the data. This separation of bits benefits to minimize the detection.

Gabor Filter and Local Binary Pattern (LBP) Algorithm:

Only the significant features of the iris is encoded using the Gabor filter and local binary pattern algorithm.Gabor filter is an outstanding technique for extracting the features in order to analyze the texture and also to detect the edge. It determines the image using Gabor functions which are similar to the human visual perception system. Gabor filters are accurately related to Gabor wavelets where the edge (points)is recognized, subsequently they can be established for a number of distention and rotations.Gabor wavelet is defined as:

$$G_{\{R,I\}} = \mathrm{sgn}_{\{R,I\}} \iint I(\alpha,\beta) e^{-i\omega(\theta_0-\alpha)} e^{-(r_0-\beta)^2/r^2} e^{-(\theta_0-\beta)^2/\phi^2} \beta d\beta d\varphi \quad (1)$$

The real part of Gabor filter is represented as:

$$G(a,b;\lambda,\theta,\psi,\sigma,\gamma) = \exp\left(-\frac{a'^2+\gamma^2 b'^2}{2\sigma^2}\right)\cos\left(2\Pi\frac{a'}{\lambda}+\psi\right) \quad (2)$$

An imaginary part of Gabor filter is represented as:

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 433-442

$$G(a,b;\lambda,\theta,\psi,\sigma,\gamma)=\exp\left(-\frac{a'^2+\gamma^2 b'^2}{2\sigma^2}\right)\sin\left(2\Pi\frac{a'}{\lambda}+\psi\right) \quad (3)$$

where $a' = a\cos\theta + b\sin\theta$ and $b' = -a\sin\theta + b\cos\theta$

In the above real and imaginary parts of Gabor filter, λ denotes the wavelength of the sinusoidal factor, θ signifies the orientation of a Gabor function, ψ denotes the phase offset, σ is the standard deviation (SD) of Gaussian envelope and γ represents the spatial aspect ratio.

The real part of Gabor output is applied to the local binary pattern (LBP) which is a form of powerful feature employed for texture classification. The textures of fake iris images are useful for spoof detection. The algorithm for LBP feature vector is generated by the following steps. Initially, the tested window is divided into cells. LBP is determined for each and every pixel by thresholding its 3*3 neighborhood pixels along with the center value of the pixel and the outcome is termed as a binary bit string. Every LBP code symbolizes a kind of micro image structure and the allocation of this structure can be employed as a texture descriptor. The LBP is formed as:

$$LBP(a_C,b_C)=\sum_{i=0}^{7}2^i s(n_i-n_C) \quad (4)$$

where c is the central pixel, n_i and n_c are the values of gray-level.

A typical LBP is advanced to multi-scale LBP which is denoted as $LBP_{s,r}$. The extended LBP is evaluated with the center value of a pixel by thresholdings equally spaced points on a circle where *r* is radius. A code formed by LBP is said to be uniform if its bit string includes two transitions bit-wisely from 0 to 1 and vice versa. The center pixel's value is always greater than the neighbor's value. This provides the binary number which further converts into decimal value. After that the histogram of pixels are evaluated and lastly feature vector is formed. LBP based approaches have been proven as beneficial in iris representation.It is also helpful for improving the performance of detection.

The process for above discussed components of iris recognition system are completed,further it takes to the spatial point pattern classifier (i.e., K-nearest neighbor (KNN) classifier). To conclude this system, analysis of iris images compares with a false acceptance rate (FAR), genuine acceptance rate (GAR), false rejection rate (FRR).

