# AN EXPERIMENTAL REVIEW OF AUTHENTICATION USING IRIS

Nitu Chauhan*

Mrinal Manjari*

## ABSTRACT

*Iris as a biometric is very rich in terms of information content. It provides one of the most secure methods of authentication and identification thanks to its unique characteristics. Once the image of the iris has been captured using a standard camera, the authentication process, involving comparing the current subject's iris with the stored version, is one of the most accurate with very low false acceptance and rejection rates.*

*This work proposes two alternative algorithms for iris recognition. The first involves the arrangement of spatial patterns of the iris image, and is detected by application of canny edge detector. The second algorithm describes the use of an Iris Signature which employs discrete wavelet transform for the same. The results of authentication for the two algorithms have been obtained and compared. Further, noise caused in the image due to variant illumination and eyelashes were also removed successfully. In the later phase of the paper, we extracted iris as an ellipse instead of a circle, and concluded that this approach enhanced the accuracy of authentication considerably.*

***Keywords****: Iris, Image, Ellipse, Recognition, Significance.*

*Lecturer, ECE Department, Echelon Institute of Technology, Faridabad.

## INTRODUCTION

In today's information technology world, security for systems is becoming more and more important. The number of systems that have been compromised is ever increasing and authentication plays a major role as a first line of defence against intruders. The three main types of authentication are something you know (such as a password), something you have (such as a card or token), and something you are (biometric). Passwords are notorious for being weak and easily crackable due to human nature and our tendency to make passwords easy to remember or writing them down somewhere easily accessible. Cards and tokens can be presented by anyone and although the token or card is recognizable, there is no way of knowing if the person presenting the card is the actual owner. Biometrics, on the other hand, provides a secure method of authentication and identification, as they are difficult to replicate and steal.

Biometric identification utilizes physiological and behavioral characteristics to authenticate a person's identity. Some common physical characteristics that may be used for identification include fingerprints, palm prints, hand geometry, retinal patterns and iris patterns. Behavioral characteristics include signature, voice pattern and keystroke dynamics. A biometric system works by capturing and storing the biometric information and then comparing the scanned biometric with what is stored in the repository.

Out of all the various physical characteristics available, irises are one of the more accurate physiological characteristics that can be used.

**The Iris**

The iris has many features that can be used to distinguish one iris from another. One of the primary visible characteristic is the trabecular meshwork, a tissue which gives the appearance of dividing the iris in a radial fashion that is permanently formed by the eighth month of gestation. During the development of the iris, there is no genetic influence on it, a process known as chaotic morphogenesis that occurs during the seventh month of gestation, which means that even identical twins have differing irises. The iris has in excess of 266 degrees of freedom, i.e. the number of variations in the iris that allow one iris to be distinguished from another. The fact that the iris is protected behind the eyelid, cornea and aqueous humor means that, unlike other biometrics such as fingerprints, the likelihood of damage and/or abrasion is minimal. The iris is also not subject to the effects of ageing which means it remains in a stable form from about the age of one until death. The use of glasses or contact

lenses (colored or clear) has little effect on the representation of the iris and hence does not interfere with the recognition technology.

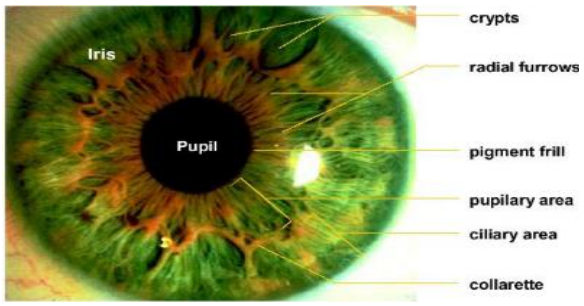



**Figure 1: The structure of the human eye**

**Advantages of Iris Recognition**

The physiological properties of irises are major advantages for using them as a method of authentication. As discussed earlier, the morphogenesis of the iris that occurs during the seventh month of gestation results in the uniqueness of the iris even between multi-birth children. These patterns remain stable throughout life and are protected by the body's own mechanisms. This randomness in irises makes them very difficult to forge and hence imitate the actual person.

