Iris Biometrics Recognition Application in Security Management

S.S. Chowhan[1] and G.N. Shinde[2]

Summary

Authentication plays a very critical role in security-related applications like e-commerce. There are a number of methods and techniques for accomplishing this key process. Biometrics is gaining increasing attention in these days. Security systems, having realized the value of biometrics, use biometrics for two basic purposes: to verify or identify users. The use of fingerprints, facial characteristics and other biometrics for identification is becoming more common. This paper overview best of Biometric application for security management. The acquisition of biometric data introduces human research and privacy concerns that must be addressed by the organizations. This paper focus Iris is the best Biometric feature for identity Management.

keywords: Biometric Identification, Finger print, Iris DNA

Introduction

Biometric is the science of recognizing a person based on physical or behavioral characteristics [1]. The commonly used biometric features include speech, fingerprint, face, voice, hand geometry, signature, DNA, Palm, Iris and retinal identification future biometric identification vein pattern identification, Body odor identification, Ear shape identification, Body salinity (salt) identification [2].

To choose the right biometric to be highly fit for the particular situation, one has to navigate through some complex vendor products and keep an eye on future developments in technology and standards. Here comes a list of biometrics with comparatives:

Fingerprints - A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification, such as traditional police method, using pattern-matching devices, and things like moiré fringe patterns and Ultrasonic. This seems to be a very good choice for in-house systems.

Conversely, fingerprint searches are challenged by database size, adding time to searches or necessitating filtering as a search acceleration technique [3]. Even so, fingerprint technology often returns multiple "possible matches," forcing introduction of human decision factors and increasing the potential for error in an authentication decision. Finger prints of a person can be faked-dead people can come to life by using a served thumb.

[1] csantu_149@rediffmail.com. COCSIT, Ambajoagi Road Indra Ghandi College CIDCO, Latur, India Nanded, India

[2] Corresponding author. shindegn@yahoo.co.in. COCSIT, Ambajoagi Road Indra Ghandi College CIDCO, Latur, India Nanded, India

Finger is not accurate as iris recognition. False accepts rate may occur and is approximately 1 in 100,000. Where as in case of Iris FAR is 1 in 1.2 million. Most of the biometric system requires physical contact with devices.

Hand geometry – This involves analyzing and measuring the shape of the hand. It might be suitable where there are more users or where users access the system infrequently. Accuracy can be very high if desired and flexible performance tuning and configuration can accommodate a wide range of applications [4]. Organizations are using hand geometry readers in various scenarios, including time and attendance recording.

Hand geometry does not match with large databases such as pregnancy or any other medication will affect hand size.

Face – Face recognition analyses facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. Because facial scanning needs extra peripheral things that are not included in basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personal [4]. The success rate of verification is affected on certain factors like age, glasses, beard shape and face covering with mask.

Thief's can don a neat mask to fool a simple face recognition Program.

Signature – Signature verification analyses the way user signs his name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. People are used to signatures as a means of transaction-related identity verification [3].

Disadvantages of signature verification are inconsistency which leads to increase errors. Difficult to obtain dynamic information from signature

Voice – Voice authentication is based on voice-to-print authentication, where complex technology transforms voice into text [4]. Voice biometrics requires a microphone, which is available with PCs nowadays. Voice biometrics is to replace the currently used methods, such as PINs, passwords, or account names. But voice will be a complementary technique for finger-scan technology as many people see finger scanning as a higher authentication form.

On other hand it can be easily deceived by people who are expert in mimicking other people's voice.

Iris – Iris as a biometric feature, it is found to be the most reliable and accurate for authentication process available today. While most biometric have 13 to 60 distinct characteristics, the iris is said to have 266 unique spots. Each eye is believed to be unique and remain stable over time and across environments (eg: weather, climate, occupational differences). It is capable of positively identifying persons without physical contact or real time human decision making [5].

