Proposed Approach for Iris Recognition in Security Based Applications

Sri Sachidanand S. Joshi[1], Bhavana. Desai[2], J. L. Kalyan[3]

[1]Assistant Professor, Dept of Information Science and Engineering
SDM College of Engineering and Technology, Dharwad- 580001, Karnataka, India
sachinjoshi055@gmail.com

[2]Research Scholar, Dept of Criminology and Forensic Science
Karnatak Science College, Dharwad- 580001, Karnataka, India
bhavanadesai19@gmail.com

[3]Associate Professor, HOD, Dept of Criminology and Forensic Science
Karnatak Science College, Dharwad- 580001, Karnataka, India
drjagdeeshkalyan@gmail.com

Abstract: *Iris recognition is the process of recognition a person by analyzing the apparent pattern of his or her iris. There is a strong scientific demand for proliferation of systems, concepts and algorithms for iris recognition and identification. This is mostly because of the comparatively short time that iris recognition systems have been around. In comparison to face, fingerprint and other biometric traits there is still need for substantial mathematical and computer vision research and insight into iris recognition. An evidence for this is total lack of publicity available adequate datasets of iris images. The use of iris can make the security arrangements more rigid in administrative sectors, confidential govt. sectors and many agencies which are completely dependent on the perfect security management. The program converts a photo of an eye to an unrolled depiction of subject's iris and matches the eye to agent's memory if match is found, it outputs a best match.*

Keywords: Iris, Acquisition, Security, Recognition, Comparison.

1. Introduction

Biometrics is the science of establishing human identity by using physical or behavioral traits such as face, fingerprints, palm prints, iris, hand geometry and voice. Iris recognition systems, in particular are gaining interest because the iris's rich texture offers a strong biometric clue for recognizing individuals. Located just behind the cornea and in front of lens, the iris uses the dilator and sphincter muscles that govern pupil size to control the amount of light that enters the eye. Further, the iris is only internal organ readily visible from outside. Thus, unlike fingerprints or palm prints environmental effects cannot easily alter its pattern. An iris recognition system uses pattern matching to compare two iris images and generate a match score that reflects their degree of similarity or dissimilarity. A key advantage of iris recognition is its stability to template longevity as barring trauma, a single enrolment can last a lifetime.

Among all the biometric techniques, facial identification is the oldest method which has been successfully used in numerous applications. Facial biometrics fails due to the changes in features caused by expressions, cosmetics, growth of facial hair as well as the difficulty of reliably extracting them in a constrained environment exhibiting imaging problems such as lighting and shadowing. Iris recognition is the most powerful biometric technology and security system to prevent unauthorized user or personal form assessing secured information or restricted areas. Iris scan employs the unique characteristics and features of the human iris in order to verify the identity of an individual.

2. Advantages and Significance of Iris

2.1 Advantages

- Iris is the internal organ that is well protected against damage. This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor.
- An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away.
- While there are some medical and surgical procedures ha can affect the color and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years.
- Iris patterns possess a high degree of randomness.

2.2 Significance

Iris has stable and distinctive features for personal identification. That is because every iris has fine and unique patterns and does not change over time since two or three years after the birth, so it might be called as a kind of optical finger print. Accurately identifying individuals is a major concern for governmental agencies, police department, medical institutions, banking and legal institutions, and corporation, to name just a few. The importance lies in the necessity for the control of fraud, efficiency in administration, and benefits to users of various systems.

Research has shown that an iris has 256 independent measurable characteristics, or degrees of freedom, nearly six times as many as a finger print. Thus, the probability of two irises producing the same code is approximately 1 in 10^{78} with the population of the earth being approximately 10^{10} people. Thus, the performance of iris recognition has many greater capabilities than any other form of Human recognition, including finger prints, Facial or voice recognition, and retinal recognition.

