Improvement of Performance Evaluation for Iris Pattern Recognition

Emmanvel Raj.M.Chirchi
Research Scholar
JNTUH
Kukatpally, Hyderabad.-500058

Dr.R.D.Kharadkar
Principal
G.H. Raisoni Institute of Engineering & Technology
Warhol, Pune-412 207

ABSTRACT

In this paper, we describe the performance improvement by reducing FAR and FRR for quality of the algorithm, as the performance evaluation is very important for fast iris identification if the image is occluded or covered by eyelid and very little iris image is retrieve or noisy image, though our algorithm works very efficiently for correct identification of person as it is important for the security system. We use CASIAv3 and UBIRISv1 database.

General Terms

Pattern Recognition for security systems.

Keywords

FAR, FRR, FTE, FTA, Iris recognition,

1. INTRODUCTION

Security Systems are in critical need of finding accurate, secure and cost-effective alternatives to passwords and personal identification numbers (PIN) as financial losses increase dramatically year over year from computer-based fraud such as computer hacking and identity theft [1].Biometric solutions address these fundamental problems, because an individual's biometric data is unique and cannot be transferred. Biometrics is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics [1][2].To control the access to secure areas or material, a reliable personal identification infrastructure is required. Conventional methods of recognizing the identity of a person by using passwords or cards are not altogether reliable, because they can be forgotten or stolen. Out of the entire existing biometric, Iris biometric is best suitable as it cannot be stolen or cannot be easily morphed by any person. We can understand how iris pattern is (as in Figure1). Anatomical structure of eye, the iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle (as in Figure2) the pattern extracted from iris is unique from persons left eye to person right eye, no two identical twins has the same iris pattern, it remains same throughout lifetime [14], developmental biology further suggests that, while the general structure of the iris is genetically determined, the particular aspects of its details are dependent upon circumstance, like the conditions in the embryonic precursor to the iris. so iris is secure and reliable biometric for security system of all biometrics. Thus this technology is now considered as providing positive identification of an individual without contact and at very high confidence levels. The table 1[16] below gives the comparison of biometrics. It isolates the eye and defines a circular pupillary boundary between the iris and the pupil portions of the image, and it defines another circular boundary between the iris and the sclera portions of the image and the system defines plurality of annular bands within the iris image. Then it adds the iris code and due to Hamming distance compares the code with stored iris codes.

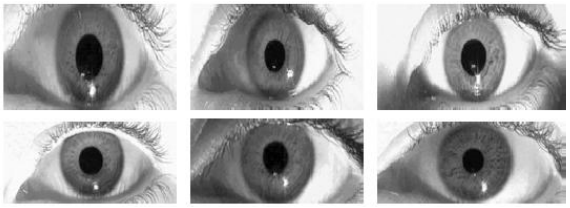


Figure1: Human Iris pattern

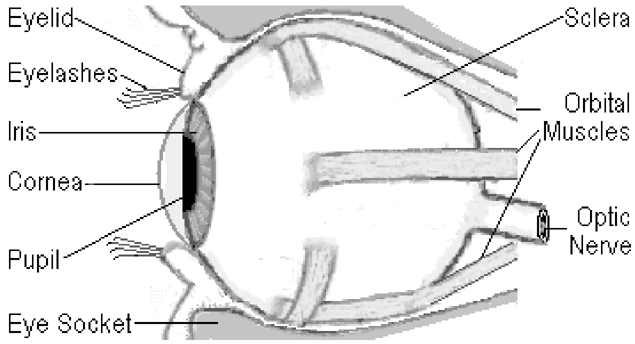


Figure2: Structure of Iris

The rest of the paper will cover section (2) background and related work, section(3) proposed work, section(5) conclusion.

Table 1: comparative list of Biometrics [16]

Method	Code Pattern	Identification rate	Security	Application
Iris	Iris Pattern	1/1200,000	High	High-security
Finger print	Finger prints	1/1,000	Medium	Universal
Voice	Voice characteristics	1/30	Low	Tele-communication
Signature	Letters shape	1/100	Low	Low-security
Face	Outline shape	1/100	Low	Low-security
Palm	Size, length, thickness of hand	1/700	Low	Low-security

2. BACKGROUND AND RELATED WORK

In biometrics there are two authentication methods they are *verification*, is based on a unique identifier which singles out a particular person and that person’s biometrics and *identification*, it is based *on* biometric iris pattern. It compares these patterns to entire database of enrolled individual instead of just a single record selected by some identifier. Biometric recognition system design is essential to the design of pattern recognition system, it is a phase by phase modular and building block of a biometric authentication system is (as in figure3).

