International Journal of Scientific & Technical Development
(A Peer-Reviewed Bi-Annual Journal) ISSN: 2348-4047

ISSUES, CHALLENGES AND ACHIEVEMENTS IN IRIS RECOGNITION: A GENERAL STUDY

***Navneet Kaur Sandhu**
*Department of Computer Science and Engineering, DeshBhagat University (Punjab) India 147301

Abstract
In recent years identification of persons has gained major importance within the world from its applications, like border security, access control and forensic. Iris recognition is one amongst the foremost booming biometric modalities because of its unique character as a biometric feature, iris identification and verification systems became one among the most accurate biometric modality. During this paper, the different steps to acknowledge an iris image which incorporates acquisition, segmentation, normalization, feature extraction and matching are discussed. The performance of the iris recognition system depends on segmentation and normalization techniques adopted before extracting the iris features. It also provides an in depth review of the numerous methods of iris recognition systems. Additionally to the current, the challenges and achievements of the iris are presented.

1 INTRODUCTION

Biometrics is describedbecause thelook at of numerousstrategies for measurements of physiological and behavioral traits that may betaken into consideration to perceive a man or woman. The biometric trendsparticularly face and iris is regularly thought of because theimportanttrendycausestrategies. Iris popularity is a manner of popularity of a personwith the aid of using analyzing random sample of the iris. The iris texture from a human eye may be used for biometric authentication and identification. The use of iris sample in a specific softwareentailsa fixedof 7elements to perceive the man or womanprimarily based totallyat the iris biometric modality.

1. Universality that everyone has the characteristics of the texture of the iris.
2. Uniqueness means that the texture characteristics of the iris are sufficiently different and can be distinguished from each other by the individual.
3. Clarity means that the randomness of the iris pattern has a very high dimension.
4. Persistence means that the texture of the iris remains constant over time.
5. Measurable indicates the ease of detection of the iris texture.
6. Performance refers to the robustness, speed, and accuracy of the technology adopted.
7. Adoption refers to how well an individual accepts adopted technology.

Background

The reason for the popularity of the iris as a biometric the characteristics of the identification technique are uniqueness, stability, longevity and reliability. However, in this study, we will discuss various problems, Challenges encountered in iris recognition. We will also discuss the achievements of the Iris in this paper. The iris is a protected internal organ that has random texture is the most reliable and stable over the lifetime, can act as a kind of live password that you don't need Remember, but always carry it with you. Every iris is different, even two irises of the same individual, and the irises of twins are different. Iris patterns are formed before birth and do not change over the course of a lifetime (Nanavati et al., 2002). Even medical procedures such as refractive surgery, cataract surgery, and cornea transplants do not affect recognizable characteristics; (Rhodes, 2002). Because of the natural protection of the eyes in the face, and the protection of the iris beneath the cornea, the iris is also resistant to injury, making it highly stable as a recognizable characteristics.

Table 1: Issues, Challenges and Achievement of Iris

Issues	Challenges	Achievements
Head Tilt or Cyclotorsion	Biometric isn't private:	Iris patterns possess a high degree of randomness.
Template Aging in Iris	Biometrics Are Hackable	Encoding and decision-making are tractable.
	Biometrics Hacks May Have Greater Consequences	

Head Tilt or Cyclotorsion

Ophthalmologic tests can be influenced by head tilt and the resulting ocular cyclotorsion. As a result, appropriate head placement has been stressed during fundus scanning. However, there is no precise mechanism for

controlling head tilt, and little is known about how tiny head tilts affect the body. The effect of a slight head tilt on ocular cyclotorsion, which is difficult to detect, was studied in this study.

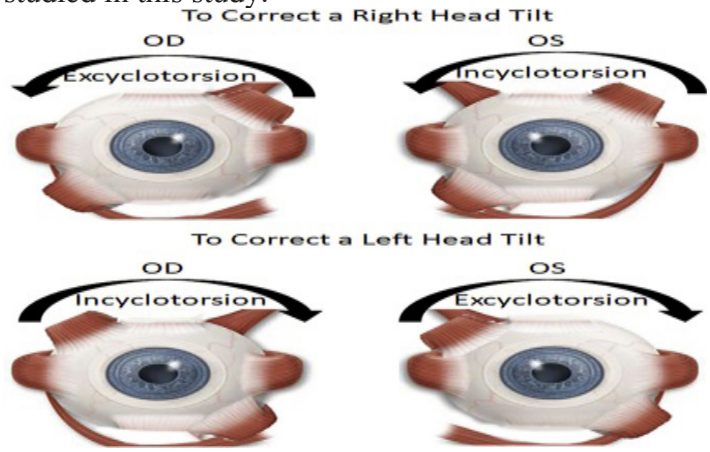

Figure 1: Head Tilt

Template Aging in Iris

The phrase "template ageing" describes the decline in biometric performance that occurs when the period between the acquisition of an enrollment image and the acquisition of the image compared to the enrollment increases.

