Iris Recognition Using Enhanced Matching Technique

P.Abinaya P.G Scholar
Dept of M.E. VLSI Design
Sri Ramakrishna Engineering College
Coimbatore, India.

N.Kirthika Assistant Professor
Dept of M.E. VLSI Design
Sri Ramakrishna Engineering College
Coimbatore, India.

Abstract: **Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. A biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual. Usually the user authentication is done using portable devices which are the personal tokens carried by the user. These personal tokens have to maintain high performance rates in authentication process. This paper deals with the designing of such personal tokens where biometric authentication is required. In this paper, iris biometrics has been chosen to be implemented. Most commercial iris recognition systems use patented algorithms developed by Daugman and these algorithms are able to produce perfect recognition rates. Several design alternatives are reported with these results, most of the needs required for the development of an innovative identification product are covered. Simultaneously, the security and cost for large quantities are also improved.**

***Keywords*: *Authentication, iris biometrics, fragile bits*.**

I. INTRODUCTION

Biometrics is a technology of recognizing an individual based on the real features possessed by the user. Among the currently existing biometric modalities, iris recognition is considered to be one of the most secure and reliable technique. Biometric authentication relies on any automatically measurable physical characteristics or personal trait that is distinctive to an individual. There are two general applications for biometrics: identification and authentication. In identification, the biometric device reads a sample, processes it and compares it against every record or template in the database. In verification, the biometric system requires input from the user, at which time the user claims his or her identity via a password, token or user name. This user input points the system to a template in the database. The system also requires a biometric sample from the user. It then processes and compare the samples to or against the user defined template[7].

This paper is concerned with the authentication process. The biometric authentication applications have two key approaches: online approach and offline approach [6]. In online approach the biometric data is accessed from the central database. In offline approach the biometric data is stored on personal tokens. The online approach has serious security and privacy issues, as the communication between the system and the central database can be attacked and the identity may be stolen or altered. So offline systems are required for high secure environment.

The Sections are organized as follows. Section II describes about the related work of iris biometric. Section III deals with the architecture for iris recognition. Section IV describes about the authentication process. In Section V, the results are discussed. Section VI concludes this paper.

II. RELATED WORK

A. *Biometric Traits*

A good biometric trait must accomplish a set of properties. Mainly they are
Universality: Every person should have the characteristic.
Distinctiveness: Any two persons should be different enough to distinguish each other based on this characteristic.
Permanence: Characteristic should be stable enough (with respect to the matching criterion) along time, different environment conditions, etc.
Collectability: Characteristic should be acquirable and quantitatively measurable.
Acceptability: People should be willing to accept the biometric system, and not feel that it is annoying, invasive, etc.
Performance: Identification accuracy and required time for a successful recognition must be reasonably good.
Circumvention: Ability of fraudulent people and techniques to fool the biometric system should be negligible.
Biometric traits can be split into two main categories:
Physiological Biometrics: It is based on direct measurements of a part of the human body. Fingerprint, face, iris, and hand-scan recognition belong to this group.
Behavioral Biometric: It is based on measurements and data derived from an action performed by the user, and thus indirectly measures some characteristics of the human body. Signature, gait, gesture, and key stroking recognition belong to this group [3][4]. However, these classifications are quite artificial. For instance in [6], the

speech signal depends on behavioral traits such as semantics, diction, pronunciation, idiosyncrasy, etc. (related to socio-economic status, education, place of birth, etc.). It also depends on the speaker's physiology, such as the shape of the vocal tract. On the other hand, physiological traits are also influenced by user behavior, such as the manner in which a user presents a finger, looks at a camera, etc.

B. Properties Of The Iris

The iris is composed of elastic connective tissue, the trabecular meshwork, whose prenatal morphogenesis is completed during the 8th month of gestation. It consists of pectinate ligaments adhering into a tangled mesh revealing striations, ciliary processes, crypts, rings, furrows, a corona, sometimes freckles, vasculature, and other features. During the first year of life a blanket of chromatophore cells often changes the color of the iris[11], but the available clinical evidence indicates that the trabecular pattern itself is stable throughout the lifespan.

