# An Iris-Based Authentication System to Prevent Iris Spoofing

Ajirtha.S [1], Anitha.S.M [2], Anusha.R.A [3], Jeni.P [4], Karthik.S [5]
[1, 2, 3, 4] Final Year Student, University College of Engineering, Nagercoil, Tamil Nadu, India.
[5] Teaching Fellow, University College of Engineering, Nagercoil, Tamil Nadu, India.

**Abstract – Human iris is considered as a reliable and accurate modality for biometric recognition due to its uniqueness. However, similar to other biometric modalities, iris recognition systems are also vulnerable to presentation attack (iris spoofing) that attempt to conceal or modify the identity. In real world application, an attacker may perform different kinds of attack to steal the legitimate user's unique iris information. An iris based authentication system, enhancing the security to prevent the iris spoofing. It uses two database that contains the iris code and user code. Iris code, which is the length between the pupil and the sclera. User code, which is the QR code act as the user's password generated by using MD5 algorithm. To check whether the user is an authenticated person, first the user's iris is needed to be scanned and then the corresponding QR code is generated form this iris information by applying the hash function. If both are matched with the already stored data in the database, the permission will be granted to the user otherwise the access will be denied.**

**Index Terms – Iris liveness detection, Iris code, QRcode, Authentication, LBP classifier.**

## 1. INTRODUCTION

Authentication is an essential step for accessing resources and services. One common biometric-based authentication approach is iris pattern recognition. In an iris based authentication system, iris images are captured from users, and features are extracted to be matched at a later stage for authentication. Iris is unique for each individual. It has distinct textures and patterns that can be used for authentication. Iris based authentication can overcome the limitations of traditional password based authentication systems that are vulnerable to brute force attack and presentation attacks. The literature shows a rise in the application of iris based authentication in areas such as immigration and border control and online banking.Recently, iris spoofing attacks have emerged as asignificant threat against traditional iris based authentication systems. For example, an attacker may obtain a printed copy of the iris of a victim and display the image in front of an authentication system to gain unauthorized access (known as presentation attack). Such attack can be performed by displaying static eye images on mobile devices or IPad (known as screen attack) . There are approaches to prevent media display attacks. However, most of them rely on static features of the iris. A number of liveness detection approaches are available, which rely on high quality camera to analyze the image. There is a need for an additional layer of defense beside the liveness detection of iris objects from images. To address this need, in this paper we propose a framework for iris code generation by considering the changes to the area between the pupil and the sclera due to light density. Our approach relies on capturing the iris area image using near infrared light. We use LBP classifier to capture the area between the pupil and the cornea. The image of the captured area is stored in the database. The approach also generates QR code from the iris image. This QR code is used as a password. During authentication, if the iris image is matched, the user is required to provide the QR code to be authenticated. The combination of the QR code and the iris image make hacking harder. We implemented a prototype of the proposed approach using Matlab.

