Iris Recognition: The Safest Biometrics

Sachin Gupta[1], Dr. Chander Kant [2]

[1]M.Tech. Student, Department of Computer Science and Applications K.U., Kurukshetra, Haryana, INDIA

[2]Assistant Professor, Department of Computer Science and Applications K.U., Kurukshetra, Haryana, INDIA

gupta015@gmail.com, ckverma@ rediffmail.com

Abstract: *In this paper, some successful iris recognition methods are listed and their performances are compared. Furthermore, the existing approaches, challenges and conclusion are described. The purpose of 'Iris Recognition' is to recognize a person from his/her iris image. Every individual has a unique iris. Iris is an important biometric method with high accuracy, performance and low error rate. Iris recognition is one of the most reliable and accurate biometric techniques available.*

Keywords: *Iris recognition, biometrics, enrollment, verification.*

1. Introduction:

Now-a-days, biometric recognition is a common and reliable way to authenticate the identity of a human being based on his physiological or behavioral biometrics [1]. A physiological biometrics traits is stable in their biometric like fingerprint, iris pattern, facial feature, hand geometry, gait pattern etc. whereas behavioral biometric traits is related to the behavior of person such as signature, speech pattern, keystroke pattern. Iris biometric is a new branch of biometric recognition, which is concerns as the most stable, safe and accurate biometric recognition method [2]. Iris recognition

is not a new idea but has only been available in practical application for the last 10 to 12 years. Iris biometric is used for security purposes and is an almost foolproof access security means because of its ability to readily identify false irises [3]. It has not been broadly used because of the cost, but has applications that are ever increasing. Iris biometric will be a vital option for security purposes in the future. Iris biometric depends on the uniqueness of the iris [4]. The unique iris patterns are formed during the six month following birth and do not change till death [5]. Furthermore it is stable with in an individual over a lifetime, each iris remain constants.

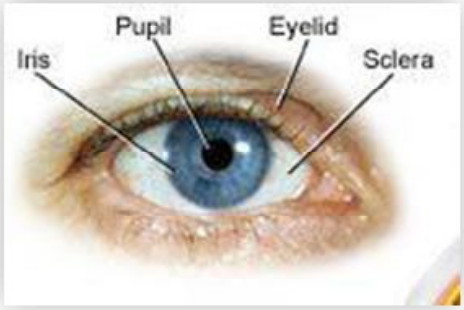

Figure1. Shows the outer structure of the iris

1.1 How Iris Recognition Work?

There are two stages in the iris scanning process for authentication: First stage is known as the Enrollment process, when a person use the iris scanner for the first time to save database that is required for the system to identify that person for later use [6]. The second stage is known as Verification process, when the system actually allows a person to get past after matching the current details with the stored database during Enrollment stage [7].

1.2 Iris Scanner Verification

During the iris verification process, a person just need to stand in front of a iris scanner and get his iris photographed to start this process. The

system is programmed to extract person's iris pattern and match it with the stored database. When it matches, person identified positively.

