IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 4, Issue 9, September 2016

Iris Recognition Security System

Priya.K.S[1], Anu Mol B[2], Vimal Raj V[3]

M.Tech Student, Dept of ECE, Cochin Institute of Science and Technology, Ernakulam, India[1]

Assistant Professor, Dept of ECE, Cochin Institute of Science and Technology, Ernakulam, India[2]

Head of the Department, Dept of ECE, Cochin Institute of Science and Technology, Ernakulam, India[3]

Abstract: Biometric systems have been researched intensively by many organization and institution. It overcomes the conventional security systems by identify "who you are". This paper discusses the current image based biometric systems. It first gives some information about why biometric is needed and what should people look for in biometric systems. Several popular image based biometric systems have been examined in this paper. The biometric systems included are face, fingerprint, hand geometry, hand vein, iris, retina and signature. Biometrics is associated with the use of unique physiological characteristics to identify an individual. The application associate with biometrics is security. Biometrics identifies an individual by measuring their physical and behavioural uniqueness or patterns, and comparing it to those on records. Iris recognition is the most unique and effective one which provides maximum security. When the case of wearing a contact lens comes then the fault mismatch chances are high. Even if the person is true the presence of contact lens makes a mismatch in the person's identification. For the proper identification there exist two sets of databases and they are IIIT-D database and ND-Contact Lens database. These two databases perform very well when compared with the other lens detection algorithms.

Keywords: Biometrics, Iris Recognition, Segmentation, Normalization.

I. INTRODUCTION

As technology advances and information and intellectual properties are wanted by many unauthorized personnel. As a result, many organizations have being searching ways for more secure authentication methods for user access. Furthermore, security has always been an important concern to many people. From Immigration and Naturalization Service (INS) to banks, industrial, military systems, and personal are typical fields where security is highly valued. It is soon realized by many, that traditional security and identification are not sufficient enough; people need to find a new authentic system in the face of new technological reality. Conventional security and identification systems are either knowledge based – like a social security number or a password, or token based – such as keys, ID cards. The conventional systems can be easily breached by others, ID cards and passwords can be lost, stolen or can be duplicated. In other words, it is not unique and not necessary represent the rightful user. Therefore, biometric systems are under intensive research for this particular reason. Humans recognize each other according to their various characteristics for ages. People recognize others by their face when they meet and by their voice during conversation. These are part of biometric identification used naturally by people in their daily life.

Biometrics relies on "something you are or you do", on one of any number of unique characteristics that you can't lose or forget. It is an identity verification of living, human individuals based on physiological and behavioural characteristics. In general, biometric system is not easily duplicated and unique to each individual. It is a step forwards from identify something you have and something you know, to something you are. Imagine how convenient it would be to activate the security alarm at your home with the touch of a finger, or to enter your home by just placing your hand on the door handle. How would you like to walk up to a nearby ATM which will scan your iris so you can withdraw money without even inserting a card or entering a PIN. You will basically be able to gain access to everything you are authorized to, by presenting yourself as your identity. This scenario might not be as far off as we might expect. In the near future, we may no longer use passwords and PIN numbers to authenticate ourselves. These methods have proven to be in secure and unsafe time and time again. Technology has introduced a much smarter solution to us: Biometrics. 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 crack able due to human nature and 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 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

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 4, Issue 9, September 2016

method of authentication and identification, as they are difficult to replicate and steal. If biometrics is used in conjunction with something you know, then this achieves what is known as two factor authentication. Biometric authentication will help in enhancing the security infrastructure against some of these threats. After all, physical characteristics are not something that can be lost, forgotten or passed from one person to another. An iris is the colored ring around the pupil. Its structure is determined during the fetal development of the eye and remains unchanged. On contrary the color of the iris can change as a result of the variable pigmentation in tissues.

