A New Algorithm for Creating Digital Certificate's Private Key from Iris

Mahbubeh Shamsi[1], AbdolReza Rasouli Kenari[2], Soudeh Shadravan[3], Farrokh Koropi[4]
1- Faculty of Computer Science, Islamic Azad University, Bardsir Branch, Iran
Email: mahboubehshamsi@yahoo.com
2- Faculty of Computer Science, Islamic Azad University, Bardsir Branch, Iran
Email: rs.reza@gmail.com
3- Faculty of Computer Science, Islamic Azad University, Bardsir Branch, Iran
Email: shadravan@yahoo.com
4- Faculty of Computer Science, Islamic Azad University, Baft Branch, Iran
Email: fkoropi@yahoo.com

Received: December 2010 Revised: February 2010 Accepted: March 2010

ABSTRACT:
Enterprises are now global, virtual and dependent on dynamic information access. Naturally, digital information is constant throughout its lifecycle. In this shifting landscape, the battlefront in security is rapidly changing from securing the perimeter to protecting the information itself. The primary advantage of public-key cryptography is increased security and convenience: private keys never need to be transmitted or revealed to anyone, but loss of a private key may cause the loss of valuable data. In this paper, we proposed a new method of using iris biometric instead of private keys, so that the iris cannot be lost, stolen or even misused. The two first stages of iris recognition are implemented as the preliminary result. Our approach is feasible to produce an iris template for using as a private key in identity identification and biometric watermarking applications.

KEYWORDS: Iris recognition, biometric identification, recognition, automatic segmentation.

1. INTRODUCTION

Governments in some countries use biometrically-enabled national identity cards. One purpose would be to detect fraudulent multiple identities. Other purposes include expedited immigration controls using biometric passports, allowing automated border crossing; and security-screening searching against watch-lists at ports of entrance. People abroad will be routinely able to enter the country without presenting a passport or explicitly asserting their identity. The biometric identification system could possibly survive so many comparisons between different pairings of persons, without making false matches.

When we compare biometric features such as face and fingerprint, retinal, hand shape, handwritten, signature, and voice dimensions, iris patterns are more stable and reliable [1]. The patterns within the iris are very unique for each person, and even the left eye is also different from the right eye iris [2].

Currently, iris recognition systems require a cooperative subject. Partial iris recognition algorithms are very important for designing systems. Therefore in this paper; we investigate the accuracy of using a partial iris for identification.

In addition, we also investigate which portion of the iris has most distinguishable patterns. To produce the private key for identification systems and decoding the subject we need to extract features from captured picture. The experimental results show that it is possible to use only a partial iris image for human identification.

1.1. Problem Background

The iris is a green/grey/brown area. In an eye image, other visible structures are the pupil in the centre and the white sclera surrounding the iris. The overlying cornea is pictured, but not visible, as it is transparent. Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irises of an individual's eyes.

These unique structures converted into digital templates, provide mathematical representations of the iris that are unambiguous positive identification of an individual. Iris recognition efficacy is rarely impeded by glasses or contact lenses [3].

First, an iris-recognition algorithm has to identify the approximately concentric circular outer boundaries

of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images. The mathematical methods used here, resemble those of modern loss compression algorithms for photographic images (e.g., [1], [4]).

In the case of Daugman's algorithms, a Gabor wavelet transform is used in order to extract the spatial frequency range that contains a good best signal-to-noise ratio considering the focus quality of available cameras. The result is a set of complex numbers that carry local amplitude and phase information for the iris image. In Daugman's algorithms, all amplitude information is discarded, and the resulting 2048 bits that represent an iris consist only of the complex sign bits of the Gabor-domain representation of the iris image ([6], [7]).

The amplitude information ensures that the template remains largely unaffected by changes in illumination and virtually negligibly by iris color, which contributes significantly to the long-term stability of the biometric template [8].

To authenticate via identification (one-to-many template matching) or verification (one-to-one template matching) a template created by imaging the iris, is compared to a stored value template in a database. For creating the iris template, the eye image will be captured by camera. If the Hamming distance is below the decision threshold, a positive identification has effectively been made. Then this image will be normalized and all noise will be removed. After that, the iris area will be extracted from other areas.