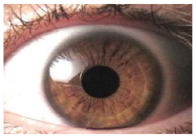

Figure 1:

Biometric Traits

For biometric traits ranking high in accuracy, fingerprints currently have the lowest costs. The iris rates high in all categories, unfortunately including cost. If the costs would sink significantly, the iris would be ideal. DNA loses points in accuracy, because it can't differentiate between monozygotic twins today [6].

There are several methods in accomplishing the process of identifying one's fingerprint.

Figure 2:

The most common method involves recording and comparing the biometrics.

For finger print pores structure and lines on the fingers.

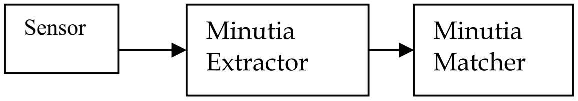

Figure 3:

A fingerprint recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher. To implement a minutia extractor, a three-stage approach is widely used by researchers. They are preprocessing, minutia extraction and postprocessing stage.

The minutia matcher chooses any two minutia as a reference minutia pair and then match their associated ridges first. If the ridges match well, two fingerprint images are aligned and matching is conducted for all remaining minutia [7].

Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis [2].

Handwritten signature verification (HSV) can be Classified into two categories: on-line HSV and off-line HSV. The former relies on dynamic attributes, such as pressure, velocity and acceleration. The latter analyzes the digitized signature images, in which dynamic features are lost. Usually three kinds of forgery can happen in signature verification. Random forgery is taking the genuine signature of others for that of the current user. Skilled forgery is produced with close imitations. It is hard to be differentiated from the genuine one only by shape variations. Simple forgery is produced with the knowledge of content but without close imitations. For example, the forger signs out of his/her memory on the genuine signature.

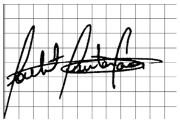

Figure 4: The grid-segmentation

Graphometric and computational feature relations

Graphometric Features

Caliber, Proportionally, white spaces, Base behavior, apparent pressure, curvature progression.

Computational Features

Space occupation, Pressure area, Stroke curvature, Stroke regularity [8].

DNA Each DNA array contains the measures of the level of expression for many genes.

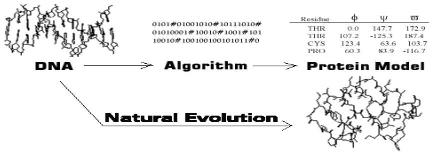

Figure 5:

These values are usually obtained by measuring the fluorescence intensity and subtracting the background. Each DNA array can be considered as a single measure of the expression of many genes for a given condition [7, 8].

If we have two genes with their corresponding expression patterns: **gene1 (e11, e12, .. e1n)** and **gene2 (e21, e22, .. e2n)**, different distances are obtained as follows. *Euclidean* distance is obtained as the square root of the summation of the squares of the differences between all pairs of corresponding values.

$$d_{1,2} = \sqrt{\sum_i (e_{1i} - e_{2i})^2} \tag{1}$$

An equivalent distance, the *squared Euclidean* distance, is the square of the *Euclidean* distance. Generally speaking, these types of distances are suitable when the aim is to cluster genes displaying similar levels of expression [9, 10].

Over view of Iris Recognition

Human Iris has epigenetic formation and it is formed part from the individual DNA, but a great deal of its final pattern is developed at random. It means that two eyes from same individual, although very similar, contain unique patterns similarly identical twins would exhibit four different iris patterns. Pattern Recognition and image processing algorithms can be used to extract the unique pattern of iris from an image and encode it into an iris template.

John Daugman [11,12] first proposed algorithm for iris recognition. His algorithm is based on Iris codes. Integro differential operators are used to detect the centre and diameter of the iris.

$$\max_{(r,x_0,yo)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x0,y0,} \frac{I(x,y)}{2\pi r} ds \right| \tag{2}$$

The image is converted from Cartesian to polar transform and rectangular representation of the region of interest is generated. Feature extraction algorithm uses the complex valued 2D Gabor wavelets to generate the iris codes which are then matched using Hamming Distance. The algorithm gives the accuracy of more than 99%. Also the time required for iris identification is less than one second.