Because the iris is a protected internal organ of the eye, behind the cornea and the aqueous humour, it is immune to the environment except for its pupillary reflex to light. (The elastic deformations that occur with pupillary dilation and constriction are readily reversed mathematically by the algorithms for localizing the inner and outer boundaries of the iris.) Pupillary motion, even in the absence of illumination changes (termed hippus)**,** and the associated elastic deformations in the iris texture, provide one test against photographic or other simulacra of a living iris in high security applications. There are few systematic variations in the amount of detectable iris detail as a function of ethnic identity or eye color[10]; even visibly dark-eyed persons reveal plenty of iris detail when imaged with infrared light.

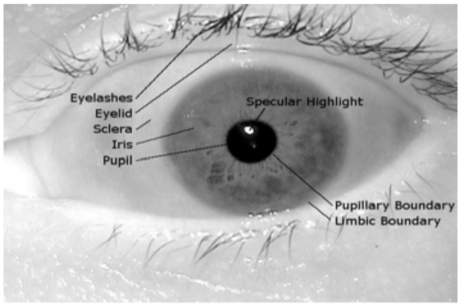

Figure 1. Human Eye

The most common iris biometric algorithm represents the texture of an iris using a binary iris code. Not all bits in an iris code are equally consistent. A bit is deemed fragile if its value changes across iris codes created from different images of the same iris [15]. In creating an iris code, a traditional iris biometrics system applies Gabor filters to a number of locations on an iris image and obtains a complex valued filter response for each location[13]. Each complex number is quantized to two bits; the first bit is set to one if the real part of the complex number is positive, and the second bit is one if the imaginary part is positive.

Consider multiple images of the same iris. A filter applied to one location on the iris produces a complex value. Across all images, the complex values for that location will be similar, but not exactly the same. Similarly, the bit from the binary quantization could be the same across all iris codes, or it may differ in some of the codes[15]. A bit in a subject's iris code is consistent if it assumes the same value for most images of that subject. A bit is fragile if it varies in value some substantial percent of the time.

III. Architecture for Iris Recognition

The block diagram for iris recognition is similar as any other biometric modality. The image of the eye is captured first then the iris is located and segmented to extract its features[7]. These features are compared with the previously stored template.

A. Proposed Architecture

The Proposed architecture should perform the following tasks.

Image Acquisition: Contrary to popular belief, iris biometrics systems do not use laser-scans to capture the image of the human eye. Instead, an infrared photo or video camera is used at a set distance to capture a high quality image of the iris[1],[3]. Working in the infrared range provides many advantages when compared to the visible range: iris ridges, nerves, and crypts are more evident [4][5]; the border between the iris and the pupil is more pronounced; and users are not exposed to annoying flashes.

Image Segmentation: This pre-processing block is related to the image acquisition. The non-detection of the iris or the quality of the captured images is typical reasons for rejection of the acquired image, thus, requiring a new capture process.

Feature Extraction : Here the iris is first normalized to a virtual circle around the pupil, which is named the iris signature[14]. Thus, the iris signature will represent the gray level values on the contour of a virtual circle, which is centered at the centroid of the pupil, with a fixed radium ř and considering angular increments of 2π/L, being L=256 , the length of the iris signature (previously fixed); (x,y) the centroid of the pupil;

Afterwards, a wavelet transform is applied to the iris signature. The vector resulting for each scale is concatenated in a unique vector for computation of the zero-crossing representation, which leads to the feature vector. For computation of the wavelet transformation[2], Mallat's fast wavelet transform (FWT) in [7] approach has been considered.

Once the wavelet is computed, the resulting vector is simplified by using its zero-crossing representation. The zero crossing representation converts the vector into a binary representation, wherein 1 represents a positive value and 0 represents a negative value, for each vector component. The number of levels used for the wavelet transform is a critical parameter, as it greatly influences the authentication performance results.

