Brazilian Journal of Forensic Sciences, Medical Law and Bioethics

Journal homepage: www.ipebj.com.br/forensicjournal

Iris patterns as a Biometric tool for Forensic Identifications: a Review

Jagmahender Singh Sehrawat[1,2], Deeksha Sankhyan[2]

[1] *Institute of Forensic Science and Criminology, Panjab University, Chandigarh, India*

[2] *Department of Anthropology, Panjab University, Chandigarh India*

Abstract: Human biometric features are considered unique, permanent, measureable and objective traits used as authentic tools for identification of an individual. Biometric authentications are increasingly utilized for identifying a genuine user or an imposter. The automated iris pattern recognition is based on the unique, non-intrusive and un-imitable micro-features of human iris. Several mathematical and statistical algorithms have been suggested for extracting and encoding iris minutiae used for pattern recognitions in automated systems. Iris scanning is an easy and non-invasive technique, having comparatively lower false acceptance and rejection rates and negligible chances of manipulations and spoofing. Despite of some limitations, iris recognition is considered a promising advancement in forensic sciences. Present review has presented the iris recognition knowledge in nutshell to the readers.

Keywords: Forensic identifications; Biometry; Iris patterns; Advantages and limitations; Review.

1. Biometric identification

Absolute personal recognition is effectively required in many applications like secure access to buildings, sensitive premises (i.e., nuclear reactors, defense establishments) laptops, cellular phones, computer systems, ATMs etc. Biometric recognition or, simply, biometrics is the automatic recognition of individuals based on their physiological and/or behavioral characteristics like fingerprints, face, hand geometry, retina, ear, iris, speech, voice, signatures, handwriting, gait etc[1]. A biometric system first captures the data, removes the redundant features, constructs a template and compares it with other templates from a database in order to verify or identify an individual. Diversification of crime, criminal and criminality has invited the focussed

http://dx.doi.org/10.17063/bjfs5(4)y2016431

attention of scientific community in recent years. Biometry is an emerging scientific modality that has simplified the authentication and identification procedures to a greater extent. The personal identification based on some biological markers of identity is an important field of biometrics which can authorize or authenticate a person from an imposter effectively. Biometrics can provide the most accurate and highly secured identification and verification systems with multiple applications[2]. The authentication via biometric verification is becoming increasingly common in security applications such as homeland security, banking, border control, access control, web-based services, welfare distribution schemes, forensics etc. Several biometric modalities have been suggested for the secured forensic applications, though each one has its own advantages and limitations. No single biometric feature can meet all the performance requirements of a system[3;] so use of multimodal biometric systems has been advocated to overcome the limitations of unimodal means of identification. The emergence of biometry and the computer technology is taken to be contemporary during second half of twentieth century. Rapid developments in computer technologies, computational capabilities and computing approaches have fantastically improved upon the image capturing process, feature extraction, feature robustness, and feature comparisons[2]. Biometric features of a person are very difficult to be forged, imitated, lost, transferred or stolen and the security systems based on such human traits require the presence of a genuine user for getting access to a particular resource.

Biometric identity signatures include some unique physical, physiological and behavioral attributes, also known by the names like biometric traits, indicators, identifiers or modalities. Physical attributes of biometry include some prints (fingerprints, footprints, lip prints, ear print), scans (facial scan, retinal/iris scan, MRI/CT scan), body odors, vein-networking etc., whereas the behavioral elements may include the voices, handwritings, signatures, typing patterns, gait patterns etc. Biometric authentications have been widely utilized by a number of government (border crossing, airport security, passport control, welfare distribution schemes, driving licenses), commercial (access control, ID cards, e-commerce, cellular phones, credit cards) and investigative/forensic (corpse identification, criminal investigation, terrorist identification, missing person identifications etc.) organizations/establishments. Rapidly growing incidents of criminal

and terrorist activities, particularly at public places (most recently in France, Dhaka and Orlando shootings and Brussels airport explosions), have necessitated the introduction of some more advanced security and surveillance systems to replace the traditional and obsolete methods[4]. The uniqueness, permanence, measurability, performance, acceptability, universality, and low circumvention are the important characteristics of a biometric trait to make it suitable for forensic identifications[5], and Iris pattern recognition is one of forensic modality having all these characteristics which can work even in non-ideal situations[3].

