Iris Biometric Recognition for Person Identification in Security Systems

Vanaja Roselin.E.Chirchi
Ph.D. Research scholar
JNT University, Kukatpally,
Hyderabad- 500085. AP, India

Dr.L.M.Waghmare
Professor & Dean (R&D)
SGGS institute of Engineering & Technology,
Vishnupuri, Nanded-431602, MS, India

E.R.Chirchi
Asst. Professor, CSE Dept
MBES COE. Ambajogai
BEED 431517, MS, India

ABSTRACT

The security is an important aspect in our daily life whichever the system we consider security plays vital role. The biometric person identification technique based on the pattern of the human iris is well suited to be applied to access control and provides strong e-security. Security systems having realized the value of biometrics for two basic purposes: to verify or identify users. In this paper we focus on an efficient methodology for identification and verification for iris detection, even when the images have obstructions, visual noise and different levels of illuminations and we use the CASIA iris database it will also work for UBIRIS Iris database which has images captured from distance while moving a person. Efficiency is acquired from iris detection and recognition when its performance evaluation is accurate.

Keywords: Biometrics, Iris identification, occluded images, UBIRIS Iris database.

1. INTRODUCTION

Today's e-security 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 [12]. Biometric solutions address these fundamental problems, because an individual's biometric data is unique and cannot be transferred.

Biometrics which refers to identifying an individual by his or her physiological or behavioral characteristics has capability to distinguish between authorized user and an imposter. An advantage of using biometric authentication is that it cannot be lost or forgotten, as the person has to be physically present during at the point of identification process [9].Biometrics is inherently more reliable and capable than traditional knowledge based and token based techniques. The commonly used biometric features include speech, fingerprint, face, Iris, voice, hand geometry, retinal identification, and body odor identification [10] as in Figure1

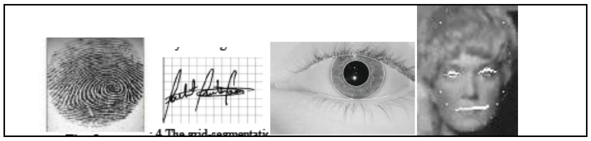


Figure1: Examples of Biometrics

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:

Facial Recognition: Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face. Facial recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists in urban areas. This biometric system can easily spoof by the criminals or malicious intruders to fool recognition system or program. Iris cannot be spoofed easily.

***Palm Print*:** Palm print verification is a slightly modified form of fingerprint technology. Palm print scanning uses an optical reader very similar to that used for fingerprint scanning; however, its size is much bigger, which is a limiting factor for use in workstations or mobile devices.

Signature Verification: It is an automated method of examining an individual’s signature. This technology is dynamic such as speed, direction and pressure of writing, the time that the stylus is in and out of contact with the “paper”. Signature verification templates are typically 50 to 300 bytes. Disadvantages include problems with long-term reliability, lack of accuracy and cost.

Fingerprint: A fingerprint as in Figure1 recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher. As it is more common biometric recognition used in banking, military etc., but it has a maximum limitation that it can be spoofed easily. Other limitations are caused by particular usage factors such as wearing gloves, using cleaning fluids and general user difficulty in scanning.

Iris Scan: Iris as shown in Figure2 is a biometric feature, found to be reliable and accurate for authentication process comparative to other biometric feature available today which is as shown Table1 (a) (b).

As a result, the iris patterns in the left and right eyes are different, and so scan be used quickly for both identification and verification applications because of its large number of degrees of freedom. Iris as in Figure 2 is like a diaphragm between the pupil and the sclera and its function is to control the amount of light entering through the pupil. Iris is composed of elastic connective tissue such as trabecular meshwork. The agglomeration of pigment is formed during the first year of life, and pigmentation of the stroma occurs in the first few years

[7][8]. The highly randomized appearance of the iris makes its use as a biometric well recognized. Its suitability as an exceptionally accurate biometric derives from [4]:

i. The difficulty of forging and using as an imposter person;

ii. It is intrinsic isolation and protection from the external environment;

iii. It's extremely data-rich physical structure.

