International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.1, No.6, October 2012 DOI:10.15693/ijaist/2012.v1i6.52-56

A Novel and Rapid Approach to Secure Iris Templates in Iris Authentication System

Poornima.S
Assistant Professor/Department of IT
SSN College of Engineering, Chennai, India

Subramanian.S
Advisor, CIET, Coimbatore, India

***Abstract*—This paper presents a fusion method for iris authentication system where a set of iris images of a given eye are fused to generate a final template by forming a weight mask template using the most consistent iris feature data. There are situations, where multiple iris images are to be considered for authentication depending on the position and motion of a human eye during input session. Templates are generated for each iris image and stored in the database for authentication. Successful iris authentication depends on how similar the stored template in the database and the final fused template. This similarity score will be indicating the degree of similarity between a pair of biometric template data under consideration. Depending on degree of similarity, individual can be identified. This increases the capacity of database and mainly the performance time of authentication. The proposed template fusion technique will not only reduce the database storage capacity requirements but also increases the system's speed during the template matching process with high performance rate and secures the iris templates by fusion method.**

Index terms - Biometrics, Feature Extraction, Fusion, Hamming Distance, Iris segmentation, Template.

I. INTRODUCTION

Automated biometrics-based personal identification systems can be classified into two main categories: identification and verification. In a process of verification, the biometrics information of an individual, who claims certain identity, is compared with the biometrics on the record that represents the identity that this individual claims [1]. The comparison result determines whether the identity claims shall be accepted or rejected. The human iris recently has attracted the attention of biometrics-based identification and verification research and development community. The iris is so unique that no two irises are alike, even among identical twins, in the entire human population.

Iris recognition system is more reliable, as iris is an internal organ of the eye and well protected from the environment, and stable over time. As a planar object its image is relatively insensitive to angle of illumination, and changes in viewing angle cause only affine transformations; even the non-affine pattern distortion caused by pupillary dilation is readily reversible. Finally, the ease of localizing eyes in faces and the distinctive annular shape of the iris, facilitate reliable and precise isolation of this feature and the creation of a size-invariant representation. In the iris alone, there are over 400 distinguishing characteristics, or Degrees of Freedom (DOF), that can be quantified and used to identify an individual (Daugman, J. & Williams, G. O. 1992). Approximately 260 of those are possible to capture for identification. These identifiable characteristics include: contraction furrows, striations, pits, collagenous fibers, filaments, crypts, serpentine vasculature, rings, and freckles. Due to these unique characteristics, the iris has six times more distinct identifiable features than a fingerprint.

The rest of this paper is organized as follows; section II presents a concise background about iris recognition techniques, section III highlights the iris recognition main steps, and introduces the proposed template fusion process and the template matching process with emphasizes on the modified Hamming distance formula, section IV presents the experimental work and section V gives the conclusion of this work.

II. RELATED WORK

The iris is an externally visible, yet protected organ whose unique epigenetic pattern remains stable throughout adult life. These characteristics make it very attractive for use as a biometric for identifying individuals. Image processing techniques can be employed to extract the unique iris pattern from a digitized image of the eye, and encode it into a biometric template, which can be stored in a database. This biometric template contains an objective mathematical representation of the unique information stored in the iris, and allows comparisons to be made between templates. Numerous works are done on this case and produced various performance results.

Reliable biometric verification and identification techniques based upon iris patterns have been presented by various researchers [2],[3],[5],[11] uses integro-differential operator in order to detect the centre and diameter of the iris. The image is then converted from polar to Cartesian and thereby rectangular representation of the region of interest is generated. The complex valued 2D Gabor filters is utilized to generate the iris codes which are then matched using Hamming Distance.

Wildes, et al., 1994 used an isotropic band-pass decomposition technique in which the first derivative of image intensity is utilized to find the location of edges corresponding to

the borders of the iris [4],[10]. Boles and Boashash, 1998 uses edge detection to localize and normalize the iris and then the zero-crossings of the wavelet transform are calculated at various resolution levels over concentric circles on the iris [11]. This algorithm is invariant to translation, rotation, scale and illumination and can handle the noisy conditions.

The performance of the system is based on the biometric template which is generated from the input iris and maintained in database. The security of the template is not guaranteed nowadays. This issue is been handled by many researchers by many cryptographic algorithms [7],[8]. Here, the same issue is handled differently by using fusion technique.