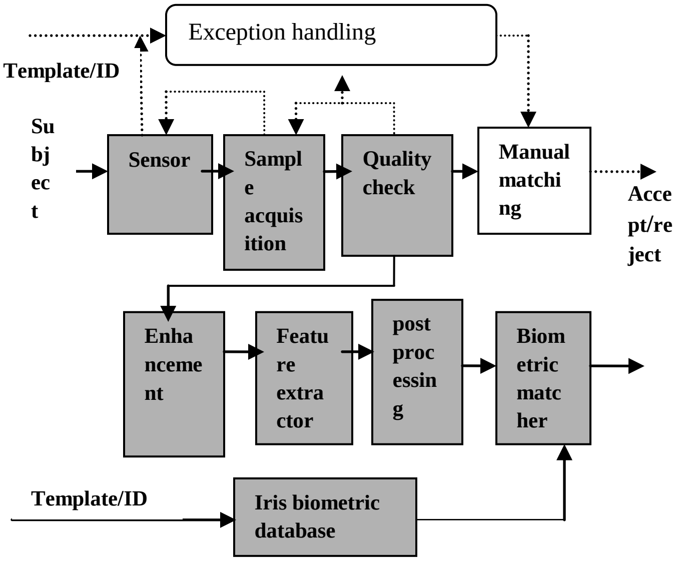


Figure 3: Iris biometric authentication system

The shaded boxes are automated processes, the white boxes are manual processes, system accuracy is done by the process of verification when enrolled subjects present their biometric identifier and correct identity to the system, the system accuracy depends on error rates i.e. chance of accepting an intruder (False Accept rate) FAR and probability of rejecting an authorized user (False Reject rate) FRR [13]. Exceptional handling is procedure of manual matching process of biometric system shown with white boxes (as in Figure 3). Subject could not use biometric authentication system, which may leads to Failure to Use (FTU), the Failure to Enroll (FTE) and Failure to Acquire (FTA). FTA is detected through the feedback loops in the sequential architecture. A biometric system’s accuracy is determined by combining the rates of false acceptance and rejection. Each error presents a unique administrative challenge. For instance, if you are protecting sensitive data with a biometric system, you may want to tune the system to reduce the number of false acceptances. However, a system that's highly calibrated to reduce false acceptances may also increase false rejections, resulting in more help desk calls and administrator intervention. Therefore, administrators must clearly understand the value of the information or systems to be protected, and then find a balance between acceptance and rejection rates appropriate to that value. A poorly created enrollment template can compound false acceptance and rejection. For example, if a user enrolls in the system with dirt on his finger, it may create an inaccurate template that doesn't match a clean print. Natural changes in a user's physical traits may also lead to errors. The point of intersection is called the crossover accuracy of the system. In general, as the value of the crossover accuracy becomes higher, the inherent accuracy of the biometric increases. Table (1) shows crossover accuracy of the different biometric technology [15].

Table2: Comparison of biometric accuracy [15]

Biometrics	Crossover Accuracy
Retinal Scan	1:10,000,000+
Iris Scan	1:131,000
Fingerprints	1:500
Hand Geometry	1:500
Signature Dynamics	1:50
Voice Dynamics	1:50

Test scenario as in [4] is verification within database of the user; the iris authentication error rates found in [4] are as in table3. FTU (failure to use) rate, the probability that a person will not use a voluntary biometric authentication system and will stick to the legacy system.

Table3: The iris verification error rates [4]

	False Reject	False Accept	FTE	FTA
Iris	0.0%	2.0%	0.5%	0.0%
Explanation	Two different iris images are falsely matched	Two images of the same iris fail to match	Iris image cannot be acquired for enrollment	Iris image cannot be acquired for verification

Subjects just present the iris and the system makes the correct or incorrect decision, where an incorrect decision i.e., error condition can only be a misidentification. For such identification systems, the FAR is a function of m, the number of subjects in database M. as in equation1.

$$FAR\ (m) \approx m \times FAR\ (1)\ldots..(1)$$

FAR is affected by m; FRR is not affected by m Bouchier et al. [5].895 iris identification transactions were recorded with 106 actual rejections i.e., FRR of 11.8%. The reasons for false iris rejects are *environmental or user error*, i.e. presenting or not clearly opening eye i.e. O**bscure** the iris, *reflection from glasses* i.e. **Glare** in the image, user difficulty i.e., non- dominant eye. The Failure to Enroll (FTE) rate is due to poor user interface.