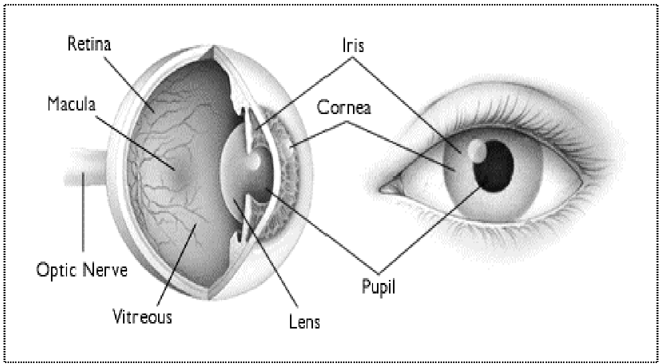


Figure2: Structure of iris.

iv. Its genetic properties—no two eyes are the same. The characteristic that is dependent on genetics is the pigmentation of the iris, which determines its color and determines the gross anatomy. Details of development, that are unique to each case, determine the detailed morphology;

v. its stability over time; the impossibility of surgically modifying it without unacceptable risk to vision and its physiological response to light, which provides a natural test against artifice.

After the discovery of iris, John G. Daugman, a professor of Cambridge University[8][9], suggested an image-processing algorithm that can encode the iris pattern into 256 bytes based on the Gabor transform.

In general, the iris recognition system is composed of the following five steps as depicted in Figure 3 According to this flow chart, preprocessing including image enhancement.

The remainder of the paper is organized as follows: Section (2) focuses on Image Acquisition Section (3) emphasizes on Preprocessing Section (4) focuses on Feature extraction Section(5) emphasizes on Pattern matching Section(6) emphasizes on identification and verification Section (7) emphasizes on conclusion of the proposed Algorithm.

2.IMAGE ACQUISITION

An image of the eye to be analyzed must be acquired first in digital form suitable for analysis. In further implementation we will be using CASIA database [17]. The main focus CASIA database is to minimize the requirement of user cooperation, i.e., the analysis and proposal of methods for the automatic recognition of Individuals, using images of their iris captured at-a-distance and minimizing the required degree of cooperation from the users, probably even in the covert mode [13].

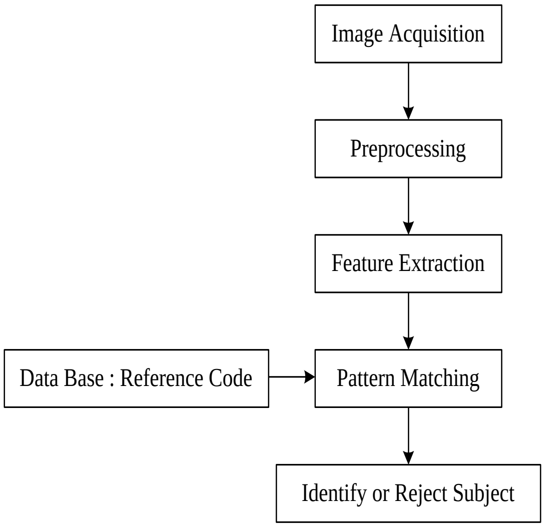


Figure 3: General steps of the iris recognition system

Table1 (a): Biometric comparison List

Method	**Coded Pattern**	**Mis-identific**	**Security**	**Application**
Iris Recognition	Iris pattern	1/1200000	High	High security facilities
Finger printing	Fingerprints	1/1,000	Medium	Universal
Hand Shape Size,	Length and thickness	1/700	Low	Low-security facilities
Facial Recognition	Outline, shape and distribution of eyes and nose	1/100	Low	Low-security facilities
Signature	Shape of letters	1/100	Low	Low-security facilities
Voice printing	Voice characteristic	1/30	Low	Telephone service

Table1 (b): Biometric comparison List

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

3. PREPROCESSING

3.1 Algorithm for detection and segmentation

- **iris detection**

Irises are detected even when the images have obstructions, visual noise and different levels of illumination. Lighting reflections, eyelids and eyelashes obstructions are eliminated. Images with narrowed eyelids or eyes that are gazing away are also accepted using wavelet algorithm.

Automatic interlacing detection and correction: The correction results in maximum quality of iris features templates from moving iris images.

Gazing-away eyes: A gazing-away iris image is correctly detected, segmented and transformed as if it were looking directly into the camera.