A practical problem of iris recognition is that the iris is usually partially covered by eye lids and eye lashes. In order to reduce the false-reject risk in such cases, additional algorithms are needed to identify the locations of eye lids and eye lashes, and exclude the bits in the resulting code from the comparison operation.

Depending on the system, this image or a binary code extracted from the image will be stored for future comparing. In this paper, we will extract a unique binary code from iris images and we will import this binary code to an asymmetric key generating algorithm. This algorithm will produce a private key related to the owner's public key. These keys are used for authentication propose.

1.2. Related Work

The system introduced by Monrose *et al*. [9] is based on keystroke dynamics. A short binary string is derived from the user's typing patterns and then combined with her password to form a hardened password. Each keystroke feature is discretized as a single bit, which allows some error tolerance for feature variation. The short string is formed by concatenating the bits. In a follow-up paper, Monrose *et al*. proposed a more reliable implementation based on voice biometrics, but with the same discretization methodology [9]. Their paper reports an improvement in performance: The entropy of the biometric key is increased from 12 bits to 46 bits, while the false rejection rate falls from 48.4 percent to 20 percent [37].

Hao and Chan made use of handwritten signatures [18]. They defined 43 signature features extracted from dynamic information like velocity, pressure, altitude, and azimuth. Feature coding was used to quantize each feature into bits which were concatenated to form a binary string. This achieved, on average, a 40-bit key entropy with a 28 percent of false rejection rate; the false acceptance rate was about 1.2 percent [19].

Fingerprints are among the more reliable biometrics and there is a long history of their use in criminal cases [32]. Soutar *et al*. reported a biometric key system based on fingerprints [31]. They extracted phase information from the fingerprint image using a Fourier transform and apply majority coding to reduce the feature variation. Instead of generating a key directly from biometrics, they introduce a method of biometric locking: A predefined random key is locked with a biometric sample by forming a phase-phase product. This product can be unlocked by another genuine biometric sample. Biometric locking appears a promising idea because the biometric key can be randomly defined. However, performance data are not reported.

Clancy *et al*. proposed a similar application based on fingerprints and used a technique called a fuzzy vault, which had been first introduced by Juels and Sudan [10,20]. In Clancy *et al*.'s work, the fingerprint minutiae locations are recorded as real points which form a locking set. A secret key can be derived from this through polynomial reconstruction. In addition, chaff points are added to the locking set to obscure the key. If a new biometric sample has a substantial overlap with the locking set, the secret key can be recovered by a Reed-Solomon code. This work is reported to derive a 69-bit biometric key, but, unfortunately, with a 30 percent false rejection rate.

Goh and Ngo combined some of the above techniques to build a system based on face biometrics [17]. They adopted the biometric locking approach used by Soutar *et al*. Eigen projections are extracted from the face image as features, each of which is then mixed with a random string and quantized into a single bit. A binary key is formed by concatenating these bits and majority-coding is added as suggested by Davida *et al*. Error correction involves polynomial thresholding, which further reduces feature variances. Goh and Ngo report extracting 80-bit keys with a 0.93 percent of false rejection rate. This is the beginning of an

approach to the parameters needed for a practical system. However, the experiments reported are based on images taken from a continuous video source with minor variations, rather than a face database. So, doubts remain about the evaluation of this work.

1.3. Problem Statement

It is difficult to perform iris recognition at a distance larger than a few meters or if the person that is to be identified is not cooperating by holding the head still and looking into the camera [15]. As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates [27, 30].

In general, public-key systems are used for digital signatures and for secure key exchange between users. However, regardless of what a user wants to do, the security is dependent on the secrecy of the private key. Because of the large size of a cryptographically-strong key, it would clearly not be feasible to require the user to remember and enter the key each time it is required. Instead, the private key may be stolen or misused.

As an alternative, we can use a new mechanism for key security by using a biometric to produce the cryptographic key [11, 12, and 13], instead of storing a large size cryptographic key. This key is produced by the iris template. When a user wishes to authenticate himself/herself, he/she will represent his/her public key embedded in his/her certificate, then a random number will be encrypted with this public key. then she will be asked to stand in front of camera. If the private key produced by her iris is able to decrypt the random key, her will be authenticated. This method offers both conveniences, as the user no longer has to store or remember a private key, and secure identity confirmation is preserved, since only the valid user can release the key.

