© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 03 | 07 | April - June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

IMPLEMENTATION ON ENHANCING IRIS BASED SECURITY SYSTEM USING EDGE DETECTION MECHANISM

Diksha Chawla, Research Scholar, Department of ECE, IIET
Kapil Sachdeva, Assistant professor , Department of ECE, IIET

Abstract: Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance. Not to be confused with other, less prevalent, ocular-based biometric technologies such as retina scanning, iris recognition uses video camera technology with subtle near infrared illumination to acquire images of the detail-rich, intricate structures of the iris which are visible externally. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual. Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with remarkably low false match rates.

[I] IRIS RECOGNITION SYSTEMS

The iris-scan process begins with a photograph. A specialized camera, typically very close to the subject, not more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes 1 to 2 seconds.

Several hundred millions of persons in several countries around the world have been enrolled in iris recognition systems, for convenience purposes such as passport-free automated border-crossings, and some national ID systems based on this technology are being deployed. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to false matches, is the stability of the iris as an internal and protected, yet externally visible organ of the eye.

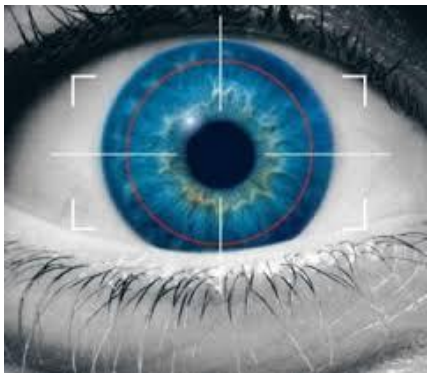


Fig: Human eye

[II] Iris as a powerful identifier

Iris is the focus of a relatively new means of biometric identification. The iris is called the living password because of its unique, random features. It is always with you and cannot be stolen or faked. The iris of each eye is absolutely unique. The probability that any two irises could be alike is one in 10 to 78^{th} power the entire human population of the earth is roughly 5.8 billion. So no two irises are alike in their details, even among identical twins. Even the left and right irises of a single person seem to be highly distinct. Every iris has a highly detailed and unique texture that remains stable over decades of life. Because of the texture, physiological nature and random generation of an iris artificial duplication is virtually impossible.

[III] PROPERTIES OF THE IRIS

The properties of the iris that enhance its suitability for use in high confidence identification system are those following:

1. Extremely data rich physical structure about 400 identifying features

2. Genetic independence no two eyes are the same.

3. Stability over time.

4. Its inherent isolation and protection from the external environment.

5. The impossibility of surgically modifying it without unacceptable risk to vision.

6. Its physiological response to light, which provides one of several natural tests against artifice.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 02 | 29 | April - June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

7. The ease of registering its image at some distance forms a subject without physical contact.

8. It intrinsic polar geometry which imparts a natural co-ordinate system and an origin of co-ordinates

9. The high levels of randomness in it pattern inter subject variability spanning 244 degrees of freedom and an entropy of 32 bits square million of iris tissue.

Iris recognition is a biometric recognition technology that utilizes pattern recognition techniques on the basis of iris high quality images. Since in comparison with other features utilized in biometric systems, iris patterns are more stable and reliable, iris recognition is known as one of the most outstanding biometric technologies. Iris images could be taken from humans eyes free from such limitations as frontal image acquisition and special illumination circumstances. Daugman's and Wildes' systems are the two earliest and most famous iris recognition systems including all iris recognition stages.

In Daugman's algorithm, two circles which are not necessarily concentrated form the pattern. Each circle is defined by three parameters (x0, y0, r) in a way that (x0, y0) determines the center of a circle with the radius of r. An integro-differential operator is used to estimate the values of the three parameters for each circular boundary and the whole image is searched in relation to the increment of radius r. In Wildes' system, gradient based Hough transform has been used to localize two iris circular boundaries. This system consists of two stages. At first, a binary map is produced from image edges by a Gaussian filter. Then, the analysis is performed in a circular Hough space in order to estimate the three parameters (x0, y0, r) for a circle.

