Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on: Performance Analysis of Iris Authentication System

[1]Reeta, [2]Er. Vandana Singla

[1]Student,Haryana Engineering College, Haryana, India

[2]Lect., Haryana Engineering College, Haryana, India

Abstract: Biometric technologies are considered more secure with respect to other authentication techniques based on passwords and Identity cards. Most reliable biometric technology in terms of identification and verification is based on iris.

Iris recognition nevertheless is computationally very costly and complicated system. Feature extraction is a significant task in the overall processing of iris authentication system. Most distinguishing information present in an iris must be extorted to provide accurate recognition of people. A feature extraction procedure is considered valuable if it decreases the size of the feature template and computational speed as well as provides high accuracy. Main objective of this review is to study various edge detectors - Roberts , Sobel and Prewitt operators used to enhance feature extraction process .

Keywords - Biometrics , Iris Authentication system , CASIA , Iris Localization

I. INTRODUCTION

Biometric technologies for personal identification have been motivated by the growing need of security in present years. The previous security systems based on passwords, ID cards, or other equipments may be inconvenient or cracked. In contrast, biometric techniques utilize physiological or behavioral characteristics, such as the face, fingerprint, palm print, iris, retina, voice & gait, *etc.*, to efficiently authenticate human's identity. These techniques exhibit the advantages of reliability and convenience.

The human iris is a ring between the pupil and the sclera. It has distinctive spatial patterns with the

Properties of being unique to each people and stable with age. After teenage, the healthy iris will remain almost unchanged. However, the iris is

behind the cornea and is therefore difficult to be faked or constructed . So that, iris recognition has more advantages over other biometric identification technologies.

For the last decade, iris recognition has been a popular research topic of biometrics. A typical and successful iris recognition system was developed by Daugman . Daugman's system used the first order derivatives of image intensity to locate the edges of iris [1] .

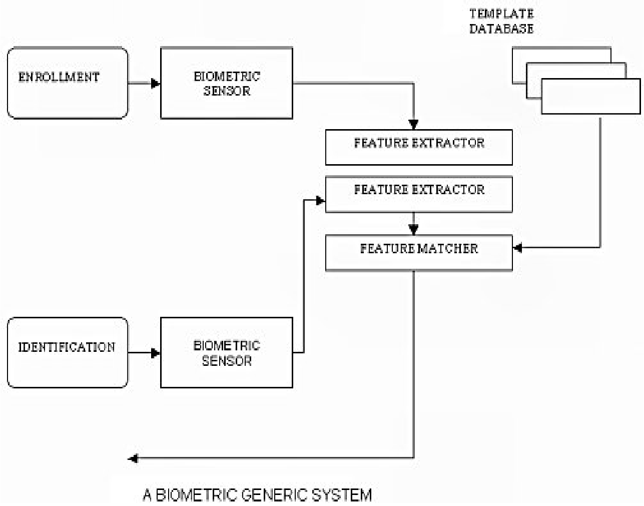


Figure 1 - Example of Biometric System

Iris Recognition Process

In iris biometric system, an important task is to extract iris feature from a given eye image. In an eye image of a person, iris is an annular part between the pupil and the white sclera. The iris part has a number of features . Since iris features are distinct from one another & considered in iris recognition process. Human iris recognition process is basically divided into two phases. The phase, which is dealt with the extraction of iris features from an eye image and stores them into database is called the "enrollment process".

Iris Matching Process

At the time of matching we capture the iris features of a human and compare it with the stored features, which are called the "matching procedure". These phases are complex and hence are divided into several sub tasks. The different steps involved in the two phases. First four tasks in both the phases are common. The task namely, "matching features" is extra in the matching process. Among all these tasks feature processing is the most important task in an iris-based biometric authentication system so far the overall performance of an iris-based biometric authentication system is concerned [2].

III. SECURITY CHALLENGES IN BIOMETRIC TEMPLATE

The advent of biometrics has introduced a secure and efficient alternative to traditional authentication schemes. Biometrics is the science of establishing or determining an identity based on the physiological or behavioral traits of an individual. These traits include fingerprints, facial features, iris, etc. In alignment with traditional authentication schemes, biometrics is a powerful tool for establishing identity.