$$h_{\{\mathrm{Re,Im}\}} = \mathrm{sgn}_{\{Re,Im\}} \int_\rho \int_\phi I(\rho,\phi) e^{-iw(\theta_0-\phi)} e^{-(r0-\rho)/\alpha^2} e^{-(\theta_o-\phi)^2/\beta^2} \rho d\rho d\phi \tag{3}$$

Log filters are constructed using

$$G(f) = \exp\left[\frac{-(\log(f/f_o))^2}{2(\log(\sigma/f_o))^2}\right] \tag{4}$$

R.P.Wildes [13] used an isotropic band pass decomposition derived from the application of laplacian of Gaussian filters to the image data like Daugman. Wildes also used first derivative of image intensity to find the location of edges corresponding to the border of the iris his system focus on upper & lower eyelids with parabolic arc. The result on this system good enough to recognize individuals in the minimum time period. M.Vatsa, R Singh and A.Noore [14] proposed a novel iris recognition system using 1D log polar Gabor wavelet and Euler numbers. 1D log polar Gabor wavelet is used to extract the textural features, and Euler numbers are used to extract topological features of the iris. The proposed decision strategy uses these features to authenticate an individual's identity while maintaining a low false rejection rate. Vector difference Matching Algorithm is used for Euler code matching for the two masked binary templates A_i and B_iHD can be calculated as:

$$\mathrm{HD} = \frac{1}{\mathrm{N}} \sum_{i=1}^{N} A_i \oplus B_i \text{ and } \mathrm{MS}_{\pi} = (1 - \mathrm{HD}) \tag{5}$$

The algorithm was tested on CASIA iris image database and found to perform better than existing approaches with an overall accuracy of 99.93%.

C.-L. Tisse and L. Michel Torres,[15] used a combination of the integro-differential operators with a Hough Transform for localization and for feature extraction the concept of instantaneous phase or emergent frequency is used. Iris code is generated by thresholding both the models of emergent frequency and the real and imaginary parts of the instantaneous phase. Finally the matching is performed using Hamming distance. 11% false reject rate was obtained by the algorithm. Hugo Proenca and Luis A. Alexandre [16] had focused on noncooperative iris recognition proposed a method for iris classification which divides the segmented and normalized iris images into six regions, makes an independent feature extraction and comparison for each region, and combines each of the dissimilarity values through a classification rule. YA-PING HUANG CHEN [17] new iris recognition algorithm is proposed which adopts Independent Component Analysis (ICA) to extract iris texture feature and competitive learning mechanism to recognize iris pattern. Experimental results show that the algorithm is efficient and adaptive to environment, e.g. it works well even for blurred iris image, variable illumination, and interference of eyelids and eyelashes. GU Hong-ying, ZHUANG Yue-ting , PAN Yun-he [18] had proposed a new iris feature extraction approach using both spatial and frequency domain is presented. Steerable pyramid is adopted to get the orientation information on iris images. The feature sequence is extracted on each sub-image and used to train Support Vector Machine (SVM) as iris classifiers. SVM has drawn great interest recently as one of the best classifiers in machine learning, although there is a problem in the use of traditional SVM for iris recognition. It cannot treat False Accept and False Reject differently with different security requirements. Therefore, a new kind of SVM called Non-symmetrical SVM is presented to classify the iris features. Fractal dimesion is used to recognize and segment textures in images (chaudhuri and sarkar, 1995) box counting dimension is used.

$$\mathrm{Dim}_{\mathrm{B}} F = \lim_{\delta \to 0} \frac{\log N_{\delta}(F)}{-\log \delta} \tag{6}$$

A. Poursaberi and B. N. Araabi[1] had proposed two different Algorithms are for iris segmentation. The first Algorithm, a circle is located around the pupil with an appropriate diameter the Iris area is encircled by the circular boundary is used for recognition purposes. The second algorithm again circle is located around the pupil with larger diameter. Hamming and harmonic mean distance classifiers are exploited as a mixed classifier in their algorithm. It is observed that relying on a smaller but more reliable part of the iris, though reducing the net amount of information, improves the overall performance. Experiment is performed on CASIA database and the performance with an accuracy of 99.31%. The sensitivity of the proposed method is analyzed versus contrast, illumination, and noise as well, where lower sensitivity to all factors is observed when the lower half of the iris is used for recognition.