III. OVERVIEW OF IRIS RECOGNITION SYSTEM

Iris authentication is one of the biometric systems which utilize iris texture patterns as a method of gathering unique information about an individual. The process consists of five major steps. These stages are image acquisition of a person eye, segmentation – locating the iris region in an eye image, normalization – creating a dimensionally consistent representation of the iris region, feature encoding – creating a template containing only the most discriminating features of the iris, and matching phase – two iris codes will be compared and a similarity score is computed using Hamming distance [3]. The input to the system will be a human eye image, and the output will be an iris template, which will provide a mathematical representation of the iris region. The design steps can be diagrammatically shown in Figure 1.

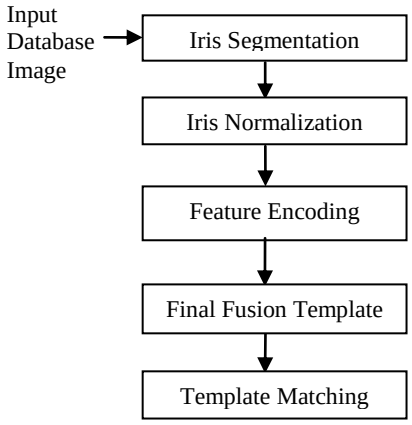

Figure1. Iris Authentication System

The algorithm handles images from CASIA database and is primarily based on the methods given by Daugman is outlined as follows:

A. Segmentation

The first stage of iris recognition is to isolate the actual iris region in a digital eye image which involves both iris localization and noise reduction procedures. 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. A technique is required to isolate and exclude these artifacts as well as locating the circular iris region. Figure 2 depicts the iris segmentation step.

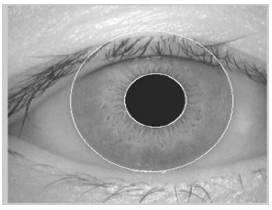

Figure 2. Iris Segmentation

Typical iris segmentation methods include Daugman's integro-differential operator [3] and edge detection using the circular Hough transform [3],[5]. Daugman's method which is used in this work, assumes the pupillary and limbic boundaries of the eye as circles and an integro-differential operator is utilized to detect the iris boundary by searching the parameter space. The circular boundary is detected when the integro-differential operator attains its maximum. The iris boundary was described with three parameters: the radius r, and the coordinates of the centre of the circle.

B. Normalization

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 normalization 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. Daugman devised a rubber-sheet model [3] which re-sampled the segmented iris region to the fixed-size rectangular image by mapping the extracted iris region into a normalized coordinate system. The homogenous rubber sheet model remaps each point within the iris region to a pair of polar coordinates (r, θ) where r is on the interval [0,1] and θ is angle [0,2π]. Figure 3 shows the normalized iris segmented above.

Figure 3. Normalized Iris

C. Feature Extraction

In order to provide accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. Only the significant features of the iris must be encoded so that comparisons between templates can be made.

Most iris recognition systems make use of a band pass decomposition of the iris image to create a biometric template. Daugman extracted the features from the normalized iris image by using convolution with 2-D Gabor filters [2]. In that system the filters are multiplied by the raw image pixel data and integrated over their domain of support to generate coefficients which describe, extract, and encode image texture information. Figure 4 shows feature encoding step. Finally, the base feature templates formed for each image of a given eye are fused to generate one final template.

Figure 4. Feature Extraction

D. Template Fusion

To improve the accuracy, most of the biometric authentication systems store multiple templates per user to account for variations in biometric data. Therefore, these systems suffer from storage space and computational overheads. In order to address these issues, there is need to optimize the computational and storage complexities by creating a reliable specimen iris template per user rather than maintaining multiple templates. The base feature templates formed for each image of a given eye are fused to generate one final template. In the fusion process, each bit is weighed according to its reliability at enrolment time. This is a simple and efficient scheme that works with any template generation method [6].

In pattern recognition the idea of image fusion is generally applied in two different ways. The first involves segmenting the image into different feature objects and fusing with the original image in order to improve the rate of object recognition. The second involves segmenting the input image into different regions and then determining the fusion weight according to the values of salience and visibility of each region, which reflect its clarity.

In this paper, the fusion strategy adapted is the majority rule in a plain voting system to combine different base templates. Let $D = \{D_1, \ldots, D_L\}$ be a set of L base templates. Each template D_i ($i = 1, \ldots, L$) assigns an input feature vector $D \in R^n$ to one of the possible C problem classes. The output of the fusion process is also a feature vector $D_f(t) \in R^n$ containing the decisions result of fusing individual templates [6].

