[Reddy et. al., Vol.6 (Iss.1): January, 2018]
(Received: Jan 11, 2018 - Accepted: Jan 23, 2018)
ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.29121/granthaalayah.v6.i1.2018.1596

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

IRIS TECHNOLOGY: A REVIEW ON IRIS BASED BIOMETRIC SYSTEMS FOR UNIQUE HUMAN IDENTIFICATION

Dr M V Bramhananda Reddy [1], Dr V Goutham [2]
[1, 2] Professor, Computer Science & Engineering, Sreyas Institute of Engineering & Technology, JNTUH, Hyderabad, India

Abstract

Biometric features are widely used in real time applications for unique human identification. Iris is one of the physiological biometric features which are regarded as highly reliable in biometric identification systems. Often iris is combined with other biometric features for robust biometric systems. It is also observed that biometrics is combined with cryptography for stronger security mechanisms. Since iris is unique for all individuals across the globe, many researchers focused on using iris or along with other biometrics for security with great precision. Multimodal biometric systems came into existence for better accuracy in human authentication. However, iris is considered to be most discriminatory of facial biometrics. Study of iris based human identification in ideal and non-cooperative environments can provide great insights which can help researchers and organizations that depend on iris-based biometric systems. The technical knowhow of iris strengths and weaknesses can be great advantage. This is more important in the wake of widespread use of smart devices which are vulnerable to attacks. This paper throws light into various iris-based biometric systems, issues with iris in the context of texture comparison, cancellable biometrics, iris in multi-model biometric systems, iris localization issues, challenging scenarios pertaining to accurate iris recognition and so on.

Keywords: Security; Biometrics; Iris Recognition; Iris-Based Biometric Systems.

Cite This Article: Dr M V Bramhananda Reddy, and Dr V Goutham. (2018). "IRIS TECHNOLOGY: A REVIEW ON IRIS BASED BIOMETRIC SYSTEMS FOR UNIQUE HUMAN IDENTIFICATION." *International Journal of Research - Granthaalayah*, 6(1), 80-90. https://doi.org/10.29121/granthaalayah.v6.i1.2018.1596.

1. Introduction

Biometrics is an automated approach which exploits measurable physiological, physical and behavioural traits of humans for identification and authentication. Physiological and behavioral are the two categories in biometrics. The former refers to hand and palm geometry, DNA, face, iris, scent signature, keystroke dynamics and fingerprints while the latter refers to voice, gait, and typing rhythm. The real world applications of biometrics include detection and border security,

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

fraud prevention, crime tracking, security, payment systems, attendance recording, physical and logical access controls, and identification of parties or individuals in general [28], [29]. Biometrics is one of the best ways in which individuals can be identified uniquely across the globe. Biometrics can be used in cryptography to secure communications in the real world networks [1].

Biometric templates when compromised, the security will be lost. To overcome this problem, cancellable biometrics approach came into existence [3], [20], and [30]. Hamming Distance Classifier (HDC) for predicting false rejection rate (FRR) and false acceptance rate (FAR) based on the hamming distance threshold was proposed [4]. Ocular biometrics was given importance by Simona and Arun [5].Studies were made on iris and face as biometric features to protect communications in mobile devices [6]

It was noted from the literature that studies were made on binary iris code for reconstruction of original iris image [7]. Investigations on iris and fingerprints together for human identification were also carried out [8]. It is focused on the UID project in India named "Aaadhar". The investigations dealt the issues with biometric systems in the wake of security attacks on multi-model biometric systems [9, 10, and 19]. Iris localization is very important activity in commercial iris recognition systems. However, they could not perform well with ideal data as they work for controlled data. Many iris localization experiments were performed [11-15]. Lee et al. [16] made sensitivity analysis on biometric systems in the wake of attacks on such systems that help in finding the robustness of biometric system. Combination of combined error correction codes and finger prints [17]; multi-model biometric system using face and iris combination [18], SVM and feature selection techniques [21], Circular Hough Transform and K-Means algorithm [21], combination of different approaches [22] were used for iris recognition. Reverse bio-orthogonal wavelet transform technique was used for reliable iris recognition [24].

Iris hazards in the presence of noise were explored [25]. Pattern recognition and its importance in iris-based biometric system were presented by Unar et al. [26] while Zhu et al. [27] used iris based biometric system for random number generator. Iris based biometric system has become one of the most active search field sand it is driven by many applications towards authentication sand recognitions of an individual identity. From the above literature, it can be noted that limited studies were carried out on Iris Based Biometric Systems for Unique Human Identification.