1.4. Framework

In this section, a major component of the proposed method will be explained. Each identification system has two major procedures: *Enrollment* and *Verification.*

The objective of enrollment procedure is extracting iris features and creating a pair key with the generated iris code. These two keys are used as the public and the private key. The public key will be stored in the certificate and the private key will be destroyed [2, 14].

The objective of verification procedure to extract iris binary code as the private key so that we decrypt an encrypted message with a public key that is embedded in a certificate. A successful decrypting process will be able to verify the identity of the certificate owner.

The enrollment and verification procedure are shown in Fig. 1 and 2 respectively.

Both enrollment and verification procedures use iris feature extraction to create a binary unique iris code from the captured eye image. This is the main component of the system and should work accurately. The iris feature extraction system will be explained in the next section in detail.

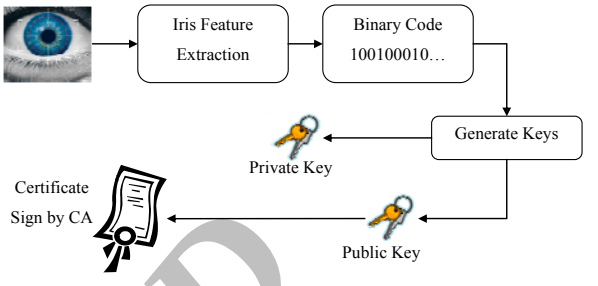

Fig. 1. Enrollment Procedure

After extracting iris features, the key generation method will generate two keys: A public key and a private key. The generated public key and other certificate information will be stored in the certificate and will be encrypted with the Certificate Authority (CA)[1] private key. Using this private key ensures that nobody except the CA can create this certificate. The private key will be destroyed for avoiding any potential attacks.

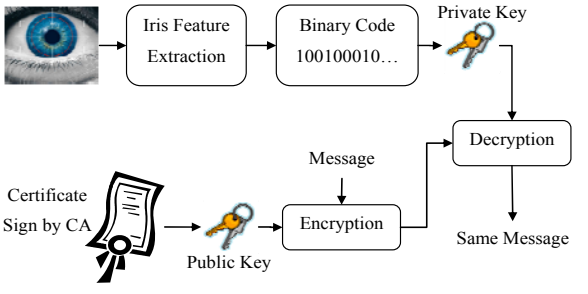

Fig. 2. Verification Procedure

Verification's first step is the same as enrollment. An eye image will be captured and its iris feature code will be extracted from the eye image. Elsewhere, the certificate will be decrypted by the CA public key. A successful decryption means that all information is to be correct. Expired date and other information will be investigated. A simple message will be encrypted with the public key existing in the certificate for verifying the identity. If the iris generated code is able to decrypt this encrypted message, the person will be verified.

[1] In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates for use by other parties.

1.5. Iris Feature Extraction

The most important step in both enrollment and verification is extracting features of iris and creating a binary iris code. The iris code is used to perform the asymmetric keys. The iris feature extraction steps are shown in Fig. 3.

There are five stages to create an iris code from the eye image. The first stage is to capture an image from the human eye with a desirably precise camera. Then the image should be prepared. The preparation step consists of removing noise, resizing image and enhancing illumination. Iris localization is the next step. In this step, iris boundary will be segmented from other parts. Normalization is the next stage of iris recognition. After normalization, the image should be passed from a filter for extracting its unique features. In the next sections, these stages will be explained.

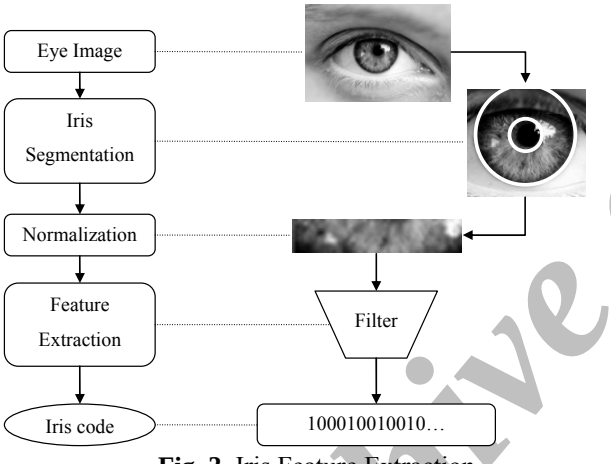

Fig. 3. Iris Feature Extraction

There are many methods for iris segmentation. In this paper and based on Daugman's deferential operator, we propose a slight nonlinear modification and reformulate the operator for speeding up the computation. The form is:

$$\max_{(n\Delta r, x_0, y_0)} \left| \sum_k \{ \frac{(G_\sigma(a_0) - G_\sigma(a_1)) \sum_m I(b_x, b_y)}{\Delta r \sum_m I(c_x, c_y)} \} \right| \quad (1)$$