In addition to the physiological benefits, iris-scanning technology is not very intrusive as there is no direct contact between the subject and the camera technology. It is non-invasive, as it does not use any laser technology, just simple video technology. The camera does not record an image unless the user actually engages it. It poses no difficulty in enrolling people that wear glasses or contact lenses. The accurateness of the scanning technology is a major benefit with error rates being very low, hence resulting in a highly reliable system for authentication.

Scalability and speed of the technology are a major advantage. The technology is designed to be used with large-scale applications such as with ATMs. The speed of the database iris records are stored in is very important. Users do not like spending a lot of time being authenticated and the ability of the system to scan and compare the iris within a matter of minutes is a major benefit [1].

**Disadvantages of Iris Recognition**

As with any technology there are challenges with iris recognition. The iris is a very small organ to scan from a distance. It is a moving target and can be obscured by objects such as the eyelid and eyelashes. Subjects who are blind or have cataracts can also pose a challenge to iris recognition, as there is difficulty in reading the iris.

The camera used in the process needs to have the correct amount of illumination. Without this, it is very difficult to capture an accurate image of the iris. Along with illumination comes the problem with reflective surfaces within the range of the camera as well as any unusual lighting that may occur. All of these impact the ability of the camera to capture an accurate image. The system linked with the camera is currently only capturing images in a monochrome format. This results in problems with the limitations of grayscale making it difficult to distinguish the darker iris colorations from the pupil [1, 2].

Although there is minimal intrusiveness with iris recognition, there is still the need for cooperation from subjects to enrol in the system and undergo subsequent authentication scans. Enrolling a non-cooperative subject would prove very difficult indeed. Inadequate training of users at the initial enrolment period will cause problems both at the initial enrolment time and subsequent authentications. Frustrated users will not help make the system any easier to use and will not be accepted by users as a convenient authentication method. Communication with users plays a major part in introducing such a system successfully.

As with all authentication methods it's important to remember to have a backup plan. Normal day-to-day problems such as system failures, power failures, network problems, and software problems can all contribute to rendering a biometric system unusable. Once users get accustomed to such a system it is unlikely that they will remember to bring their other forms of identification with them to the office. System administrators also have the additional pressure of ensuring the system that stores the iris record database is properly secured to prevent tampering with the data stored.

**Applications of Iris Recognition**

The most obvious use of iris recognition technology is within the computing environment. There is a lot of valuable data stored on a company's network and being able to access the network with a username and password is the most common method of authentication today. If a username and password is stolen then this gives the thief all of that person's access privileges and this can be detrimental to a company in today's competitive environment. Implementing an iris recognition system to authenticate users on the network means that there are no passwords to steal and no tokens to lose. Users are only able to access the systems they have privileges to access and it's very difficult for someone to replicate an iris for authentication. The technology can not only be used for securing log on but also in areas such as file and directory access, web site access and key access for file encryption and decryption. In a network environment, a system may be configured to compare the live

template to the stored template and if a match is found then the user's access privileges are passed back to the client. In other implementations, after a match is found, the server returns a username and password to the client, which then transmits this information to the network server to allow access to the systems the user has privileges to. Enterprise applications are also being worked on in the areas of e-commerce, healthcare applications for medical records protection, insurance and brokerage transactions [1,8].

Another area iris recognition is useful with is physical security to data centres or computer rooms. Mounting a scanner by the access door and authenticating people via their iris is a good method of ensuring only those whose templates are in the database for computer room access are actually allowed in. This helps to alleviate problems associated with swipe card access where some systems have to be manually programmed with specific card numbers and robust processes need to be in place to ensure access lists are regularly reviewed. Swipe cards are also easily lost, stolen or borrowed.