In this paper, the concept and some of the important biometric systems which are Iris based are deliberated along withthe security issues of the iris based human identification systems.

The remainder of the paper is structure as follows. Section II reviews iris templates and cancellable biometrics. Section III focuses on biometric binary strings. Section IV throws light on multi-model biometrics. Section V presents GA for iris reconstruction. Section VI focuses on security issues with biometric systems. Section VII and VIII discuss about iris localization and iris recognition systems. Section IX concludes the paper.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

2. Iris Templates and Cancellable Biometrics

There is a study on iris-templates for crypto-biometric schemes as in [1]. This scheme helps users to get secret keys by using her biometric template. Fuzzy extractors are used to make the scheme robust. The scheme has both enrolment phase and verification phase. The enrolment ensures polynomial security and verification phase, also has polynomial complexity, and takes care of verifying the identity of users. Few authors focused on functional dual tree complex wavelet for biometric security and its applications include transient signal processing, image transmission, image compression and biometrics.

Biometric templates when compromised, the security will be lost. To overcome this problem, cancellable biometrics approach came into existence. This will take care of transformation functions in order to hide the original template. In this case the transformed biometric template when compromised, the original template can be used to make newtransformation [30]. Towards cancellable biometrics as in [3] studied different fusion approaches in order to achieve cancellable recognition with multi-biometrics. They focused three cancellable transformations on two biometric modalities based on iris and voice. There is a methodology used for cancellable biometrics approach which is as shown in Figure 1. Two modalities are demonstrated with two biometric templates.

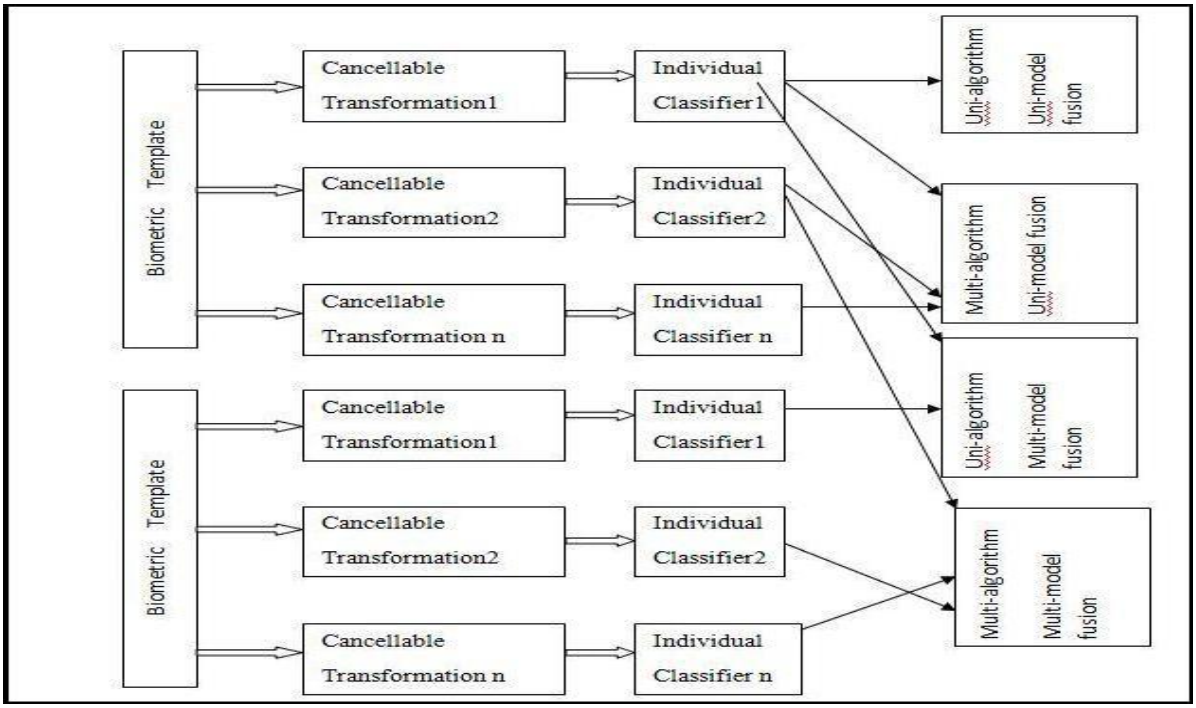

Figure 1: Overview of methodology for cancellable biometrics [3]