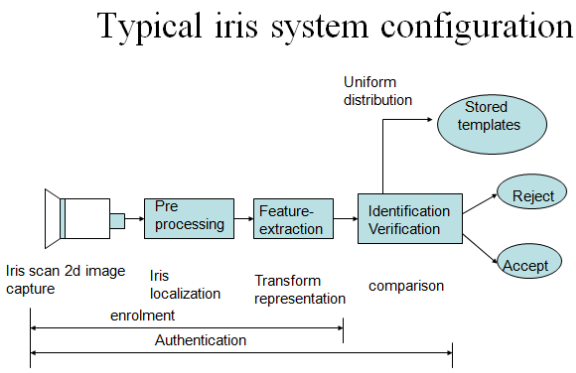
In segmentation step of the algorithm proposed in, a set of one-dimensional signals is extracted from iris image using the values of illumination intensity on a set of pupil centered circular contours which have been localized through use of edge detection techniques. In iris images are projected vertically and horizontally to estimate the center of the iris. Also, this method has been utilized for eyelash segmentation and lightening reflection removal in. The algorithm proposed in predicts the optimization of iris biometric system on a bigger set of data on the basis of Gaussian model obtained from a smaller set of data. Also, an iris recognition system has been proposed in which is used for frontal iris images and for an iris image which is not taken from frontal view.

When frontal iris image is not available for a particular individual, in this system the issue is considered through maximizing Hamming distance between the two mentioned images or through minimizing Daugman's integro- differential operator. Next, the image is transformed to a frontal image. An algorithm is presented to find eyelash and eyelids occlusions on iris in a completely close up image similar to Daugman's method in. In 3D environment, this algorithm searches for three parameters as with (x, y) in center and radius of z.

Major characteristics of iris recognition

- Iris is thin membrane on the interior of the eyeball.
- Iris pattern remains unchanged after the age of two and does not degrade overtime or with the environment.
- Iris patterns are extremely complex than other biometric patterns

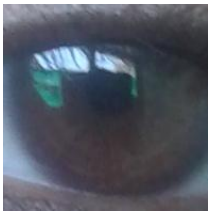
[IV]TYPICAL IRIS RECOGNITION SYSTEM



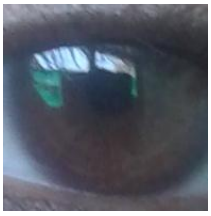
[V] Iris recognition implementation

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 02 | 29 | April - June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Step 1: Acquisation of image of iris: Scan the image of eye or take it by digital camera



Step2: Before comparison we crop image of eye.



Step 3

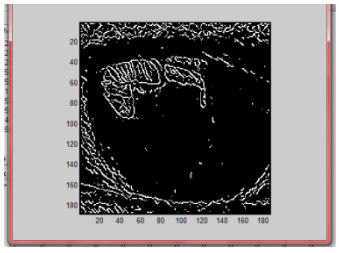
Store image as matrix in i

>>i=imread('eye1.jpg')

Step 4

Apply canny to i matrix and store in ii

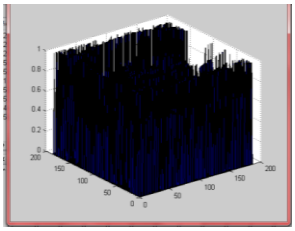
>> ii=canny(i,1,1,1)



Step 5

Create histogram using surf command

>>surf(ii)



[VI]APPLICATIONS

Iris-based identification and verification technology has gained acceptance in a number of different areas. Application of iris recognition technology can he limited only by imagination. The important applications are those following: ATM and iris recognition: in U.S many banks incorporated iris recognition technology into ATM for the purpose of controlling access to one bank accounts. After enrolling once (a 30 second process), the customer need only approach the ATM, follow the instruction to look at the camera, and be recognized within 2-4 seconds. The benefits of such a system are that the customer who chooses to use bank ATM with iris recognition will have a quicker, more secure transaction. Tracking Prisoner Movement: The exceptionally high levels of accuracy provided by iris recognition technology broadens its applicability in high risk, high-security installations. Iris scan has implemented their devices with great success in prisons in Pennsylvania and Florida. By this any prison transfer or release is authorized through biometric identification. Such devices greatly ease logistical and staffing problems. Applications of this type are well suited to iris recognition technology. First, being fairly large, iris recognition physical security devices are easily integrated into the mountable, sturdy apparatuses needed or access control, The technology phenomenal accuracy can be relied upon to prevent unauthorized release or transfer and to identify repeat offenders re-entering

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 02 | 29 | April - June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

prison under a different identity. Computer login: The iris as a living password.