Performance Analysis:

This section presents the result analysis for proposed work in which the spoofed iris image is detected by using the normalization method and feature extraction method. The classification accuracy and timing analysis of the algorithm are given in table I.In the presence of uncertainty, true positive rate or sensitivity is used to test the robustness of the results of a proposed system. It is calculated based on the following equation:

$$Sensitivity=\frac{TP}{TP+FP} \quad (5)$$

Here, TP denotes true positive and FP is the false positive. Specificity or true negative rate measures the proportion of negatives which are correctly estimated without any condition. It is calculated by the following equation:

$$Specificity=\frac{TN}{TN+FP} \quad (6)$$

Receiver operating characteristics (ROC)are produced by plotting the fraction of true positives out of the total actual positives (TPR) vs. the fraction of the false positives out of the total actual negatives (FPR) at different thresholds whereTPR is the true positive rate and FPR is the false positive rate. The false rejection rate (FRR) is the measure of the probability that the biometric security system will incorrectly reject an access attempt by an authorized user.

$$FRR=\frac{\text{The number of false rejections}}{\text{The number of identification items}} \quad (7)$$

The false acceptance rate (FAR) is the measure of the probability that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

$$FAR=\frac{\text{The number of false acceptances}}{\text{The number of identification items}} \quad (8)$$

Fig.8 shows a ROC curve, which is a plot of the true positive rate against false positive rate for all possible systems and calculates the entire performance of the system. Table II depicts the experimental results, where

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 433-442

FAR (False acceptance rate), FRR (False rejection rate) and the GAR (Genuine acceptance rate) which described as (1-FRR) are presented. The proposed method (i.e., MLBP) outperforms the other existing methods in accuracy.The LBP provides faster execution by its computational simplicity while compared with the evaluation of GLCM (He, X., *et al.*, 2007), iristextons (Wei, Z., *et al.*, 2008), Ada-boost classifier (He, Z., *et al.*, 2009).

Table I: Results of Classification Accuracy and Timing Analysis.

Methodology	Accuracy	Time in seconds
Iris recognition	95%	0.0239 s
Spoof detection	100%	13.2761 s
Spoofed iris recognition (Both training and testing)	100%	14.1671 s

Peak signal-to-noise ratio:

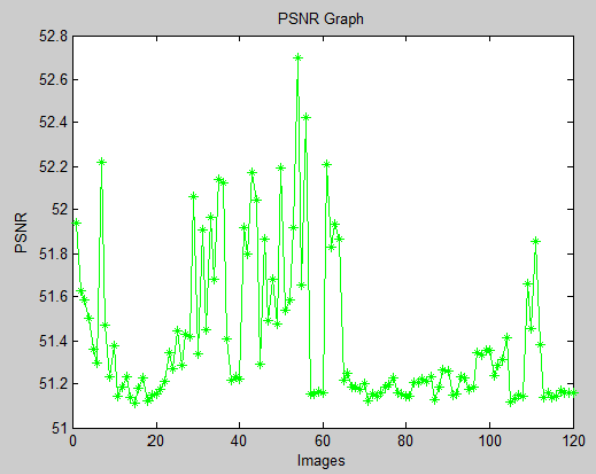

Fig. 7: Peak signal-to-noise ratio graph.

The peak signal-to-noise ratio (PSNR) is the ratio between the maximum power of signal to the power of noise. Thevalue indicates the spoofed image and original image contents that are at most similar. In this proposed method 120 images are used. For these images the PSNR value is as shown in fig. 7.