3. Methods

3.1 Image Acquisition

It is the process of acquiring high definition iris image from pre collected images. These images should clearly show the entire eye especially iris and pupil part

3.2 Image Preprocessing and Segmentation

Preprocessing of the image is necessary to obtain image points or image pixels that are on the desired curve in the image space. The acquired image always contains not only the iris but also some relevant parts (e.g. eyelid, pupil). Under some conditions, the brightness is not uniformly distributed. In addition, different eye-to-camera distance may result in different image sizes of the same eye. For the purpose of analysis, the original image needs to be processed. The processing is composed of two steps:

1. Iris Localization: In this stage, we should determine an iris part of the image by localizing the position of the image derived from inside the limbus (outer boundary) and outside the pupil (inner boundary), and finally convert the iris part into a suitable representation. Because there is some obvious difference in the intensity around each boundary, an edge detection method is easily applied to acquire the edge information**.**

2. Iris Boundary Detection: It is used to find complex object boundaries by marking potential edge points corresponding to places in an image where rapid change in brightness occurs. After edge points have been marked, they can be merged to for lines. Edge detection operators are based on idea that edge information in an image is found by looking at the relationship of a pixel with its neighbors. In other words, edge is defined by discontinuity in gray values. An edge separates two distinct objects.

3.3 Pupil Boundary Detection

Firstly the gray level value for each pixel in the image for the corresponding RGB components. Then, we perform binarization by adaptively selecting a reasonable threshold and scan the whole image line by line on pixel basis, to find

the circular pupil region to determine the outer boundary, diameter and centre of the pupil.

3.3 Normalization

Iris of different people may be captured in different size, for the same person also size may vary because of the variation in illumination and other factors.

3.4 Feature Extraction

Iris provides abundant texture information. A feature vector is formed which consists of the ordered sequence of features extracted from the various representation of the iris images.

3.5 Pattern Matching

The feature vectors are classified through different threshold techniques like hamming distance, weight vector and winner selection, dissimilarity function etc.
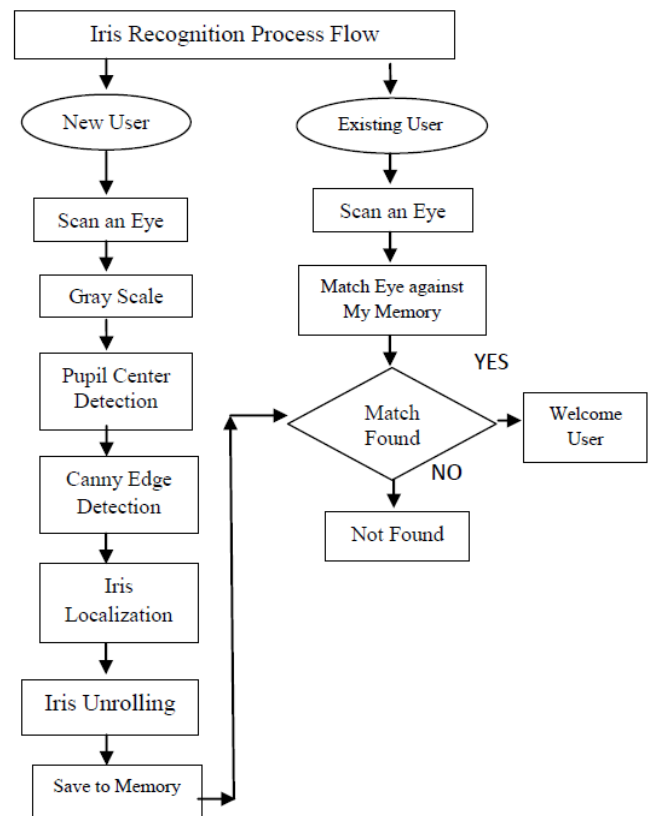
4. Proposed System and Algorithms Used

Figure 1: Proposed System Model

4.1 Iris Recognition Algorithms

Eye Image with Blink: This type of eye image does not focus iris properly. The following steps may be applied to check the quality.

Step 1: Evaluate Gray level of pixel in the eyelid area.

Step 2: Eye data have flashing noise is been proceeded to preprocessing module.

Detection of Eyelash: Eyelash interference is serious issue in Feature extraction process.

Step 1: The line detector is used to find out line component between inner boundary and Iris area.
Step 2: If the end point of line component is under pupil centre then iris area is interfered by eyelash otherwise iris is in normal condition.

Detecting Spectacles reflection: Spectacles reflection in iris area is another issue in feature extraction.
Detect Truncated Iris area: Truncation of iris pattern may be present in eye images.