Void and iris datasets are used to make experiments. For transformations, three techniques are used namely convolution, interpolation, and bio-hashing. When compared, the interpolation has proved to be more accurate. Overall performance is improved when Sum or SVM techniques are used in all the cases analysed. With different fusion approaches, multi-biometric cancellable recognition was achieved. The results revealed that using multiple transformations can improve

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

the robustness of the cancellable biometrics approach. In both the template cases, the cancellable transformations are generated and then multiple individual classifiers are generated. Finally multi-algorithm and multi-modal fusion is used for final transformation [3]. There is a study [20] on cancellable multi-biometrics based on adaptive bloom filters and iris codes.

3. Biometric Binary Strings

Hamming Distance Classifier (HDC) for predicting False Rejection Rate (FRR) and False Acceptance Rate (FAR)

Based on the hamming distance threshold was proposed [4]. The proposed approach can be used in the real world biometric modalities such as face, signature, and iris and fingerprint texture. Moreover, they proposed a template protected biometric authentication system.

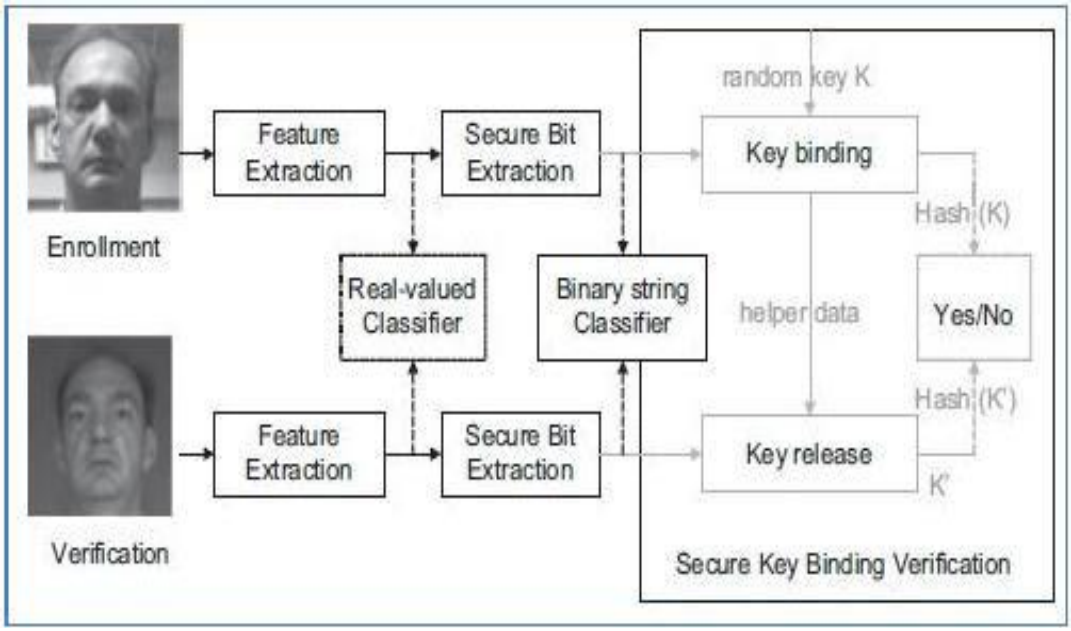

Figure 2: Overview of template protected biometric verification system [4]

As can be seen in Figure 2, it is evident that there are two phases such as enrolment and verification. In either case, feature extraction is made and real-valued classifier is built. There are two important modules such as secure bit extraction and secure key binding verification. The former module is used for transforming real-valued features into a binary string which is further used in secure key binding verification. The latter module is meant for verification of the protected target biometric string. Such string is bound with cryptographic key for highest level of security [4].

4. Multi-Model Biometrics

There is studied iris and face as biometric features to protect communications in mobile devices [6]. As the mobile devices are vulnerable to various attacks, authentication with iris and face could prevent them. They built a mobile management system using biometrics which is

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

embedded in mobile devices. This solution can also be used in security-critical applications in the real world. Their system is named FIRME which has the architecture as presented in Figure 3.