Iris recognition is also being utilized or considered in other areas of daily life. ATMs are a major area where iris recognition is being trialled. The use of this technology with ATMs means that customers can discard their plastic cards and PINs thus eliminating the possibility of having cards and/or PINs stolen or lost. The banking industry is also involved in looking at implementing the technology in over the counter transactions with customers. This would reduce the requirement for customers to produce identification, bank books, account numbers etc and would result in faster transaction times that leave the bank teller with more time to concentrate on the level of service provided to the customer [1,7].

Iris recognition is being considered in areas where there is a need for large throughput and queuing. For example border clearance, ticket less air travel, transportation and airport security. Airport security has seen a huge increase in focus in this regard. The aim behind this is to speed up processing of passengers and to detect illegal immigrants into a country. The concept is that passengers will have one of their irises stored in a database. When arriving at the airport, instead of presenting their passport, they proceed to a kiosk where their iris will be scanned by a camera and matched with the record stored in the database. Once a match is confirmed a barrier will open and the passenger is able to proceed as normal.

## IRIS RECOGNITION

### Iris Image Acquisition

It is to capture a sequence of iris images from the subject using a specifically designed sensor. Since the iris is fairly small (its diameter is about 1 cm) and exhibits more abundant

texture features under infrared lighting, capturing iris images of high quality is one of the major challenges for practical applications. It is of prime importance to have adequate hardware set-up to capture iris image with sufficient precision. For our purpose, we have taken our database from the site: http://phoenix.inf.upol.cz/iris/ [9].

A sample from the database is shown:

**Figure 2: Sample of iris**

**Pre-Processing (Noise Removal)**

In case of iris recognition, the database images have inherent noise such as eyelashes and variant illumination.

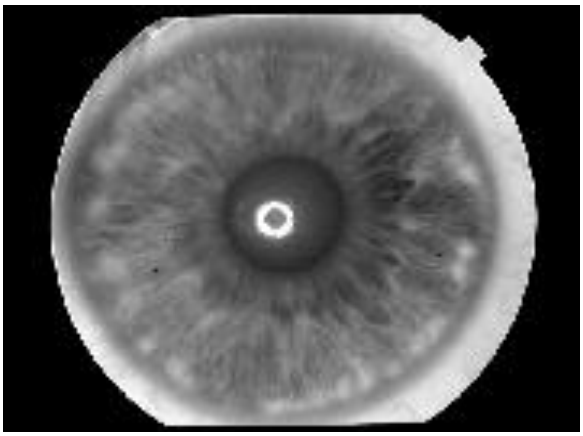
Variant illumination can be taken care by simple image processing methods such as Histogram Equalization and Adaptive Quotient Thresholding.

For eyelashes, it can be detected and the relate pixels labelled as noise pixels. These pixels are rendered redundant using Iris Binarization[11,3].

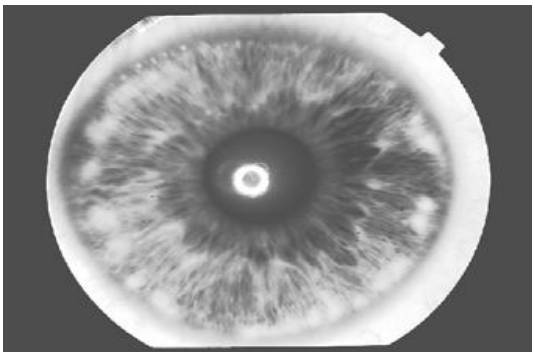
**Histogram Equalization**

This method usually increases the global contrast of many images, especially when the usable data of the image is represented by close contrast values. Through this adjustment, the intensities can be better distributed on the histogram. This allows for areas of lower local contrast to gain a higher contrast without affecting the global contrast. Histogram equalization accomplishes this by effectively spreading out the most frequent intensity values as shown in Figure 3 [10, 6].