- **Correct iris segmentation**: is achieved under these conditions:

Perfect circles fail. VeriEye uses active shape models that more precisely model the contours of the eye, as perfect circles do not model iris boundaries.

The centers of the iris inner and outer boundaries are different Figure8. The iris inner boundary and its center are marked in red; the iris outer boundary and its center are marked in green.

Iris boundaries are definitely not circles and even not ellipses Figure9.and especially in gazing-away iris images.

Iris boundaries seem to be perfect circles. The recognition quality can still be improved if boundaries are found more precisely Figure10. Compared to perfect circular white contours.

- **Locating Iris**

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 (see Figure4)[4][6][15].The Daugman’s system, Integro differential operators as in (1) is used to detect the center and diameter of iris and pupil respectively.

$$\max(r,x0,y0)=\left\{\frac{\partial}{\partial r}\int_0^{2\pi} I(r*\cos\theta+x0,r*\sin\theta+y0)\right\}$$

--- (1)

Where (x0, y0) denotes the potential center of the searched circular boundary, and r its radius.

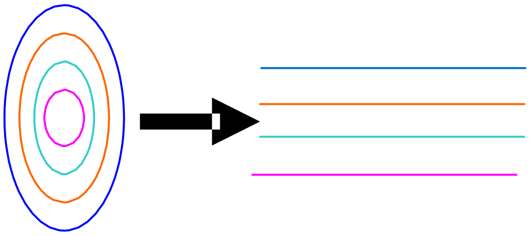


Figure 4: Polar transformation [16].

3.2 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 (see Figure 4,5) remaps each pixel in the pair of polar co-ordinates(r, θ) where r and θ are on interval [0,1] and [0,π] respectively. The unwrapping in formulated as in (2) [1][14][16].

$$I(x(r,\theta),y(r,\theta))\rightarrow I(r,\theta) \text{ --- (2)}$$

Such that

$$\left.\begin{aligned} x(r,\theta)&=(1-r)x_p(\theta)+rx_i(\theta),\\ y(r,\theta)&=(1-r)y_p(\theta)+ry_i(\theta)\end{aligned}\right\} \text{ --- (3)}$$

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. (See Figure4) shows polar transformation.

4. FEATURE EXTRACTION

The most important step in automatic iris recognition is the ability of extracting some unique attributes from iris, which help to generate a specific code for each individual. Gabor and wavelet transforms are typically used for analyzing the human iris patterns and extracting features from them,

Steps for feature Extraction:

- Apply 2DDWT with Haar up to 5-level decomposition
- Using 4th level, 5th level decomposition details construct the feature vector.
- Binaries the details getting from step no.3
- Store these feature vectors.

In (Figure 6(a)) [1][2][4] a conceptual chart of basic decomposition steps for an image is depicted. The approximation coefficients matrix cA and details coefficients matrices cH, cV and cD (horizontal, vertical, and diagonal, resp.) Obtained by wavelet decomposition of the input image are shown in (see Figure 6(b)) [4][14]. The definitions used in the chart are as follows.

(i) *C* ↓ denote downsample columns—keep the even indexed columns.

(ii) *D* ↓ denote downsample rows—keep the even-indexed rows.

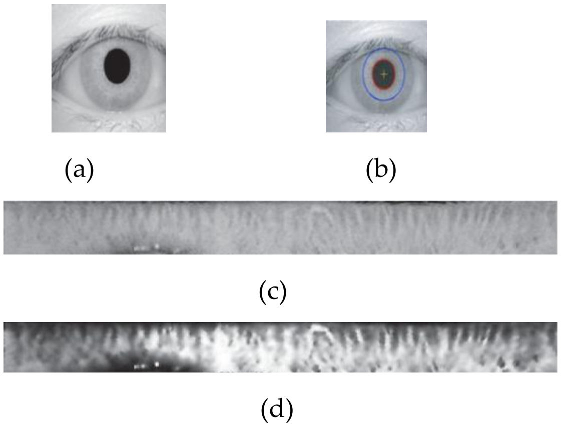
(iii) Lowpass D denotes the decomposition lowpass filter.

(iv) Highpass D denotes the decomposition highpass filter.