Hugo Proença and Luís A. Alexandre [21] "Toward Noncooperative Iris Recognition: A Classification Approach Using Multiple Signatures", had focus on non-cooperative iris recognition, i.e., the capture of iris images at large distances, under less controlled lighting conditions, and without active participation of the subjects. This increases the probability of capturing very heterogeneous images (regarding focus, contrast, or brightness) and with several noise factors (iris obstructions and reflections) propose an iris classification method that divides the segmented and normalized iris image into six regions, makes an independent feature extraction and comparison for each region, and combines each of the dissimilarity values through a classification rule. Experiments show a substantial decrease, higher than 40 percent, of the false rejection rates in the recognition of noisy iris images.

Biometric Measurements

There are two factors which indicate the level of accuracy, or reliability, of any given biometric. They are False Reject Rate (FRR) and False Accept Rate (FAR).

The justification for identification for the user is identified not only from his or her own personal features but also those of others, as normally would be considered a false acceptance. The user, however, does not notice the systems mistake. Mathematically under ideal conditions as it could be

$$\mathrm{FRR}_{\mathrm{N}} = \mathrm{FRR}_1(1-\mathrm{FAR}_1)^{N-1}$$

Probability of occurring for authorized users (p$_B$(n)) and unauthorized users (p$_N$(n)):

$$p_N(n) = \frac{\text{Nor of Measurement occurs for unauthorized}}{\text{Total nor of measurement for Unauthorized User}}$$

$$p_N(n) = \frac{\text{Nor of Measurement occurs for authorized}}{\text{Total nor of measurement for authorized User}}$$

Effectiveness of Iris Authentication

Now days, security is one of the important factor in the field of information technology, business, e-commerce, military and etc. For this reason Personal identification has become very important some methods of identification are used such as PIN, Password, ID card, Signatures that are widely used and have some draw backs. ID card or PIN can be stolen or forgotten and signatures can be limited. Most of the Companies started to use biometric authentication to protect high confidential assests. Iris detection is one of the most accurate and secure means of biometric identification. Iris has many properties which make it ideal biometric recognition. The iris has the unique characterstics of very little variation over life period yet a multitude variation between individuals. Iris not only differs between identical twins but also from left to right eye.

Most of the Iris detection algorithm use random circles to determine the iris parameters.

Iris begins to form in the third month of gestation [19] and the structures creating its pattern are largely complete by the eight month, although pigment accretion can continue into the first postnatal years. Its complex pattern can contain many distinctive features.

In 1993 John.G. Daugman first proposed methods for encoding and recognizing iris patterns it has been deployed in public trails, including those by British Telecom, US Sandia Labs, UK National Physical Laboratory, The National Biometric Center of SJSU, Siemens, Unisys, LG, IriScan, Iridian, Sarnoff. All these organization have reported false acceptance is zero in all tests.

Most modern iris detection algorithms produce what is known as iris mask. The mask represents the portion of the iris obstructed by the eyelid or eyelash. This portion can be ignored when doing the iris code comparison.

Comparison of Iris codes

Comparision problem comes when we want authenticate a new user. The eye image is captured and iris code is produced from the image then the new code is compared to the stored database. (Eg: The hamming distance can be used any two equal length binary vectors is simply the number of bit position in which they differ divided by length of the vectors. In this way, two identical vectors will differ in their bits giving a Hamming distance of 0.5)

Advantages of Iris

- It is highly protected, internal organ of the eye.
- Patterns can be captured from distance.
- It posses high degree of randomness
- Encoding and decision making are tractable analysis & encoding time is one second.

- Search speed: 100,000 Iris Codes per second on 300 MHz CPU.