**Results:**



**Before**



**After**

**Figure 3: Images before and after Histogram Equalization**

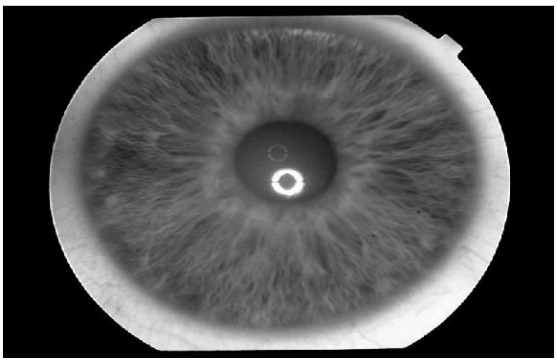
**Adaptive Quotient Thresholding**

The adaptive method computes several histograms, each corresponding to a distinct section of the image, and uses them to redistribute the lightness values of the image. Ordinary histogram equalization simply uses a single histogram for an entire image.

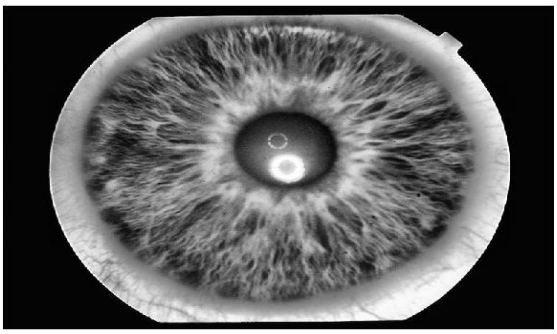
The quotient thresholding partitions an image in a database into foreground and background such that a ratio between the foreground and background of all images in the database are maintained [10].

Consequently, adaptive histogram equalization is considered an image enhancement technique capable of improving an image's local contrast, bringing out more detail in the image (Figure 4).

**Results:**



**Before**



**After**

**Figure 4: Images before and after Adaptive Quotient Thresholding**

**Iris Binarization**

Iris Binarization is a method to remove the noise pixels, which are infact effect of eyelashes, from the image before preceding further to implement the localization algorithm. This ensures increase in the efficiency of the verification [18].

The grayscale image is transformed into a binary image by thresholding. That is, all pixels having intensity greater than the threshold are made black, and similarly all those with intensity lower than the threshold are made white. The threshold used is in direct relation with the average intensity of the image. The coefficient that we have used is 0.52.

**Significance of Binarization:**

The significant advantage that Iris Binarization has is that it eliminates the noise added by eyelashes. It is strikingly efficient in encountering the noise caused due to the reflection of eyelashes on the eye, while taking the image. These reflections may or may not be present in different sets of images. This very fact causes greater chances of error in detection. Thus, it is very vital to remove the effect of these reflections.

Figure 5 shows two images of the same eye of the same person. As is evident from the images, the first image hardly has any eyelash reflections, while the same is reasonably visible in the second one.

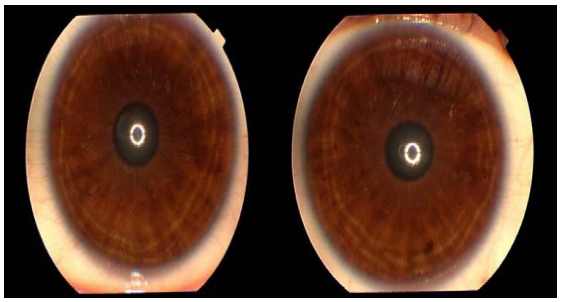
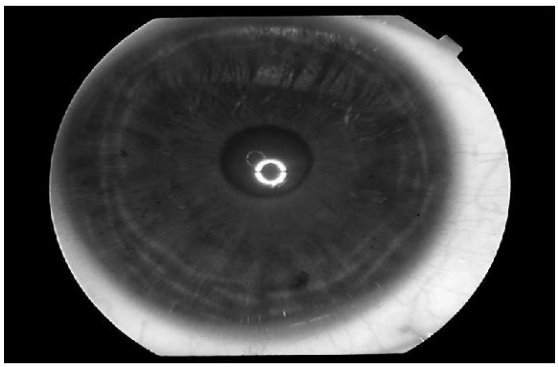


**Figure 5: Images without and with reflection of eyelashes**

**Results:**



**Before**

**After**

**Figure 6: Images before and after Iris Binarization**

As we can see in Figure 6, the noise has been significantly captured in the pixels that are black in the binarized image. Specifically, in our area of interest that is the iris region. Being aware of the outer radius of the circular iris, we come to know about the noise pixels within the boundary. These pixels are rendered useless, and their contribution is not taken into account in the pattern recognition algorithms.