Present review article has been written with an intention to provide an in-depth and nutshell overview of iris recognition as a biometric tool of recognition to the readers. The conclusive information presented in some recently published studies was integrated to present the current status of iris pattern recognition as a forensic tool. The related articles published in some journals and books were searched through online search engines like Pubmed, Scopus, Embase, Web of Science etc., and, the information regarding uses, advantages, limitations, algorithms developed, and future probabilities of iris pattern recognitions and biometry as a whole were extracted out to present this review.

2. Iris recognition as a forensic tool

The ocular region of human eye possesses the most accurate, highly reliable, well protected, fairly stable and almost unforgable biometric signatures like iris, retina and sclera vein patterns; the iris being the most significant among them[6-7]. Iris recognition is based upon its unique and stable textured features like crypts, furrows, nevi, corona and freckles[7-8]. It analysis the random patterns of the iris by mathematical pattern recognition algorithms or techniques. The automated iris pattern recognition is among the most recent biometric methods having tremendous potential as an infallible mode of personal identification, especially at high security areas like airports, nuclear reactors, embassies, parliaments, immigration controls etc. Iris patterns can also be used in airport check-in, criminal identification, access control, computer logins, e-commerce, welfare disbursements, missing children identification, passports, time and attendance monitoring systems etc.[4] Iris pattern acquisition is one of the important attributes

included in the unique identification number called '*Aadhaar* number' given to every Indian citizen. It has been widely utilized in various critical application areas because of its unique, stable and non-invasive characteristics.

Iris is an eye muscle that regulates the size of the pupil to control the amount of light entering the eye and its coloration pattern depends upon the amount of melanin pigment present in it[9-10]. Iris is a multi-layered structure lying in front of the crystalline lens and the ciliary body which separates the anterior and posterior chambers of eye. It is present in the form of a truncated cone possessing unique and random features like freckle, coronas, crypts, furrows, pigments, blood vessels etc[9,11, 12] (Figure 1). Such randomly distributed and irregularly shaped micro-structures of human iris (i.e., minutiae) start developing early intra-uterine life, though it fully develops within a month after birth[5, 3-15].

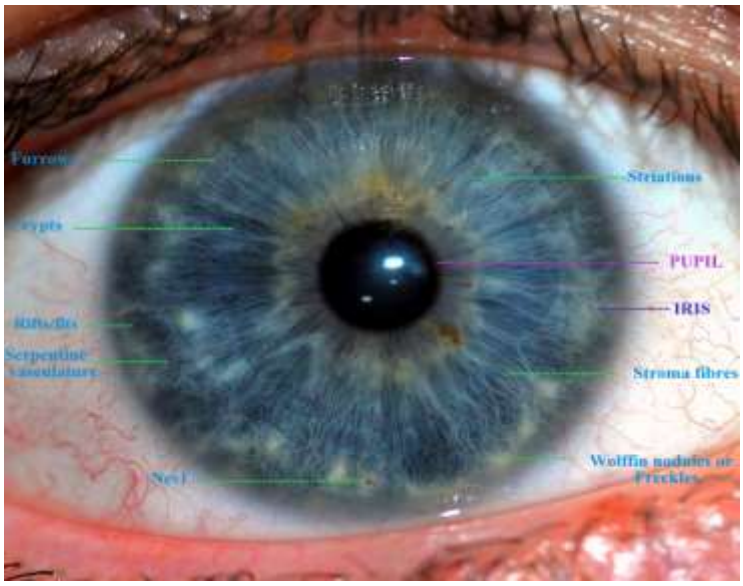

Figure 1. Iris minutiae and features

Iris recognition is an accurate, fast, easy to use, non-intrusive and inimitable or unforgable mean of authentication and identification that can replace current methods of passwords, token cards, pin numbers, OTPs etc. Unique features of iris make it one of the most secured methods of authentication, having negligible false acceptance and rejection rates pattern imitations etc., [16-18]. The distinctive features of iris are colour, radial trabecular meshwork, contraction furrows, coronas, serpentine vasculature,