(v) The blocks under “Rows” convolve with filter of block the rows of entry.

(vi) The blocks under “Columns” convolve with filter of block the columns of entry.

(vii) *Ii* denotes the input image.



(a) (b)

(c)

(d)

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

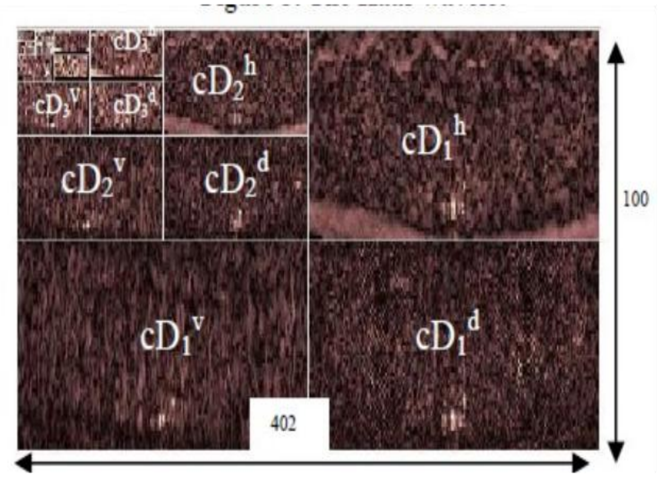


Figure 6(a) Conceptual diagram of basic decomposition steps for an image.

Only the fourth and fifth vertical and diagonal coefficients can be taken to express the characteristic patterns in the iris-mapped image. Thus we can represent each image applied to the Haar wavelet as the combination of six matrices as in (4).

$$\left.\begin{array}{ccc} cD_4^h & \text{and} & cD_5^h \\ cD_4^v & \text{and} & cD_5^v \\ cD_4^d & \text{and} & cD_5^d \end{array}\right\} \text{-------------- (4)}$$

5. PATTERN MATCHING

5.1 Binary Coding Scheme

It is very important to represent the obtained vector in a binary code because it is easier to find the difference between two binary code-words than between two number vectors. In fact Boolean vectors are always easier to compare and to manipulate. In order to code the feature vector first observed some of its characteristics. Now found that all the vectors that we obtained have a maximum value that is greater than 0 and a minimum value that is less than 0. If “Coef” is the feature vector of an image than the following quantization scheme converts it to its Equivalent code word

- if Coef(i) >=0 then Coef(i)=1
- if Coef(i) < 0 then Coef(i)=0

The next step is to compare two code words to find out that they represent same person or not.

5.2 Matching using hamming distance

The Hamming distance (HDs) between input images and images in each class are calculated, then the two different classifiers are being applied as follows [1][4][14].

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 (5)[4].

$$HM = \frac{length(code)}{\sum_{i=1}^{length(code)} (1/code(i))} \text{ --- (5)}$$

Steps for matching using hamming distance:

- Compare feature vector of database images with feature vector of query image.
- Calculate the hamming distances for each database feature vector.
- Find out the minimum hamming distance.

The iris codes in the database are used to find out which iris codes come from the same eye. Hamming distance is chosen because of its speed in calculating dissimilarity between binary codes. Hamming distance two Boolean is as shown in (6)

$$HD=\frac{1}{N}\sum_{i=1}^{N} \quad X_I \otimes Y_I \text{--------(6)}$$

Where N is the number of bits in the feature vector, X_i is the i^th feature of the tested iris, and Y_i is the i^th feature of the iris template. If two bit patterns are completely independent, such as iris templates generated from different irises, the Hamming distance the two patterns will be close to 1. If two patterns are derived from the same iris, the Hamming distance between them will be close to 0, since they are highly correlated and the bits should agree between the two iris codes.

The maximum Hamming distance that exists between two irises belonging to the same person is 0.32. Thus, when comparing two iris images, their corresponding binary feature vectors are passed to a function responsible of calculating the Hamming distance between the two [15]. The decision of whether these two images belong to the same person depends upon the following result:

- If HD <= 0.32 decide that it is same person
- If HD > 0.32 decide that it is different person (See Figure7) shows the iris code matching process.

