

Biometric Iris Recognition for Person Identification using Cumulative Sum Algorithm

Emmanuel Raj.M.Chirchi, Dr.R.D.Kharadkar

Abstract— Quality of the iris pattern is achieved by using cumulative sum algorithm for feature extraction and this emphasis fast iris identification. In this paper, we describe the performance improvement by reducing FAR and FRR for quality of the algorithm, as the performance evaluation is most important for efficient iris identification if the image is occluded or covered by eyelid and very less iris image is retrieve or noisy image, though our algorithm works efficiently for correct identification of person as it is very important for the security system. We use publicly available database CASIA and UBIRISv1.

Index Terms: - Pattern Recognition, Biometric security systems, 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

Anatomical structure of eye, the iris is a muscle with in 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 melanin pigment within the muscle (as in Fig.2) the pattern extracted from iris is unique from persons left eye to person right eye,

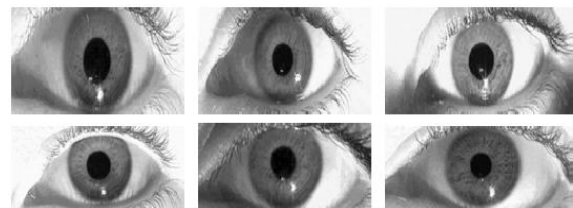


Fig.1: Human Iris pattern

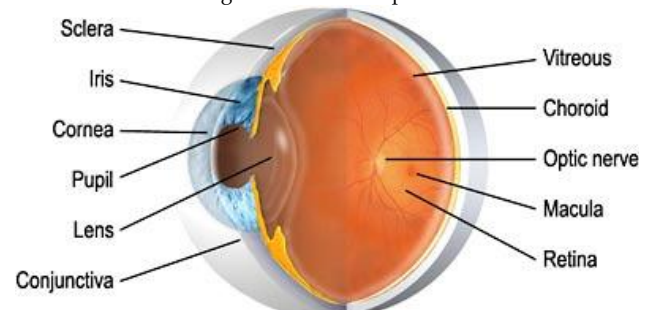


Fig.2: Structure of Iris

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

• ¹Research Scholar, Jawaharlal Nehru Technological University Hyderabad, Kukatpally, Hyderabad 500058, Andra Pradesh, INDIA. E-mail: er.chirchi@gmail.com

• ²Principal, G.H. Rasoni Institute of Engineering & Technology Wagholi, Pune - 412 207, Maharashtra, INDIA. E-mail id: r_kharadkar@yahoo.com

Understand how iris structure is (as in Fig.1).

below gives the comparison of biometrics. The table 1 clearly shows that the out of all biometrics iris is the best as its identification rate is one person is rejected out of 1200,000 iris pattern, so we chose iris biometric for identification for our research work.

Table 1: comparative list of Biometrics

| Method | Code Pattern | Identificat ion 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 |

Iris 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 (as shown in Fig. 2). Then it adds the iris code and due to Hamming distance compares the code with stored iris codes. 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]. Test scenario as in [4] is verification within database of the user; the iris authentication error rates found in [4] are as in table 3.

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 |

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. 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 equation 1.

$$FAR(m) \approx m \times FAR(1) \dots (1)$$

FAR is affected by m; FRR is not affected by m. Bouchier et al., [5],[13]. 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. Obscure 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. The performance of iris recognition can be improved if FRR & FAR reduced. The FAR and FRR can be calculated using eq 2 and eq 3.

$$FAR(\%) = \frac{\text{No. of false accepted}}{\text{total No. of Imposter attempts}} \dots (2)$$

$$FRR(\%) = \frac{\text{No. of false Rejected}}{\text{total No. of authentic attempts}} \dots (3)$$

2. Pros, Cons and Applications

➤ Pros

- ✓ Iris biometric accuracy is very high compared with other biometrics as in table 1.
- ✓ The verification time taken by Iris biometric is very less i.e., 5 seconds or less depending on the identification system and algorithms.