Where

$$\begin{aligned} a_0 &= (n-k)\Delta r, a_1 = (n-k-1)\Delta r, \\ b_x &= k\Delta r \cos(m\Delta\phi) + x_0, \\ b_y &= k\Delta r \sin(m\Delta\phi) + y_0, \\ c_x &= (k-2)\Delta r \cos(m\Delta\phi) + x_0, \\ c_y &= (k-2)\Delta r \sin(m\Delta\phi) + y_0 \end{aligned} \quad (2)$$

All stages of iris segmentation are shown in Fig. 4.

The Daugman's operator needs a potential center point of the iris and a range of probable radiuses. We proposed a binning approach to find a potential center point. We assume that the darkest pixel in last binned image is the center of iris. Because all eye's pupil is black. Then we input this center point with the suggested radius to Daugman's operator to find the boundary of iris. The details algorithm will be described in section 2.1.

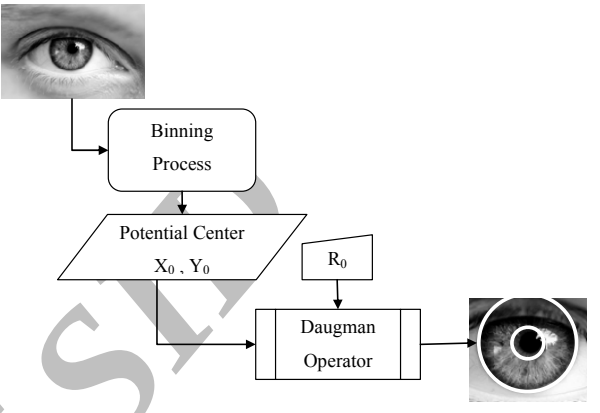

Fig. 4. Iris Segmentation Flowchart

In the normalization, the iris region is transformed so that it has fixed dimensions to allow comparisons between the same iris images. The inconsistencies between the same eye images are due to stretches of the iris caused by dilation of pupil from different illuminations. Among other factors that cause dilation are; eye rotation, camera rotation, head tilt and varying image distance. A good normalization process must produce different iris regions for different irises in the same condition and it must produce constant dimensions for the same irises in different conditions. Another great challenge is that the pupil region is not always concentric within the iris region, and it is usually slightly nasal. Daugman's rubber sheet model explains remap of each iris region's point to the polar coordinates (r,θ) where the distance $[0,1]$ is r and the angle $[0,2\pi]$ is θ.

The remapping of the iris region from (x,y) Cartesian coordinates to the normalized non-concentric polar representation is modeled as

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

With

$$\begin{aligned} x(r,\theta) &= (1-r)x_p(\theta) + rx_1(\theta) \\ y(r,\theta) &= (1-r)y_p(\theta) + ry_1(\theta) \end{aligned} \quad (4)$$

Where the iris region image is $I(x,y)$, the original Cartesian coordinates are (x,y) and the normalized polar coordinates are (r,θ).

The coordinates of the pupil and iris boundaries along the θ direction are: x_p, y_p and x_1, y_1. The rubber sheet model is useful for accounting pupil dilation and

size inconsistencies. This model however does not compensate for rotational inconsistencies.

For this problem, two iris templates are aligned with matching in shifting the iris templates in the θ direction.

As mentioned before, there are many wavelet filters for extracting iris features [21, 23, 24, and 25]. The proposed scheme of feature extraction is to map the iris ring to a rectangular block image which is counter clockwise and divided into eight sub images the we analyze the 8 sub images. A feature vector consists of an ordered sequence of the features extracted from the local information contained in the 8 sub images. Thus, the feature elements capture the local information and the ordered sequence captures the invariant global relationships among the local patterns.