A typical biometric system comprises of several modules. The **Sensor module** assumes the raw biometric data of an individual in the form of an video , audio signal. Then **Feature Extraction module** operates on the biometric signal and extracts a prominent set of features to represent the signal during user enrollment the extracted feature set labeled with the user's identity is stored in the biometric system and is known a template. After that **Matching module** compares the feature set extracted during authentication with the enrolled template and generate matching score. The **Decision module** processes these matching score to determine or verify the identity of an individual. Thus, a biometric system may be viewed as a pattern recognition system whose function is to divide a biometric signal into one of several identities (viz., identification) or into one of two classes - genuine and impostor users (viz., verification). While a biometric system can enhance user convenience. it is also susceptible to various types of threats as discussed below-

1. **Circumvention:** An intruder may gain access to the system protected by biometrics and peruse sensitive data such as medical records pertaining to a legitimately recruited user. Apart from violating the privacy of the recruited user, the pretender can also modify sensitive data.
2. **Repudiation:** A legitimate user may access the facilities offered by an application and then claim that an intruder had surrounded the system. for example- A clerk of a bank may change the financial records of a customer and then deny responsibility by claiming that an intruder could have possibly stolen her biometric data.
3. **Covert acquisition:** An intruder may surreptitiously obtain the raw biometric data of a user to approach the system. For instance, the potential fingerprints of a user may be lifted from an object by an intruder and later used to construct a digital or physical artefact of that user's finger.
4. **Collusion:** An individual with wide super-user privileges (such as an administrator) may deliberately modify system parameters to permit incursions by an intruder.
5. **Coercion:** An impostor may force a legitimate user (e.g., at gunpoint) to grant him access to the system.
6. **Denial of Service (DOS):** An attacker may overwhelm the system resources to the point where legitimate users desiring access will be denied service. For good example, a host that processes access requests can be flooded with a large number of fake requests, because of that overloading its computational resources and preventing valid requests from being processed.[3]

III. RELATED WORK

A number of journals and research papers have been studied. The various aspects of the problem were studied.

Iris Authentication

Two phases are involved during iris authentication process using a biometric system- enrollment and authentication. Throughout enrollment features sets are extracted from iris textures and saved in database. on authentication the features are elicited from query iris template and classified against the database. Current iris recognition systems perform exhaustive matching with high computational complexity as large databases are to be studied. hence this new iris recognition system will play a vital role in reducing both the search time and computational complexity by classifying into different categories [4].

Steps for Iris Authentication System

1. Feature Selection

The iris is an externally visible and well protected organ whose unique epigenetic pattern remains stable across adult life. These features make it very appealing for use as a biometric for describing individuals. Image processing techniques can be applied to extract the unique iris pattern from a digitalized image of eye and encoding it into a biometric template, which can be stored in a database. That biometric template comprises an objective mathematical representation of unique information stored in iris, and allows comparisons between templates. When someone wants to be identified by iris authentication system their eye is first photographed and then a template generated for their iris region. This template is then compared with other templates stored in database until either a matching template is found and the subject is discovered & no match is found and the subject continues undefined. [5].

Adhyana G. et. al (2014) Iris recognition system is the most reliable system for an individual recognition. At that time many applications have been carried out with this feature such as the time attendance system for high security environment etc. The established method applied on the security is not reliable such as the passwords may be forgotten or hacked and ID cards may be lost. Iris biometric authentication is acquiring importance in recent times. In the overall working of iris biometric in an iris-based biometric authentication system, feature choice is an important work. This approach is based on the iris and the retina of the eye. The iris and retinal patterns are captured via a camera or video-based image acquisition system. The uniqueness of an individual's iris and retinal patterns helps in identifying and verifying the user.[6]

George C.C.et.al (2009) Traditional identity verification in computer systems are done based on Knowledge based and token based identification these are prone to fraud. Unfortunately, these may often be disclosed or changed. A true and accurate identification/verification technique may be designed using biometric technologies. Biometric authentication employs unique combinations of measurable physical characteristics-- fingerprint, iris of the eye etc. that cannot be readily imitated or forged by others.