- ✓ Iris is highly protected by the internal organs as it is between cornea and sclera as in Fig.2.
- ✓ Iris patterns possess a high degree of randomness in terms of variability: 244 degrees-of-freedom, entropy: 3.2 bits per square-millimeter, uniqueness: set by combinatorial complexity [16].
- ✓ Once we achieve iris pattern they remain stable throughout the life time.
- ✓ For person identification through Iris pattern, the entity should be present physically for authentication process so hacking is impossible.
- **Cons**
- ✓ For storage of Database it requires lot of memory.
- ✓ The cost of Iris identification system device is high as compared to other biometrics.
- **Applications**[16]
- ✓ Iris pattern is used as living passport for National border controls, Computer login password.
- ✓ Iris pattern is used as authentication for cell phone and other wireless-device-based.
- ✓ Iris patterns are used for securing access to bank accounts at cash machines such as ATM.
- ✓ Iris is used as personal certificate for driving licenses, national ID cards, forensics, birth certificates, and credit cards.
- ✓ Iris is used as an anti-terrorism security screening at airports.
- ✓ Iris is also used in secure financial transactions such as electronic commerce, banking.
- ✓ Iris is also used as Biometric-Key Cryptography for security systems.

The outline of the paper is organized as follows Section(1) Introduction, section(2) Pros, Cons and Applications, section(3) proposed work, section(4) conclusion.

3. Proposed work

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

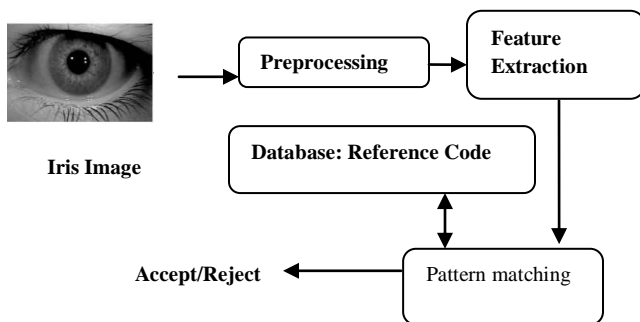


Fig 4: Steps for iris recognition System

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*: The quality and relevance of data is assessed to determine its suitability for the application *Separation*: 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 Fig5) [7],[9],[12]. The Daugman's system, Integro differential operators as in (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].

- Rescaling the iris image at a given scale factor to reduce computational complexity.
- Performing vertical median filter.
- Extracting the image edge with 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) , forming binary image histogram as the outer (sclera) boundary, where (x_p, y_p) lies on the rectangle interval $(x_p \pm 5, y_p \pm 5)$. The additional constraint imposed on this boundary is that 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.

$$\max_{(r,x_0,y_0)} |G\sigma(r) * \frac{\partial}{\partial r} \oint_{x_0,y_0} \frac{I(x,y)}{2\pi r} ds| \dots \dots (2)$$

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:

- Determining the edge of upper and lower eyelids by searching the two curves satisfied $x(t) = at^2 + bt + c, t \in$

[0, 1] based on histogram Hough transformation. The difference between two curves is search area.

- 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 be 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 Fig.5), remaps each pixel in the pair of polar co-ordinates(r, θ) where r and θ are on interval [0,1] and $[0,\pi]$ respectively. The unwrapping is formulated as in eq. (3) [8].

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \dots (3)$$

Such that

$$\begin{pmatrix} (r, \theta) = (1 - r)x_p(\theta) + rx_i(\theta) \\ (r, \theta) = (1 - r)y_p(\theta) + ry_i(\theta) \end{pmatrix} \dots (4)$$

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 θ direction, respectively.