3. PROPOSED WORK

The proposed research work has the following steps (as in figure4)

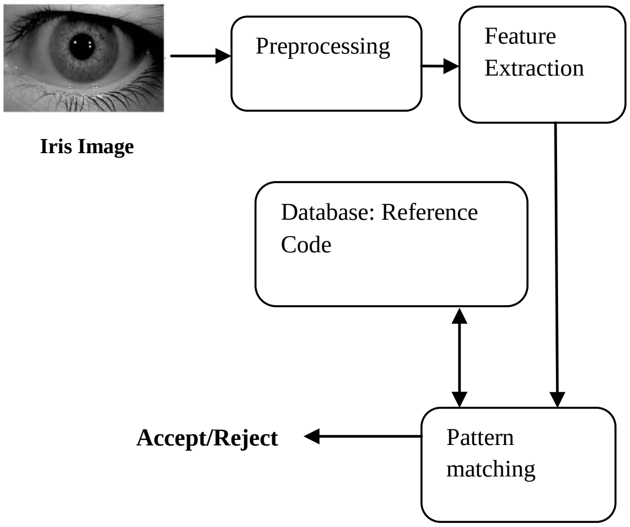


Figure4: Steps for iris recognition System

3.1 Image Acquisition

Image acquisition step is considered to be one of the most sensitive and important for the quality of image to be processed, data extracted from raw input determines the performance of the entire system to a large extent. Two of the related issues are: *Assessment of quality*: It means the quality and relevance of data is assessed to determine its suitability for the application *Separation:* It means separating the relevant data from the whole chunk of information to obtain the object of interest. Careful selection of data further helps improve the performance of the system and avoiding undesirable measurements. as image of the eye to be analyzed must be acquired first in digital form suitable for analysis so we are using database available in public domain such as Chinese Academy of science-Institute of Automation (CASIA v3)[11] and UBIRIS for noisy iris images[10].

3.2 Preprocessing

The image is converted to some form suitable for rest of processing like conversion of gray scale to binary image.

3.2.1 Locating Iris

Before performing iris pattern matching, the boundaries of the iris should be located. In other words, we are supposed to detect the part of the image that extends from inside the limbus (the border between the sclera and the iris) to the outside of the pupil. The first processing step consists in locating the inner and outer boundaries of the iris and second step to normalize iris and third step to enhance the original image(as in Figure5) [7][9][12]. The Daugman's system, Integro differential operators as in eq(2) is used to detect the center and diameter of iris and pupil respectively. In order to increase the performance, a coarse-to-fine strategy is exploited as follows [7].

- To reduce computational complexity rescaling the iris image with a given scale factor.
- Vertical median filter has to perform to minimize noise.
- Image edge is extracted using Candy operator and
- Voting the maximum circle (x_s, y_s, r_s) based on searching the inner (pupillary) boundary $(x_p, y_{p,}, r_p)$.
- Construct histogram of binary image as the outer (sclera) boundary, where (x_p, y_p) lies on the rectangle interval $(x_p \pm 5, y_p \pm 5)$.
- The inner circle lies within the circle that describes the sclera boundary.
- Localizing accurately the outer and inner boundary based on the rough boundary of earlier steps by using effective integrodifferential operator as in eq(2).

$$\max_{(r,x0,y0)} \left| G\sigma(r) * \frac{\partial}{\partial r} \oint_{x0,y0} \frac{I(x,y)}{2\pi r}\, ds \right| \ldots\ldots..(2)$$

The iris may be occluded by eyelids or corrupted by eyelashes in some cases. In order to get rid of noise, eyelids and eyelashes detection is provided:

- Based on histogram Hough transformation, calculate the edge of upper and lower eyelids by searching the two curves satisfying eq (3).

$$X\ (t) = at^2 + bt + c,\ t \in [0, 1] \ldots\ldots (3)$$

- Eyelashes are detected according to two situations:
  1. If one line exists on the area below upper eyelash, it is considered as a separate eyelash;
  2. If the variance of some given small window in the iris image less than threshold, it is regarded **as** multiple eyelashes. Through such process, the eyelashes can he marked and excluded when iris is encoded.