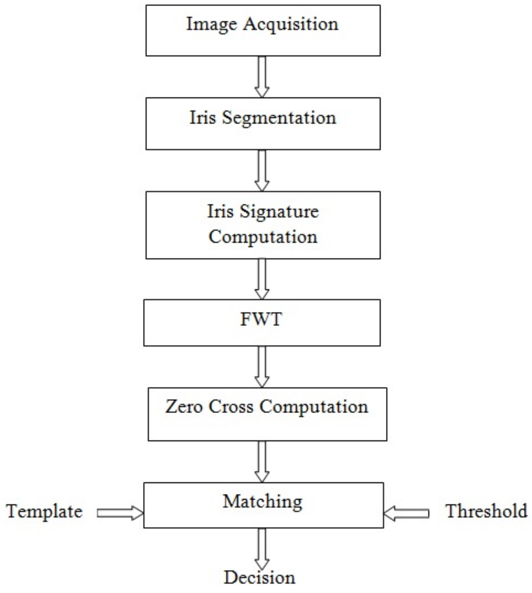

Figure 2. The Proposed Block Diagram

Matching: The Hamming distance is used for comparing vectors [9]. If the distance obtained is below a predefined threshold level, the studied sample is considered to belong to the user whose template is being studied. Selection of the threshold level usually depends on the final application.

To improve the accuracy and reliability of iris recognition we present a metric, called the fragile bit distance, which quantitatively measures the coincidence of the fragile bit patterns in two iris codes. In discussing fragile bits in the iris code, it is important to note that we are not saying that parts of the iris itself are unstable. The iris structure is generally considered highly robust, changing very little over time. Instead, bit fragility occurs when the inner product between a filter and a particular part of the iris produces a result with small magnitude or with a phase close to the quantization boundary. Therefore, the consistency of each bit in the iris code is dependent upon a combination of: 1) the iris texture at a certain position, 2) the filter used to analyze that texture, and 3) the quantization method for the filter response [15].

When using fragile bit masking, we mask a significant number of bits because the filter response produced an output with small magnitude. Rather than completely ignoring all information from those locations, we would like to find a way to make some beneficial use of those bits.

In order to compute fragile bit distance, we need to store occluded bits and fragile bits separately. Therefore, each iris template will consist of three matrices: an iris code i, an occlusion mask m, and fragility mask f. Unmasked bits are represented with ones and masked bits are represented with zeros. Specifically, unoccluded bits and consistent bits are marked as ones, while occluded and fragile bits are zeros. Take two iris templates, template A and template B. The FBD is computed as follows:

$$FBD = \frac{\left\| m_A \cap m_B \cap \overline{f_A \cap f_B} \right\|}{\left\| m_A \cap m_B \right\|} \qquad (1)$$

where ∩ represents the AND operator, and the line over $f_A \cap f_B$ represents the NOT operator. The norm (‖ ‖) of a matrix tallies the number of ones in the matrix.

IV. Authentication Process

The human iris contains a very unique pattern which can be used as the basis for biometric identification of individuals. Iris patterns possess high inter-class dependency, and low intra-class dependency, furthermore, the iris is enclosed by the cornea, making the iris pattern stable throughout adult life. These features make iris recognition, potentially, a very accurate biometric technology, allowing non-intrusive scanning with a low failure rate. Iris recognition involves first extracting the iris from a digital eye image, and then encoding the unique patterns of the iris in such a way that they can be compared with pre-registered iris patterns. Since each individual iris has enormous pattern variability, large databases can be searched without fear of a false match. The use of dedicated hardware permits simultaneous computing processes, i.e., several processes can be computed at the same time

A. Image Acquisition

The first step is the acquisition of the image. Here the image is acquired from the ICE 2005 database. The next follows the segmentation

B. Iris Segmentation

The first stage of iris recognition is to isolate the actual iris region in a digital eye image. The iris region can be approximated by two circles, one for the iris/sclera boundary and another, interior to the first, for the iris/pupil boundary. The eyelids and eyelashes normally occlude the upper and lower parts of the iris region. Also, specular reflections can occur within the iris region corrupting the iris pattern.

The success of segmentation depends on the imaging quality of eye images[12]. The persons with darkly pigmented irises will present very low contrast between the pupil and iris region if imaged under natural light, making segmentation more difficult[9]. The segmentation stage is critical to the success of an iris recognition system, since data that is falsely represented as iris pattern data will corrupt the biometric templates generated, resulting in poor recognition rates.

It was decided to use circular Hough transform for detecting the iris and pupil boundaries. This involves first employing Canny edge detection to generate an edge map [5]. Vertical and horizontal gradients were weighted equally for the inner iris/pupil boundary. In order to make the circle detection process more efficient and accurate, the Hough transform for the iris/sclera boundary was performed first, then the Hough transform for the iris/pupil boundary was performed within the iris region, instead of the whole eye region, since the pupil is always within the iris region. After this process was complete, the parameters such as the radius, and x and y centre coordinates for both circles are stored.