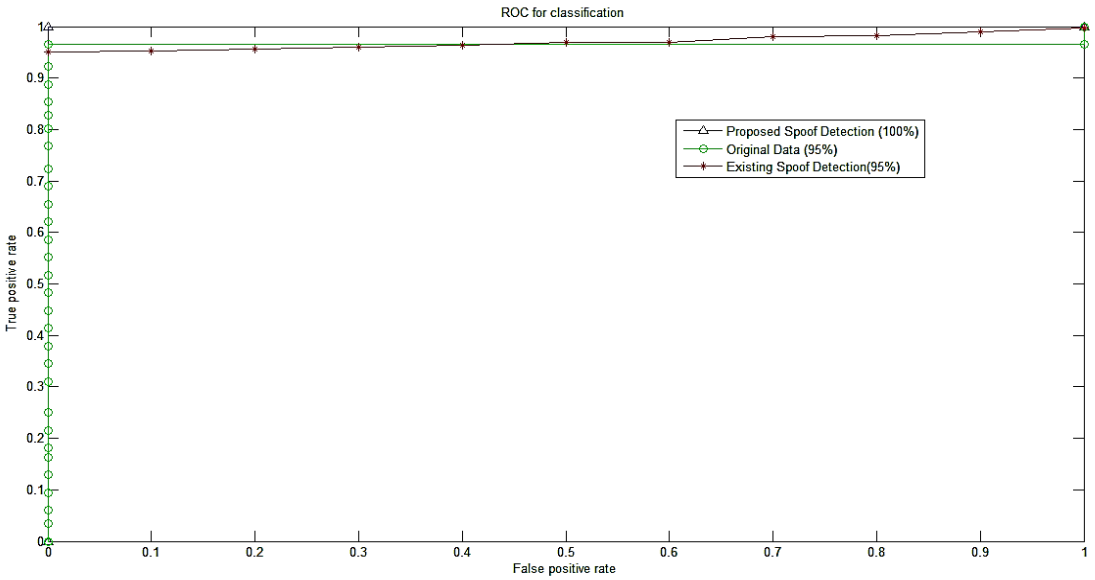

Fig. 8: Results of spoof iris detection using the Gabor wavelet followed by local binary pattern (LBP) description is as in the equation (1) and (4). Original data corresponds to performing authentication using genuine iris images in the CASIA database. Proposed spoof detection shows the authentication performance obtained when comparing all the spoofed iris images with the images from the CASIA

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 433-442

database. The true positive rate in proposed spoof detection is 100%, whereas in existing spoof detection is 95%.

Table II: The overall performance of the learned classifiers via (He, Z., *et al.*, 2009; Wei, Z., *et al.*, 2008; He, X., *et al.*, 2007) and the Proposed method.

ALGORITHM	FAR (%)	FRR (%)	GAR (%)
He (2007)	4.33	6.84	93.16
Wei (2008)	3.67	6.91	93.09
He (2009)	0.67	2.64	97.34
Proposed	0.56	0.67	99.33