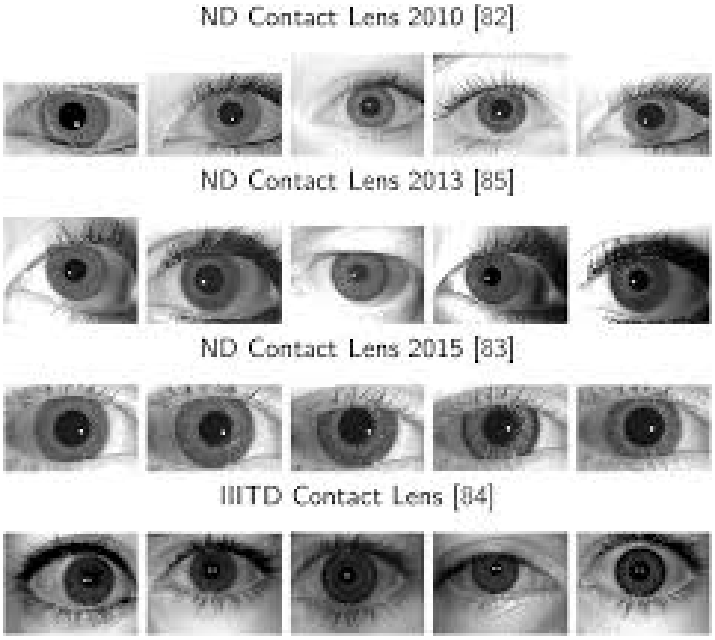

Figure 2: Template Aging

Challenges of Iris Recognition

Biometric is not private:

Biometrics seems secure on the surface. After all, only you have ears, eyes and digital printing. But that doesn't necessarily make it any more secure than passwords. Passwords are inherently private because you are the only one who knows. Of course, hackers can get it through brute force or phishing attacks, but normally people can't access it. Biometrics, on the other hand, are public in nature. Think about it: your ears, eyes, and face are exposed. You reveal your eyes every time you look things. With fingerprint recognition, you'll leave your fingerprints everywhere you go. With voice recognition, someone Record your voice. Basically, all of these identifiers are easily accessible. Your pictures are stored in more places than you think. Facebook not only recognizes your face, but every store you visit records and saves your image in database to identify you and analyze your shopping habits. In fact, 48 states use software to determine you use images taken without your consent for commercial purposes. And law enforcement countries can store your images without consent. The problem is identity management and security. Personally Identifiable Information (PII) Must HaveAccess control in place to protect against identity theft. All it takes is a hacker can compromise one of these databases to leak and steal your biometric identity.

Biometric is Hackable

A hacker can quickly acquire access to someone's account if they have a picture of their ear, eye, or finger. The hacker received high-resolution photographs of the politician's thumb from press briefings and used VeriFinger software to reconstruct the imprint. If you believe an eye scan is more secure, think again. By putting a contact lens over a snapshot of a user's iris, hackers deceived the Samsung S8's iris recognition technology.

Biometrics Hacks May Have Greater Consequences

Because a biometric reveals a portion of a user's identity, it can be used to falsify legal documents, passports, or criminal records if stolen, causing far more harm than a stolen credit card number. Although biometrics may be the security solution of the future, it is not yet time to throw away your passwords. Biometrics adds another layer of protection, but it isn't perfect.

Conclusion

Biometric identification of people has become more important around the world as a result of applications including border security, access control, and forensics. Because of its unique properties, iris recognition is one of the most popular biometric modalities. Iris recognition is a method of identifying a person by examining a random pattern on their iris. Human biometric authentication and identification can be done using the iris texture of a human eye. The steps for recognizing

iris images are explained in this study, which include acquisition, segmentation, normalization, feature extraction, and matching.