Disadvantages of Iris

- Partially occluded by eyelids.
- Some negative connotations.
- Obscured by eyelashes, lenses, reflections.
- Illumination should not be visible or bright.

Iris Database

There are some databases, which are freely available to public they are CASIA, MMU, BATH, UPOL, ICE, WVU and UBIRIS.

CASIA database is widely used for biometric purposes. CASIA-IrisV3 [20] includes three subsets which are labeled as CASIA-IrisV3-Interval, CASIA-IrisV3-Lamp, CASIA-IrisV3-Twins. CASIA-IrisV3 contains a total of 22,051 iris images from more than 700 subjects. All iris images are 8 bit gray-level JPEG files, collected under near infrared illumination. Iris images of CASIA-IrisV3-Interval were captured with our self-developed iris camera CASIA-IrisV3-Interval is a superset of CASIA V1.0 which has been requested by and released to more than 1,500 researchers/teams from 70 countries and regions (as of June 2006). CASIA V1.0 contains 756 iris images from 108 subjects. In order to protect our IPR in the design of our iris camera (especially the NIR illumination scheme), the pupil regions of all iris images in CASIA V1.0 were automatically detected and replaced with a circular region of constant intensity to mask out the specular reflections from the NIR illuminators. UPOL images were captured with an optometric frame work, obtaining optimal images with extremely similar characteristics. ICE and WVU database contains images with more noise factors, their lack of images with significant reflections within the iris rings constitutes a weak point regarding the simulation of noncooperative imaging conditions. Oppositely, images of the UBIRIS database were captured under natural lighting and heterogenous imaging conditions, which explains their higher heterogeneity. Each data set enables, respectively, 1,800 and 78,000 intra and interclass comparisons. Images of the UBIRIS data sets contain iris. Obstructions by eyelids and eyelashes, poor focused and motion blurred irises, and irises with specular and lighting reflections, while those of the CASIA and ICE data sets contain, almost exclusively, iris obstructions by eyelids and eyelashes and a small number of poorly focused images.

Conclusion

We briefly focused on iris biometric comparing with other biometric application. The performance of iris is best as compared to other biometrics. With the need of security systems at location such as national borders and airports iris recognition is emerging as one of the identification systems.

- Authentication based upon physical attributes of individuals
- There are many biometric
- measurements that can be used, depending on the application
- Biometrics must be implemented properly to be effective and the consequences considered
- Biometrics will become increasingly prevalent in day-to-day activities where proper identification is required

References

1. A. Poursaberi and B.N. Arrabi, "*Iris Recognition for Partially occluded images Methodology and Sensitive Analysis*", Hindawi Publishing corporation journal on Advances in Signal Processing, vol 2007, Article ID 36751, 12...
2. D.Zhang Automated Biometrics Technologies and systems Kluwer Academic, Boston, Mass, USA, 2000.
3. Iris Recognition, "*How iris Recognition works*", http:// www.lgiris.com/iris/works.html, 09 Jan 2007.
4. "Biometric Technology", http:// www.peterindia.net/Biometric/Biometric.org.
5. Paulo Eduardo Merloti, "Experiment on Human Iris Recognition Using Error Back Propagation Artificial Neural Network", Prepared for Neural Network Class (CS533) of Spring Semester of 2004.
6. "Bioidentification", http:// www.bromba.com/faq/biafaqe.htm, 17 Feb 2007.
7. Wu Zhili, "*Fingerprint Recognition*", Ph.D.Thesis, Hong Kong Baptist, University, 2002.
8. liang wan, Zhou-chen lin, Rong chun Zhao, " *off-line Signature Verification Incorporating the prior mode*l", Multimodal user interface Group, Microsoft Research, Asia, Beijing 100080, China.
9. Cesar Santos, Edson J.R, Justino, Flavio Bertolozzi, Robert Sabaourin, "An off-line Signature Verification Method Based on the questioned document expert's Approach and a Neural Network Classifier", Catolica do Parana, Rua Imaculada onceicao,1155,Curitiba, PR, Brazil.
10. Alfonso Valencia, Joaquin Dopazo, " *A Hierarchical unsupervised growing neural network for clustering gene expression Pattern*".
11. John .G. Daugman, "*High Confidence Visual Recognition of Persons by a test of statistical Independence*", IEEE Trans, Pattern Analysis and Machine intelligence, vol.15, no.11, pp-1148-1161, 1993.