The main role of the iris is to control the size of the pupil and adjust the amount of light which enters through the pupil into the eye interior. It is surrounded by the sclera, which is a white area of tissues and blood vessels, and it is covered by a transparent layer called cornea. The whole iris is visible only with eyes wide open, as eyelids and eyelashes usually occlude the lower and upper part of it. Iris features remain constant over an individual's lifetime and are not subject to changes produced by the effects of aging as other biometric features may be. For these reasons, the human iris is an ideal feature for highly accurate and efficient identification systems. The possibility of using the iris to distinguish individuals is over 100 years old, but the first patent for the automated iris biometric system was obtained by Flom and Safir in 1987 [6]. However the most important work in the field of the iris recognition was done by Daugman [5]. He introduced the first method for iris image segmentation, unique feature extraction and matching, which with slight modifications are used in today world and which are the reference models for other algorithm.

II. SECURITY SYSTEM

Biometric verification provides authentication of a person based on the unique characteristics possessed by the individual. Biometric systems have been developed based on various features, such as fingerprint, facial image, voice, hand geometry, handwriting, iris, and retina. Among them iris is considered as one of the most reliable and accurate candidates because, iris is unique for individuals and it is well protected and difficult to modify. A thorough understanding of Iris code is essential, because 100 million people have been enrolled in many biometric personal identification and template protection methods have been developed based on Iris code. Nowadays hackers can decompress the Iris code and they generate the iris template. Using this iris template hacker can break the high level security, and they easily misuse our information. This is over come by using randomized attributes. In this paper the color image is converted to gray scale, and is median filtered, and then the pupil is detected and normalized. During this process, threshold value is obtained and it is termed as Iris code. It is unique for every person. Among the biometric verification methods iris recognition is considered one of the most accurate and robust. Iris features can be easily extracted from eye images and they can be efficiently compared. However if the biometric reference template or set of biometric features are disclosed, the whole biometric system becomes useless for an individual, because the biometric information cannot be canceled or revoked as passwords. Therefore there is a need to perform iris features matching without revealing either the biometric data acquired during the verification process or the reference template from the database. Generally the biometric verification is based on the comparison between the features extracted from the input and the template. Due to the uniqueness of the biometric characteristics, the storage of the reference template is a key factor for the entire system security. Therefore it is essential to protect the template from possible attacks. One approach is to encrypt the template using a secret key before storing it. When a verification task is requested, the matcher decrypts the template and performs the comparison. Depend on application different biometric systems will be more suited than others. It is known that there is no one best biometric technology, where different applications require different biometrics. Some will be more reliable in exchange for cost and vice versa, see Fig.1

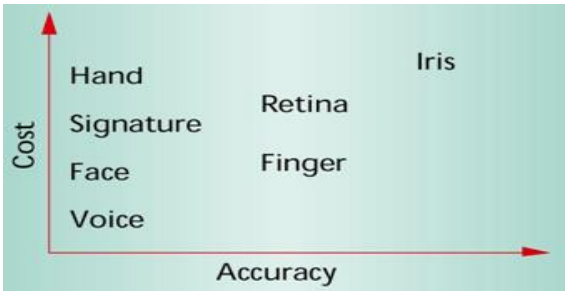

Fig.1. Cost Vs Accuracy

Proper design and implementation of the biometric system can indeed increase the overall security. Furthermore, multiple biometric fusions can be done to obtain a relative cheaper reliable solution. The image based biometric utilize many similar functions such as Gabor filters and wavelet transforms. Image based can be combined with other biometrics to give more reliable results such as liveliness (ECG biometric) or thermal imaging or Gait based biometric systems. The iris is highly protected and ideal for handling applications requiring management of large user groups, like voter ID management. The iris recognition techniques potentially prevent unauthorized access to ATMs, cellular phones, desktop PCs, workstations, buildings and computer networks. The accuracy of iris recognition systems is proven to be much higher compared to other types of biometric systems like fingerprint, handprint and voiceprint.