## ELLIPTICAL DETECTION

The eye is assumed to cover a significant portion of the image acquired by a standard video camera. The system must be robust to occlusion (e.g. eyelids), skin and eye shape variations, image quality, and perform reliably in unstructured, general illumination conditions. Gaze and iris position within the image are unconstrained. The primary target is the determination of the iris centre with an accuracy of 5 pixels in a 360x280 image [8].

Figure 07 shows eye images with moderate eye occlusions and moreover with the subject mostly looking directly into the camera. These images are low-difficulty images and the reason for this is that the portion of the eye that is of interest to us, that is the iris, is circular. The above mentioned techniques can be easily used in these images.

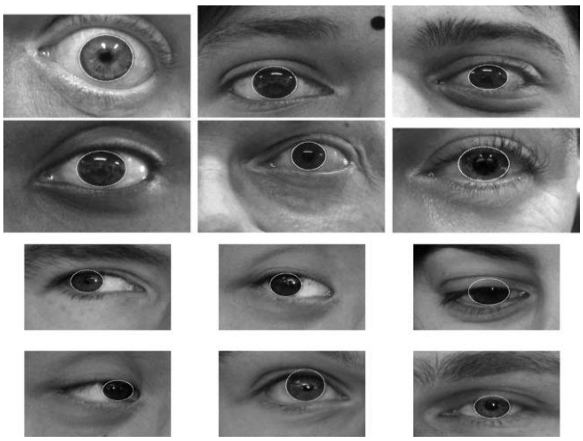


**Figure 07: Examples of low-difficulty images [15]**

However, Figure 08 shows a set of images have a heavily occluded iris, and the image quality is also low in aspects of blur, motion etc, and more importantly the eye is looking elsewhere in most of the images. These images thus form challenging images and considering the iris as a circle becomes unjustified. Thus, elliptical detection is essential in these situations.

Figure 8: Examples of detection for Challenging images, including heavily occluded Iris, lower Image Quality (e.g. blur, motion)

## EXPERIMENTAL RESULTS

The experimental results of iris recognition are shown and compared using two standard error rates False Acceptance Rate and False Acceptance Rate.

- False Accept Rate or False Match Rate (FAR or FMR) – the probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percent of invalid matches.
- False Reject Rate or False Non-Match Rate (FRR or FNMR) – the probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percent of valid inputs being rejected.
- Genuine Acceptance Rate (GAR) = 100- FRR

In our work, we have used a database comprising of images of 50 different individuals, each having three images for the left eye and three for the right. Each eye was considered as "of a different person"; i.e., each person has two identities, the one of the left eye and the one of the right one. That makes 100 "virtual" different users. The system was so trained to two images, that is to say that their information was extracted and stored separately initially. And, the remaining image is used as test sample which is fed to the system to draw results for authentication.

The results are tabulated in the chronological order of our approach. The results for the elliptical and circular approach as well as those for the three different feature matching techniques have been compared.

