International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(2), pp.178-186
DOI: http://dx.doi.org/10.21172/1.102.30
e-ISSN:2278-621X

A THOROUGH SURVEY ON SECURITY ISSUES OF IRIS BIOMETRICS AND OPEN RESEARCH CHALLENGES

Puja Ghosal[1], Debanjan Das[2], Indrajit Das[3]

Abstract— Biometric authentication systems nowadays are widely deployed for secured access in myriad application domains. Such a system deals with distinct physical and behavioral traits of human being to recognize individuals uniquely. Fingerprint, face, and iris are some of the most widely employed characteristics which are currently adopted in present biometric authentication system. Though biometric is generally considered more reliable and stable than existent authentication systems, yet it suffers from certain flaws which need to be resolved prudently to make this a global commercial success worldwide. For this very reason, this paper focusses on highlighting the strengths and limitations of Iris Biometric System. The paper also offers an extensive survey which reveals new research facets. Besides an extensive review of the existent work conducted, in this domain, the aforesaid literature reviews are discussed in details along with the comparative tabular analysis. Finally the paper gives the future research scope to overcome the addressed research gap.

Keywords- Iris Biometric System; Presentation attacks; Iris Spoofing; Presentation Attack Detection(PAD); Liveness Detection; Template Security; Independent Component Analysis(ICA).

1. INTRODUCTION

Biometrics is the study of automated methodologies for perceiving a person's identity. The term 'biometric' is often categorized as physical versus behavioral characteristics that can be employed to verify a person's identity. Relying on physical properties of an individual offers both simplicity and ease of usage. At the same time, it becomes more reliable to facilitate identification and authentication of different individuals that are widely deployed nowadays for not only in access control and surveillance but also in national and international security systems [1].

Biometric applications can be broadly segregated into two different categories: identification and authentication. When the user's identity is unknown, then identification is performed. This is done by the system wherein it searches the database of enrolled users and matches the biometric data of a particular user with the biometric data of all the enrolled users. On the other hand, authentication is the procedure of verifying the user's identity when his corresponding biometric data is furnished. Presently, both the applications are in use and deployed ubiquitously.

As a matter of fact nowadays devices can be secured by usage of a secure password system. But traditional passwords generally employ a mix of alphanumeric characters/symbols which are mostly cumbersome and often difficult to memorize. This causes user frustration and prevents users from easy access of business data on such devices. Biometric authentication measures offer secured and easy access to systems that can be offered as a natural substitute to conventional password schemes. Several techniques of biometry have already been considered for recognition of a person. However the most popular present day technique involves the fingerprints, face and iris biometric recognition schemes in particular [2].

Simultaneously, nowadays owing to recent sophisticated technological inventions; various security breaches such as spoofing attacks have been created by sharp malicious minds to defeat the security services offered by such biometric measures. Despite offering countless benefits, biometric measures too are vulnerable to several security assaults some of which include; presentation of fake biometric user traits (such as synthetic fingerprints, gait, signature etc.) or previously intercepted biometric data can be used to launch replay attacks by intruders etc. [3,4,5,6,7].

Iris recognition scheme has gained significant popularity among all presently existent biometric modalities (such as face, fingerprint, gait, signature etc.) for authenticated access owing to its intrinsic security and non-intrusiveness. It offers multiple benefits like; high reliability both in terms of identification and verification tasks; its uniqueness for every individual; being an intrinsic eye component, it is well protected from environmental hazards and even remains moderately stable with age [8,9].

However, despite offering multiple advantages, iris biometric systems are highly vulnerable to many security breaches exclusively at the sensory level. Various kinds of attacks specifically with respect to threats using printed iris images or more recently through cosmetic contact lenses which have come to practice. In general, assaults in the biometric system can be universally categorized as direct (presentation and spoofing assaults) and indirect assaults.

[1] Department of Information Technology, Meghnad Saha Institute of Technology, Kolkata, India
[2] Department of Information Technology, Meghnad Saha Institute of Technology, Kolkata, India
[3] Department of Information Technology, Meghnad Saha Institute of Technology, Kolkata, India

The remaining paper is organized in the following manner. Section II provides a synopsis of the iris biometric system. Section III discusses an extensive survey on the existent work on iris biometric security domain and additionally a comparative analysis is furnished among the discussed author contributions. Section IV depicts a comparative analysis of the various mentioned techniques that are used in Iris Biometric Detection System. Section V puts forth the open research issues, problems and challenges associated with iris biometric authentication system. In section VI, the statistics of publications are discussed and section VII concludes the paper.