III. INPUT IMAGE AND DATABASES

The image of the iris can be captured using a standard camera using both visible and infrared light and may be

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 4, Issue 9, September 2016

either a manual or automated procedure. The camera can be positioned between three and a half inches and one meter to capture the image. In the manual procedure, the user needs to adjust the camera to get the iris in focus and needs to be within six to twelve inches of the camera. This process is much more manually intensive and requires proper user training to be successful. The automatic procedure uses a set of cameras that locate the face and iris automatically thus making this process much more user friendly. The iris recognition process begins with image acquisition a process which deals with the capturing of a high quality image of the iris while remaining non-invasive to the human operator. Image acquisition uses LED based point light sources in conjunction with a wide angle camera no more than 3 feet from the subject's eye.

By carefully positioning the light source below the operator, reflection of point source can be avoided in the imaged iris. The system makes use of light, which is visible to human eye. Infrared illumination can also be employed. This system requires the operator to self position his eye in front of the camera. It provides the operator with a live video feed back via beam splitter. This allows the operator to see what the camera is capturing and to adjust his position. Once a series of images of sufficient quality is acquired, it is automatically forwarded for subsequent processing. The first phase of our method is to collect a large database consisting of several iris images from various individuals. Images in the database are stored in bitmap format on the hard drive of the computer that will be used to analyze them. The database needs to be dynamic. The images can be captured using a CCD camera, which should have a resolution of at least 512 dpi to create a meaningful detailed image. However, to capture the rich details of the iris patterns, a camera at a minimum image resolution of 70 pixels should be used. Special cameras with an illumination of 70mm to 90mm wavelengths are required for imaging. Imaging must also be done with light reflecting at special angles depending on the wavelength so as to capture the rich patterns and striations. The camera can be a still camera or a video camera. A video camera is highly preferable so that iris aliveness can be tested.

With the increasing use of contact lenses, multiple types and colors of lenses are available with different textures by several manufacturers. To the best of our knowledge, there is no database that captures the variations across colors and textures in lenses. Further, different lens manufacturers may have different technologies for contact lens creation. To analyze the effect of these parameters on iris recognition, we have prepared the IIIT-D Contact Lens Iris (CLI) database. This section presents the details of the database and the performance evaluation of a commercial iris recognition system in both presence and absence of contact lenses. The IIIT-D CLI database is prepared with three objectives: (1) Capture images pertaining to at least 100 subjects, (2) For each individual, capture images without lens, with transparent (prescription) lens, and with color cosmetic lens, and (3) capture images with variations in iris sensors and lenses (colors and manufacturers). Both left and right iris images of each subject are captured and therefore, there are 202 iris classes. The lenses used in the database are soft lenses manufactured by either CIBA Vision or Bausch and Lomb. For color cosmetic lenses, four colors are used and to study the effect of acquisition device on contact lenses, iris images are captured using two iris sensors: (1) Cogent dual iris sensor (CIS 202) and (2) VistaFA2E single iris sensor. The database contains minimum five images of each iris class in each of the above mentioned lens categories for both the iris sensors. The following figure shows how a contact lens looks like and how they are placing in to the eye.

Fig.2. Contact Lens

IV. IRIS RECOGNITION

Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irises of an individual's eyes. Not to be confused with another less prevalent ocular-based technology, retina scanning, and iris recognition uses camera technology, and subtle IR illumination to reduce specular reflection from the convex cornea to create images of the detail-rich, intricate structures of the iris. These unique structures converted into digital templates, provide mathematical representations of the iris that yield unambiguous positive identification of an individual. Figure.3 shows the block diagram for iris recognition. The given steps are carried out while the iris recognition process.