In the simple voting system (by majority), the final decision is taken according to the number of votes given by the individual classifiers to each one of the classes, thus assigning the test pattern to the class that has obtained a majority of votes. When working with data sets that contain more than two classes, in the final decision ties among some classes that are very frequently obtained.

Given a set of L base templates $B = \{B_1, \ldots, B_L\}$. Let b_{ij}^{l}, i=l, . . . , n and j= 1, . . . , m denote the entry at the i^{th} row and the j^{th} column of the base template B^l and l= 1, . . . , L. Voting index [6] is given as

$$\varphi_{ij}^{B} = \frac{1}{L} \sum_{l=1}^{L} b_{ij}^{l} \quad (1)$$

The entries of the final template generated from the fusion of the L base templates are defined as follows:

$$b_{ij}^{L} = \begin{cases} 1, & \emptyset_{ij}^{b} > 0.4 \\ 0, & \emptyset_{ij}^{b} \leq 0.4 \end{cases} \quad (2)$$

The bit reliability is determined during the generation of the final template using the weight template for a given class. The weight template entries are associated with the corresponding final template entries and are calculated as follows:

$$\omega^{B}{}_{ij} = \begin{cases} \emptyset^{B}{}_{ij} & \emptyset^{B}{}_{ij} > 0.4 \\ 1 - \emptyset^{B}{}_{ij} & \emptyset^{B}{}_{ij} \leq 0.4 \end{cases} \quad (3)$$

The corrupted bits in the final template are accounted due to occlusion and/or illumination, the set of masks corresponding to a given set of base templates are also fused into a final mask M and a mask weight W_m is generated.

$$\emptyset_{ij}^{M} = \frac{1}{L} \sum_{l=1}^{L} m_{ij}^{l} \quad (4)$$

$$m_{ij}^{f} = \begin{cases} 1, & \emptyset_{ij}^{M} > 0.4 \\ 0, & \emptyset_{ij}^{M} \leq 0.4 \end{cases} \quad (5)$$

$$\omega_{ij}^{M} = \begin{cases} \emptyset_{ij}^{M}, & \emptyset_{ij}^{M} > 0.4 \\ 1 - \emptyset_{ij}^{M}, & \emptyset_{ij}^{M} \leq 0.4 \end{cases} \quad (6)$$

E. Template Matching

Hamming distance is used as a metric for the process of matching in iris recognition. The Hamming distance gives a measure of similarity between two bit patterns. In comparing the bit patterns D and P, the Hamming distance (HD) [3], is defined as the sum of disagreeing bits over N, the total number of bits in the bit pattern.

$$\text{HD} = \frac{1}{N} \sum_{1}^{N} D_i \oplus P_i \quad (7)$$

The Hamming distance algorithm employed also incorporates noise masking, so that only significant bits are used in calculating the Hamming distance between two iris templates. Now when taking the Hamming distance, only those bits in the iris pattern that corresponds to '0' bits in noise masks of both iris patterns will be used in the calculation. The Hamming distance will be calculated using only the bits generated from the true iris region, and this modified Hamming distance formula [6] is given as

$$HD = \frac{\sum_{i}^{N} (T_i \oplus P_i) \cap M_i^T \cap M_i^P}{N - \sum_{i}^{N} M_i^T \cap M_i^P} \quad (8)$$

where N, the number of bits represented by each template and D and P are the two templates to be compared and M^T and M^P are the corresponding noise masks.

IV. PERFORMANCE EVALUATION

Initially thirty peculiar images from CASIA database are chosen for experiment. The iris is segmented and normalized using Daugman's method. The iris features are extracted using gabor wavelets. Finally, the generation of the final templates is achieved in two steps. First, a base template and noise mask are generated for each eye image of an individual in the database containing multiple eye images (both left and right) of a single human. Second, weight template associated with the final template is generated for each base template. This final fused template is compared with all the enrolled final templates and a Hamming distances are estimated to find the minimum threshold.

In this work, three independent databases are created, one to enroll templates of left and right iris and second to enroll the final template of left iris and third to enroll the final templates of right iris. Instead of storing multiple templates for each orientation of an individual's eye, this fusion work reduces the storage size of database by fusing the different images of left iris and fusing the images of right iris of an individual into two different final templates.

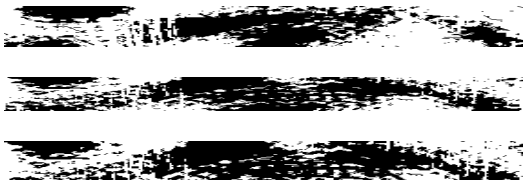

Figure 5. Final template samples

The multiple base templates of an iris (either left or right) are fused to generate a final template (Figure 5) which is used for further matching in authentication process. This fusion technique will reduce the database size maximum upto 85% as well the time during matching process is fastening up. In turn increases the overall performance of authentication process which is indicated in Table I.