National Border Controls: The iris as a living password. Telephone call charging without cash, cards or PIN numbers. Ticket less air travel. Premises access control (home, office, laboratory etc.). Driving licenses and other personal certificates. Entitlements and benefits authentication. Forensics, birth certificates, tracking missing or wanted person Credit-card authentication. Automobile ignition and unlocking; anti-theft devices. Anti-terrorism (e.g.: suspect Screening at airports) Secure financial transaction (e-commerce, banking). Internet security, control of access to privileged information. Biometric key Cryptography for ncrypting/decrypting messages.

[VII] IRIS RECOGNITION: CHALLENGES

Every biometric technology has its own challenges. When reviewing test results, it is essential to consider the environment and protocols of the test. Much industry testing is performed in laboratory settings on images acquired in ideal conditions. Performance in a real world application may result in very different performance as there is a learning curve for would-be user of the system and not every candidate will enroll properly or quickly the first time. There are some issues which affect the functionality and applicability of iris recognition technology in particular.

[VIII] FUTURE SCOPE

In future iris recognitions process is found most secure as compared to other biometric techniques. And it may be useful to enhance secure transaction in banks and other financial organization. However there are many challenges in frequent use of this technology but in future due to advent of new technology it would be possible to use this technology easily. Enterprise and government both acknowledge the convergence of physical and information security environments, but there are new security challenges on the horizon - just-in-time inventory control, sophisticated supply chain management, and even a phenomenon called "coopetition"-in which companies that compete in some areas, cooperate in others. Managing this convergence of physical and information security requirements now drives security system architecture design and implementation, and is an increasingly key factor in biometric technology selection. Managing convergence will only become a more complex task because as the IT and communications becomes increasingly wireless, the need for robust identity management will become more acute. Iris ID sees iris technology as a natural "fit" for in the physical, infosec, and wireless arenas. We envision a day when iris recognition technology will be deployed in ways that eliminate fraud, provide non-repudiation of sales, authenticate funds transfers, provide signature verification, credit card authorization, and authorized access to healthcare records, intellectual property, and so much more.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, 2006, pp. 125-143.

[2] J. Daugman, "New Methods in Iris Recognition", IEEE Trans. on Systems, Man, and Cybernetics, Vol. 37, No. 5, 2007, pp. 1167-1175.

[3] R. Wildes, "Iris Recognition: an Emerging Biometric Technology", Proceedings of the IEEE, Vol. 85, No. 9, 1997, pp. 1348-1363.

[4] W. Boles, and B. Boashash, "A Human Identification Technique Using Images of the Iris and Wavelet Transform", IEEE Trans. on Signal Processing, Vol. 46, No.4, 1998, pp. 1185-1188.

[5] W. Kong, and D. Zhang, "Accurate Iris Segmentation Based on Novel Reflection and Eyelash Detection Model", in International Symposium on Intelligent Multimedia, Video and Speech Processing, 2001, pp. 263-266.

[6] L. Ma, and T. Tisse, "Personal Recognition Based on Iris Texture Analysis", IEEE Trans. on PAMI, Vol. 25, No. 12,2003, pp. 1519-1533.

[7] N. Schmid, M. Ketkar, H. Singh, and B. Cukic, "Performance Analysis of Iris Based Identification System the Matching Scores Level", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, 2006, pp. 154-168.

[8] V. Dorairaj, A. Schmid, and G. Fahmy, "Performance Evaluation of Iris Based Recognition System Implementing PCA and ICA Encoding Techniques", in Proceedings of SPIE, 2005, pp. 51-58.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 02 | 29 | April - June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

[9] C. Fancourt, L. Bogoni, K. Hanna, Y. Guo, and R. Wildes, and N. Takahashi, and U. Jain, "Iris Recognition at a Distance", in Proceedings of the International Conference on Audio and Video-Based Biometric Person Authentication, 2005, pp. 1-13.