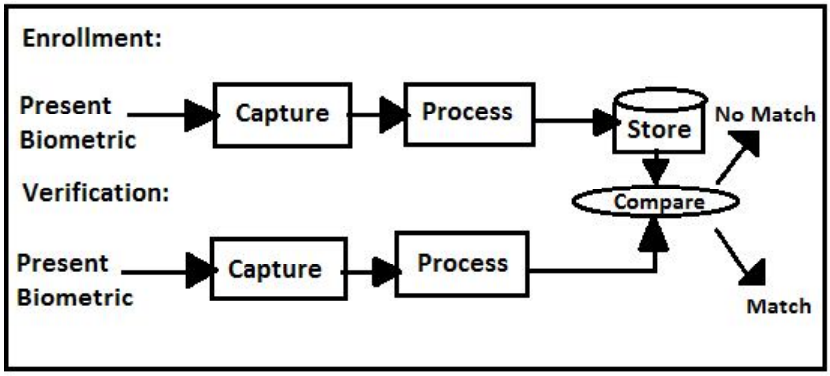

Figure-2. shows the enrollment and verification process

Iris biometrics depends on the uniqueness of the iris. Iris is an important biometric method with very high accuracy and performance. If it compare with other biometric traits, then it is unique in all type of biometrics. The most important benefit of iris biometric is its stability. The iris remains stable for a lifetime because it is not controlled to the environment [8]. The process of iris recognition is a little bit complex. It starts by scanning a person's iris .The person stand in front of a camera for at least one or two second allowing the camera to scan their iris. An algorithm processes the digital image produced by the camera to locate the iris. Once the iris has been located, another algorithm encodes the iris into a phase code that is the 2048-bit binary demonstration of an iris. The phase code is then compared with a database of phase codes looking for a match. For eg. 300 MHz Sun Microsystems processor more than 1,00,000 iris codes can be compared in a single second. In a matter of a one or two seconds a person can have his iris scanned and matched to an iris pattern in a stored database to identifying the person.

1.3 How Iris is Safest Biometric?

Iris recognition is the most accurate biometric technologies in all and there are several other factors in favor of iris recognition applications such as:

1.3.1 Accuracy:

Every iris is perfectly unique. A subject's left and right iris is different from each other as they are from any other person's. It has been calculated that the probability of searching two identical irises is on an almost one in a one million cases [9]. Another different impacting accuracy is that no human interference is required to "set" thresholds for False Accept and False Reject performance. Instead, the human element plays no role in performance standards for this technique; while an unmatched FAR (False Accept Rate) performance of one in one million is delivered [10]. Iris Access system takes over 240 degrees of freedom or unique characteristics in symbolizing its algorithmic template. On the other hand, other biometric traits such as fingerprints, facial recognition and hand geometry have far less detailed input in template construction as compared to iris biometric. In fact, it is probably fair to say that one iris template contains more data than is collected in creating templates for a finger, a face and a hand combined. This is one important reason why iris recognition can use with confidence.

1.3.2 Stability:

Stability is the most important feature in case of iris biometric. Other biometric traits such as fingerprints, facial recognition, hand geometry are changes significantly over time. Reenrollment is required in case of other biometric traits. Voice change. Hands and fingers grow. The type of labor one does, even weather temperature or one's medical condition can result in template changes in other technologies. But in case of iris biometric, the patterns in the iris are constant from age 1 to death [11].

1.3.3 Fast:

Iris recognition method is very fast as compared to other biometric techniques. It takes only one or two seconds in their working and represents

accurate and high performance results. In contrast, fingerprint technique takes more time to search from database and it also takes more space in memory to store the database for a single person. Iris biometric technology is designed to deliver 1:N searching of large databases in real time [12]. Looking at speed in conjunction with accuracy, there's simply no other technology that can deliver high accuracy authentication in anything close to the real-time performance of iris recognition.

Table1: Performance comparison of various Biometric Traits.

Characteristics / Biometric Traits	Universal	Unique	Permanence	Collectable	Performance	Acceptability	Potential to fraud
Face	High	Low	Medium	High	Low	Low	Low
Fingerprint	Medium	High	High	Medium	High	Medium	Low
Iris	**High**	**High**	**High**	**Medium**	**High**	**Low**	**Low**
Signature	Low	Low	Low	High	Low	High	High
Voice	Medium	Low	Low	Medium	Low	High	High
Vein	Medium	Medium	Medium	Medium	Medium	Medium	Low

1.3.4 Scalable:

In case of iris biometric, very large databases can be managed and speedily searched without demotion of performance accuracy [13]. For eg. Iris Recognition and the Iris Access 3000 are ideal for large-scale ID applications or enterprise physical security and applications characterized by large databases. As iris data templates require only 512-bytes of storage per iris.

2.1 Error Rate of Iris Biometric:

The accuracy of the system in identifying and verifying enrolled users is described by:

- False Match Rate (FMR)
- False Non-match Rate (FRR).