Fast matching: Configurable matching speed varies from 50,000 to 150,000 comparisons per second**.** The highest speed still preserves nearly the same recognition quality (see Figure 11)[5].

6.IDENTIFICATION AND VERIFICATION

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.

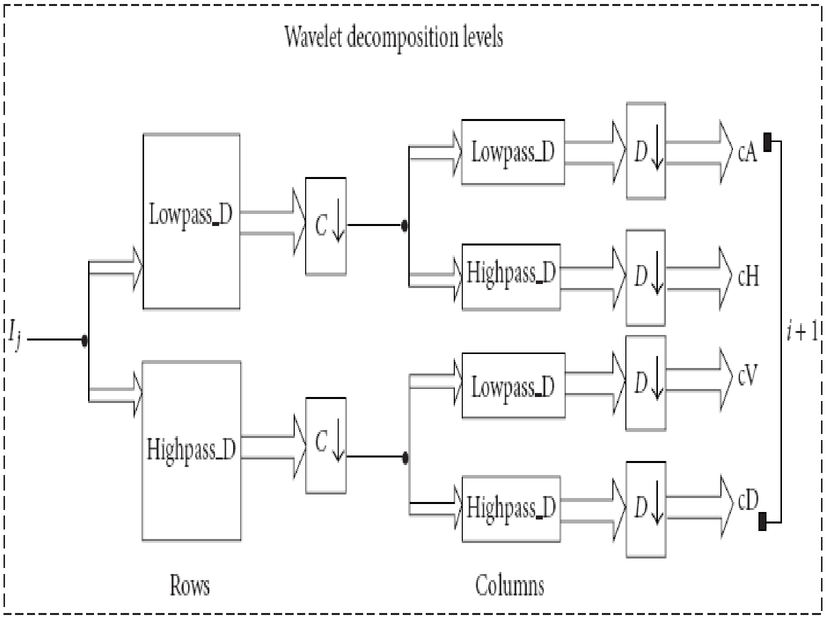


Figure 6(b) wavelet decomposition steps diagram

7. CONCLUSION

A proposed research work is to enhance the algorithm for efficient person identification for other area of applications by increasing FRR more than 0.33% as the VeriEye algorithm [5] results with FRR 0.32% and FAR 0.001%. Wavelets iris recognition algorithm is suitable for reliable, fast and secure person identification. Wavelet, Gabor filter and the range of hamming distance for Haar wavelet is less i.e., 0.2866 to 0.5111, for robust and fast matching for healthcare application for patient identification. Proposed algorithm focus on the algorithm for rapid and accurate iris identification even if the images are occlude further algorithm will also focus on robust iris recognition, even with gazing-away eyes or narrowed eyelids which solves all the security related problems.

8. ACKNOWLEDGEMENTS

I would like to thanks to our principal, staff of MBES college of Engineering, Ambajogai, for their kind support and providing facility to do my research work.

9. REFERENCES

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

[2] D.E.Benn, M.S.Nixon and J.N.Carter, “Robust eye Extraction using H.T. “ AVBPA’99

[3] Shimaa M.Elsherief, Mhamoud E.Allam and Mohamed W.Fakhr,”Biometric Personal Identification based on Iris Recognition”,IEEE,2006.

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

[5] Verieye iris recognition concept for performance evaluation ,http:// www.neurotechnology.com

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

[7] L.M. Waghmare, S. P. Narote, A.S. Narote, “Biometric Personal Identification Using IRIS”, Proceedings of International Conference on Systemic, Cybernetics and Informatics, ICSCI - 2006, Pentagram Research Centre – Hyderabad, pp. 679-682, Jan 2006

[8] E. Wolff, Anatomy of the eye and orbit, H. K. Lewis, London, UK, 7th edition, 1976.

[9] John Daugman,”How Iris works” *IEEE Transaction* on circuit and systems for Video Technology, VOL.14, No.1, January 2004.

[10] D.Zang Automated biometrics technologies and systems Klumer Academics, Boston, Mass, USA, 2000.

[11] A.S.Narote, S.P.Narote, M.B. Kokare, L.M. Waghmare, “An Iris Recognition Based on Dual Tree Complex Wavelet Transform” published in the proceedings of IEEE International Conference TENCON 2007, Taiwan during Oct. 30-Nov. 02, 2007.