2. IRIS BIOMETRIC SYSTEM

The eye is a very crucial visionary sense organ of living beings and iris is a very delicate eye component which refers to the heavily pigmented ring of tissue encircling the pupil via which light can enter the interiors of the eye. Fig.1. below clearly depicts a detailed diagram of the human eye and all the different parts responsible for our vision.

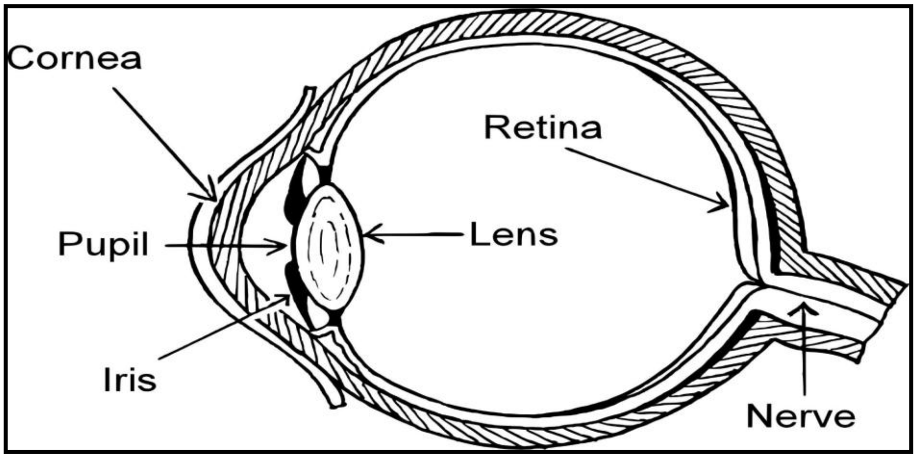

Figure 1. Human Eye Diagram

Fig.2. below illustrates the general structure of an Iris Biometric Detection System. After an image of eye is captured, most iris recognition systems follow a sequential set of activities ranging from the detection of iris location to its segmentation for feature extraction followed by its matching against previously stored template. These have been described briefly below from a conceptual viewpoint.

2.1 Iris Acquisition

Nowadays, cameras that take infrared photographs and videos are used in iris biometric systems. The camera is employed at a predetermined distance for capturing high-quality iris images. Using the infrared range offers some benefits which are briefly stated here; firstly the crypts, nerves and ridges of the iris are more clearly visible [10]; secondly the fine border which segregates the pupil from the iris is more prominent; and lastly, the users will no longer be exposed to the disturbing flashes within the visible light range.

2.2 Iris Segmentation

The motive of this technique is to separate the eye components from the image, locate the iris and separate it from other eye components for further analysis and processing. There are some other crucial tasks to be performed in this phase. They include enhancement of image quality, noise minimization and highlighting the iris ridges for consequent analysis. Several proposals have been forwarded by researchers to implement effective iris location and segmentation some of which have been briefly mentioned here. Daugman [11] has forwarded the adoption of an integro-differential operator that works by inspecting pixel level differences between the circles that are drawn in the image. Sanchez-Avila et al [12] has proposed a same approach that works by inspecting maximum pixel level differences between the circles which are drawn in the image whereas other authors have advocated the usage of the Hough transform for circle detection etc. [13-15].