References

1. Baker, S., Bowyer, K. W., and Flynn, P. J. (2009). Empirical evidence for correct iris match score degradation with increased time lapse between gallery and probe images. In International Conference on Biometrics, pages 1170–1179.
2. Baker, S., Bowyer, K. W., Flynn, P. J., and Phillips, P. J. (2012). Template aging in iris biometrics: Evidence of increased false reject rate in ICE 2006. In Burge, M. and Bowyer, K. W., editors, Handbook of Iris Recognition. Springer.
3. Bowyer, K. W., Baker, S. E., Hentz, A., Hollingsworth, K., Peters, T., and Flynn, P. J. (2009). Factors that degrade the match distribution in iris biometrics. In Identity in the Information Society, volume 2, pages 327–343. Springer.
4. Czajka, A. and Pacut, A. (2010). Iris recognition system based on Zak-Gabor wavelet packets. Journal of Telecommunications and Information Technology, 4:10–18. Daugman, J. (1993). High confidence visual recognition of persons by a test of statistical independence. IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(11):1148–1161.
5. Fenker, S. P. and Bowyer, K. W. (2011). Experimental evidence of a template aging effect in iris biometrics. In IEEE Computer Society Workshop on Applications of Computer Vision, pages 232–239.
6. Fenker, S. P. and Bowyer, K. W. (2012). Analysis of template aging in iris biometrics. In CVPR Biometrics Workshop, pages 1–7. Flom, L. and Safir, A. (1987). Iris recognition system. Patent. US 4,641,349.
7. Monro, D. M., Rakshit, S., and Zhang, D. (2007). DCTbased iris recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence – Special Issue on Biometrics: Progress and Directions, 29(4):586–595. Neurotechnology (2012). VeriEye SDK, version 4.3, revision 87298.
8. Rankin, D., Scotney, B., Morrow, P., and Pierscionek, B. (2012). Iris recognition failure over time: The effects of texture. Pattern Recognition, 45:145–150. Shchegrova, S. (2012). Analysis of iris stability over time using statistical regression modeling. In Biometric Consortium Conference & Technology Expo, September 18-20, 2012, Tampa, Florida USA. SmartSensors (2012). MIRLIN SDK, version 2.23.2.
9. Tome-Gonzalez, P., Alonso-Fernandez, F., and OrtegaGarcia, J. (2008). On the effects of time variability in iris recognition. In IEEE Conference on Biometrics: Theory, Applications and Systems, pages 1–6. IEEE.
10. Adelson, E.H., Anderson, C.H., Bergen, J.R., Burt, P.J. and Ogden, J.M. 1984. Pyramid methods in image processing. Radio Corporation of America Engineer. 29, 33-41.
11. Avila, S.C. and Reillo, S.R. 2005. Two different approaches for iris recognition using Gabor filters and multiscale zero-crossing representation. Pattern Recognition. 38, 231–240.
12. Bachoo, A.K. and Tapamo, J.R. 2005. Texture detection for segmentation of iris images. Proceedings of the Annual Research Conference of the South African Institute of Computer Information Technologists, South Africa, September 20-22, 2005, 236–243.
13. Camus, T.A. and Wildes, R.P. 2002. Reliable and fast eye finding in close-up images. Proceedings of the International Conference on Pattern Recognition, Quebec, Canada, August 11-15, 2002, 389–394.
14. Chowhan, S.S. and Shinde, G.N. 2009. Evaluation of statistical feature encoding techniques on iris images. Proceedings of the World Research Institutes World Congress on Computer Science and Information Engineering. Los Angeles, CA, March 31- April 2, 2009, 71-75.
15. Cole, L., Austin, D. and Cole, L. 2004. Visual object recognition using template matching. Proceedings of the Australian Conference on Robotics and Automation. Canberra, Australia, December 6 - 8, 2004, 1-8.
16. CY Lab (2011). Iris and face recognition. http://www.cylab. cmu.edu/partners/success-stories/iris-recognition.html [October 5, 2011]
17. Daugman, J. 1993. High confidence visual recognition of persons by a test of statistical independence. Institute of Electrical and Electronic Engineers Transactions on Pattern Analysis Machine Intelligence. 15, 1148– 1161.
18. Daugman, J. 1994. Biometric personal identification system based on iris analysis. United States Patent, March 1, 1994.
19. Daugman, J. 2003. The importance of being random: Statistical principles of iris recognition. Pattern Recognition. 36, 279-291.
20. Daugman, J. 2007. New methods in iris recognition. Institute of Electrical and Electronic Engineers Transactions on Systems, Man, and Cybernetics. 37, 1167 – 1175.

21. Eyetrackingupdate (2010). Beware of problems with iris recognition. http://eyetrackingupdate.com /2010/11/03/ beware-problems-iris-recognition/ [November 7, 2011]
22. Fancourt, C., Bogoni, L., Hanna, K., Guo, Y., Wildes, R., Takahashi, N. and Jain, U. 2005. Iris recognition at a distance. Proceedings of the International Conference on Audio- and Video-Based Biometric Person Authentication. Hilton Rye Town, New York, U.S.A., July 20- 22, 2005, 1–13.
23. Gonzaga, A. and Dacosta, R.M. 2009. Extraction and selection of dynamic features of the human iris. Proceedings of the XXII Brazilian Symposium on Computer Graphics and Image Processing.
24. Sarajevo, Brazil, October 11-15, 2009, 202-208.
25. Gupta, P., Mehrotra, H., Rattani, A., Chatterjee, A. and Kaushik, A.K. 2006. Iris recognition using corner detection. Proceedings of the 23rd International Biometric Conference, Montreal, Canada, July 16-21, 2006, 1-5.
26. Hanna, K., Mandelbaum, R., Mishra, D., Paragano, V. and Wixson, L. 1996. A system for non-intrusive human iris acquisition and identication. Proceedings of the International Association of Pattern Recognition Workshop on Machine Vision Applications, Tokyo, Japan, November 12-14, 1996, 200-203.
27. He, Y., Cui, J., Tan, T. and Wang, Y. 2006. Key techniques and methods for imaging iris in focus. Proceedings of the 18th International Conference on Pattern Recognition, Hong Kong, September 18, 2006, 557–561.
28. Jain, A.K., Ross, A. and Prabhakar, S. 2004. An introduction to biometric recognition. Institute of Electrical and Electronic Engineers Transactions on Circuits and Systems for Video Technology. 14, 4-20.