striations, freckles, rifts, fits, etc., (Figure 1), which remain unaffected from the ageing process of a person [6-8]. More accurate scanning devices have provided higher accuracies to iris recognition as a mean of authentication within minutes. The deliberate disfigurement or distortion of iris images is almost impossible which further increases its reliability and stability as one of the most informative biometric modalities[19]. In 1936, Frank Burch was the first to propose that iris color and its patterns are unique to each and every individual which can be used for recognition purposes. No two irises are alike, even in identical twins or two side eyes of the same person[20].

Iris identification methods can be classified into three main categories i.e., Wavelet transformation and canny edge detection, Hamming distance, Eigen values and Eigen vector based iris matching methods[21]; the latter two methods have better robustness and accuracy than the first method. The unique iris patterns can be extracted from a digitalised eye image by using some image processing techniques. Such patterns can be encoded into a biometric template (a mathematical representation of unique iris patterns) to be stored in a database which allows comparisons between different templates. Some mathematical and statistical algorithms have been used to encode the digital templates for identification of genuine individuals or the imposters. John Daugman (1987) developed the first mathematical algorithm to automate the identification of iris. A number of encoding and processing algorithms have been developed to automate iris minutiae [3, 8, 12-13, 15, 22-23] since then. Few of such methods and algorithms are IrisScan, Iridian, IrisGuard, Oki, Morpho, MASEK, VASIR, OSIRIS etc., which are based on the morphology, distance transform, Gaussian filters, Gabor filters, and neural networks etc., of the iris. However, no universal algorithm has been validated till-date to place iris recognition suitably among other biometric identification methods. Nabti and Bouridane[15] have proposed a multi-scale approach for effective iris region localization and to ensure its increased accuracy and performance.

3. Iris recognition process and its advantages

The basic iris recognition process involves four steps i.e., image acquisition, iris feature extraction, iris pattern matching and digital representation[11-12, 15]. Acquisition involves capturing the full digitalized image of the eye, preferably from a distance ranging from 10 cm to 1 m. The visual and infrared lights used in camera help in capturing unique minute details of iris and in isolating the iris from pupil, respectively; though the combination of these two types of lights are suggested to provide much better results[18, 24]. Iris patterns as a forensic tool have an edge over the other means of biometric identifications due to certain reasons. Iris scanning is an easy and non-invasive technique (as iris remains well protected within layers), have lesser chances of its manipulations or spoofing[9, 11, 15]. Iris patterns have small intra-class variability and high degree of randomness. Unlike retina, iris does not get decomposed immediately after death and hence can be utilized for corpse identification up to certain hours after death. Trokielewicz et al[25] reported that more than 90% iris images captured few hours after death (under mortuary conditions) were still correctly recognizable and the serious iris deterioration begun approximately 22-hours post-mortem. Thus, human iris can be successfully used for biometric authentication even after death, though within certain limited period. The richness of texture details in iris images enhances its suitability for forensic identifications[15]. Iris patterns don't get altered even after surgical operation of eye; and also the use of eyeglasses or contact lenses do not interfere in iris pattern recognitions[11, 14, 18]. Iris matching is possible even for blind people having their iris intact[18]. Researchers have shown that the iris scans have comparatively low false acceptance and rejection rates[14, 22], so iris methods are preferred for security management of highly secured areas.