## 2. RELATED WORK

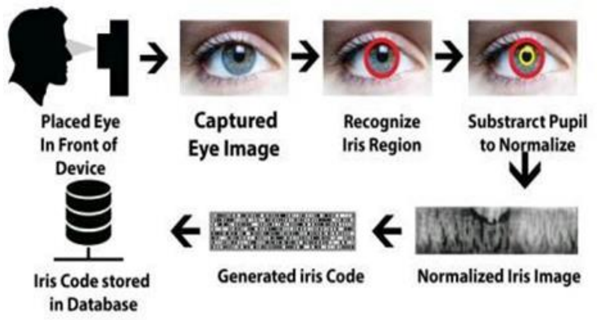
In this section we describe related work and the approaches used to detect attacks on iris-based authentication systems. Pacut et al. [4] detect liveness of iris by analyzing the frequency spectrum as it reveals signatures within an image. Ratha et al. [5]split images of biometric fingerprints known as shares. These shares are stored in different databases. During authentication, one of the shares acts as an ID while another share is retrieved from the central database to be matched with a known image. Andreas et al. [6] rely on PRNU which is the difference between the response of a sensor and the uniform response from light falling on camera sensor. This approach captures the noise level information (irrelevant data) from iris images. Given that a new iris image is required to authenticate, the PRNU fingerprints from stored images are compared with the given one. Puhan et al. [19] detect iris spoofing attacks using texture dissimilarity. As the illumination level is increased to an open eye, the pupil size decreases. Printed iris does not demonstrate such change of the pupil. High value of normalized Hamming distance between a captured image and known image results in warning of spoofed image. Adam et al. [9] detect live iris based on amplitude spectrum analysis. In this approach, a set of live iris images are analyzed to obtain the amplitude levels while performing Fourier transformation. A fake iris image has dissimilar amplitude levels compared to the real iris image. Karunya et al. [11] assess captured iris image quality to detect spoofing attacks. color, luminance level, quantity of information, sharpness, general artifacts, structural distortions, and natural appearance are qualities that can be used to differentiate between real images from fake images. Thavalengal [14] detects liveness of iris based on multi spectral information. This method exploits the acquisition workflow for iris biometrics on smartphones using a hybrid visible (RGB)/near infrared (NIR) sensor. These devices are able to capture both RGB and NIR images of the eye and iris region in synchronization. This multi-spectral information is mapped to a discrete feature space. The NIR image detects flashes in a printed paper and no image in case of a video shown for authentication. If a 3D live model is shown, an image shows „red-eye effect which could be used to detect iris liveness. Huang et al. [15] rely on pupil constriction to detect iris liveness detection. The ratio of iris and pupil diameters is used as one of the considerations during authentication. Liveness prediction is evaluated based Support Vector Machine (SVM) classifier. A database of fake irises, printed images, and plastic eye balls is built for training and testing of SVM classifier. As the intensity of light increases, the pupil size decreases. The SVM can differentiate the real iris from a fake one. Kanematsu et al. [16] detect liveness based on variation of light brightness. This approach relies on the variation of iris patterns induced by a pupillary reflex for various levels of brightness. Similar to anti-virus programs that include a database of viruses, this approach relies on a database of fake irises to detect fake authentication attempts. Mhatre et al. [17] extract features and encrypt with Bio- Chaotic Algorithm. The input image is divided into parts to apply the Bio-Chaotic algorithm. An image is segmented and randomly one block of the image is selected to hide a secret message using a unique key. The entire image is encrypted. The graph of both original and encrypted iris image is generated so that one can see the difference after the encryption process. Only authorized user knows about the selected block selected and the key so an attacker fails to fraud. The decryption process is the reverse of encryption process. With the increase in use of biometrics for human identification, control shifts to identifying the factors that affect the performance of biometric authentication systems. Bio-metric authentication systems use behavioural or physical characteristics to authenticate a user. These systems have become more reliable sources of authentication as compared to the traditional means like passwords or hardware tokens such as smart cards. Reliability of biometric authentication systems lies in the fact that, unlike passwords and smart cards, biometrics cannot easily be forged, shared, compromised or forgotten. Biometric is considered to be highly unique among all human population. Genetically, same identities including twins and irises of left and right eye of the same person represent different iris patterns. Another important property of biometric is its stability. Recognition involves either verification or identification. Verification is one to one comparison where claim of an identity is verified. Identification is one to many comparison where an identity is watched against an entire database. An iris recognition system captures human eye image using a near infrared iris sensor which passes through three steps to be transformed into an iris template. It is created for their iris region. It contains the unique information of the iris and the information is stored in the database.

## 3. PROPOSED MODELLING

At the heart of our proposed approach, we generate iris code using the classifiers. The iris code is generated by enrolling real world users and the code is saved in a database. The code is generated again from a new image during authentication for matching. In this section, we describe the system design in detail.

### 3.1. Iris code and QR code generation:

Iris is the situated colored ring of muscle around the eye pupil which controls the diameter and the size of the pupil and the amount of light that could reach the retina. Using an iris scanner (a camera for scanning iris), a person‟‟s eye is scanned. The data ofthe iris is unique to each person. The camera takes a picture of the eye region in both normal RGB light and infrared light. Infrared lights have longer wavelengths than normal red lights and are not visible to the human eye. The infrared light helps during the recognition phase to reveal unique features for dark colored eyes which cannot be detected by normal light.