A. Performance Metrics

We evaluate mainly the performance according to the following metrics.

False Acceptance: The FAR presents a greater security concern, because unauthorized access is granted. The false acceptance should be kept low.

False Rejection: FRR occurs when users are granted access but should have been denied access. The false rejection should be kept low.

Equal Error Rate: The ratio false acceptance and false rejection. This should be kept low to higher the accuracy.

B. Results

In this experiment, an improvement in the speed of the matching process was noticeable by the fact that instead of comparing an introduced image template with 450 base templates, we compare the given template with only 100 final templates. The improvement in computational speed is also asserted by the fact that 25% of computation time in the shifting process is only required in the proposed algorithm, we vary the no. of images as 30, 50 up to 150.

Table I Performance Results

Fusion	DB size (KB)	Threshold	Acceptance Ratio %	Performance Time
Without Fusion	N	0.4	99.9%	M secs
With Fusion of left irises	< (N/25)	0.4	99.6 %	M/2 secs
With Fusion of right irises	< (N/25)	0.4	99.7%	M/2 secs
With Fusion left & right irises	< (N/50)	0.4	79%	M/4 secs

V. CONCLUSION

Normally the features are extracted from any of iris images of an individual and respective template is generated for matching. High probability of attacking this feature template may exist. Also multiple images of the same iris may be required to improve the performance of an iris authentication system. Hence the storage size of the template database will be high normally. In order to provide better security and to manage the database size, this work presents an fusion algorithm by which a given set of base templates of left images or right images nor both left and right iris images are fused to generate final templates which further used in matching process for authentication. This results in such a way that storage size can be reduced up to 75% by this method which in turn increases the overall performance of the authentication system, also decreases the probability of attacks on those feature templates.

REFERENCES

[1]. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay, Tai-hoon Kim. IRIS Texture Analysis and Feature Extraction for Biometric Pattern Recognition. International Journal of Database Theory and Application, 2005, pp. 53-60.

[2]. W.W. Boles, A wavelet transform based technique for the recognition of the human iris. In Proceedings of the International Symposium on Signal Processing and its Application, ISSPA, Gold Coast, Australia, 1996, pp. 25-30, August.
[3]. J. G. Daugman, Statistical Richness of Visual Phase Information: Update on Recognizing Persons by Iris Patterns. International Journal of Computer Vision, 2001, Vol. 45, No. 1, pp. 25 – 38.
[4]. R. Wildes, J.C. Asmuth, G.L. Green, S.C. Hsu, R.J. Kolczynski, J.R. Matey and S.E. McBride, A system for automated iris recognition. In Proceedings of the IEEE Workshop on Applications of Computer Vision, 1994, pp. 121-128.
[5]. John Daugman, High confidence visual recognition of persons by a test of statistical independence. IEEE Trans. Pattern Anal. Mach. Intell. 1993, 15 (11), pp. 1148–1161.
[6]. Aly I. Desoky, Hesham A. Ali, Nahla B. Abdel-Hamid, Enhancing Iris recognition system performance, IEEE Transactions, 2010, pp 21-26.
[7]. A.K. Jain, R. Bolle and S. Pankanti, Biometrics: Personal Identification in Network Society. Kluwer Academic Publishers, 1999.
[8]. A.K. Mohapatra, Madhvi Sandhu, Biometric Template Encryption. International Journal of Advanced Engineering & Application, 2010, pp. 282-284.
[9]. John Daugman, How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology, 2004, 14(1): 21–30.
[10]. R. P. Wildes, Iris Recognition: An Emerging Biometric Technology. In Proceedings of the IEEE, 1999, Vol. 85, No. 9, pp.1348-1363.
[11]. W. W. Boles and B. Boashash, A Human Identification Technique Using Images of the Iris and Wavelet Transform. IEEE Transactions on Signal Processing, 1998, Vol. 46, No. 4, pp. 1185-1188.
[12]. Y. Zhu, T. Tan and Y. Wang, Biometric personal identification based on iris pattern. In Proceeding of 15th International Conference on Pattern Recognition, 2000, vol. 2, pp. 801-804.
[13]. Yong Wang, Jiu-Qiang Han, Iris feature extraction using independent component analysis. In Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 2005, pp.18-21.