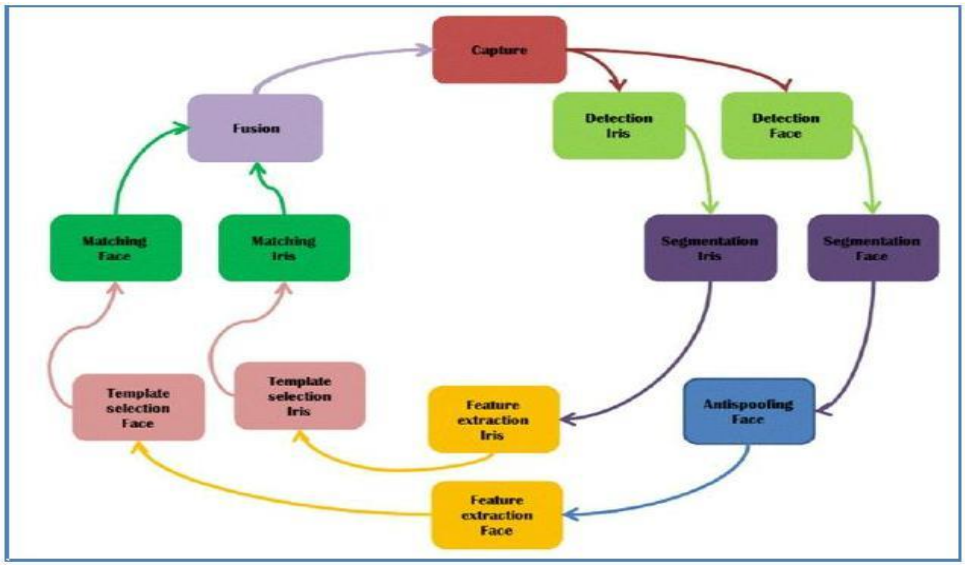

Figure 3: Combination of iris and face for recognition [6]

As can be seen in Figure 3, it is evident that there are many phases for modelling face and iris and fusing them for recognition. The phases include capture, detection of iris, detection of face, segmentation of iris, segmentation of face, feature extraction of iris, anti-spoofing of face, feature extraction of face, template selection for iris and face, matching of iris and face and fusion. With the help of the two models and fusion, the system is able to recognize humans live. There is a framework focused on biometric systems for mobiles using data mining techniques and ECG based identification [23]. There is studied [8] iris and fingerprints together for human identification. They focused on the UID project in India named "Aaadhar". The combination of iris and fingerprints make the system robust and can uniquely identify humans across the globe.

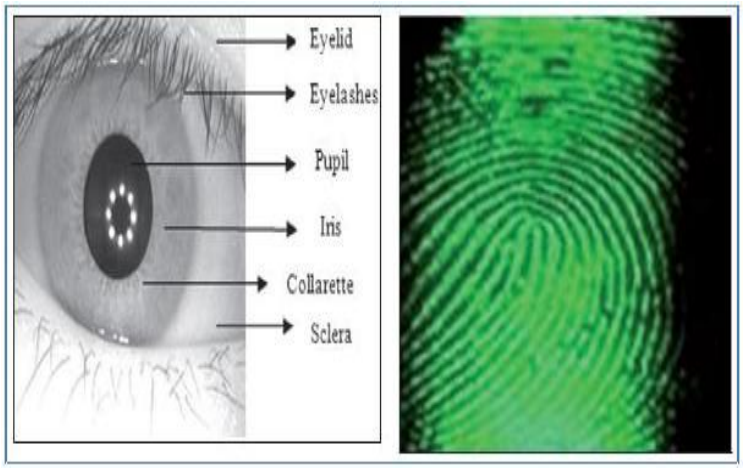

Figure 4: Combination of iris and fingerprint for biometric security [8]

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

From Figure 4, it can be assumed that the iris of human eye and fingerprints together form a basis for high security in human identification. The fusion of these two is challenging for feature selection. However, many real world systems are using the combination of both. For finding similarity in trained and testing samples two distance measures such as Mahalanobis distance and Euclidean distance are used. Thus the identity of a person can be established.

5. GA for Iris Reconstruction

There is a framework [7] used binary iris code for reconstruction of original iris image. Probabilistic approach was used along with genetic algorithms for iris image reconstruction from given binary templates. This solution was proved realistic and had potential to support iris as reliable biometric feature for human identification. This solution has three phases namely segmentation, normalization and occlusion mask and encoding. These three phases are as visualized in Figure 5.