12. John .G. Daugman,"*Statistical Richness of Visual Phase Information: update on Recognizing Persons by Iris Patterns*", International Journal of Computer Vision, vol.45, no.1, pp-25-38, 2000.
13. R. P. Wildes, "Iris Recognition: An Emerging Biometric Technology," Proceedings of the IEEE, Vol. 85, No. 9, 1999, pp. 1348-1363
14. M. Vatsa, R. Singh, and A. Noore, " *Reducing the False Rejection Rate of Iris Recognition Using Textural and Topological Features*", International Journal of Signal Processing, vol.2, no.2, ISSN1304-4494, 2005.
15. C.-L. Tisse and L. Michel Torres, "*Robert, Person Identification Technique Using Human Iris Recognition*", *Proceedings of the 15th International Conference on Vision Interface*, 2002, pp. 294-299.
16. Hugo Provencal, Luís A. Alexandre," *Toward Noncooperative Iris Recognition: A Classification Approach Using Multiple Signatures"*, IEEE Trans, on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, April 2007.
17. YA-PING HUANG, SI-WEI LUO, EN-YI CHEN, "*An Efficient Iris Recognition System*", Proceedings of the First International Conference on Machine Learning and Cybernetics, Beijing, 4-5 November 2002.
18. GU Hong-ying, ZHUANG Yue-ting , PAN Yun-he,"*An iris recognition method based on multi-orientation features and Non-symmetrical SVM",* Journal of Zhejiang University SCIENCE, ISSN 1009-3095.
19. John .G. Daugman,"The importance of being random: Statistical Principles of iris recognition ", Pattern Recognition Society, Published by Elsevier Science Ltd, 279-291, 2001.
20. CASIA–IrisV3- http://www.cbsr.ia.ac.cn/IrisDatabase.htm.
21. Hugo Proença and Luís A. Alexandre," Toward Noncooperative Iris Recognition: A Classification Approach Using Multiple Signatures", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 29, NO. 4, APRIL 2007.
22. John .G. Daugman, "How Iris Recognition Works", IEEE Trans, Circuit and Syst for Video Tech., vol.14, no.1, pp-21-3-, Jan 2004.
23. John .G. Daugman, " Complete discrete 2-D Gabor transform by Neural Network for image analysis and Compression", Acoustics, Speech and Signal Processing,IEEE Trans, vol.36, 1169-1174,1998.
24. John .G. Daugman, Cathryn Dowing," Epigenetic randomness, Complexity and Singularity of Human iris patterns", PROC.R.SOC.land.B Revised 14 December 2000.

25. Schultz, R.C., Ives, R.W., " *Biometric Data Acquisition using MATLAB GUI's* " 35^{TH} ASEE/IEEE Frontiers education conference ,Oct 19-22, 2005, Indianapolis.

26. Jim Bezdek, "*Fuzzy models-what are they, and why?,*" *IEEE Trans. on Fuzzy Systems,* Vol. 1, No. 1, pp. 1-6, February 1993.

27. Ahmad M. Ibrahim, *Introduction to Applied Fuzzy Electronics.* New Delhi: Prentice Hall of India, 1999. pp 27- 139.

28. D. Driankov, H. Hellendoorn, and M. Reinfrank, *An Introduction to Fuzzy Control.* New Delhi: Narosa Publishing House, 1997.

29. G.J. Klir and T.A. Folger, *Fuzzy Sets, Uncertainty and Information.* New Delhi: Prentice Hall of India, 1995 pp 50- 150.

30. H.K. Kwan and Y. Cai, "*A Fuzzy neural network and its application to pattern recognition,*" *IEEE Transactions on Fuzzy Systems*, Vol. 2, No. 3, pp. 185-192, August 1994.