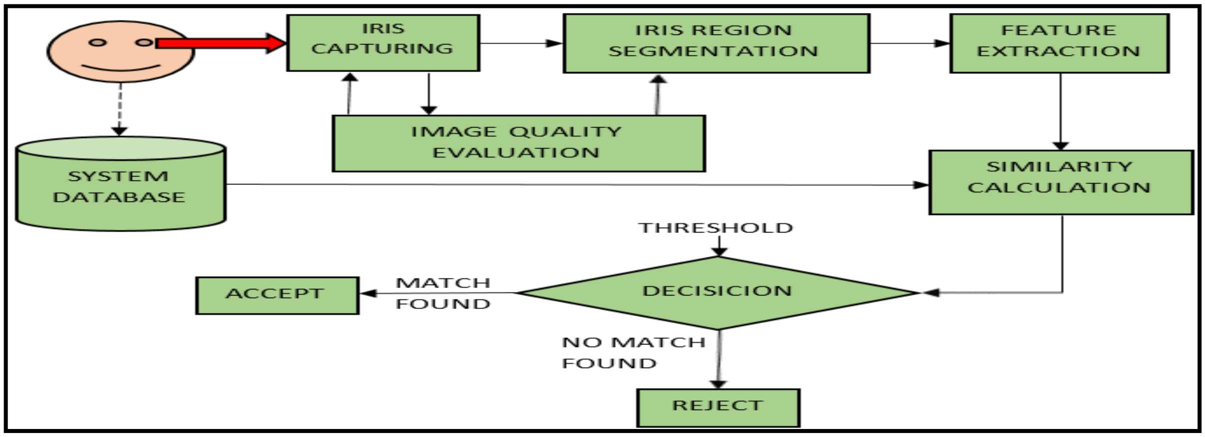

Figure 2. Iris Biometric Detection System

2.3 Feature Extraction

Among the multiple advocated iris feature extraction approaches by varied researchers; the most popular model for this phase belongs to the contribution from the author Daugman [11] where he has characterized this stage by a sequence of essentially four steps; firstly the segmented iris image is normalized and this is a necessary step as the pupil size varies for different light intensities. Next, using the polar coordinate system he has conclusively considered drawing an imaginary line around the pupil (termed as the “iris signature”). Then he has conducted an extensive study of the phase information by applying the Gabor filters. Finally the process ends with the codification of the aforesaid phase information in terms of the quadrant where the phase belongs. Another author Wildes [14] has performed the extraction by employing the Gaussian or the Laplacian filters to obtain multiple different scale pictures for the purpose of posterior comparison. Authors Sanchez–Avila et al. has proposed two different approaches for extracting the iris features in [12]: the first one adopts the Gabor filters employed for extracting the segmented iris image in small portions, while the second one is primarily based on the usage of dyadic wavelet transformations and their zero-crossing representation.

2.4 Classification

Among the many proposed iris feature matching algorithms by renowned authors worldwide; the most popular model for this stage again belongs to the contribution from the author Daugman [11] who has proposed the adoption of Hamming distance approach for matching the iris patterns of the sample under inspection with the already stored template. Here the sample and template vectors are XORed and if the value obtained is beneath a certain predefined value (threshold value), then the sample is said to be matched with the template else not. However the setting up of this threshold value is final application specific. Another method of classification proposed by Wildes [16, 17, 18] is based on texture analysis which uses the Fisher’s linear discriminant function. Another method of classification is developed by Ya-Ping Huang [19] who developed a system that adopts Independent Component Analysis to extract iris texture features. SVM classifiers are also used to analyze data used for classification and regression analysis.

The next section gives a detailed survey on the existing iris biometric attack detection system and the various algorithms used to detect the biometric attacks both direct and indirect.

3. SURVEY ON IRIS BIOMETRIC ATTACKS DETECTION SYSTEM

Over the time, various researchers throughout the world have already worked in the domain of Iris Biometric Detection System and have utilized and conceived a heap of calculation that assesses the execution of their proposed approaches and plans. In this section, we have presented a detailed survey of the existing along with the corresponding accuracy of computational executions.

Researchers Adam Czajka et al. [20] has proposed a significant method for eye liveness detection using the dynamic state of the pupils. Owing to the lack of public databases, he employed an iris capture device to construct his own customized database by registering changes in Pupil sizes when subjected to visible light stimuli. His paper introduces a challenge-response countermeasure based on the spontaneous changes in the pupil stimulated by active light. The countermeasures are extremely effective when the pupil dynamics estimates captured over a short time interval are used. However this work too has certain limitations that are enlisted here; Firstly, the evaluation and measurement computation of the dynamic features of the eye incurs time and all applications might not allow an additional 2 seconds for iris capture. Secondly, variation of dynamic features for different age population groups vary significantly especially for infants or elderly people. Such scenarios also need to be incorporated here as possible test cases to calculate the accurate performance of the proposed scheme. Thirdly, exceptional or abnormal scenarios during experimental analysis needs to be considered such as ingestion of drugs or alcohol; altered psychological states such as stress, relaxation, mental load etc., which bring about changes in the dynamic features of the eye.

Another interesting piece of work on lightweight iris-based biometrics are been carried out by a group of researchers De Marsico et al. [21] where both face and iris recognition schemes having modular architecture are integrated with an anti-spoofing algorithm to offer secure authenticated access to mobile devices using Android. Here, the sequential steps which follow comprises; image acquisition, anti-spoofing , detection, segmentation, feature extraction and matching both the iris and face separately followed by fusion of obtained results. One of its limitations is its satisfactory performance in outdoor testing that can be investigated and undertaken as future research topic.