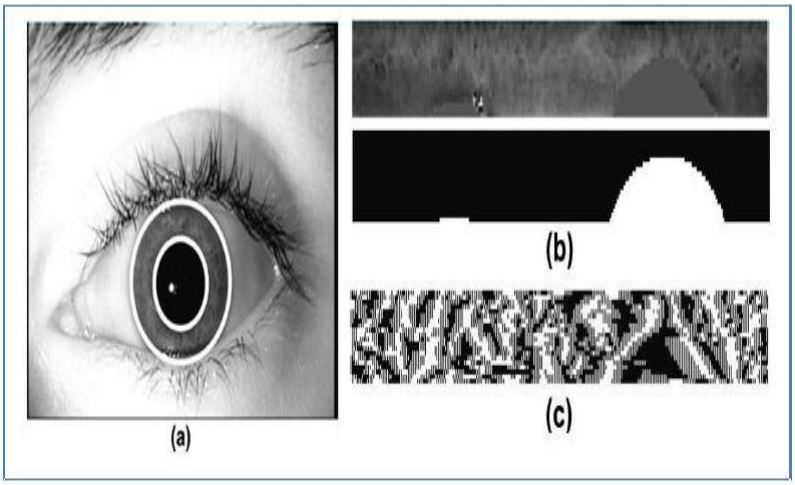

Figure 5: General phases in iris recognition [7]

As can be seen in Figure 4, it is evident that the solution has three phases. In the first phase segmentation takes place. In the second phase normalization takes place for transforming iris segments into a rectangular image.

The encoding phase uses some sort of filtering that can for binary representation of iris image or iris code which is further used for human authentication.

6. Security Issues with Biometric Systems

Biometric systems that make use of multiple features of biometrics have been reported to face attacks. Though biometric technology captures what is being done and who is doing it, there are direct and indirect attacks directed towards face and iris fusion. Recent research revealed that multi-model biometric systems are vulnerable to spoofing attacks. There might be other software based attacks still unexplored in the real world. According to research as in [9] spoofing attacks are considered direct attacks that are made with synthetic biometric features or iris images that are forged. Indirect attacks are the attacks that are made on the inner modules of the biometric

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

system. They are classified into three types namely attacks to the system database, attacks to the communication channels, and attacks on the feature extractor. They proposed an attack to break the security of multi-model biometric system. Their attack demonstrates that the biometrics verification system can get compromised at four stages such as segmentation, normalization and feature encoding and matching. Their experiments proved that the software based attack was able to reveal the vulnerabilities of the multi-model biometric system.

A research [10] presented a hypothesis "genetically undistinguishable irises have texture similarity that is not detected by iris biometrics". Genetically identical irises can be found with twins and both eye irises of same person. However, the similarity between genetically identical irises is not detected by iris biometrics. This provides more security as the biometrics is assumed to be highly secure. Some of the challenging queries with respect to left/right human irises are as presented in Figure 6.

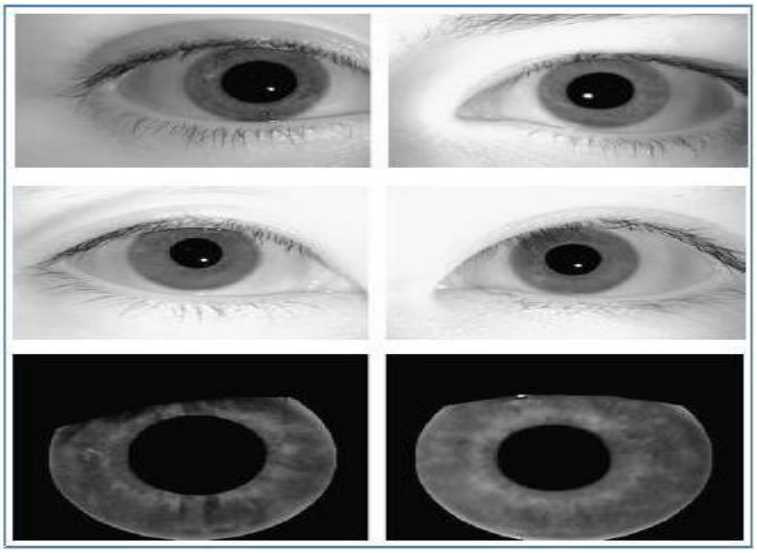

Figure 6: Challenging iris queries that causes incorrect responses [10]

Though the iris pairs are matching, the responses were that they are unrelated. This is due to the hypothesis taken by the researcher which has been proved. Sometimes it is possible to depend on human experts when iris technology is unable answer correctly [10]. In similar lines a sin [19] made experiments on the hypothesis that "texture has effects on iris recognition". Their experiments proved that over a period of time iris recognition failure is attributed to the effects of texture and found the need for dealing with texture.