4. Limitations of iris patterning as a biometric modality

Iris, itself, is a very small organ to be scanned from a distance. Iris recognition is a challenging task to be performed with desired accuracy from a distance larger than a few meters. Some factors which may discourage scanning process for iris pattern recognition include the illumination and contrast differences, inadequate image quality, occlusion of eyelids and eyelashes, non-linear deformations, rotation differences,

defocus, reflective surfaces, stop and stare interface of cameras, advancing age changes like drooping eyes etc.[8-9, 11, 121-13, 23, 26]. Intensive exposure to environmental contaminants like pollutants, metal vapors, smoke etc., may affect iris pigmentations and its discrimination capabilities[11]. Diseases like cataract, iritis, iridocyclitis, diabetes etc., may also affect iris scanning[13]. Some medical and surgical procedures often affect the overall shape and colour of an iris; however, the fine structure details of iris remain intact for many decades. Iris recognition requires extremely dedicated arrangements for imaging and sufficient cooperation from the user/subject. Venugopalan and Savvides[27] reported that development of spoofed iris, accurately identical to actual iris, is also possible. To make iris recognition a human-friendly technique (especially for forensic purposes), the similarities between irises should be made visualizable, interpretable and explainable[28]. Benaliouche and Touahria[22] found that iris and fingerprints have the same matching speed and accuracy, however, multimodal approach may give better results for recognition process with lower errors. Inspite of various limitations and problems discussed above, iris scan may be taken as a promising advancement in the forensic contexts as well in industry for commercialization purposes.

5. Conclusions

The iris pattern recognition is relatively a very recent biometric modality that can contribute significantly in forensic identifications of an individual. Human iris patterns are unique, permanent, un-imitable, measureable and universal features that ensure their use as an objective biometric modality. The unique features of iris make it one of the most secured methods of authentication. There are some advantages and inherent difficulties using iris patterns as infallible mean of identification, however, the use of iris patterns for authentication and identification purposes has a tremendous scope in forensic sciences. The scientific community is continuously involved in research to develop a universal iris-based algorithm that may help its unanimous acceptance as a biometric tool for authentication and identification. Iris patterns remain stable for few hours after death and hence can be valuable adjunct for identification of a recently dead person, if other features don't allow the same. Being a comparatively newer technology, extensive testing and research is required before confirming use of iris patterns at

higher levels of security. The use of single biometric trait/marker is, often, prone to spoofs or imitations, so a multi-modal biometric system having more objectivity, reliability and legal acceptability is suggested for forensic identifications.

References:

1. Rahulkar AD, Holambe RS. Iris image recognition: wavelet filter-bank based iris feature extraction schemes.Springer; London. pp. 1-22
2. Awad AI, Hassanien AE. Impact of some biometric modalities on forensic science. In: Muda AK, Choo YH, Abraham A, Srihari SN (eds). Computational intelligence in digital forensics: investigation and applications, Studies in computational intelligence; Springerlink; 2014. p. 47-62.
3. Zhou Z, Yingzi D, Belcher C. Transforming traditional iris recognition systems to work in non-ideal situations. IEEE Transactions on Industrial Electronics 2009; 56 (8): 3203-3213. http://dx.doi.org/10.1109/TIE.2009.2024653
4. Unar JA, Seng WC, Abbasi A. A review of biometric technology along with trends and prospects. Pattern Recognition 2014; 47: 2673-2688. http://dx.doi.org/10.1016/j.patcog.2014.01.016
5. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology 2004; 14(1): 4-20. http://dx.doi.org/10.1109/TCSVT.2003.818349
6. Daugman J. High confidential visual recognition of persons by test of statistical independence. Pattern Anal. Mach. Intel. IEEE Trans.1993; 15(11):1148–1161. http://dx.doi.org/10.1109/34.244676
7. Daugman J. How iris recognition works. IEEE Trans.Circuits Syst.Video Technol. 2004; 14:21–30. http://dx.doi.org/10.1109/TCSVT.2003.818350
8. Daugman, J. New Methods in Iris Recognition. IEEE Transactions on Systems, Man and Cybernetics 2007; 37(5): 1167-1175. http://dx.doi.org/10.1109/TSMCB.2007.903540
9. Blythe P, Fridrich J. Secure Digital Camera. In proceedings of Digital Forensic Research Workshop (DFRWS), Baltimore, MD, 2004.
10. Yoon S, Choi SS, Cha SH, Lee Y, Tappert CC. On the individuality of iris biometric. ICGST-GVIP J. 2005; 5(5): 63-70. http://dx.doi.org/10.1007/11559573_135
11. Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication. IBM Systems J. 2001; 40(3): 614-634. http://dx.doi.org/10.1147/sj.403.0614