Placed Eye In Front of Device
Captured Eye Image
Recognize Iris Region
Substrarct Pupil to Normalize
Normalized Iris Image
Generated iris Code
Iris Code stored in Database

We implemented a prototype in OpenCV platform that detects iris region with pupil (using classifiers). Next, we identify the pupil area in the center of iris region and normalize the iris area image in black and white mode. We then subtract the iris area from the pupil area (which reflects the area based on papillary response for current illumination level). An iris code is generated using the papillary response area, which is 512-digit number. The iris code is then stored in the database for a new user during enrollment. It is checked for matching during the authentication process. For matching, we rely on Hamming distance between the two images. Hamming distance computes the number of dissimilar bits among two codes assuming the code length for both images is the same.

For example, if image A=1001, and image B=1100, the H(A,B) = 2 (as the second and fourth bits of A and B are dissimilar). One limitation of storing only iris code and relying on it for authentication is that the approach is vulnerable to presentation attacks. If an attacker can obtain the printout of the iris image under correct illumination level, then the attacker would obtain access to the system. To prevent this, we generate a QR code to act as a password. Unlike, traditional text-based password, the QR code is an image representation, it is read by a reader and converted to a bit string to be compared with known strings. We now discuss our proposed approach of generating the QR code. From the iris image, we separate the Red, Green, and Blue color planes. The color information is presented as matrix (*Mat* object in OpenCV.

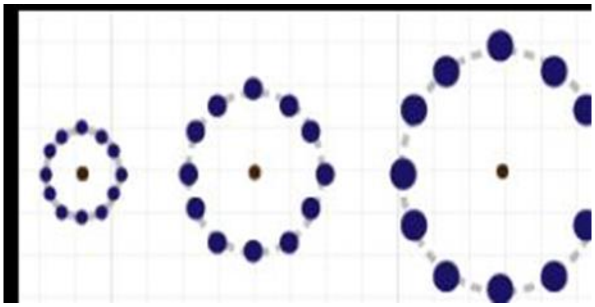
We then generate Hash value by combining hashes for each of the planes as follows:

H = H(R) XOR H(G) XOR H(B)

Here, H(R) is the hash generated from the Red color plane matrix, and XOR the Boolean operator. The length of the hash is 128 bits (16 bytes). We apply Message Digest (MD5) hash algorithm to generate hashes out of matrix information. We then generate a micro QR code using the hash information. A micro QR code can have 25 alphanumeric characters (for error correction level M). The provided length is sufficient to our goal.

Classifiers for Iris Recognition:

In this section we discuss classifier that we use to detect iris patterns from images. The classifiers is Local Binary Pattern. Local Binary Patterns (LBP) are visual descriptors for texture classification. It combines Histogram of Oriented Gradients (HOG) descriptor used for detection and recognition of objects. Figure explains three neighborhoods to define texture and calculate local binary pattern. Steps for LBP cascade classifier feature calculation is given below:



1. Divide the examined window into cells (e.g. 16x16 pixels for each cell).
2. Compare the pixel value of the center with each of the 8 neighboring pixels in a cell (on its left-top, left-middle, left-bottom, right-top, etc.). Follow the pixels along a circle, i.e. clockwise or counterclockwise.
3. If the center pixel value is greater than the neighbor's value, consider "0". Otherwise, "1". This gives an 8-digit binary number.
4. Determine the histogram of the frequency of each "number" over the cell. This histogram can be seen as a 256-dimensional feature vector. Occurring (i.e., each combination of which pixels are smaller and which are greater than the center).
5. Concatenate (normalize) histograms of all cells. This gives a feature vector for the entire window.

Similar to Haar-Cascade classifier, we trained LBP classifiers with a set of negative and positive image samples. The feature vectors used were from OpenCV platform.