7. Iris Localization in Frontal Eye Images

Iris localization is very important activity in commercial iris recognition systems. However, the validation of method sis limited to laboratory data and not for realistic data. A research [11] proposed an algorithm that proved to be robust with not ideal data which is less constrained. It has operations like localizing outer and inner boundaries of iris, and the process of suppressing specular reflections. It also has regularization of circular boundaries. The results of this research

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

reveal that the algorithm is robust in presence of eyelids occlusions, eyelashes, hair, contact lens and glasses. The overview of the algorithm is as presented in Figure 7.

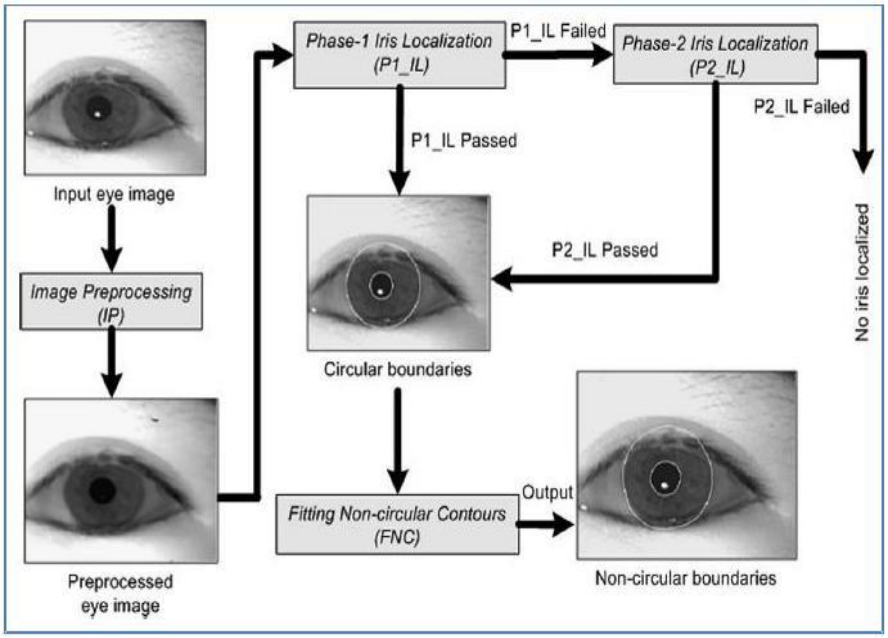

Figure 7: Overview of the algorithm [11]

As can be viewed in Figure 7, it is evident that the given eye image is subjected to preprocessing before applying two phases of iris localization and finally dealing with non-circular boundaries. The experiments conclude that specular reflections very useful in iris recognition, two phase strategy is robust, circular Hough transform can withstand and deal with broken contours, active contours and radial gradients can be used for regularizing inner and outer iris contours [11]. Research in similar lines focusing on gray level intensity [12], radial-gradient operator, and Hough transform for iris localization. In similar fashion, research [13] explored gray level statistics and image projection function for iris recognition. Yet in another experiment a s i n [14] used Hough transform, eccentricity and histogram-bisection for iris localization purposes. In another significant research activity as in [15] focused on non-ideal data for non-circular iris localization by proposing a new localization technique.

8. Other Approaches to Iris Recognition

Research as in [5] focused ocular biometrics including iris recognition. Ocular biometrics became popular as they are proved to be secure biometric features. They focused on the sclera texture and vasculature patterns for biometric authentication to form an ocular-based recognition system. Biometrics is the science of identifying people based on their behavioural or physical traits such as face, iris, fingerprints and voice. As in paper [17] combined error correction codes and finger prints in order to build an effective biometric system. There is a study [18] focused on a multi-model biometric system using face and iris combination. SVM and feature selection techniques were used in the recognition process. A research [21] proposed an algorithm for iris segmentation using Circular Hough Transform and K-Means algorithm. The experiments were

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

made on iris recognition in unconstrained environments. Similar study was made as in [22] using combination of different approaches for iris recognition. The following Table presents various statistical comparisons of biometric techniques.