Gabor filtering is a well known technique in texture analysis. We filter each sub image at different directions with different frequencies, and then obtain a feature value from each filtered sub image. A feature vector is a collection of all the features from each filtered sub image.

Gabor's elementary functions are Gaussians modulated by sinusoidal functions. It is shown that the functional form of Gabor filters conforms closely to the receptive profiles of simple cortical cells, and Gabor filtering is an effective scheme for image representation. A two dimensional (2D) even Gabor filter can be represented by the following equation:

$$G(x,y,\theta,f)=\exp\left\{-\frac{1}{2}\left[\frac{x'^2}{\delta_{x'}^2}+\frac{y'^2}{\delta_{y'}^2}\right]\right\}\cos(2\pi f x') \tag{5}$$

$$x'=x\cos\theta+y\sin\theta$$

$$y'=y\cos\theta-x\sin\theta$$

Where f is the frequency of the sinusoidal plane wave along the direction θ from the x-axis, $\delta_{x'}$ and $\delta_{y'}$ are the space constants of the Gaussian envelope along x' and y' axes respectively.

The frequency parameter f is often power of 2. In our experiments, the central frequencies used are 2, 4, 8, 16, and 32 cycles/degree. For each central frequency f, filtering is performed at $\theta = 0^o$, 45^o, 90^o and 135^o. So, there are a total of 20 Gabor filters with different frequencies and directions. Each sub image is respectively filtered by these Gabor filters. This leads to a total of 160 (20 for each sub image) output images from which the iris features are extracted.

In our algorithm, the binary code is the average absolute deviation (AAD) of each output image defined as follows:

$$V=\frac{1}{N}\sum_{N}\left|f(x,y)-m\right| \tag{6}$$

Where N is the number of pixels in the image, m is the mean of the image, and $f(x, y)$ is the value at point (x, y). These features are arranged to form a 1D feature vector of the length 160 for each input image.

After the creation of the binary iris code, we create the asymmetric keys from the iris code. The details of key generation process will be described in the next section.

1.6. Asymmetric Key Generation

As you can see in Fig. 5, asymmetric key generation process needs two input parameters. The first one is the iris generated code from the iris recognition stage and the second one is two big prime numbers, p and q.

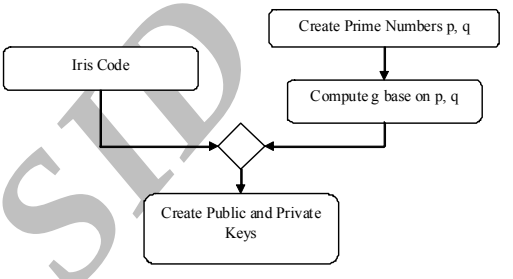

Fig. 5. Asymmetric Key Generation

The process of key generation from iris code is given below:

- Create two prime numbers *p, q*
  - *2512 < p < 21024*
  - *q is a prime divisor of p – 1*
  - *2159 < q < 2160.*
- Compute $g = (h^{(p-1)/q} \bmod p)$.
  - h is any integer
  - $1 < h < (p – 1)$.

Let x be the iris code generated from the previous stage so that $0 < x <$ q. Compute $y = (g^x \bmod p)$.

The integers, *p, q* and *g* can be public and can be common to a group of users. A user's private and public keys are x and y respectively. They are normally fixed for a period of time [16, 22].

2. IRIS SEGMENT ALGORITHM

Based on the above equations, the following is the implemented steps of the algorithm:

1. Get an input image I .
2. Use $I_k = \mathrm{B}\{I_{K-1}, f\}, k = 1..K$ for series of binned images
3. For I_K , find a minimum and after that assume it is the center $(x_0^{(K)}, y_0^{(K)})$ of the pupil.
4. For each image $I^{(K)}$ $k = 0..K$ starting from more to less binned images.
5. Construct a set of potential centers around the point defined by initial values obtained as a result of the previous stage

$$\left(x_0^{(K)}, y_0^{(K)}\right) \in C^{(K)} \tag{7}$$

Where:

$$C^{(K)} = \left\{\left(\hat{x}_0^{(K)} - \lfloor f_k/2 \rfloor\right)..\left(\hat{x}_0^{(K)} + \lfloor f_k/2 \rfloor\right)\right\} \times \left\{\left(\hat{y}_0^{(K)} - \lfloor f_k/2 \rfloor\right)..\left(\hat{y}_0^{(K)} + \lfloor f_k/2 \rfloor\right)\right\} \quad (8)$$