12. Sun Z, Zhang H, Tang T, Wang J. Iris image classification based on hierarchical visual codebook. IEEE Transactions on Pattern Analysis and Machine Intelligence 2014; 36(6): 1120-1133. http://dx.doi.org/10.1109/TPAMI.2013.234
13. Wildes RP. Iris Recognition: an emerging biometric technology. Proceedings of IEEE 1997; 85(9): 1348-1363. http://dx.doi.org/10.1109/5.628669
14. Jain AK, Ross AA. Introduction to biometrics. In: Jain AK, Flynn P, Ross AA (eds.); Handbook of Biometrics: Springer-Verlag; 2008. P.1-22. http://dx.doi.org/10.1007/978-0-387-71041-9_1
15. Nabti M, Bouridane A. An effective and fast iris recognition system based on a combined multi-scale feature extraction technique. The Journal of Pattern Recognition Society 2007; 41: 868-879. http://dx.doi.org/10.1016/j.patcog.2007.06.030
16. Ghosh P, Rajashekharbabu M. Authentication using iris recognition with parallel approach. Inter J Comp Sci Network Sec. 2013; 13(5): 87:93
17. Prasad R, Shinde S, Khobragade SV. An Iris Authentication: Best Method of Biometric Authentication. Inter J Engg Res Tech. 2014.; 3(5):1490-1493
18. Adebisi S. Contemporary Tools in Forensic Investigations: The Prospects and Challenges. The Internet J Forensic Sci. 2008; 4(1): 1-8
19. Zuo J, Ratha NK, Connell JH. Cancelable iris biometric: pattern recognition. 19th International Conference on Pattern Recognition (ICPR), December 8-11, 2008, Tampa, Florida, USA
20. Proenca H, Alexandre LA. Towards covert iris biometric recognition: experimental results from NICE Contests. IEEE Transactions on Information Forensics and Security 2012; 7(2): 798-808. http://dx.doi.org/10.1109/TIFS.2011.2177659
21. Bowyer KW, Hollingsworth K, Flynn PJ. Image understanding for iris biometrics: a survey. Computer Vision and Image Understanding, Elsevier, 2008 (110): 281-307
22. Benaliouche H, Touahria M. Comparative study of multimodal biometric recognition by fusion of iris and fingerprint. The Scientific World J. 2014;6: 1-13; http://dx.doi.org/10.1155/2014/829369.
23. Virginia RA, Pedro TG, Fernando AF, Galbally J, Fierrez J, Javier OG. Direct attacks using fake images in iris verification. In: Virginia RA, Pedro TG, Fernando AF, Galbally J, Fierrez J, Javier OG (eds); Biometrics and Identity Management 181-190.
24. Hosseini MS, Araabi BN, Hamid SZ. Pigment melanin: pattern for iris recognition. IEEE Transac Instr Measut 2010; 59 (4): 792-804. http://dx.doi.org/10.1109/TIM.2009.2037996

25. Trokielewicz M, Czajka A, Maciejewicz P. Post-mortem human Iris recognition. 9th IAPR International Conference on Biometrics (ICB 2016), June 13-16, 2016, Halmstad, Sweden. http://dx.doi.org/10.1109/icb.2016.7550073
26. Belcher C, Yingzi D. A Selective Feature Information Approach for Iris Image-Quality Measure. IEEE Trans Infor Forensics and Secu. 2008; 3(3): 572-577. http://dx.doi.org/10.1109/TIFS.2008.924606
27. Venugopalan S, Savvides M. How to generate spoofed irises from an iris Code template. IEEE Trans Infor Forensics and Secu. 2011; 6(2): 385-395. http://dx.doi.org/10.1109/TIFS.2011.2108288
28. Chen J, Shen F, Chen DZ, Flynn PJ. Iris recognition based on human-interpretable features. IEEE Trans Infor Forensics and Secu. 2016; 11(7): 1476-1485. http://dx.doi.org/10.1109/TIFS.2016.2535901