Researcher Komogortsev et.al. [22] brought forth an innovative countermeasure against spoofing which utilizes eye gesture as a liveness component indicator. In this paper they displayed that the biometrics involving eye gestures are resistant to spoofing assaults having employed a linear model of an oculomotor plant. This approach can be seamlessly integrated with almost any iris recognition system currently present as it only requires a standard image sensor. However, some primary limitations of the aforesaid work are discussed below; firstly, the linear models of the oculomotor plant considered here has only been owing to the size of the available datasets and its operational and computational constraints. However, the human visual model manifests a wide array of non-linear attributes that can only be effectively and approximately estimated by usage of linear models. As far as the prevalent knowledge is concerned, the oculomotor plant does not exhibit any such model that achieves a foolproof depiction of the human visual system. Secondly, before the utilization of the anti-spoofing measures, the issue of precise quantification of the intrinsic spoof-ability of biometrics pertaining to eye gestures in particular can be adopted by having a comparative study of eye biometric authentication accuracies by involving both the presence and absence of the attack vectors. Unfortunately no such approach has been undertaken in the aforesaid work that can definitely be an interesting theme for future research in this domain. Finally, another drawback of the presented work is the adoption of a software-based approach for simulation of biometric attack vectors. Unfortunately, the engineering precision required to generate a potential physical clone of the oculomotor plant has created issues thus making it difficult and infeasible to deploy it in the current undertaken approach.

Researchers Raul Sanchez-Reillo et.al. [23] came up with a solution which deals with personal tokens with mandatory biometric authentications. Here iris biometric is chosen to be incorporated because of its low error rate and robustness. The algorithms which are associated in this system are efficient enough to glorify the capability of the system. Simultaneously, the security and cost for large quantities are also improved. The results obtained in this study enhance the road to future research with the integration of cryptographic modules that may provide more security to all data transmissions on the go. Another area of future research is identifying tokens that combine the benefits of both the platforms that are developed herein and exploring optimal hardware solutions to do so.

Researchers Ankita Satish et.al. [24] considered Canny edge operator which is used for segmentation that gives better results in identifying edges with a certain threshold value. Gabor filtering is used for separating the features and K-out-of-n is used to categorize for identical patterns. The experiments have been performed on CASIA databasev2.0. The Fault Accept Rate (FAR) and Fault Recognition Rate (FRR) calculated for K-out-of-n classifier gave an accuracy of 95% and 99% for the suggested system using Euclidean Distance Classifier.

Researchers Mohtashim Baqar et.al. [25] suggested a method on Iris recognition system based on thorough learning. Gaussian filtering is used as a preprocessing technique to remove the highlights from the Iris image. Weighted centroid-of-eye is used as a guideline for segregating contour points. RVLNR-NN is used for classification purpose. CASIA Iris database was used to conduct the experiments. The results obtained from these models depict supreme results with a recognition rate of 99.92%.

Researchers B. H Shekar et.al. [26] suggested a vigorous technique for feature extraction and encoding purpose. Both the left and right iris are used for feature extraction. Furthermore, encoding procedures need to be carried out separately for both of them. Experiments were conducted on IITD, MMU v2 and CASIA v4 database. The results that are obtained from these mentioned techniques provide a recognition rate of 99%, 95% and 91% respectively.

Researchers Kavita Joshi et.al. [27] showed the maximum reduction in Fault Accept Rate (FAR) and Fault Recognition Rate (FRR).Canny Edge Detection approach is used for segmentation of the Iris image which helps in locating the inner iris boundary that in turn brings about the outer iris boundary. ID Log-Gabor filter and HAAR Wavelet transform helped in extracting the features. Hamming Distance is used for classifying the matching purpose. Experiments had been conducted on CASIA Iris v4 database and the outcomes that were obtained, showed an improvement in its Fault Recognition Rate (FRR). However, this did not reduce the FRR to 0. But the combination of Gabor and HAAR feature extraction method provides better FRR results (FRR almost decreases to zero).

Researchers Rocky et.al. [28] suggests identifying the iris with databases among the non-ideal and ideal iris. Median and Gaussian filters were used for the initial stage of processing, to enhance the image. 3D GLCM was used for extracting the features which were then trained using Elman Recurrent Neural Network algorithm. Experiments were conducted on CASIA v4 database for non-ideal iris and CASIA v1 for ideal iris databases. The results that were obtained, shows an improvement in the Fault Recognition Rate of 91.1% and 94.22% respectively.