[12] R.Kevin, “E-Security for E-Government” A Kyberpass Technical White Paper, April 2001, www.kyberpass.com.

[13] Proença,H. and Alexander, {L.A.},” {UBIRIS}: A noisy iris image database”, 13th International Conference on Image Analysis and Processing - ICIAP 2005,Springer, VOL. LNCS3617,pages 970-977,address Cagliari, Italy, September-2005.

[14] A.Poursaberi and B.N.Araabi,"Half eye wavelet based method for iris recognition" proceeding of the 2005 5th International Conference on Intelligent Systems Design and Applications (ISDA'05) 0-7695-2286-06/05 © 2005 IEEE.

[15] Sandipan P. Narote, Abhilasha S. Narote and Laxman. M. Waghmare, "Iris based recognition system using Wavelet transfer", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11, November 2009.

[16] 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*

[17] CASIA–Iris V3,http://www.cbsr.ia.ac.cn/IrisDatabase.htm

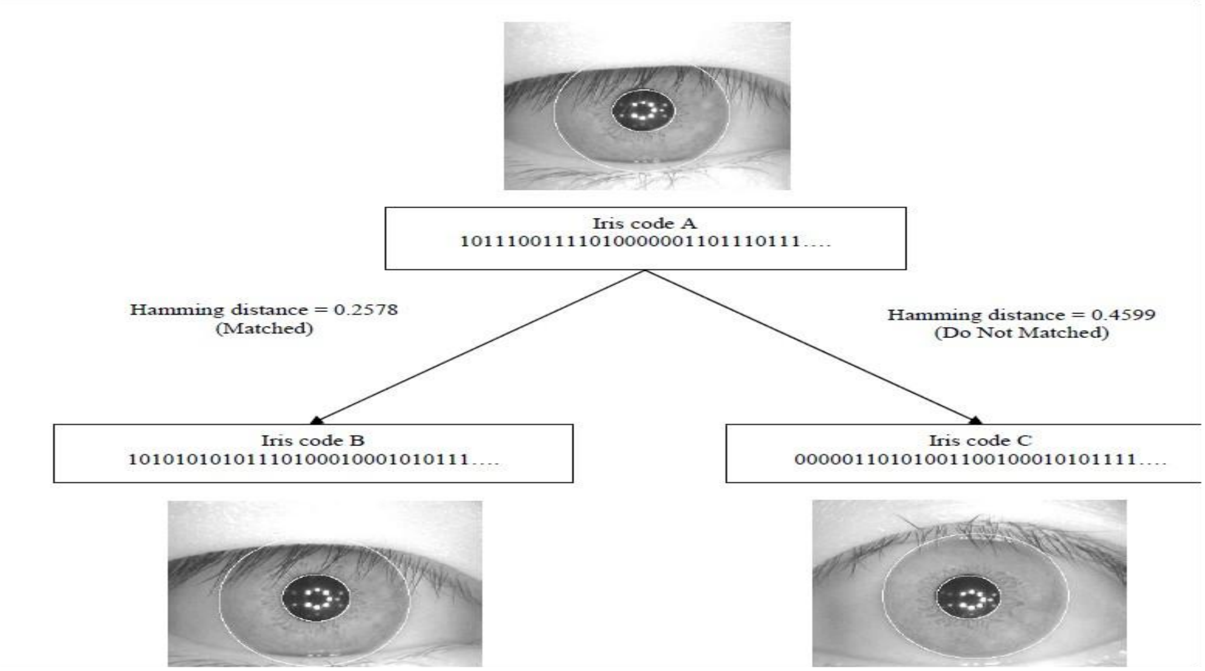


Figure 7: iris code matching process

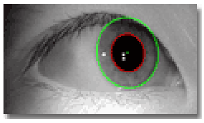


Figure 8

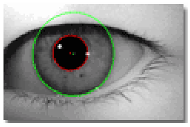


Figure 9

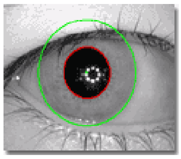


Figure 10

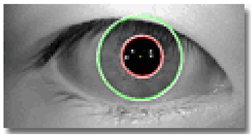


Figure 11