4.2 Algorithm for Iris Segmentation

Step 1: Rotate eye image 180 degrees to avoid the detection of thick eye broses as a pupil boundary.
Step 2: Detect the position of camera flash.
Step 3: Gray level value is used to detect iris inner boundary.

4.3 Algorithm for Iris Normalization

Step 1: Set any point as a reference point in iris portion.
Step 2: Draw concentric circles using the reference point.
Step 3: Repeat step2 until iris outer boundary is reached.
Step 4: Collect all pixels, in a circle to construct a pattern.
Step 5: The image right triangular portion is removed and mapped into left portion.

4.4 Algorithm for Iris Matching

Step 1: Each iris code is divided into 2 subsets: T1 and T2. Initial pattern matching is done separately on each of the T1 and T2 subsets, using the usual Hamming Distance approach.
Step 2: Initial pattern matching is also done treating the two subsets as a single entity.
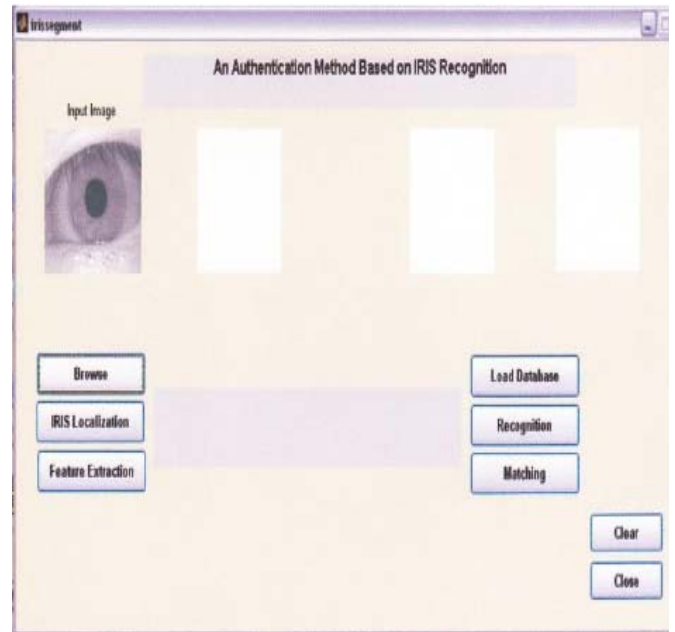
5. Results