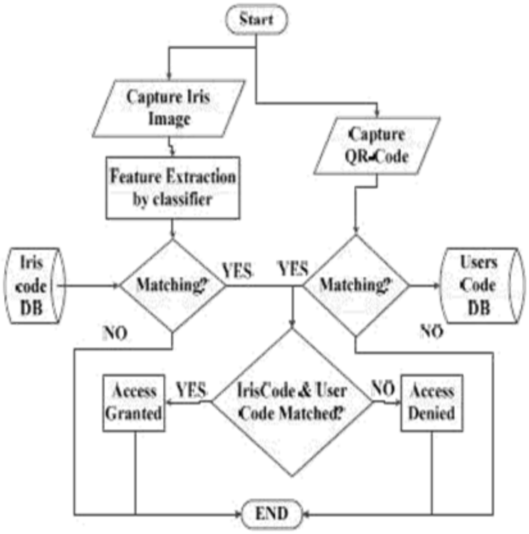
Algorithm LBP

```
Function LBP_Im=LBP(Input_Im,R)
Input image LBP image
If size(Input_Im,3)==3
    Arrayimageconversion□Input_Im=
     rgb2Gray(Input_Im)
End
Size of the LBP label L=2*R
C=round(„-„„2)
Input_Im=uint8(Input_Im)
Find Row,column values
row_max=size(Input_Im,1)-L+1
col_max=size(Input_Im,1)-L+1
calculate LBP pattern□condition
for i=1:row_max
    for j=1:col_max
        A=Input_Im(i:i+L-1,j:j+L-l)
        A=A+1-A(L,L)
        A(A>0)=1
        LBP_Im(i,j)=A(L,L)+A(L,L)*2+
         A(L,L)*4+A(L,1)*8+A(L,1)*16+
         A(L,1)*32+A(1,L)*64+A(1,L)*128
end
```

## 3.2 Authentication process:

In the proposed approach, there are two databases for each user; one for iris code and another for assigned user code. Iris code is user‟s iris information and the user code is QR code that is generated using the user‟s iris information.

First, a camera is used to take images of the iris. Features are extracted from captured iris images and liveness is calculated. Now, the QR code is generated. The user code and iris code is stored in the database. During authentication, the iris image is captured using a camera and the features are extracted. Then the user provides the QR code (as a password). If there is a match between the iris of the user and the database of iris code, and user code matches the provided QR code, then the user is granted access otherwise denied.



Principal Component Analysis:

Principal Component Analysis (PCA) is a measurable system that uses an orthogonal change to change over an arrangement of perceptions of conceivably associated factors into an arrangement of estimations of straightly uncorrelated factors called key parts. The quantity of unmistakable main part is equivalent to the littler of the quantity of unique factors or the quantity of perceptions less one. This change is characterized in such a way that the primary key part has the biggest conceivable fluctuation and each succeeding segment in turn has the most astounding change conceivable under the limitation that it is orthogonal to the procedure segments. The subsequent vectors are an uncorrelated orthogonal premise set. PCA delicate to the relative scaling of the first factors.

It is basic technique for removing applicable data from befuddling informational collections. PCA gives a compelling intends to lessen a mind boggling informational index to bring down measurement. In PCA, set of orthogonal premise vectors is produced from an arrangement of test pictures is lessened to the detriment of little loss of data. Question pictures are anticipated by a similar predominant vectors and coordinating to the example pictures is finished by looking at the coefficients coming about out of projection.

- Begin with a picture informational index of size m*n.
- Discover the mean of the picture.
- subtract the mean from every pixel of the picture and register the covariance framework.
- Discover the eigen esteems and eigen vectors. Duplicating the first dataset by an eigen vector turns the reflectance vector for a pixel to get the important part.
- Iris recognition system using PCA involves two phases,
    - Training Phase
    - Recognition Phase

## 4. RESULTS AND DISCUSSIONS

Using the latest technology like iris scanning and QR code, we could implement a cost effective and reliable security system. In order to implement the recognition scheme, we extract LBP features from our iris image which in turn are further classified using principle component analysis. We also propose a secondary scheme that includes a QR code which can strengthen the security of our system.

- Performance of Local Binary Pattern is measured using accuracy of the image.

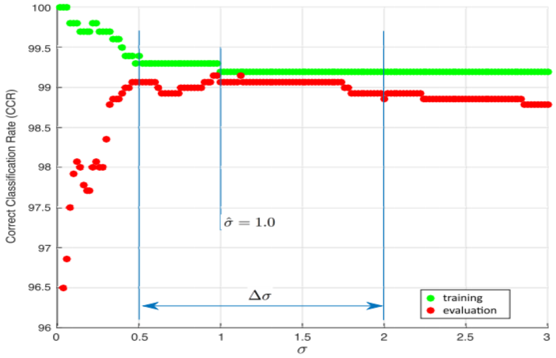
$$\sigma = \sqrt{\varepsilon\,(x-\overline{x})^{2}}\;/n$$