Researchers Habiebeh Naderi et.al. [29] presented a biometric recognition system having three modes. It had Iris, Palm print and fingerprint recognition system. Canny edge detection and Hough Transform have been used to detect and select the area of interest and separate it from the rest. Wavelet transform and Gabor filter are used to extract features from the image.

Hamming Distance was used for categorization purpose. Experiments were conducted which showed an improved and better rate of MIR when CASIA database was used.

Researchers Chiara Galdi et.al. [30] gave a distinguished and fast method to identify the iris in smart phones by considering the features of color and textures. Euclidean distance to extract color descriptor between color histogram of the two images was used. Different classifiers were also used. Experiments were conducted which show better results on the Apple I phone 5(ip5) and Samsung galaxy-s4 (gs4) with AUC rate of 98% and 80% respectively.

Researchers Sarika Solanke et.al. [31] gave an idea on the characteristics needed for iris recognition technology to make it visually attractive when used in an authentic system. Average filter and median filter were used to enhance the iris image. 1-D log polar Gabor transform and DCT were used to extract the features of an iris image. Hamming Distance classifier is used for classification purpose. Experiments were conducted that showed improved better rate of 9.5% on UBIRIS v2, 4.3% on FRGC database and 25% on CASIA v4 database.

The next section offers a comparative analysis among the aforesaid iris biometric detection systems on the basis of the following parameters: author, paper name, preprocessing, feature extraction, classification, database, recognition rate and future scope.

4. COMPARATIVE STUDY OF DIFFERENT IRIS BIOMETRIC DETECTION SYSTEM ALONG WITH THEIR COMPUTATIONAL ACCURACY

A contrast investigation of the various existing iris biometric detection systems are abridged in the following table (Table 1). The table depicts the different methods used by the researchers and their accuracies and drawbacks.

Table - 1 Comparative analysis of Iris Biometric Detection System

Author	Paper Name	Preprocessing	Feature Extraction	Classification	Database	Recognition Rate	Future Scope
Adam Czajka	Pupil dynamics for Iris Liveness Detection [20]	Circular Approximation of Pupil	No feature Extraction Method due to the Low dimensionality Of the feature space.	Linear and Non linear Support Vector Machine (SVM)	Iris Movies	92%	The computational time needs to be reduced and more dynamic test conditions need to be considered like for different age groups and cases concerning intake of drugs
De Marsico, M., Galdi, C., Nappi, M., Riccio	FIRME : Face and Iris Recognition for Mobile Engagement (Only Iris Recognition Part) [21]	Iris segmentation for Identification Systems (ISIS)	Cumulative SUMs (CSUM) algorithm is used to generate the feature	Hamming Distance	MICHE database	97%	It provides satisfactory performance in outdoor testing and needs to be looked upon
Oleg V. Komogortsev, Alexey Karpov and Corey D. Holland	Attack of Mechanical Replicas: Liveness Detection with Eye Movements [22]	No Segmentation	Oculomotor Plant Characteristic (OPC) is used to generate the feature vector	Regression SVM with RBF Kernel	EMDB Database	97%	A foolproof depiction of human visual system should be developed and included in the oculomotor plant