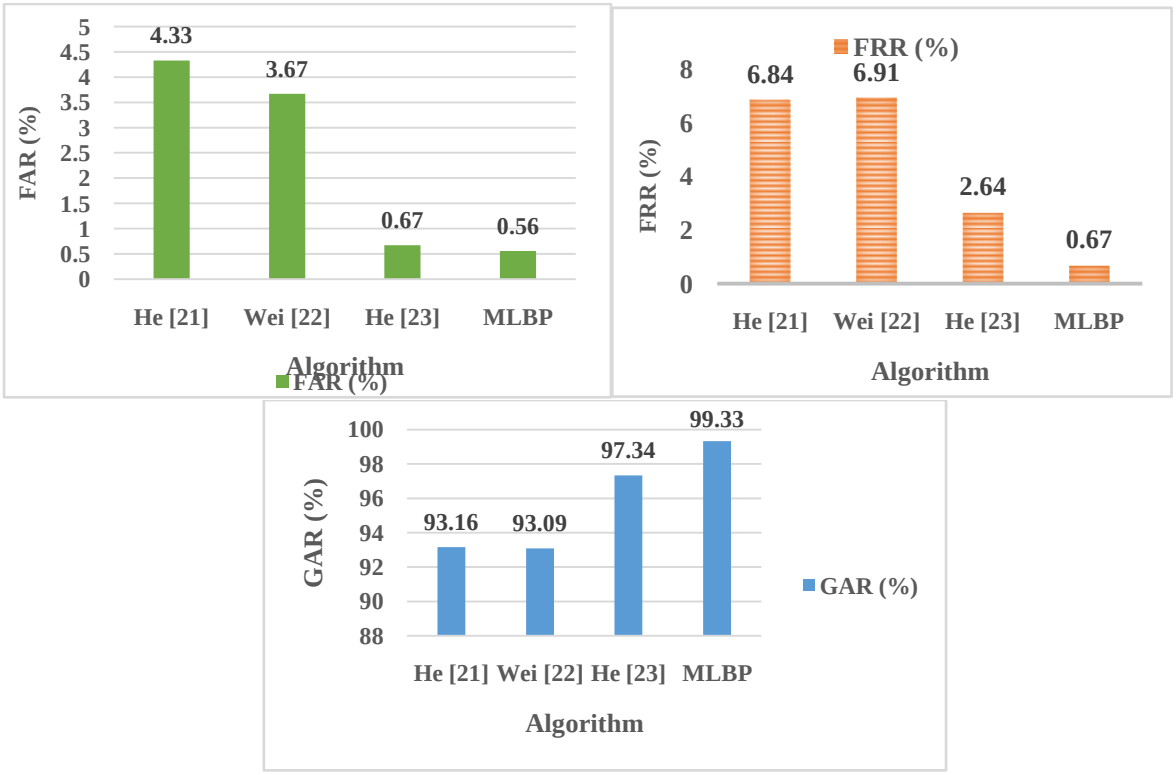

Fig. 9: The overall performance of the learned classifiers via (He, Z., *et al.*, 2009; Wei, Z., *et al.*, 2008; He, X., *et al.*, 2007) and the proposed method (a) False acceptance rate (FAR), (b) False rejection rate (FRR), and (c) Genuine acceptance rate (GAR=1-FRR).

Table III: Performance Analysis of existing and proposed spoof detection.

Performance Analysis	Existing Spoof Detection	Proposed Spoof Detection
Sensitivity	95%	100%
Specificity	99.83%	100%
Correct classification	95%	100%

Table III analysis the performance of existing and proposed spoof detection from the derivation of a confusion matrix such as true positive rate, true negative rate, and correct classification.ROC plot is a threshold independent measure which plots the sensitivity in x-axis and specificity in y-axis as shown in fig. 8.

The output of Gabor wavelet and MLBP algorithms:

Gabor filters are used for edge extraction that smears the edge information. It captures the entire frequency spectrum during the feature extraction method. The magnitude co-efficient of the Gabor filter output is used as a feature to identify boundaries for iris images. The LBP outlines the local gray-level structure and takes a local neighborhood around each pixel. It is defined for 3*3 neighborhoodsand the extended LBP is evaluated with the center value of a pixel by thresholdings equally spaced points on a circle along with *r* as radius. Thus, it provides the output for MLBP algorithm in as in fig.10 (a) and (b).Gabor wavelets and local binary patterns altogether provides better performance.

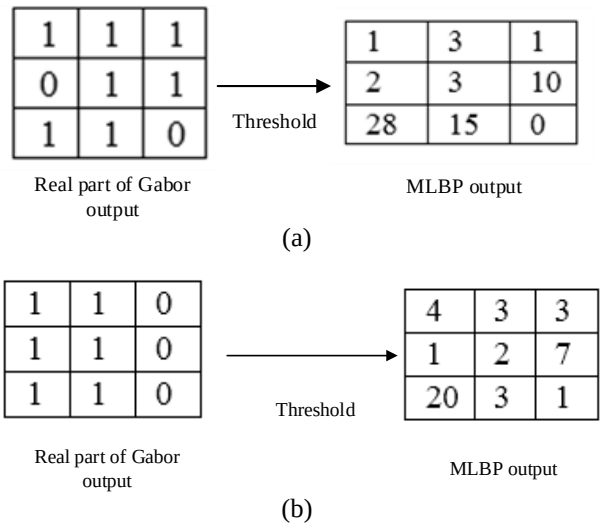

Fig. 10: The multi-scale LBP output (a) for left iris image, and (b) for right iris image.

Conclusion:

In this paper, the robustness of iris recognition system with spoofing attack is explained. The dataset images are enhanced using image enhancement techniques. It is later subjected to multi-scale local binary pattern (MLBP) algorithm for extracting the efficient features to represent the images. This algorithm is a combination of Gabor wavelet followed by local binary pattern description (LBP) where the magnitude coefficient from Gabor wavelets takes as its input. A spatial point pattern classifier is used to check the verification process. Both dataset iris images and synthetically spoofed iris images are evaluated by the algorithm in order to increase a genuine acceptance ratio (GAR).