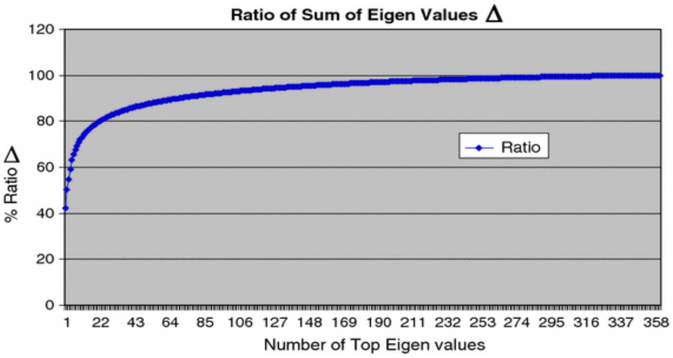
- Performance of Principal Component Analysis based on producing accurate result.

Means = mean(x)

Covariance = cov(mean,m,1)

Eig = eig(Covariance)





## 5. CONCLUSION

In our system, the authentication of the user is checked using PCA algorithm. Initially, using LBP classifier the full dataset is processed and get the LBP image of structured component and then we generate the histogram for this structured component and stored to the database. Then using Principal Component Analysis particular user's iris image is processed and matched with the processed image that is stored in the database. If the data is matched then check the QR code. Both are matched, the access is granted for the user otherwise the access is denied.

## REFERENCES

[1] M. Boatwright, & X. Luo, "What do we know about biometrics authentication?" In Proceedings of the 4th Annual Conference on Information security curriculum development, September 2007.

[2] S. Sheela & P. Vijaya, "Iris recognition methods-survey," International Journal of Computer Applications, 3(5), pp. 19-25, 2010.

[3] R. Raghavendra, Kiran B Raja, Christoph Busch, "Presentation Attack Detection for Face Recognition using Light Field Camera," IEEE Transactions on Image Processing (TIP), 24(3), March 2015, pp.1060,1075.

[4] A., Pacut, A. Czajka, "Aliveness detection for iris biometrics," In Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology, October 2006, pp. 122-129.

[5] N. K. Ratha, J. Connell, & R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM systems Journal, 40(3), 2001, pp. 614-634.

[6] Andres Uhl, Yevonne Holler, "Iris sensor Authentication using Camera PRNU Fingerprints," Proc. of 5th IARP International Conference on Biometric (ICB*)*, 2012.

[7] C. Li, W. Zhou, "Iris recognition based on a novel variation of local binary pattern," The Visual Computer, October 2015, Volume 31, Issue 10, pp 1419–1429

[8] J. Roberts, Eye-Scanning Rolls Out at Banks Across U.S., June 2016, Accessed from http://fortune.com/2016/06/29/eye-scanning-banks/

[9] A. Czajka, "Database of iris printouts and its application: Development of liveness detection method for iris recognition," In 18th International Conference on Methods and Models in Automation and Robotics (MMAR*)*, 2013, pp. 28-33.

[10] J. Daugman, Iris Recognition at Airports and Border Crossings, Accesed http://www.cl.cam.ac.uk/~jgd1000/Iris_Recognition_at_Airports_and_Border-Crossings.pdf

[11] R.Karunya, & S. Kumaresan, "A study of liveness detection in fingerprint and iris recognition systems using image quality assessment.," Proc. of International Conference on Advanced Computing and Communication Systems, 2015, pp. 1-5.

[12] Eyelock, https://www.eyelock.com/

[13] Iridis, http://www.irisid.com/productssolutions/technology-2/iris recognition technology

[14] S. Thavalengal, T. Nedelcu, P. Bigioi, & P. Corcoran, "Iris liveness detection for next generation smartphones," IEEE Transactions on Consumer, Vol. 62, Issue 2, 2016, pp. 95-102.

[15] X. Huang, C. Ti, Q. Hou, A. Tokuta, & R. Yang, "An experimental study of pupil constriction for liveness detection," Proc. of IEEE Workshop on Applications of Computer Vision (WACV*)*, 2013, pp. 252- 258.

[16] M. Kanematsu, H. Takano, & K. Nakamura, "Highly reliable liveness detection method for iris recognition," Proc. of 46th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE*)*, 2007, pp. 361-364.