**Results in verification using Elliptical Detection**

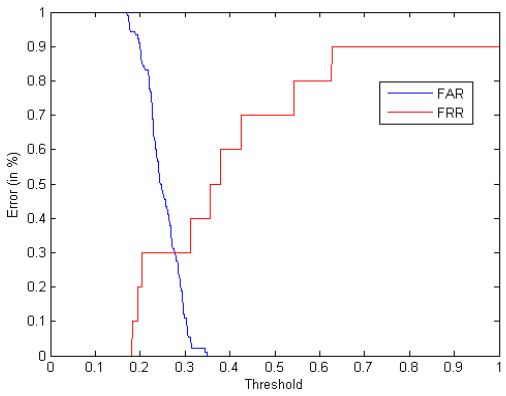



**Figure 09: Graph for results in verification using Iris Code**

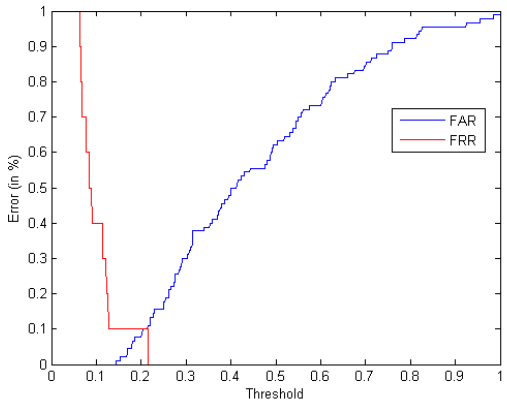



**Figure 10: Graph for results in verification using Iris Signature**

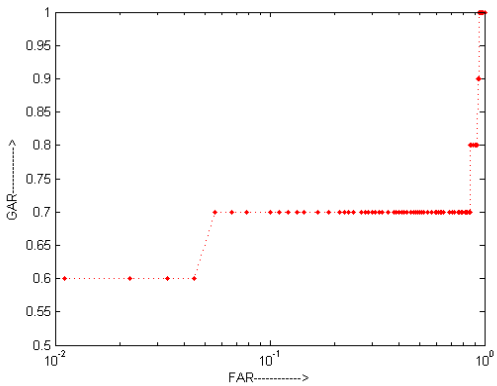



**Figure 11: ROC curve for verification using Iris Code**

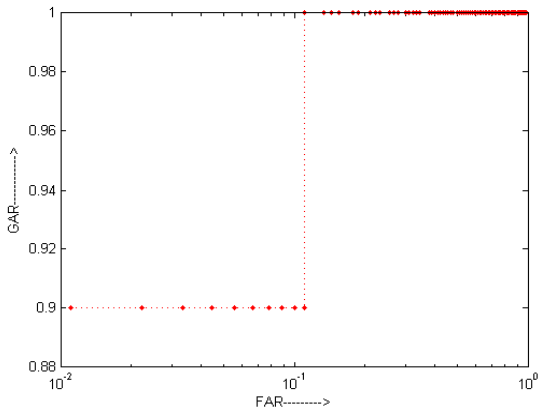



**Figure 12: ROC curve for verification using Iris Signature**

From Figures 09 and 10, it can be seen that for detection using iris codes, the area under the intersection region of the FAR and FRR curves is greater compared to the area in case of detection using iris signatures. The area of intersection refers to the region where both false acceptance and false rejection is occurring. And therefore a greater area will essentially imply

higher probability of error in the algorithm. Thus, the two curves indicate that the iris signature algorithm is a better approach than the iris code algorithm.

The same result can be observed from Figures 11 and 12, which show the ROC curves for the two algorithms. For iris codes, 100% recognition is achieved at a FAR of 1%, where as the same is achieved for iris signatures at a FAR of 0.111%. Also, the value of GAR at a FAR of 0.01% has been obtained to be 60% for iris codes and 90% for iris signatures. This also emphasizes that detection using iris signature is better than iris codes.