Raul Sanchez-Reillo, Judith Liu-Jimenez and Belen Fernandez-Saavedra	Iris Biometrics for Embedded System [23]	Hough Transform	Wavelet Transform is used	Hamming Distance	ICE 2005 Database	95%	No work is done on Liveness detection and hence this area needs to be looked upon
Ankita Satish Adhau and D Shedge	Iris Recognition methods of a Blinked-Eye in Non-ideal Condition [24]	Canny-edge Detection	Gabor Filtering is used to generate the feature vector	K-out-of-n ED	CASIA	95% - 99%	Algorithms should develop to robust in its results.
Mohtashim Baqar, Azfar Ghani, Azeem Aftab, Saira and Sajid Yasin	Deep Belief Networks for Iris Recognition based on Contour Detection [25]	Canny-edge detection & Gaussian Filtering	Depending upon filter response contour points are extracted	RVLRNN	CASIA	99.92%	Need to extend to larger database and new deep method should be developed to get better accuracy
B H Shekar, Sharada S Bhat	Steerable Riesz Wavelet based Approach for Iris Recognition [26]	Particle Swarm Optimization and circular Hough Transform	Log Gabor, Riesz and TSE filtering is used to generate the feature vector	Fuzzy c-means clustering (FCM) and Weighted Mean Hamming Distance	IITD MMU v2 CASIA v4	99% 95% 91%	It provides satisfactory performance in outdoor testing and needs to be looked upon
Kavita Joshi and Sunil Agrawal	An Iris Recognition Based Robust Intrusion Detection System [27]	Canny-edge detection & HAAR Transform	Log Gabor Wavelet and HAAR Wavelet	Hamming Distance	CASIA	100%	Work to be carried for other artificial intelligence techniques to improve FRR.
Rocky Yefrenes, Dillakr Martini and Ganantoweintiri	A Novel Approach for Iris Recognition [28]	Gaussian Filter CHT method	3D-GLCM is used to generate the feature	NN	CASIA v4 CASIA v1	91% 94.22%	Work to be carried with other approaches like NBP method.
Habibeh Naderi, Behrouz Haji Soleimani, Babak Nadjar Araabi and Hamid Soltanian Zadeh	Fusing Iris, Palm print and Fingerprint in a Multi-Biometric Recognition System [29]	Hough Transform and Canny edge detection	Wavelet Transform & Gabor filter	Euclidian Distance	CASIA	97%	There is still a scope for developing a better algorithm and use larger database.
Chiara Galdi and Jean-Luc Dugelay	Fusing Iris Colour and Texture information for fast Iris Recognition on mobile devices [30]	Grey World Normalization (a color normalization technique)	Watershed Transform is used to generate the feature vector	Color and Texture Based Multi-Classifier and classifier fusion (weighted sum)	MICHE database	98%	It provides satisfactory performance in outdoor testing and needs to be looked upon

Sarika B Solanke and Ratnadeep R Deshmukh,	Biometrics-Iris Recognition System: A study of promising approach for secured authentication [31]	Normalization using the radial scan method	Wavelet or Multi-wavelet approach is used to generate the feature	Hamming Distance, Euclidian Distance	UBIRIS v2 FRGC CASIA v4	92% 89% 98%	Work needs to be done to enlarge the algorithm for Powerful recognition with human iris and palm print pattern identification

The following section provides details regarding the open issues and the research gaps.

5. OPEN ISSUES

A recent survey revealed that presently no existent anti-spoofing measure has attained a very low error rate. However, the ever-increasing demand for minimal PAD (Presentation Attack Detection) failure rates have opened up interesting open research challenges and issues across myriad domains that have been briefly discussed in details below.

5.1. Mobile Liveness Detection

A current industrial survey has estimated that by 2018, almost 3.4 billion mobile phone users will adopt biometric measures on their mobile phones for secured access [32]. However, the existent iris liveness detection methodologies are un-suitable for mobile applications owing to either the complexity of the features that are being analyzed or the high cost incurred during computation. Thus, to make such applications more practical and usable, researchers worldwide must resolve the issue of presentation attacks on mobile devices prudently.

5.2 Spoof Material–Invariant Liveness Detection

A major issue with iris liveness detection technique is that it is often based on an infeasible and priori known spoof fabrication material which limits its application in real life scenarios where the nature of assaults are highly erratic. Accordingly, researchers must devise a generic and standard iris liveness detection methods to identify varied or previously undetected spoofing assaults. Although it is practically infeasible to devise training PADs with potential materials and techniques, yet one possible surrogate is to devise an analytical layout of the spoofs characterized by different materials, techniques etc.

5.3 Correlation of Liveness Values with Match Scores

In general, iris liveness detection normally produces a liveness measure value. However, the relation as to how one can correlate the measured liveness values with biometric match scores is yet to be systematically analyzed and investigated. This is to be done in order to resolve presentation assaults. Thus, this issue can be an interesting research topic in future where researchers should propose methods or models that combine both or analyze the existent logical relation between them if any.

5.4 Template Security

Recent conducted surveys and studies reveal that reverse biometrics (i.e. regeneration of the authentic biometric sample from its corresponding specimen) raises a protest against the familiar and well known assumption that templates lacks the sufficient data needed to grant the regeneration of the original sample. However, the regenerated characteristic might itself serve as a spoofing assault. Reverse biometry can also be abused to generate fabricated data sets or augment existent, real spoofed data sets.