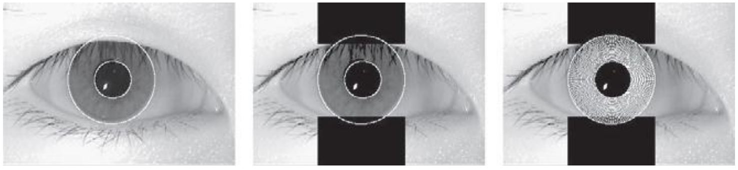
Unimodal biometric systems have variety of problems such as noisy information, intra-class

Variations, restricted degree of freedom, non-universality and unacceptable error rates. Multimodal biometrics refers the combination of two or more biometric modalities in a single

Identification system. The aim of paper is to identify whether the integration of iris and fingerprint biometrics overcome the hurdles of unimodal biometric system. This paper discusses the various scenarios that are possible to improve the performance of multimodal biometric systems using the combined characteristics such as iris and fingerprint, the level of fusion (multimodal fusion) is applied to that are possible and the integration strategies that can be adopted in order to increase the overall system performance[7]

2. Image Segmentation

A good segmentation algorithm should involve two procedures: iris localization and noise reducing. The iris localization procedure take the acquired image and find both the boundary between the pupil and iris and also between the iris and the sclera. The noise reducing process refers to localizing the iris from the noise (non-iris parts) image. These include the sclera, eyelids,pupil, eyelashes & artifacts.[8]



(a) Iris localization (b) Occlusion effect (c) Noise Reduction

Figure 2- Iris Segmentation

Yulin Si et al. presented in this paper segmentation algorithms is the in efficiency of eyelash detection. Some real iris textures will be misclassified as eyelashes when there exists sharp contrast in the iris region. Based on directional filters, a new eyelash detection method is proposed with much fewer misclassifications. Second, in the iris feature extraction process, a multi-scale and multi-direction data fusion strategy is introduced in this work, and the combination of adaptive scale selection and improved matching criteria will better explain the iris textures. Then Third , in order to increase the response time for the 1: N search in a huge iris database, an iris listing method based on corner detection is presented [9].

3. Image Compression

John D. et .al (2008) We investigate three schemes for severe compression of iris images in order to assess what their impact would be on recognition performance of the algorithms deployed today for identifying people by this biometric characteristic. Presently, standard iris images are 600 times larger than the Iris Code templates computed from them for database reposition and search. But it is administratively wish that iris data should be stored, transmitted & embedded in media in the form of images rather than as templates computed with proprietary algorithmic program. To accommodate that goal with its significances for bandwidth & storage, we present strategies that combine region-of-interest (ROI) isolation with JPEG and JPEG2000 compression at serious levels, and we test them using a publicly available database of the iris images. We express that it is possible to compress iris images to as little as 2000 bytes with minimal impact on recognition performance. Only some 2% to 3% of the bits in the Iris Code templates are changed by such serious image compression and we calculate the information per code bit introduced by each compression scheme [10].

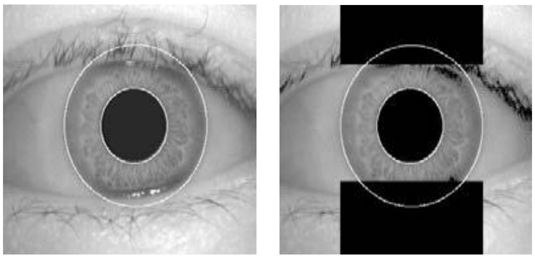
4. Iris Localization

Iris localization mainly involves two basic procedures, one is to detect eye lids and the

Other is boundary detection. The first step involves extraction of circular shaped iris rim by removing the noisy areas. Eyelids & eyelashes block upper and lower parts of the iris. Thus these areas must be segmented. Then second step is to detect the inner and outer boundaries of iris. One is at the transition area of iris and sclera and the other is at the iris and pupil.

Wildes et. al

Canny edge detection is performed both in vertical direction and horizontal directions. The iris images in CASIA database have iris radius 80 to 150 and pupil radius from 30 to 75 pixels. Canny edge detection is used to create edges in horizontal direction and then Hough transform is applied on it. Whenever the maximum Hough space is less than the threshold it represents non blockage of eyelids. For insulating eyelashes it is easier by using thresholding because they are darker when compared with other elements in eye [11].



(a) Iris after boundaries observed
(b) Iris image following noise removal
Figure 3 - Iris Localization

5. Feature Extraction & Matching

Somnath Dey . et . al (2010) In this we address this issue and present an approach to feature extraction and feature matching technique. We apply Daubechies D4 wavelet with 4 levels to extract features from iris figures. These characteristics are encoded with 2 bits by quantizing into 4 quantization stages. With our proposed approach it is possible to represent an iris template with only 304 bits but existing approaches require as many as 1024 bits.