Table 1: various biometric techniques

Technique/coded/pattern	Misidentification rate	Security/applications
Iris recognition – Iris pattern	1/1200000	High, high security zone
Finger printing	1/1000	Medium, universe
Hand figure – size, length, shape of hand	1/700	Low, less safety zone
Facial recognition – Outline, shape and distribution of eyes and nose	1/100	Low, less safety zone
Signature – shape of letters, writing order, pempressure	1/100	Low, less safety zone
Voice printing voice characteristics	1/30	Low – telephonic services

The various technical issues involved in the recognition of iris can be subdivided into four parts. The first set of issues includes image acquisition. The second step includes segmentation of the iris from the iris image. The third part concerns with feature extraction from the segmented iris image. Finally the fourth part deals with the matching algorithms to match the iris pattern.

9. Conclusions and Future Work

In this paper, our focus is on iris as biometrics feature for secure authentication and identification of humans uniquely across the globe. Iris is one of the physiological biometric features which are regarded as highly reliable in biometric identification systems. It is used in multimodal biometrics and in combination with cryptography. It is also considered to be most inequitable of facial biometrics. However, it is found that iris localization in influenced by texture. When it is not interpreted properly, commercial iris-based biometric systems provide inaccurate results while identifying humans. Moreover, it is important that iris-based identification systems should work with both ideal and non-ideal iris images otherwise the security will be at stake. This study revealed that iris-based biometric systems tend to provide false results in non-cooperative environments. Another important insight is that iris can be used in mobile communications with smart devices. Cancellable biometrics is useful for robust security in the presence of attacks. There are direct and indirect attacks on multimodal biometrics that need to be overcome. Further research is required in order to see that such attacks cannot break security of systems which are based on biometrics. With these insights in mind, in future, we focus on ATM terminal design using iris recognition in banking domain.

References

[1] R. Álvarez Mariño, F. Hernández Álvarez, L. Hernández Encinas. (2012). A crypto-biometric scheme based on iris-templates with fuzzy extractorse. Information Sciences, 195, p91-102.

[2] GauravBhatnagar, Jonathan Wua, Balasubramanian Ramanb. (2012). Fractional dual tree complex wavelet transform and its application to biometric security during communication and transmission. Future generation computer systems, 28, 1, 2012, p254-267.