5.5 Cross Sensor and Cross Dataset Liveness Detection

The cross sensor setting is the setting in which the training data and testing data are from different sensors. The cross dataset setting is the setting in which the training data and testing data are from different datasets. Both of these have not attained much consideration and focus of researchers worldwide till date. However, both are equally important to the real-world applications for iris liveness detection scenarios. So, both cross sensor and cross dataset liveness detection issues can be undertaken as future potential research directions.

5.6 Challenge and Response Based Liveness Detection

In challenge and response based iris liveness detection approach, the system mandates users, for instance, blinking the eyes repeatedly to make sure that haphazard instructions are executed effectively. However, of course this approach has a few drawbacks. It is less user friendly, not accepted that easily and incurs high cost of computing. Thus, researchers must focus on designing a new, original, user-friendly, optimal and uncomplicated response methods.

The next section puts forth the statistics of publications pertaining to the existent iris biometric detection scenarios.

6. STATISTICS OF PUBLICATIONS ON IRIS BIOMETRIC DETECTION SYSTEM

This section discusses the statistics of existing publications on Iris Biometric Detection System. The search for these statistics were carried out with the following keywords; iris biometric detection, segmentation and feature extraction system. The search statistics (in Table 2) is considered for conference publications, journals and magazines, early access articles, books/e-books, chapter publications

Table – 2 IEEE Publication Statistics

Type	Iris Biometric Detection	Iris Biometric Segmentation	Iris Biometric Feature Extraction
Conference Publications	456	413	1007
Journals and Magazines	53	51	116
Early Access Articles	0	0	3
Books	0	0	1

The next section deals with the conclusion of the paper.

7. CONCLUSION

This review paper puts forth a detailed survey of the existent research contributions from myriad authors conducted specifically in the domain of security of iris biometrics. Additionally a tabular comparative analysis of the discussed author contributions have been presented for the sake of further ease of understanding and simplicity. Further this paper also summarizes the prevalent open research issues and challenges that are existent particularly in this domain. We have also conclusively reviewed that well-known opinions about security and ideas relying on iris biometry are flawed and needs to be again looked into in the future, in order to make biometric authentication system a global commercial success worldwide.

8. REFERENCES

[1]. A. K. Jain, A. Ross, "Introduction to biometrics" in Handbook of Biometrics, New York, NY, USA:Springer-Verlag, pp. 1-22, 2008.

[2]. J. A. Unar, W. C. Seng, and A. Abbasi, “A review of biometric technology along with trends and prospects,” Pattern Recognit., vol. 47, no. 8, pp. 2673–2688, Aug. 2014.

[3]. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of artificial ‘gummy’ fingers on fingerprint systems,” Proc. SPIE, vol. 4677, pp. 275–289, Apr. 2002.

[4]. J. Galbally et al., “An evaluation of direct attacks using fake fingers generated from ISO templates,” Pattern Recognit. Lett., vol. 31, no. 8, pp. 725–732, 2010.

[5]. T. Matsumoto, “Artificial irises: Importance of vulnerability analysis,” in Proc. 2nd Asian Biometrics Workshop, vol. 45. 2004.

[6]. V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, “Direct attacks using fake images in iris verification,” in Biometrics and Identity Management (Lecture Notes in Computer Science), vol. 5372, , 2008, pp. 181-190.

[7]. N. Kose and J.-L. Dugelay, “On the vulnerability of face recognition systems to spoofing mask attacks,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2013, pp. 2357–2361.

[8]. M. Faundez-Zanuy, “Biometric security technology,” IEEE A&E Syst. Mag., vol. 21, no. 6, pp. 15–26, Jun. 2006.

[9]. K. Bowyer, K. Hollingsworth, and P. Flynn, “Image understanding for iris biometrics: A survey,” Comput. Vision Image Understand., vol.110, no. 2, pp. 281–307, 2008.

[10]. H. Davson, The Physiology of the Eye. New York: Little, Brown and Company, 1963.

[11]. J. G. Daugman, “High confidence visual recognition of persons by a test of statistical independece,” IEEE Trans. Patt. Anal. Mach. Intell., vol. 15, no. 11, pp. 1148–1161, Nov. 1993.

[12]. C. Sanchez-Avila and R. Sanchez-Reillo, “Two different approaches for iris recognition using gabor filters and multiscale zero-crossing,” Patt. Recog., vol. 38, no. 2, pp. 231–240, 2005.