Canny edge detection is used to create an edge map, and only horizontal gradient information is taken[4],[5]. Also, the lines are restricted to lie exterior to the pupil region, and interior to the iris region.

C. Iris Signature Computation

Here the iris is first normalized to a virtual circle around the pupil, which is named the iris signature. Thus, the iris signature will represent the gray level values on the contour of a virtual circle, which is centred at the centroid of the pupil, with a fixed radium ř and considering angular increments of 2π/L, being L=256 , the length of the iris signature (previously fixed); (x,y) the centroid of the pupil;

i.e., $I_S = I_E(x + \check{r}cos\theta . y + \check{r}sin\theta)$ (2)

The RTL schematic of iris signature computation is given as

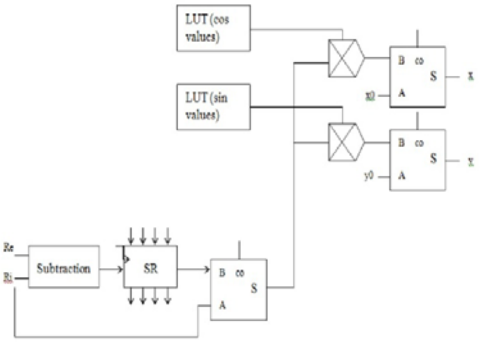

Figure 3. Iris signature computation

D. FWT

Once the iris region is successfully segmented from an eye image, the next stage is to transform the iris region so that it has fixed dimensions in order to allow comparisons. The dimensional inconsistencies between eye images are mainly due to the stretching of the iris caused by pupil dilation from varying levels of illumination. The normalisation process will produce iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location[13]. Another point of note is that the pupil region is not always concentric within the iris region, and is usually slightly nasal. This must be taken into account if trying to normalise the 'doughnut' shaped iris region to have constant radius.

The basic building block of the forward discrete wavelet transform filter bank is the decimator which consists of an FIR filter followed by a down-sampling operator Down-sampling an input sequence x[n] by an integer value of 2, consists of generating an output sequence y[n] according to the relation y[n] = x[2n]. Accordingly, the sequence y[n] has a sampling rate equal to half of that of x[n].

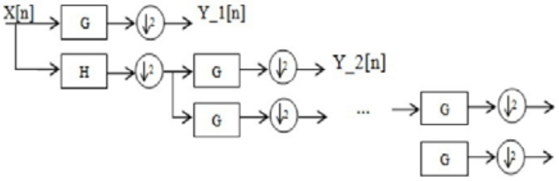

Figure 4. FWT

The basic building block of the inverse discrete wavelet transform filter bank is the interpolator which consists of an FIR filter proceeded by an up-sampling operator. The up-sampler inserts an equidistant zero-valued sample between every two consecutive samples on the input sequence x[n] to develop an output sequence y[n] such that y[n] = x[n/2] for even indices of n, and 0 otherwise. The sampling rate of the output sequence y[n] is thus twice as large as the sampling rate of the original sequence x[n].

E. Zero Cross Computation

An important practical and theoretical issue is to understand whether the multi scale edges carry all the information of the original signal. Indeed, for pattern recognition applications, some important components of the signal should be removed, when representing it with multi scale zero-crossings as in [8][13]. Completeness by itself is not sufficient as for most applications the representation must also be stable. This means that a small perturbation of the representation should correspond to a small modification of the original signal. Pattern recognition is an important domain of application for such a zero-crossing representation. The sharp variation points of a signal are often the most important features to identify patterns.