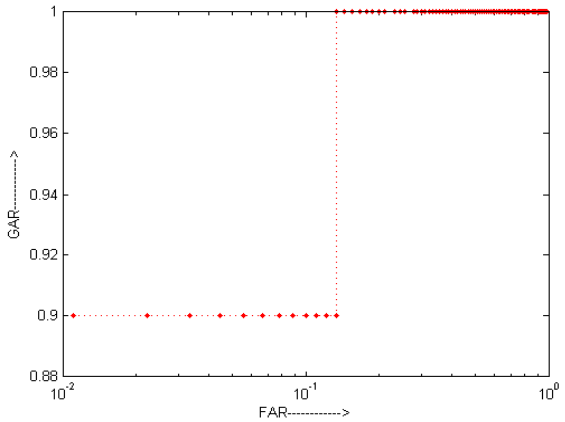



**Figure 13: ROC curve for circular detection using iris signatures**

Figure 13 shows the ROC curve for circular detection using iris signatures. Comparing this with Figure 32 which shows the curve for elliptical detection, it is observed that the value of FAR for which the curve jumps to 100% genuine acceptance is larger in case of circular detection. In case of circular detection, 100% GAR is obtained at 0.133% FAR, while for elliptical detection, it is obtained at 0.111% FAR. These results back our literature review and highlight the face that elliptical detection is an enhanced way of approaching the iris recognition problem than circular detection.

## CONCLUSION

In this paper, we have developed several iris recognition approaches and obtained several results to show the performance of each approach. Firstly, as a constituent of pre-processing, the inherent noise on the irises was removed using three different approaches: Histogram Equalization, Adaptive Quotient Thresholding and Iris Binarization. Thereafter, two different feature extraction algorithms have been used: one of them based on edge detection generating Iris Codes and the second based on discrete wavelet transform generating Iris Signatures. Also, these algorithms have been tested with three different pattern recognition methods, based on two distances: Euclidean and Hamming. Finally, the iris was mapped onto an ellipse instead of a circle.

Experimental results have shown that the best metric in all cases turns out to be Iris Signature. It obtains exceptionally good results for feature extraction algorithm. It is also important to emphasize that elliptical detection is a more preferred and enhanced outlook to the problem than circular detection as it takes into consideration the extra information that is left out in the latter. The same is evident from the results.

## POSSIBLE FUTURE EXTENSION

Presently, all our approaches deal with gray level patterns of iris. Possible future extensions include the use of vast color information stored in the iris images. The images used are taken from a standard database but to make possible augmentation in the algorithm and to test its performance, image acquisition hardware can be set up. Algorithms for noise removal can be used to eliminate noisy or spoofed images at the time of registration itself before going into iris recognition. Also, the work can be scaled to the next level by real time implementation of our algorithms which would require usage of high level programming languages and tools.

## REFERENCES

1. *Penny Khaw, "Iris Recognition Technology for Improved Authentication"*, SANS Security Essentials (GSEC) Practical Assignment, Version 1.3, 2002
2. L. Flom, A. Safir, "*Iris Recognition System*", U.S. Patent No. 4641349, U.S. Government Printing Office, Washington DC, 1987
3. John Daugman, "*High Confidence Recognition of Persons by IrisPatterns*", Security Technology, IEEE 35th International Carnahan Conference on, 2001, pp 254-263
4. W.W. Boles, Boashash, "*A Human Identification Technique Using Images of the Iris and Wavelet Transform*", IEEE Trans on Signal Processing, 1998, 46(4), pp 1185-1188
5. R.P.Wildes, J.C. Asmuth, et. al, "*A System for Automated Iris Recognition*", Proc of the Second IEEE Workshop on Application of Computer Vision, 1994, pp 121-128
6. S. Tsuji and F. Matsumoto, "*Detection of ellipses by a modified Hough transformation*," IEEE Transactions on Computers, pp. 777–781, 1978.
7. J. Canny "*A Computational Approach to Edge Detection*", IEEE Transaction on Pattern Analysis and Machine Intelligence Vol. 8, 679- 714,1986.
8. Alex Yong Sang Chia, Maylor K. H. Leung, "*Ellipse detection with Hough Transform in one dimensional parametric space",* ICIP, pp. 333–336, 2007
9. http://phoenix.inf.upol.cz

10. Ya-Ping Huang, Si-Wei Luo, En-Yi Chen, "*An Efficient IrisRecognition System*", Proceedings Of The First International Conference On Machine Learning And Cybernetics, Beijing, pp. 450-455, 4-5 November 2002
11. Wai-Kin Kong, David Zhang, "*Detecting eyelash and reflection foraccurate iris segmentation*", International Journal of Pattern Recognition, Vol. 17, pp. 1025-1034, 2003