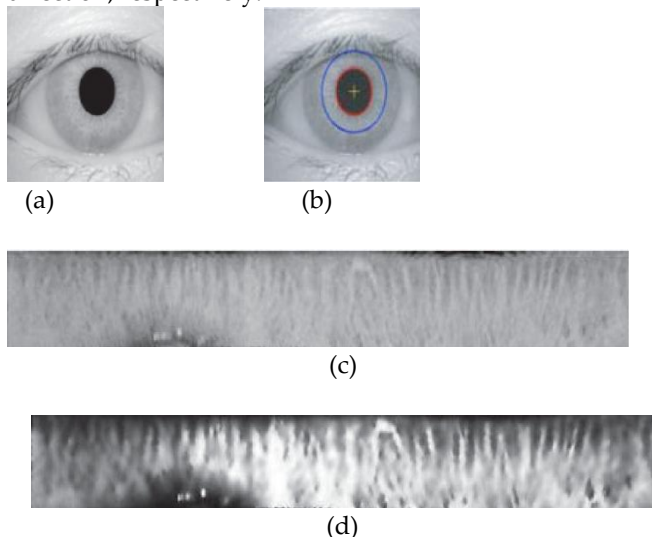


Fig. 5: (a) Original image; (b) localized iris; (c) normalized iris; and (d) enhanced iris.

3.3 Feature Extraction

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

Step1. Divide normalized iris image into basic cell regions for calculating cumulative sums. (One cell region is a $m \times n$ pixels size, and an average grey value is used as a representative value of a basic cell region to calculate the cumulative sum)

Step2. Basic cell regions are grouped in a horizontal direction and in a vertical direction (as in Fig. 6). (Five basic regions are grouped into a group)

Step3. Calculate cumulative sums over the each group as in eq(5).

Step4. Generate iris feature codes.

The commulative sums are calculated as follows: Suppose that X_1, X_2, \dots, X_5 mean five representative values of each cell regions within a group.

✓ First calculate the average $\bar{X} = \frac{X_1 + X_2 + X_3 + \dots + X_5}{X_5}$

- ✓ Calculate cumulative sum from 0: $S_0 = 0$
- ✓ Calculate the other cumulative sums by adding the difference between current value and the average to the previous sum,

$$i.e., S_i = S_{i-1} + (X_i - \bar{X}) \text{ for } i=1,2,\dots,5 \dots (5)$$

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

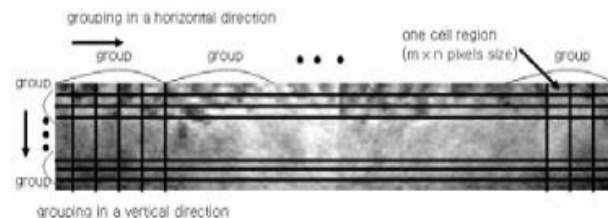


Fig.6: Divide normalized iris image into cell regions and grouping of cell regions.

- if S_i located between MAX and MIN index
- if S_i on upward slope
 - Set cell's iris_code to "1"
- if S_i on downward slope
 - set cell's iris_code to "2"
- else
 - set cell's iris_code to "0"

This algorithm 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 eq (6).

$$HD = \text{XOR}(\text{codeA}, \text{codeB}) \dots (6)$$

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 eq (7)[9],[10].

$$HM = \frac{\text{length}(\text{code})}{\sum_{i=1}^n \frac{1}{\text{code}(i)}} \dots (7)$$

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. Conclusion

In this research work we propose to measure performance evaluation with two error rates i.e., FAR, FRR on the bases of the measurement we generate histogram of the algorithm, so we achieve quality of improvement for person identification by getting accurate feature of iris pattern which is yield by using Cumulative Sum algorithm and by reducing False rejection rate by increasing hamming distance value and reducing False Acceptance by decreasing hamming distance value.

Acknowledge

I owe my sincere thanks to my honorable research supervisor for his continues guidelines throughout my research work and my whole hearted gratitude to our esteem institute MBES COEA's Principal, staff, friends for their help and support to do my research work.

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", ISFAC, 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 TISSEI, Lionel MARTINI, 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] <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 Hassaniien, "An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory", AMO - Advanced Modeling and Optimization, Volume 5, Number 2, 2003.
- [16] John Daugman's web page, <http://www.cl.cam.ac.uk/~jgd1000/>