The FAR, also known as False Match Rate describes the number of times when a person inaccurately positively matched. On the other hand, the FRR, also known as a False Non-Match Rate describes the number of times when a person should be identified positively is instead rejected. Both error rates are interdependent –if one rate raises the other rate sinks. The crossover rate, or the equal error rate, is the intersection of the rate of these two events. Lower the crossover rate, the better the rating of the biometric system.

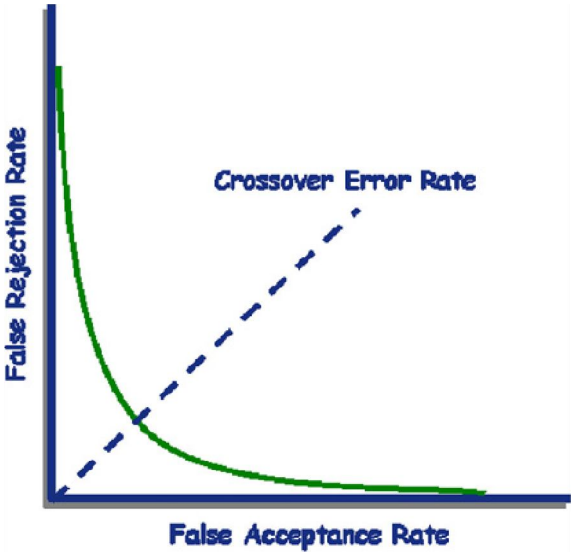

Figure 3. shows equal error rate

The configuration of these error rates must depend on the security requirements. Very high security requires a low FAR even if the FRR is high [16]. Entitled users can be rejected by mistake or need several identification procedures, before the system accept them. Iris recognition, compared to other biometrics technologies, has the lowest FAR and FRR. As the following

graph shows, iris recognition is constantly above 1% in the FAR and constantly at 0.00001% at FRR.

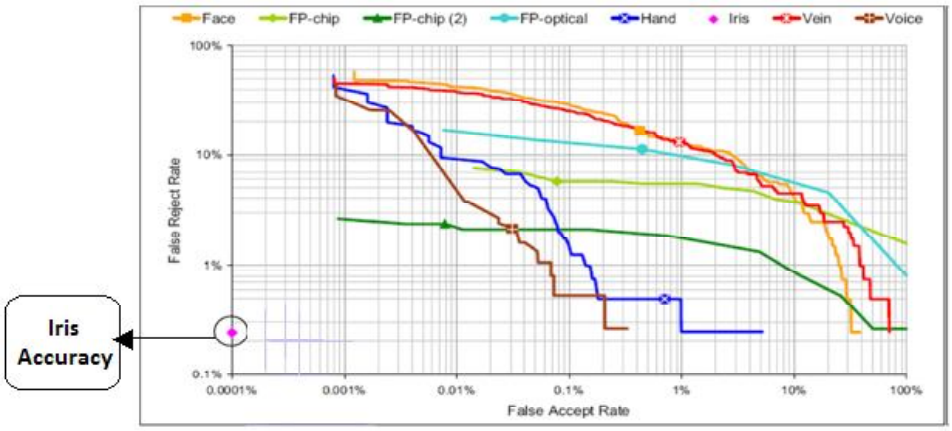

Figure-4.Detection error trade off: FAR vs. FRR.

2.2 Challenges of Iris Recognition:

There are still barriers to acceptance of iris scanning as a complete replacement for other types of biometrics:

1. The cost is very high. This is a big jump over most fingerprint solutions.
2. The sensors are somewhat cumbersome to place on a users desk for a second factor for system login [17]. Although many vendors do supply a USB cable for PC connectivity, this technology looks like it will be relegated to physical security applications in the short term.
3. One of the greatest challenges the country is faced with is the repeated attempts of former expellees to re-enter the country (foreign nationals expelled for various violations). Various control measures were implemented to detect such cases. However, these measures appeared to be inadequate to control and detect the return of deportees back in the country.