6. Construct a set of potential radiuses

$$r^{(K)} \in \left\{\left(\hat{r}^{(K)} - \lfloor f_k/2 \rfloor\right)..\left(\hat{r}^{(K)} + \lfloor f_k/2 \rfloor\right)\right\} \quad (9)$$

7. Find

$$\left(\breve{r}, \breve{x}, \breve{y}\right) = \arg\max_{(r,x,y)} \sum_{m=1}^{M} \begin{pmatrix} I_x\left(x_m, y_m\right)\cos\alpha_m \\ + I_y\left(x_m, y_m\right)\sin\alpha_m \end{pmatrix} \quad (10)$$

8. Recompute $\left(\breve{r}^{(K)}, \breve{x}^{(K)}, \breve{y}^{(K)}\right)$ to the finer grid using f_K

$$\left(\breve{r}^{(K-1)}, \breve{x}^{(K-1)}, \breve{y}^{(K-1)}\right) = f_K\left(\breve{r}^{(K)}, \breve{x}^{(K)}, \breve{y}^{(K)}\right) \quad (11)$$

2.1. The Normalization Algorithm

Our algorithm on normalization of iris regions is based on Daugman's rubber sheet model. Since the pupil can be non-concentric to the iris, a remapping formula is needed to rescale points depending on the angle around the circle. This is given by

$$r' = \sqrt{\alpha}\beta \pm \sqrt{\alpha\beta^2 - \alpha - r_I^2} \quad (12)$$

With

$$\alpha = o_x^2 + o_y^2$$

$$\beta = \cos\left(\pi - \arctan\left(\frac{o_y}{o_x}\right) - \theta\right) \quad (13)$$

The displacement of the centre of the pupil in regard to the centre of the iris is given by o_y, o_x the distance between the edge of pupil and the edge of iris at an angle is r', around the region is: θ and the radius of the iris is: r_I

In order to prevent non-iris region data from corrupting the normalized representation, data points which occur along the pupil border or the iris border are discarded as the same as Daugman's rubber sheet model. Fig. 6 shows the outline of the normalization process and Fig. 7 show the result of the normalization process.

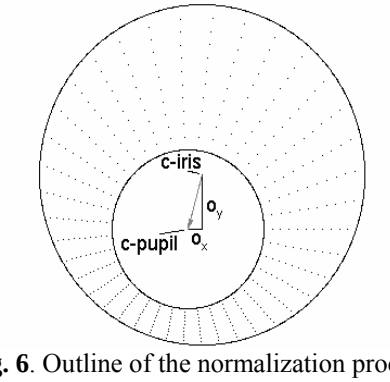

Fig. 6. Outline of the normalization process

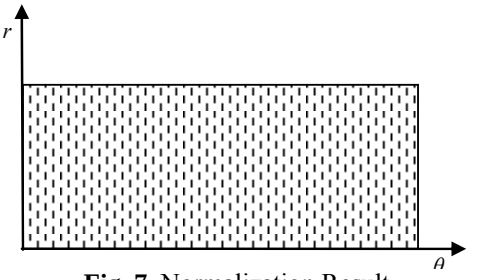

Fig. 7. Normalization Result

2.2. Result

There are many standard iris databases that could be employed in iris researches [9]. Two standard iris databases [28, 29] have been selected for preliminary results. CASIA and MMU iris databases are employed for testing the implemented algorithms.

The above algorithm is implemented with Delphi programming language. In this case, more than 100 irises are randomly selected among the above databases. During detecting iris by this algorithm, the most important thing is to set correct parameters. There are four parameters in the algorithm:

1. Smoothing Factor: This parameter is used in the binning stage and indicates the width of the binning square.
2. Binning Stage: It means that how many times the algorithm should bin the original image.
3. Suggest Radius: The radius of the pupil in the last binned stage.
4. Circle Sample: The number of points taken into integration over the circle.

We have tested the algorithm in three different phases. In the first phase all parameters are fixed for all images. We use Smoothing Factor = 3, Binning Stage = 4, Suggest Radius = 1 and Circle Sample = 64. The results are summarized in Table 1.