3.2.2 Cartesian to polar reference transform

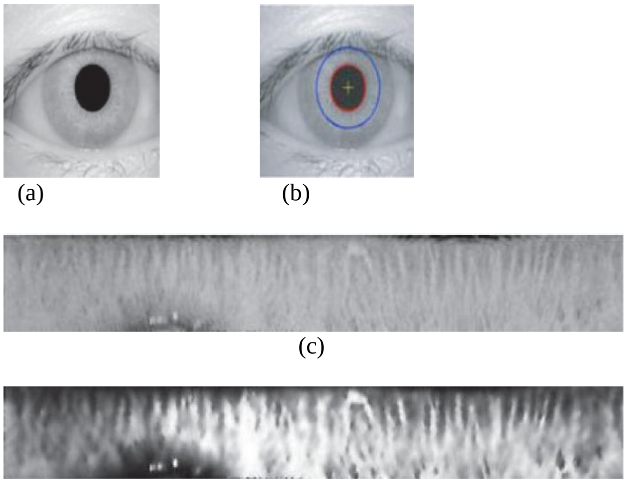
Cartesian to polar reference transform suggested by J.Daugman authorizes equivalent rectangular representation of the zone of interest (as in Figure5), remaps each pixel in the pair of polar co-ordinates(r, Ɵ) where r and Ɵ are on interval [0,1] and [0,π] respectively. The unwrapping is formulated as in eq. (4) [8].

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \ldots.. (4)$$

Such that

$$\begin{pmatrix} (r,\theta) = (1-r)x_p(\theta) + r x_i(\theta) \\ (r,\theta) = (1-r)y_p(\theta) + r y_i(\theta) \end{pmatrix} \ldots\ldots (5)$$

where $I(x, y)$, (x, y), (r, Θ), (x_p, y_p), (x_i, y_i) are the iris region, Cartesian coordinates, corresponding polar coordinates, coordinates of the pupil, and iris boundaries along the Ɵ direction, respectively.



(a) (b)

(c)

(d)

Figure 5: (a) Original image; (b) localized iris; (c) normalized iris; and (d) enhanced iris.

3.3 Feature Extraction

Normalized iris image is used for features extraction. Overall feature extraction processing is as following: [6]

Step l. Divide normalized iris image into basic cell regions for calculating cumulative sums (as in Figure 6).

Step2. Basic cell regions are grouped in a horizontal direction and in a vertical direction (as in Figure 6). (Five basic regions are grouped into a group)
Step3. Calculate cumulative sums over the each group
(as in equation (6)).
Step4. Generate iris feature codes.

The commulative sums are calculated as follows: Suppose that X1, X2,. .., X5 mean five representative values of each cell regions within a group.

- ✓ First calculate the average $\bar{X} = \frac{X1+X2+X3.....+X5}{X5}$
- ✓ Calculate cumulative sum from 0: S0 = 0
- ✓ Calculate the other cumulative sums by adding the difference between current value and the average to the previous sum,

i.e., $S_{i=} S_{i-1}$+(X_i-X) for i=1,2,…5 …..(6)

After calculation cumulative sums, iris codes are generated for each cells using following algorithm after obtaining MAX and MIN values among cumulative sums[6].

```
If $S_i$ located between MAX and MIN index
If $S_i$ on upward slope
          Set cell's iris_ code to "1"
If $S_5$ on downward slope
          Set cell's iris_code to "2"
else
          Set cell's iris_code to "0"
```

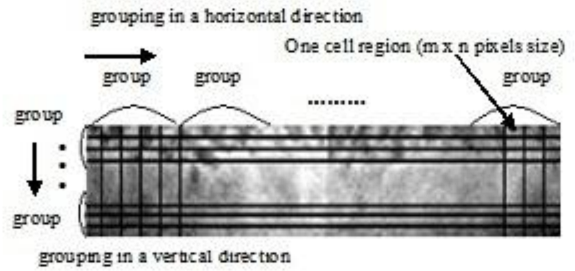

grouping in a horizontal direction
One cell region (m x n pixels size)
group
group
....
group
group
group
grouping in a vertical direction

Figure6: Divide normalized iris image into cell regions and grouping of cell regions.

This algorithm[6] generates iris codes by analyzing the changes of grey values of iris patterns. Upward slope of cumulative sums means that iris pattern may change from darkness to brightness. Downward slope of cumulative sums means the opposite change of upward slope.

3.4 Pattern Matching

By comparing similarities between feature vectors of two irises to determine that they are accepted or rejected. Since feature vector is binary, the matching process will be fast and simple accordingly. Performance of classifiers is based on minimum Hamming Distance (MHD) as in (7).

HD=XOR (codeA, codeB) ….. (7)

Where codeA and CodeB are the templates of two images. When an iris image is captured in system, the designed classifier compares it with the whole images in each class. The Hamming distance (HDs) between input images and images in each class are calculated, then the two different classifiers are being applied as follows [8][9].