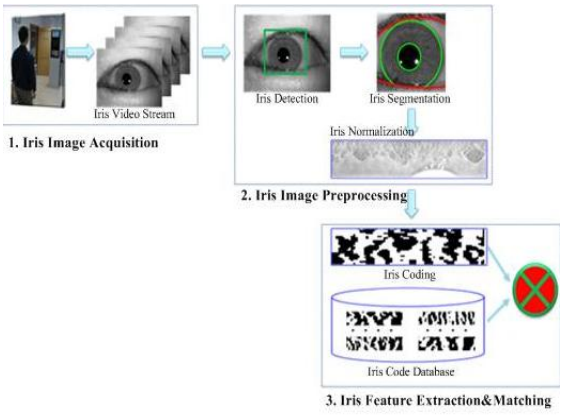

Figure.3. Block Diagram for Iris Recognition

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 4, Issue 9, September 2016

The iris is an externally visible, yet protected organ whose unique epigenetic pattern remains stable throughout adult life. These characteristics make it very attractive for use as a biometric for identifying individuals. Image processing techniques can be employed to extract the unique iris pattern from a digitized image of the eye, and encode it into a biometric template, which can be stored in a repository database. The biometric template contains an objective mathematical representation of the unique information stored in the iris, and it allows comparisons to be made between templates. When a subject wishes to be identified by iris recognition system, their eye is first photographed, and then a template created for their iris region. This template is then compared with the other templates stored in a database until either a matching template is found and the subject is identified, or no match is found and the subject remains unidentified. Although prototype systems had been proposed earlier, it was not until the early nineties that Cambridge researcher, John Daugman, working automated iris recognition systems. The Daugman system is patented and the rights are now owned by the company Iridian Technologies. The Daugman system is the most successful and most well-known, and also many other systems have been developed. Other notable ones include the systems of Wildes.

The first stage of iris recognition is to isolate the actual iris region in a digital eye image. The iris region can be approximated by two circles, one for the iris/sclera boundary and another, interior to the first, for the iris/pupil boundary. The eyelids and eyelashes normally occlude the upper and lower parts of the iris region. Also, specular reflections can occur within the iris region corrupting the iris pattern. A technique is required to isolate and exclude these artefacts as well as locating the circular iris region. The success of segmentation depends on the imaging quality of eye images. Images in the CASIA iris database do not contain specular reflections due to the use of near infra-red light for illumination. However, the images in the LEI database contain these specular reflections, which are caused by imaging under natural light. Also, persons with darkly pigmented irises will present very low contrast between the pupil and iris region if imaged under natural light, making segmentation more difficult. The segmentation stage is critical to the success of an iris recognition system, since data that is falsely represented as iris pattern data will corrupt the biometric templates generated, resulting in poor recognition rates.

V. SEGMENTATION

The segmentation includes localization of iris inner and outer boundaries and localization of boundary between iris and eyelids. Both the inner boundary and the outer boundary of a typical iris can be taken as circles. But the two circles are usually not co-centric. Compared with the other part of the eye, the pupil is much darker. We detect the inner boundary between the pupil and the iris. The outer boundary of the iris is more difficult to detect because of the low contrast between the two sides of the boundary. We detect the outer boundary by maximizing changes of the perimeter- normalized along the circle. The technique is found to be efficient and effective. Canny Edge Detection is the detection technique used for segmentation and it is implemented using image management tool in lab view and vision module. The next step is to localize the circular edge in the region of interest. Canny edge detection operator uses a multi-stage algorithm to detect a wide range of edges in images. It is an optimal edge detector with good detection, good localization and minimal response. In localization we used this detection, in which the inner and outer circles of the iris is approximated, in which inner circle corresponds to iris/pupil boundary and outer circle corresponds to iris/sclera boundary. But the two circles are usually not concentric.

Also, comparing with other parts of the eye, the pupil is much darker. The inner boundary is detected between the pupil and the iris. At the same time, the outer boundary of the iris is more difficult to detect because of the low contrast between the two sides of the boundary. So, we detect the outer boundary by maximizing changes of the perimeter along the circle. Iris segmentation is an essential process which localizes the correct iris region in an eye image. Circular edge detection function is used for detecting iris as the boundary is circular and darker than the surrounding. The Canny algorithm basically finds edges where the grayscale intensity of the image changes the most. These areas are found by determining gradients of the image.