In addition, we assign different weights to different iris region to compare two iris templates which significantly increases the exactness. After that we match the iris template based on a weighted similarity amount. Experimental results on several iris databases substantiate the efficacy from our technique. [12]

Lim et al. and Ali et al.

decomposed an iris image into four levels using 2D Haar wavelet transform and quantized the fourth-level high-frequency information to form an 87- bit code.[13]

L. Ma et al.

Constructed a bank of spatial filters, whose kernels are suitable for iris authentication to represent local texture features of the iris and thus achieved much better results. The one-dimensional continuous wavelet transform is used to decompose iris image in [13].

Here, each decomposed one-dimensional wave form is approximated by an optimal piece wise linear curve connecting a small set of node points, which is used as a feature vector.[14]

IV. CONCLUSION

This paper discusses the performance of various segmentation techniques for iris recognition to increase the overall accuracy. The automatic segmentation model using Integro differential equations and Hough transform proved to be very successful. The CASIA database provides good segmentation as the eye images had been taken specifically for iris recognition research and boundaries of iris pupil and sclera were clearly distinguished. We have studied the effects of various schemes for image compression on iris recognition performance. The performance of iris recognition systems highly depends on segmentation and normalization.

REFERENCES

[1] C. C. TSAI, J. S. TAUR AND C. W. TAO+ , "Iris Recognition Using Gabor Filters and the Fractal Dimension", Journal Of Information Science And Engineering 25, 633-648 (2009)

[2] Somnath Dey and Debasis Samanta, " Improved Feature Processing for Iris Biometric Authentication System", World Academy of Science, Engineering and Technology Vol:4 2010-03-20

[3] Anil K. Jain, Arun Ross, Umut Uludag "Biometric Template Security: Challenges And Solutions".

[4] Patnala S. R. Chandra Murty1, E. Sreenivasa Reddy2, and I. Ramesh Babu3," Iris Recognition System Using Fractal Dimensions of Haar Patterns", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 2, No.3, September 2009

[5] Dhananjay Ikhar1, Vishwas Deshpande2 & Sachin Untawale3**,** "Implementation of Reliable Open Source IRIS Recognition System" , International Journal on Theoretical and Applied Research in Mechanical Engineering (IJTARME) ISSN : 2319 – 3182, Volume-2, Issue-4, 2013.

[6] Adhyana Gupta1, Dr. Pratistha Mathur2 **, "** Iris Recognition using Feature Detection Techniques in Matlab Simulink Model Blockset" , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 7, July 2014 .

[7] George Chellin Chandran . J 1 Dr. Rajesh. R.S 2, "Performance Analysis of Multimodal Biometric System Authentication", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.

[8] Aly I. Desoky, Hesham A. Ali, Nahla B. Abdel-Hamid , "Enhancing iris recognition system performance using templates fusion", Ain Shams Engineering Journal (2012) 3, 133–14

[9] Yulin Si, Jiangyuan Mei, Huijun Gao*, "*Novel Approaches to Improve Robustness, Accuracy and Rapidity of Iris Recognition Systems", IEEE Transactions On Industrial Informatics, VOL. 8, NO. 1, February 2012.

[10] John Daugman and Cathryn Downing , “Effect of Severe Image Compression on Iris Recognition Performance”, IEEE Transactions On Information Forensics And Security, Vol. 3, No. 1, March 2008 .

[11] R. Wildes, “Iris Recognition: An Emerging Biometric Technology”, Proceedings of the IEEE, vol. 85, pp 1348-1363, 1999.

[12] Somnath Dey and Debasis Samanta , “Improved Feature Processing for Iris Biometric Authentication System”, World Academy of Science, Engineering and Technology Vol:4 2010-03-20

[13] Jafar M. H. Ali and Aboul Ella Hassanien, “ An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory”, AMO -Advanced Modeling and Optimization journal, 5(2):93–104, 2003.

[14] Shinyoung Lim, Kwanyong Lee, Okhwan Byeon, and Taiyun Kim, “ Efficient Iris Recognition through Improvement of Feature Vector and Classifier” , ETRI Journal, 23(2):61–70, June 2001.

[15] Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang, “Efficient Iris Recognition by Characterizing Key Local Variations”, IEEE Transactions on Image Processing, 13(6):739–750, June 2004.

[16] L. Ma, Y. Wang, and T. Tan,”Iris Recognition Using Circular Symmetric Filters”,In Proc. of the 16th International Conference on Pattern Recognition, volume II, pages 414–417, 2002

[17] L. Ma, T. Tan, Y. Wang, and D. Zhang,” Personal Identification Based on Iris Texture Analysis.”,IEEE Transaction on Pattern Analysis and Machine Intelligence, 25(12):1519–1533, December 2003.