I. In the first classifier, the minimum HD between input iris code and codes of each class is computed.
II. In the second classifier, the harmonic mean of the *n* HDs that have been recorded yet is assigned to the class as in (8)[9].

$$HM = \frac{lengt\ h(code\ )}{\sum_{i=1}^{lengt\ h(code\ )}(\frac{1}{code\ (i)})} …..(8)$$

3.5 Accept/Reject

Final phase of proposed work is accept subject code or reject the subject code it depends on identification and verification modes are two main goals of every security system based on the needs of the environment. In the verification stage, the system checks if the user data that was entered is correct or not (e.g., username and password) but in the identification stage, the system tries to discover who the subject is without any input information. Hence, verification is a one-to one search but identification is a one-to-many comparison

.

4. ACKNOWLEDGMENT

My sincere thanks to our esteem institute MBES COEA's principal, staff, friends for their help and support to do my research work, and very grateful to my honorable research guide for their continous guideline for my work.

5. CONCLUSION

In proposed research work we measure performance evaluation with two error rates i.e., FAR, FRR using the following eq. (9) for False Acceptance Rate and False Rejection Rate in eq. (10)

$$FAR(\%) = \frac{No.of\ false\ accepted}{total\ \ No.of\ Imposter\ \ attempts} \ldots.. (9)$$

$$FRR(\%) = \frac{No.of\ false\ Rejected}{total\ \ No.of\ authentic\ \ attempts} \ldots\ldots (10)$$

on the bases of the measurement we generate histogram of the algorithm, so we improve the algorithm by reducing False rejection rate by increasing hamming distance value and reducing False Acceptance by decreasing hamming distance value.

6. REFERENCES

[1] R.P. Wilde, “Iris recognition: An Emerging Biometric Technology Proc. IEEE, Vol.85, no.9, pp. 1348-1363, 1997.

[2] W. Boles and B. Boashash,” A Human Identification Technique using images of the Iris and Wavelet Transform “, IEEE Trans. signal processing, vol. 46, no.4,pp.1185-1188,1998.

[3] C. H. Daouk, L. A. El-Esber, F. D. Kammoun and M. A. Al Alaoui.,” Iris Recognition”, IEEE ISSPIT 2002, Marrakesh- page 558.

[4] T.Mansfield and G.Kelly,D.Chandler, and J.Kane,“Biometric product testing final report”,center for mathematics and scientific computing, national physics laboratory, Middlesex, UK, March 2001.

[5] F.A.Bouchier, J.S.Athens, and G.Wells. “Laboratory evaluation of the iriscan prototype biometric identifier. Technical report SAND96-1033 RS-8232-2/960378”, sandia National Laboratories, Albuquerque, NM, April 1996.

[6] Jong-Gook Ko , Yeon-Hee Gil and Jang-Hee Yoo, “Iris Recognition using Cumulative SUM based Change Analysis”,ISPAC,IEEE,2006.

[7] YA-PING HUANG, SI-WEILUO, EN-YICHEN, ”An Efficient iris recognition system”, proceeding of the first international conference on machine learning and cybernetics, Beijing 4-5 November 2002.

[8] Christel-loïc TISSE1, Lionel MARTIN1, Lionel TORRES 2, Michel ROBERT “Person identification technique using human iris recognition”.

[9] A.Poursaberi and B.N.Araabi, “iris recognition or partially occluded images: methodology and sensitivity Analysis” Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2007, Article ID 36751, 12 pages…

[10] Proença, H. and Alexandre,”{UBIRIS}: A noisy iris image database”,13th International Conference on Image Analysis and Processing - ICIAP 2005, Springer , LNCS 3617 pages 970-977, Cagliari, Italy September 2005.

[11] CBSR, http://www.cbsr.ia.ac.cn/IrisDatabase

[12] John Daugman. “Recognizing persons by their iris patterns “Cambridge University, Cambridge, UK.

[13] Ruud M. Bolle, jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, “Guide to Biometrics”, Springer International edition.

[14] John Daugman,” How Iris recognition works”, IEEE transactions on circuits and systems for video technology, vol. 14, no. 1, January 2004

[15] Jafar M. H. Ali, Aboul Ella Hassanien,” An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory”, AMO - Advanced Modeling and Optimization, Volume 5, Number 2, 2003.

[16] Y. Zhu, T. Tan, and Y. Wang, Biometric Personal Identification Based on Handwriting Proc. 15th Int'l Conf. Pattern Recognition, pp. 801-804, 2000