Once the wavelet is computed, the resulting vector is simplified by using its zero-crossing representation. The zero crossing representation converts the vector into a binary representation, wherein 1 represents a positive value and 0 represents a negative value, for each vector component to generate a zero-crossing representation from the normalized iris signature[9],[12]. Since the normalized iris signature represents a closed ring, it is naturally periodic with period N, and the zero-crossing representation will also be periodic since the wavelet coefficients are periodic. This means that the representation is independent from the starting point on iris virtual circles. For example zero cross computation of given fig is shown as

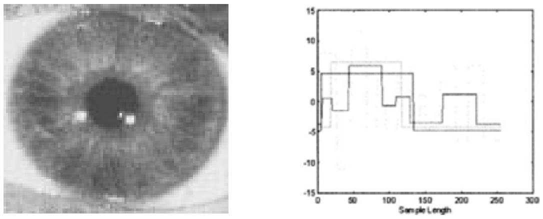

Figure 5. Sample Image and Zero Cross Representation

F. *Matching*

The template that is generated in the feature encoding process will also need a corresponding matching metric, which gives a measure of similarity between two iris templates. This metric should give one range of values when comparing templates generated from the same eye, known as intra-class comparisons, and another range of values when comparing templates created from different irises, known as inter-class comparisons. These two cases should give distinct and separate values, so that a decision can be made with high confidence as to whether two templates are from the same iris, or from two different irises.

For matching, the Hamming distance was chosen as a metric for recognition, since bit-wise comparisons were necessary [7]. Although, in theory, two iris templates generated from the same iris will have a Hamming distance of 0.0, in practice this will not occur.

From the calculated Hamming distance values, only the lowest is taken, since this corresponds to the best match between two templates. Although the best results in time and hardware are obtained from a pipeline structure, the authors have selected a different solution, which is slower but smaller.

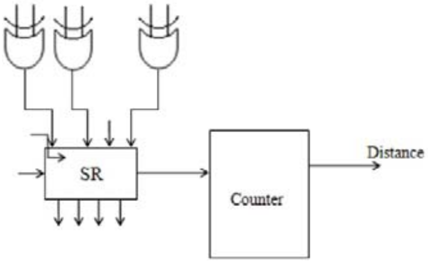

Figure 6. Matching Implementation

The reason for this is that filtering takes much longer than matching; no improvement is achieved here by speeding up the matching process. Fig. 6 illustrates the matching implementation chosen for the dedicated hardware.

The most common iris biometric algorithm represents the texture of an iris using a binary iris code. Not all bits in an iris code are equally consistent. A bit is deemed fragile if its value changes across iris codes created from different images of the same iris [15]. Previous research has shown that iris recognition performance can be improved by masking these fragile bits. The FBD is computed as given in eqn 1. The FBD expresses the fraction of unoccluded bits masked for fragility in the comparison. This metric is large for impostor comparisons and small for genuine comparisons.

Even though the FBD is not as powerful a metric as the Hamming distance, we can combine the features to create a better classifier than Hamming distance alone. To combine Hamming distance and FBD, we first tried a weighted average technique. We combined the two scores using the equation

$$\text{Score}=\alpha \times \text{HD} + (1-\alpha) \times \text{FBD} \qquad (3)$$

We varied the parameter α in steps of 0.1 from 0 to 1, and calculated the equal error rate for each run. Multiplication can be used as an alternative method of score fusion

$$\text{Score}= \text{HD} \times \text{FBD} \qquad (4)$$

V. Experimental Results

Therefore authentication is achieved by the fusion of hamming distance and fragile bit distance. The comparison for error rates are given in the Table I. The comparison of area, power and timing report are given in the Table II.

TABLE I. Comparison for Error Rates

Method	EER
HD	8.70×10^{-3}
0.6HD+0.4FBD	8.02×10^{-3}
HD×FBD	7.99×10^{-3}

TABLE II. Comparison of Area, Power and Time

Matching Techniques	Computation Time(ns)	Power(mW)	Area(Gate Counts)
HD	16.207	90	7977
HD×FBD	16.207	86	8574

VI. Conclusion

In many applications user authentication has to be carried out by portable devices. This project provides solutions to designing such personal tokens where biometric authentication is required. In the case of high security environments, where low error rates are extremely important, the microprocessor solution is recommended, especially when the number of users in the system is relatively high; however, if the number of users is low or size and execution times are significant constraints, the dedicated hardware solution should be chosen. Thus by using enhanced matching technique i.e., fusion of hamming distance and fragile bit distance produces good recognition rates.

Future Work

The results obtained in this study direct future research into the integration of cryptographic modules that would secure all data transmission. Another research area would explore optimal hardware solutions for identification tokens that combine the benefits of both platforms developed herein (i.e., using HW/SW code sign).