The algorithm runs in 5 separate steps:

1. Smoothing: Blurring of the image to remove noise.
2. Finding gradients: The edges should be marked where the gradients of the image has large magnitudes.
3. Non-maximum suppression: Only local maxima should be marked as edges.
4. Double thresholding: Potential edges are determined by thresholding.
5. Edge tracking by hysteresis: Final edges are determined by suppressing all edges that are not connected to a very certain (strong) edge.

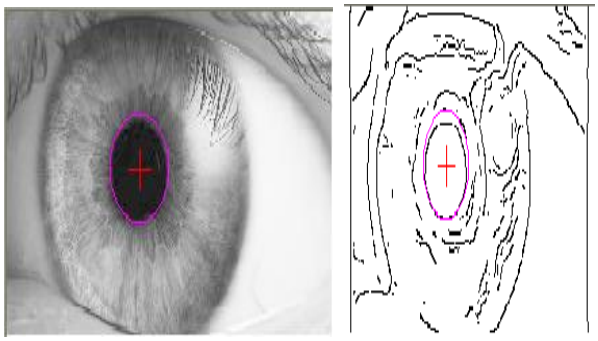

Figure 4 Canny Edge Detection

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 4, Issue 9, September 2016

The acquired iris image has to be preprocessed to detect the iris, which is an annular portion between the pupil (inner boundary) and the sclera (outer boundary) both shown in figure 5 and 6 respectively. The first step in iris localization is to detect pupil which is the black circular part surrounded by iris tissues. The center of pupil can be used to detect the outer radius of iris patterns.

The important steps involved are:

1. Pupil detection (Inner Circle)
2. Outer iris localization

External noise is removed by blurring the intensity image. But too much blurring may dilate the boundaries of the edge or may make it difficult to detect the outer iris boundary, separating the eyeball and sclera. Thus a special smoothing filter such as the median filter is used on the original intensity image. This type of filtering eliminates sparse noise while preserving image boundaries. After filtering, the contrast of image is enhanced to have sharp variation at image boundaries using histogram equalization.

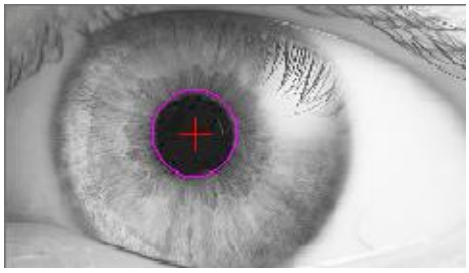

Fig.5. Detection of inner pupil boundary

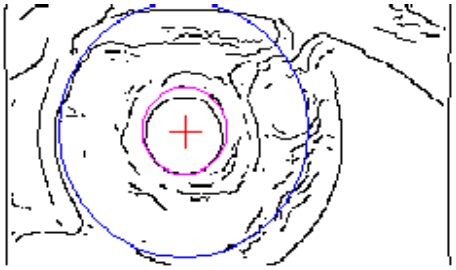

Fig.6. Detection of outer pupil boundary

VI. NORMALIZATION

Once the iris region is successfully segmented from an eye image, the next stage is to transform the iris region so that it has fixed dimensions in order to allow comparisons. The dimensional inconsistencies between eye images are mainly due to the stretching of the iris caused by pupil dilation from varying levels of illumination. Other sources of inconsistency include, varying imaging distance, rotation of the camera, head tilt, and rotation of the eye within the eye socket. Figure.7 shows the iris normalization process. The normalization process will produce iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location. Another point of note is that the pupil region is not always concentric within the iris region, and is usually slightly nasal. This must be taken into account if trying to normalize the doughnut shaped iris region to have constant radius.

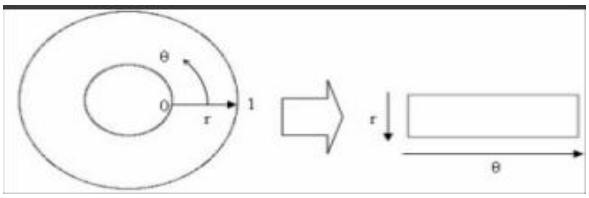

Figure.7. Iris Normalization

In order to provide accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. Figure.8 shows the image of an iris code. Only the significant features of the iris must be encoded so that comparisons between templates can be made. Most iris recognition systems make use of a band pass decomposition of the iris image to create a biometric template.