[3] Anne M.P. Canuto, Fernando Pintro, João C. Xavier-Junior. (2013). Investigating fusion approaches in multi-biometric cancellable recognition. Expert Systems with applications, 40, 6, p1971-1980.
[4] C.Chen and R.Veldhuis. (2011). Extracting biometric binary strings with minimal area under the FRR curve for the hamming distance classifier. Signal processing, 91, 4, p906-918.
[5] Simona Crihalmeanu and Arun Ross. (2012). Multispectral scleral patterns for ocular biometric recognition. Pattern Recognition Letters, 33 (1), p1860-1869.
[6] Maria De Marsico, Chiara Galdi, Michele Nappi, Daniel Riccioc. (2014). FIRME: Face and Iris Recognition for Mobile Engagement. Image and Vision Computing. P1161-1172.
[7] Javier Galbally, Arun Ross, Marta Gomez-Barrero, Julian Fierrez, Javier Ortega-Garcia. (2013). Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. Computer Vision and Image Understanding, 117 (1), p1512-1525.
[8] Ujwalla Gawande, Mukesh Zaveri, Avichal Kapur. (2013). bimodal biometric system: feature level fusion of iris and fingerprint. Biometric Technology Today, p7-8.
[9] Marta Gomez-Barrero, Javier Galbally, Julian Fierrez. (2014). Efficient software attack to multimodal biometric systems and its application to face and iris fusion. Pattern Recognition Letters, 36 (1), p243-253.
[10] Karen Hollingsworth, Kevin W. Bowyer, Stephen Lagree, Samuel P. Fenker, Patrick J. Flynn. (2011). genetically identical irises have texture similarity that is not detected by iris biometrics. Vision and Image Understanding, 115 (1), p1493-1502.
[11] Farmanullah Jan, Imran Usman, Shahrukh Agha. (2012). Iris localization in frontal eye images for less constrained iris recognition systems. Digital Signal Processing, 22 (1), p971-986.
[12] Farmanullah Jana, Imran Usman, Shahid A. Khana, Shahzad A. MalikaaDepartment. (2013). Iris localization based on the Hough transform, a radial-gradientoperator, and the gray-level intensity. Optik - International Journal for Light and Electron Optics, 124 (1), p5976-5985.
[13] Farmanullah Jan, Imran Usman, Shahrukh Agha. (2013). A non-circular iris localization algorithm using image projection function and gray level statistics. Optik - International -241.
[14] Farmanullah Jan, ImranUsman,ShahrukhAgha (2013).Reliable iris localization using Hough transform, histogram-bisection, and eccentricity. Signal Processing, 93 (1), p230
[15] Farmanullah Jan, Imran Usman, Shahid A. Khan, Shahzad A. Malik. (2014). A dynamic non-circular iris localization technique for non-ideal data. Computers & Electrical Engineering, p215-226.
[16] Yooyoung Lee, James J. Filliben, Ross J. Micheals, P. Jonathon Phillips. (2013). Sensitivity analysis for biometric systems: A methodology based on orthogonal experiment designs. Computer Vision and Image Understanding, 117 (1), p532-550
[17] Peng Li, Xin Yang, Hua Qia, Kai Cao, Eryun Liu, Jie Tian. (2012). an effective biometric cryptosystem combining fingerprints with error correction codes. Expert Systems with Applications, 39 (1), p6562-6574
[18] Heng Fui Liau and Dino Isa. (2011). Feature selection for support vector machine-based face-iris multimodal biometric system. Expert Systems with Applications. 38 (1), p11105-11111.
[19] D.M. Rankin, B.W.Scotney, P.J.Morrow a, B.K.Pierscionek. (2012). Iris recognition failure over time: The effects of texture. Pattern Recognition, 45 (1), p145-150.
[20] C. Rathgeb and C. Busch. (2014). Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters. Computers & Security, 42 (1), p1-12.
[21] Shaaban A.Sahmoud, IbrahimS.Abuhaiba. (2013). Efficient iris segmentation method in unconstrained environments. Pattern Recognition, 46 (1), p3174-3185.
[22] Gil Santos and Edmundo Hoyle. (2012). A fusion approach to unconstrained iris recognition. Pattern Recognition Letters, 33 (1), p984-990.
[23] Khairul Azami Sidek, Vu Mai, Ibrahim Khalil. (2014). Data miningin mobile ECG basedbiometric identification. Journal of Network and Computer Applications. 44 (1), p83-91.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1162210

[24] R. Szewczyk, K.Ggrabowski, M. Napieralska, W. Sankowski, M. Zubert, A. Napieralski. (2012). A reliable iris recognition algorithm based on reverse biorthogonal wavelet transform. Pattern Recognition Latyters. 33(1), p1019-1026.
[25] B.Thiyaneswaran, R.Kandiban and Dr. K.S. JayaKumar. (2012). Elimination of IRIS hazards intended for localization using visible features of iris region. Procedia Engineering. 38(1), p246-252.
[26] J.A.Unar, WooChawSeng, AlmasAbbasi. (2014). A review of biometric technology along with trends and prospects. Pattern Recognition. 47(1), p2673-2688.
[27] Heguihu, Cheng Zhao, Xiangde Zhang, Lianping Yang. (2013). A novel iris and chaos-based random number generator. Computers & Security. 36(1), p40-48.
[28] Jin Ok Kim, Woongjae Lee, Jun Hwang, Kyong Seok Baik, Chin Hyun Chung, Lip print recognition for security systems by multi-resolution architecture, Future Gener. Comput. Syst. 20 (2) (2004) 295-301.
[29] D. Maltoni, D.Maio. A.k. Jain, S. Prabhakar. Handbook of Fingerprint Recognition, Springer Verag, Berlin, Germany, 2003.
[30] Maltoni, D.Maio. A.k. Jain, S. Prabhakar. (2009). Handbook of Fingerprint Recognition, (2nd Ed.). Springer publishing Company, Incorporated.

*Corresponding author.
E-mail address: bramhareddy999@ gmail.com