Figure 2. Selecting Input Image

Figure 3. Completion of Localization
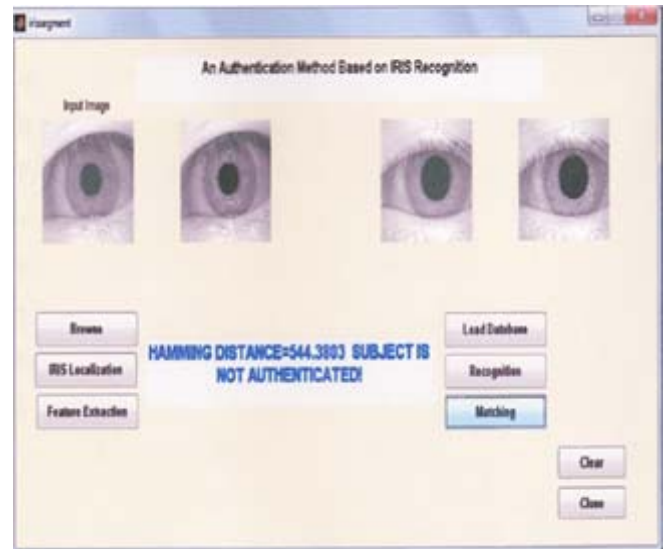

Figure 4. Feature Extraction

Figure 5. Load Database

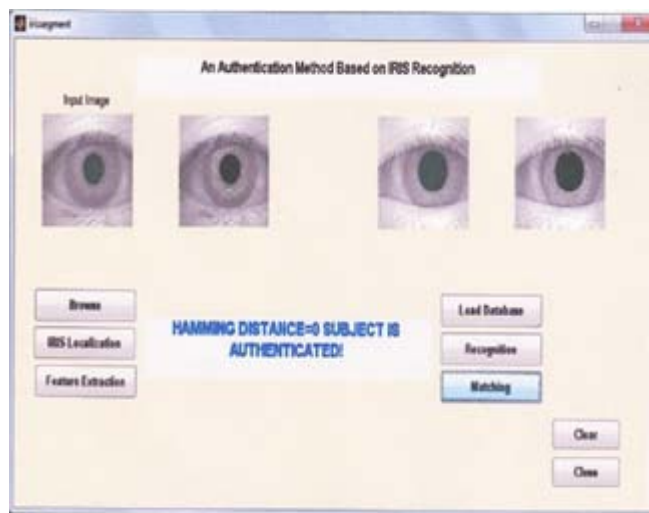**Figure 6.** Recognition

Figure 7. Matching

Figure 8. Not Matching.

6. Conclusion

Iris Recognition technology has the depth to last for a long time. The excepted growth in the demand for iris recognition products is increasing day by day. Authorizing the user with user Pin and physical token is not enough for applications where the importance of user being really the one certified is emphasized. If biometric technologies are not used we accept the possibility that the token and secrecy of Pin can be compromised. Biometrics provides means to treat the possible user candidates uniquely. While doing so biometric system handles unique data scanned from the user. Secrecy of this information has to ensure by strong cryptographic methods. The best case could still be that the biometric templates would never leave the scanner device, with or without encryption. The result should only be grating he scanning device, which could be special smart card carried by user itself, to complete the challenge-response sequence needed. In that case your fingerprint may be the password, but the problem with management of public and secrete cryptographic keys stays the same. Although iris recognition is still in its final research and development stage throughout the world, it has many possible applications, some of which are secure access to bank case machine accounts, Ticketless air travels, Driving license, and other personal certificates, Internet security, control of access to privilege information. This could be very helpful for security purposes in government administrative agencies to take most care of confidential matters. There is no matter of surprise if Iris recognition replaces other personal identification methods in near future due to its performance compared to other biometrics.

References

[1] Daugman J, "Biometric Decision Landscapes", Technical Report No. TR482, University of Cambridge Computer Laboratory, 1999(technical report style)
[2] J. G. Daugman, "Biometric Personal Identification System based on Iris Analysis", U. S patemt 5, pp 291,560, March 1 1994
[3] J. G. Daugman, "High Confidence Visual Racognition of Persons by a Test of Statistical Independence", IEEE

Trans. Pattern Analytical Mach. Intell., vol. 15 no. 11, pp 1148-1161, 1993(journal style)

[4] J. G. Daugman, "Recognizing Persons by their Iris Patterns", In Biometrics: Personal Identification in Networked Society, Kluwer, pp 103-121, 1998.

[5] John G. Waugman, "High Confidence Visual Recognition Persons by a Test of Statistical Independence," IEEE Transactions on Pattern Analysis and Machine Intelligence,   vol.-15, no.- 11, pp 1148-1160, November 1993(journal style)

[6] Richald P. Wildes, "Iris Recognition an Emerging Biometric Technology" Proceedings of the IEEE, vol.-85, no.-9, pp 1348 – 1362, September 1997(conference style)

[7] W.W. Boles and B. Boashash, "A Human Identification Technology using images of the Iris and Wavelet Transform." IEEE Transactions on Signal Processing, vol. 46, no. 4, pp 1185- 1188, April 1998(journal style)

[8] R. P. Wildes "A System for Automated Iris Recognition", Proceedings of the IEEE, vol. 64, no. 10, pp 121-128, June 1994(journal style)

[9] K. Jain, "Fundamentals of Digital Image Processing" Prentice Hall Publication Pvt. Ltd (book style)

[10] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", Addison Wesley (book style)

[11] Randy Crane, "A Simplified Approach to Image Processing", Prentice – Hall Publication Pvt. Ltd (book style)

Author Profile

Sri Sachidananda S Joshi, Assistant professor at SDM College of Engineering and Technology from Dharwad Karnataka, areas of interest are Network Security, Computer Networks.

Bhavana Desai, Research scholar, pursuing PhD in Forensic Science from Karnataka University, Dharwad, Karnataka. Her areas of interest are Finger prints, Document verification, and toxicology.

Dr. J L Kalyan, Associate professor HOD of Criminology and Forensic Science in Karnataka Science College Dharwad. His areas of interest are Finger prints, Document verification.