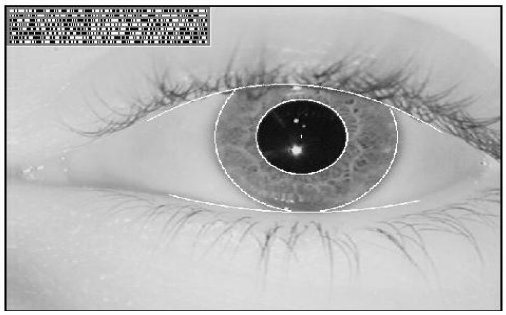

Figure.8. Iris Code

The template that is generated in the feature encoding process will also need a corresponding matching metric, which gives a measure of similarity between two iris templates. This metric should give one range of values when comparing templates generated from the same eye, known as intra-class comparisons, and another range of values when comparing templates created from different irises, known as inter-class comparisons. These two cases should give distinct and separate values, so that a decision can be made with high confidence as to whether two templates are from the same iris, or from two different irises.

VII. SIMULATION AND RESULT

Using MATLAB R2014a iris recognition is implemented. The lens patterns are extracted from the input and comparison of input image with the database carried out. If the extracted pattern matched with any of the image in the database then the security system will authenticate the person. Else if the extracted pattern shows a mismatch with the database then we can say that the person is not true, no authentication will take place. And we can restrict his entry by this because he is a fake one.