Acknowledgement

The authors thank the Management and Principal of Sri Ramakrishna Engineering College, Coimbatore for providing excellent computing facility and encouragement.

References

[1] Bowyer, K. Hollingsworth, K. et al (2008) 'Image Understanding For Iris Biometrics: A Survey', Comput. Vision Image Understand., Vol.110, No.2, pp.281–307.

[2] Daubechies, I. (1990) 'The Wavelet Transform, Time-Frequency Localization And Signal Analysis', IEEE Transformation and Information Theory., Vol.36, pp.961-1005.

[3] Daugman, J. (Nov. 2006) 'Probing The Uniqueness And Randomness Of Iriscodes: Results From 200 Billion Iris Pair Comparison', Proc. IEEE, Vol.94, No.11, pp.1927– 1935.

[4] Daugman, J. (Oct. 2007) 'New Methods In Iris Recognition', IEEE Trans. Syst., Man Cybern. B, Cybern., Vol.37, No.5, pp.1167–1175.

[5] Daugman, J. G. (Nov. 1993) 'High Confidence Visual Recognition Of Persons By A Test Of Statistical Independece', IEEE Trans. Patt. Anal. Mach. Intell., Vol.15, No.11, pp.1148–1161.

[6] Faundez-Zanuy, M. (Jun. 2006) 'Biometric Security Technology', IEEE A&E Syst.Mag., Vol.21, No.6, pp.15–26.

[7] Judith Liu-Jimenez, Raul Sanchez-Reillo, and Belen Fernandez-Saavedra, (2011) 'Iris Biometrics for Embedded Systems', IEEE Transactions on Very Large Scale Integration

[8] Mallat, S. (Jul. 1991) 'Zero-Crossing Of Wavelet Transform', IEEE Trans. Inf.Theory, Vol.37, No.4, pp.1019–1033.

[9] Masek, L. (2003) 'Recognition Of Human Iris Patterns For Biometric Identification', Master's thesis, Sch. Comput. Sci. Softw. Eng., Univ.Western Australia, Perth.

[10] Matey, J. R. Naroditsky, O. et al (Nov. 2006) 'Iris On The Move: Acquision On Images For Iris Recognition In Less Constrained Enviroments', Proc. IEEE, Vol.94, No.11, pp.1936–1947.

[11] Ritter, N. Owens, R. et al (Sep. 1999) 'Location Of The Pupil-Iris Boder In Slit-Lamp Images Of The Cornea', in Proc. Int. Conf. Image Anal. Process, pp.740–745.

[12] Ross A. and Shah, S. (Apr. 1998) 'Segmenting Non-Ideal Irises Using Geodesic Active Contours', in Proc. Biometr. Symp., 2006, pp.1–22.

[13] Sanchez-Avila C. and Sanchez-Reillo, R. (2005) 'Two Different Approaches For Iris Recognition Using Gabor Filters And Multiscale Zero-Crossing', Patt. Recog., vol38,No.2, pp.231–240.

[14] Tisse, C. Martin, L. et al (2002) 'Personal Identification On Technique Using Human Iris Recognition', in Proc. Vision Interface, pp.294–299.

[15] Hollingsworth Karen P., Bowyer Kevin W. (Dec. 2011),' Improved Iris Recognition through Fusion of Hamming Distance and Fragile Bit Distance', IEEE Transactions vol. 33, no. 12 .

ABINAYA. P received the Bachelor of Engineering degree in Electronics and Communication Engineering from SSM College of Engineering, Namakkal, India, in 2010. She is currently pursuing Master of Engineering degree from the Department of VLSI Design, at Sri Ramakrishna Engineering College, Coimbatore. Her area of interest includes VLSI architecture, Biometrics, Digital Electronics, Communication systems.

Kirthika.N received the Bachelor of Engineering degree in Electronics and Communication Engineering from Avinashalingam University, Coimbatore, India, in 2009 and received Master of Engineering degree from the Department of VLSI Design, Anna University of Technology, Coimbatore, India. She is currently working as Assistant Professor at Sri Ramakrishna Engineering College, Coimbatore. Her area of interest includes solid state devices, VLSI fabrication & VLSI architecture.