[13]. L. Ma, T. Tan, Y.Wang, and D. Zhang, “Efficient iris recognition based characterizing key local variations,” IEEE Trans. Image Process., vol. 13, no. 16, pp. 739–750, Jun. 2004.

[14]. R. P. Wildes, “Iris recognition: An emerging biometric technology,” Proc. IEEE, vol. 85, no. 9, pp. 1348–1363, Sep. 1997.

[15]. C. Tisse, L. Martin, L. Torres, and M. Robert, “Personal identification on technique using human iris recognition,” in Proc. Vision Interface, 2002, pp. 294–299.

[16]. R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J.Matey, and S. McBride, “A machine-vision system for iris recognition”, Machine Visual Application, Vol. 9, pp. 1-8, 1996.

[17]. R. Wildes, “Iris recognition: an emerging biometric technology”, IEEE Proceedings, Vol. 85, pp. 1348-1363, 1997.

[18]. R.P.Wildes, J.C.Asmuth, G.L. Green, S.C.Hsu, R.J,Kolczynski, J.R.Matey, S.E.McBride, David Sarno_ Res. Center, Princeton, NJ, “A System for Automated Iris Recognition”, Proceedings of the Second IEEE Workshop on Applications of Computer Vision, 1994.

[19]. Ya-Ping Huang, Si-Wei Luo, En- Yi Chen, “An efficient iris recognition system”, International Conference on Machine Learning and Cybernetics, pp. 450-454, 2002.

[20]. Adam Czajka , “Pupil Dynamics for Iris Liveness Detection”, IEEE Trans. on Information Forensics and Security, vol. 10, no. 4, April, 2015.

[21]. De Marsico, M., Galdi, C., Nappi, M., Riccio, D., 2014. FIRME: Face and Iris Recognition for Mobile Engagement. Image and Vision Computing, Elsevier, 2014.

[22]. Oleg V. Komogortsev, Alexey Karpov and Corey D. Holland, "Attack of Mechanical Replicas: Liveness Detection with Eye Movements", IEEE Trans. on Information Forensics and Security, vol. 10, no. 4, April, 2015.

[23]. Raul Sanchez-Reillo, Judith Liu-Jimenez and Belen Fernandez-Saavedra, "Iris Biometrics for Embedded Systems", IEEE Trans. on VLSI System , vol. 19, no. 2, February, 2011.

[24]. Ankita Satish Adhau and D Shedge, "Iris Recognition methods of a Blinked-Eye in Non-ideal Condition," IEEE International conference on Information Processing, ISBN 4673-7758, pp. 75-79, 2015.

[25]. Mohtashim Baqar, Azfar Ghani, Azeem Aftab, Saira and Sajid Yasin, "Deep Belief Networks for Iris Recognition based on Contour Detection," IEEE International conference on Open source Systems and Technologies, ISBN 5090-5586, pp. 72-77, 2016.

[26]. B H Shekar, Sharada S Bhat, "Steerable Riesz Wavelet based Approach for Iris Recognition," IEEE Asian Conference on Pattern Recognition, ISBN 4799-6100, pp. 431-436, 2015.

[27]. Kavita Joshi and Sunil Agrawal, "An Iris Recognition Based Robust Intrusion Detection System," IEEE Annual India Conference, ISBN 4673-6540, pp. 1-6, 2015.

[28]. Rocky Yefrenes, Dillakr Martini and Ganantoweintiri, "A Novel Approach for Iris Recognition," IEEE Region Symposium, ISBN 5090-0931, pp. 231-236, 2016.

[29]. Habibeh Naderi, Behrouz Haji Soleimani, Babak Nadjar Araabi and Hamid Soltanian Zadeh, "Fusing Iris, Palmprint and Fingerprint in a Multi-Biometric Recognition System,"IEEE International Conference on Computer and Robot vision, ISBN 5090-2491, pp. 327-334, 2016.

[30]. Chiara Galdi and Jean-Luc Dugelay, "Fusing Iris Colour and Texture information for fast Iris Recognition on mobile devices," IEEE International conference on Pattern Recognition, ISBN 50903-4847, pp. 160-164, 2016.

[31]. Sarika B Solanke and Ratnadeep R Deshmukh, "Biometrics-Iris Recognition System: A Study of Promising Approach for Secured Authentication," IEEE International Conference on Computong for Sustainable Global Development, ISBN 3805-4421, pp. 811-814, 2016

[32]. A. Goode, Mobile Biometric Security Market Forecasts 2013–2018, Goode Intelligence, 28 Oct. 2013.