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 4, Issue 9, September 2016

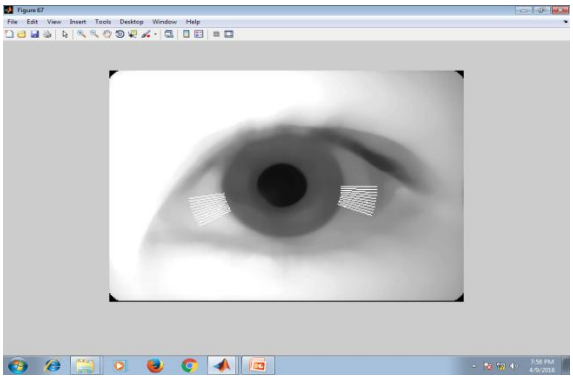

Fig.9. Segmentation

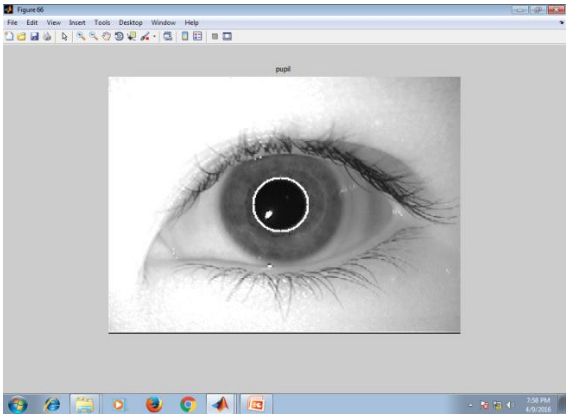

Fig.10. Pupil extraction

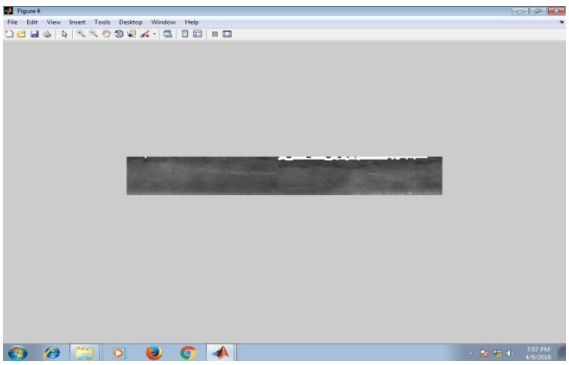

Fig.11. Comparison

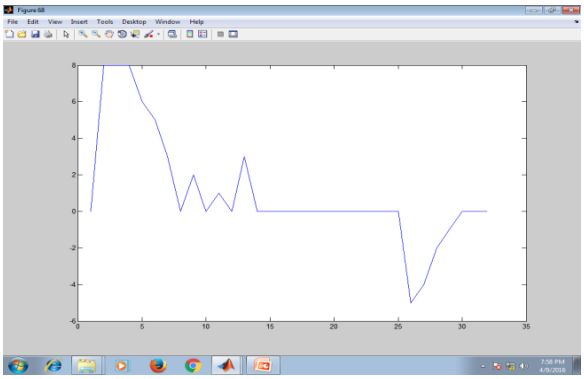

Fig.12. Performance Graph

Here we did the entire iris pattern matching, and we have all the contact lens patterns available in the market within our database. Due to the cost limitations in this paper only a certain numbers are saved in the database. And the simulation results obtained are shown in Figure.9, 10, 11 and 12. Figure.9 shows the segmentation process in which the localization is taking place. Figure.10 shows the pupil extraction, the inner pupil extraction is carried out here. Figure.11 shows the matching or comparison and in this step the authentication process is done. Figure.12 shows the overall performance graph of the security system.

VIII. CONCLUSION

The uniqueness of the iris and low probability of a false acceptance or false rejection all contribute to the benefits of using iris recognition technology. It provides an accurate and secure method of authenticating users onto company systems. Iris recognition system has been developed steadily with the help of MATLAB and some mathematical calculations; also by adding the entire lenses patterns available in the market to the database and by extracting these patterns from the input all the limitations put forward by the previous papers are solved here. Many individuals wear their prescribed contact lenses at all times. Thus, it is important to consider scenarios where we compare contact and non contact lens images of the same subject. It is possible that the contact lenses may magnify or alter the texture of the iris in such a way as to further increase the match scores between the contact lens and non contact lens images. And here we solved these problems by adding the entire lens patterns in to the database and we are extracting them whenever we need. Hence we improved the quality of the authentication process and the whole security system.

REFERENCES

[1] DakshaYadav,Student Member, IEEE, Naman Kohli,Student Member, IEEE, James S. Doyle, Jr., Student Member, IEEE, Richa Singh, Member, IEEE, Mayank Vatsa,Member, IEEE, Kevin W. Bowyer, Fellow, IEEE "Unraveling the Effect of Textured Contact Lenses on Iris Recognition"2015.

[2] Adityavardhan Chavali1, Dr. C. Nalini2U.G Student, Department of CSE, Bharath University, Selaiyur, Chennai, India Professor, Department of CSE, Bharath University, Selaiyur, Chennai., India IJIRSET Vol. 4 Issue 3 "Observing the Effects of Colored Lenses on Iris Recognition using Feature Extraction Technique" March 2015.

[3] James S. Doyle, Jr., Student Member, IEEE, and Kevin W. Bowyer, Fellow, IEEE "Robust Detection of Textured Contact Lenses in Iris Recognition using BSIF" 2015.

[4] Gokul Kishan1 Dr. N Vishwanath2 1PG Student 2Professor 1,2Department of Computer Science Engineering 1,2Toc H Institute of Science and Technology "An Enhanced Approach for Identification of Cosmetic Contact Lenses on Iris Recognition" 2015

[5] Gao Xiaoxing1, Feng Sumin2, Cui Han11Shijiazhuang University of Economics, Shijiazhuang 050031, China2Shijiazhuang Engineering Vocational College ,Shijiazhuang 050031, China International journal on smart sensing and intelligent systems vol. 8, no. 2 " Enhanced iris recognition based on image match and hamming distance" June 2015.

[6] Pedro Silva, Eduardo Luz, Rafael Baeta, David Menotti computing Department Federal University of Ouro reto - UFOPOuro Preto, MG, Brazil "An Approach to Iris Contact Lens Detection based on Deep Image Representations" June 2015.