REFERENCES

Akhtar, Z., *et al.*, 2011. "Spoof attacks on multimodal biometric systems," in *Int. Conf. Information and Network Technology*, pp: 46-51.

Al-khassaweneh, M., *et al.*, 2012. "A hybrid system of Iris and Fingerprint recognition for security applications," in *Open Systems (ICOS), 2012 IEEE Conference on*, pp: 1-4.

Bodade, R. and S. Talba, 2010. "'Novel approach of accurate iris localisation form high resolution eye images suitable for fake iris detection," *International journal of information technology and knowledge management*, 3(2): 685-690.

Bodade, R. and S. Talbar, 2011. "Fake Iris Detection: A Holistic Approach," *International Journal of Computer Applications*, 19(2).

Bonnen, K., *et al.*, 2013. "Component-based representation in automated face recognition,".

Connell, J., *et al.*, 2013. "Fake iris detection using structured light," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, pp: 8692-8696.

De Martino, J.M., *et al.*, 2012. "LBP-TOP based countermeasure against face spoofing attacks," in *International Workshop on Computer Vision With Local Binary Pattern Variants-ACCV*.

Galbally, J., *et al.*, 2012. "Iris liveness detection based on quality related features," in *Biometrics (ICB), 2012 5th IAPR International Conference on*, pp: 271-276.

George, A.M. and C. Anand Deva Durai, 2013. "A survey on prominent iris recognition systems," in *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*, pp: 191-195.

Godara, S. and R. Gupta, 2013. "Neural Networks for Iris Recognition: Comparisons between LVQ and Cascade Forward Back Propagation Neural network Models, Architectures and Algorithm," *Neural Networks*, 3(1).

Han, W.Y., *et al.*, 2014. "Iris Recognition based on Local Mean Decomposition," *Appl. Math*, 8(1L): 217-222.

He, X., *et al.*, 2007. "Statistical texture analysis-based approach for fake iris detection using support vector machines," in *Advances in Biometrics*, ed: Springer, pp: 540-546.

He, Z., *et al.*, 2009. "Efficient iris spoof detection via boosted local binary patterns," in *Advances in Biometrics*, ed: Springer, pp: 1080-1090.

Hughes, K. and K.W. Bowyer, 2013. "Detection of Contact-Lens-Based Iris Biometric Spoofs Using Stereo Imaging," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, pp: 1763-1772.

Kathikeyan, T. and B. Sabarigiri, 2012. "Countermeasures against IRIS spoofing and liveness detection using Electroencephalogram (EEG)," in *Computing, Communication and Applications (ICCCA), 2012 International Conference on*, pp: 1-5.

Moghadam, F.M., *et al.*, 2013. "A New Iris Detection Method based on Cascaded Neural Network," *Journal of Computer Sciences and Applications*, 1(5): 80-84.

O'Connor, B. and K. Roy, 2013."Facial Recognition using Modified Local Binary Pattern and Random Forest," *International Journal*.

Puhan, N., *et al.*, 2011. "A new iris liveness detection method against contact lens spoofing," in *Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on*, pp: 71-74.

Radu, P., *et al.*, 2013. "A Colour Iris Recognition System Employing Multiple Classifier Techniques," *Electronic Letters on Computer Vision and Image Analysis*, 12(2): 54-65.

Rathgeb, C., 2013. "Towards enhancing the security and accuracy of iris recognition systems," *Datenschutz und Datensicherheit-DuD*, 37(6): 367-370.

Robson Schwartz, W., *et al.*, 2011. "Face spoofing detection through partial least squares and low-level descriptors," in *Biometrics (IJCB), 2011 International Joint Conference on*, pp: 1-8.

Venugopalan, S. and M. Savvides, 2011. "How to generate spoofed irises from an iris code template," *Information Forensics and Security, IEEE Transactions on*, 6(2): 385-395.

Wei, Z., *et al.*, 2008. "Counterfeit iris detection based on texture analysis," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, pp: 1-4.