3. Conclusion and Future Scope:

Based on the performance, applications, reliability, ease of use, software and hardware devices that currently support it, iris recognition technology has potential for widespread use. Iris recognition technology cost comparably much better with many other biometric traits. Iris recognition is the most secure biometric technology available [18]. Iris recognition removes the need for physical contact with the biometric measure device and is used for both verification and identification process. Iris recognition technology has advantage over other type of biometric technologies, due to its low error rate (FAR and FRR) [19]. Iris recognition has made great strides in the last 10 years. It scores well compared to the other biometric technologies, both in ease of use and in reliability [20]. It has not been broadly used because of the cost, but has applications that are ever increasing. Iris biometric will be a vital option for security purposes in the future.

4. References:

[1] Jain,A.K.,Bolle,R. and Pankanti, S., Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers,1999, p.37.

[2] Woodward, N.M. Orlans, and P.T. Higgins, *Biometrics*, The McGraw-Hill Company, Berkeley, California, 2002.

[3] Henahan, Sean. (2002). *The Eyes Have It*. Retrieved November 14, 2005.

[4] R.P.Wildes, “Iris Recognition: An Emerging biometric technology” Proceeding of the IEEE, vol. 85, pp. 1348-1363, Sep 1997.

[5] L. Ma, T. Tan, Y. Wang, D. Zhang (2003). Personal Identification Based on Iris Tecture Analysis, *IEEE Patt. Anal. Mach. Intell.,* number 25, pp. 1519-1533.

[6] Daugman, J. (2009) How iris recognition works, Chapter 25 in: The essential guide to image processing, by Bovik, A., Edited by: Elsevier BV.

[7] Jain, A.; Nandakumar, K. and Ross, A. (2005) Score Normalization in Multimodal Biometric Systems, Pattern Recognition, vol. 38(12), 2270–2285

[8] C. Tisse, L. Martin, L. Torres, M. Robert (2002). Person Identification Technique Using Human Iris Recognition, *Proc. Vision Interface*, pp. 294-299.

[9] J. Dougman (2003). The importance of being random: Statistical Principles of Iris recognition, *Pattern recognition*, number 36,pp. 279-291.

[10] Z. Sun, T. Tan, and X. Qiu, "Graph Matching Iris Image Blocks with Local Binary Pattern," Advances in Biometrics, vol. 3832, pp. 366-372, Jan. 2006.

[11] J. Dougman (2004). How Iris Recognition Works, *IEEE Transactions on Circuits and Systems for Video Technology*, number 14, pp. 21-30.

[12] Cui J L, Wang Y H, Tan T N, et al. A Fast and Robust Iris Localization Method Based on Texture Segmentation[C]. In Proceeding of SPIE, Bellingham, WA, 2004, 5404: 401-408.

[13] J. Wayman, A. Jain, D. Maltoni, and D. Maio, Biometric Systems. Springer, 2005.

[14] Chander Kant, Sheetal Verma "Web security using Biometrics" published in National Conference on Total Quality Management held at Vaish College of Engg, Rohtak 10th March 2007.

[15] Chander Kant, Rajender Nath, Sheetal Chaudhary "Biometrics Security using Steganography" published in CSC online Journal "International 150 Journal of Security" Malashiya Vol-II Issue-I, PP 1-5 2008.

[16] P. J. Phillips, W. T. Scruggs, A. J. O'Toole, P. J. Flynn, K. W. Bowyer, C. L. Schott, M. Sharpe (2007). FRVT 2006 and ICE 2006 Large-Scale Results.

[17] Mansfield, A.J., Kelly, G.,Chandler, P. and Kane, J. "Biometric product testing final report",May 2003.

[18] Jain, A.K., Pankanti, S. and Prabhakar S., "Biometric recognition: security and privacy concerns", *IEEE Security and Privacy*,March/ April 2003, pp. 33-42.

[19] S. Kanade, D. Petrovska-Delacretaz and B. Dorizzi, "Cancelable iris biometrics and using error correcting codes to reduce variability in biometric data," *Computer Vision and Pattern Recognition (CVPR)*, 2009.

[20] Makram Nabti, Ahmed Bouridane, "An effective and fast iris recognition system based on a combined multiscale feature extraction technique", Pattern Recognition, 41 (2008), pp. 868 – 879.