Table 1. Execution result with fixed parameters

Iris Database	Percentage of Correctness		
	Correct Detect	Correct Pupil or Correct Iris	Wrong Detect
CASIA	73	16	11
MMU Iris Database	77	14	9

In this phase, we see that wrong detections could be corrected by changing the parameters. For example, as you can see in Fig. 8, the iris isn't detected correctly in the left image, but by changing the smoothing factor to 5, this has been reclaimed (see the right image).

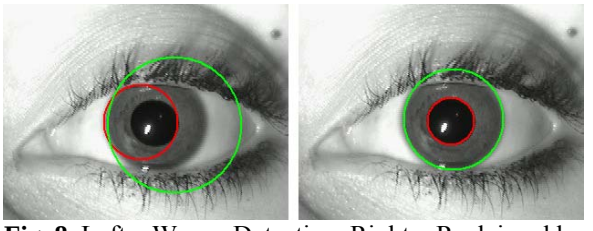

Fig. 8. Left – Wrong Detection, Right – Reclaimed by changing parameters

In the second phase, we try to change the parameters for wrong detections and test them again to obtain a better result. By default we set the parameters similar as before, however in wrong detection we adjust the parameters until it is correctly detected. The results of the second phase are shown in Table 2.

Table 2. Execution Result with Vary Parameters

Iris Database	Percentage of Correctness		
	Correct Detect	Correct Pupil or Correct Iris	Wrong Detect
CASIA	91	7	2
MMU Iris Database	94	5	1

It is observed that the results are significantly improved, but still there is some incorrect detection. In some cases, the pupil may be correctly detected, conversely incorrect detecting the pupil. After adjusting the value of the parameter, the pupil is wrongly detected. In the third phase, different parameter values are adopted to improve the detection rate. The results of the third phase are summarized in Table 3. The final detection of some iris images is depicted in Fig. 9.

Table 3. Execution Result with Separate Parameters

Iris Database	% of Correctness	
	Detected	Undetected
CASIA	98	2
MMU Iris Database	99	1

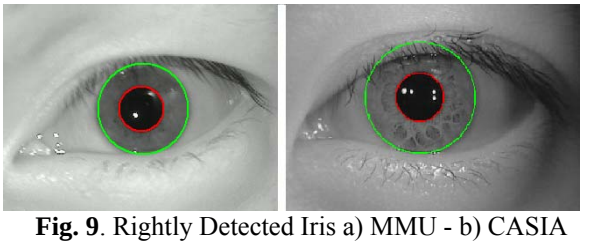

Fig. 9. Rightly Detected Iris a) MMU - b) CASIA

The normalization process proved to be successful and some results are shown in Fig. 10. However, the normalization process is unable to perfectly reconstruct the same pattern from images with varying amounts of pupil dilation, since deformation of the iris results in small changes of its surface patterns.

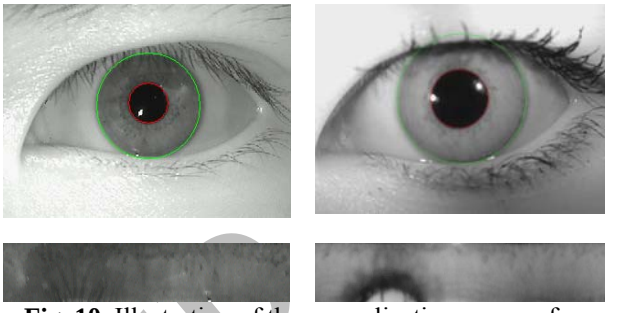

Fig. 10. Illustration of the normalization process for two images of the same iris taken under varying conditions

Normalization of two eye images of the same iris is shown in Fig. 10. The pupil is smaller in the bottom image; however the normalization process is able to rescale the iris region so that it has constant dimensions. In this example, the rectangular representation is constructed from (360 * (Iris Radius – Pupil Radius)) data points in each iris region. Note that rotational inconsistencies have not been accounted by the normalization process, and the two normalized patterns are slightly misaligned in the horizontal (angular) direction. Rotational inconsistencies will be accounted for in the matching stage.

The critical step of the algorithm is to set correct parameters. By using fixed parameter values, the algorithm automatically detects both the iris and the pupil. However, the rate of correct detection is low and it is not acceptable. Conversely by allowing manual intervention of parameters set by the user for wrong detection, the accuracy rate increases as shown in Fig. 11.

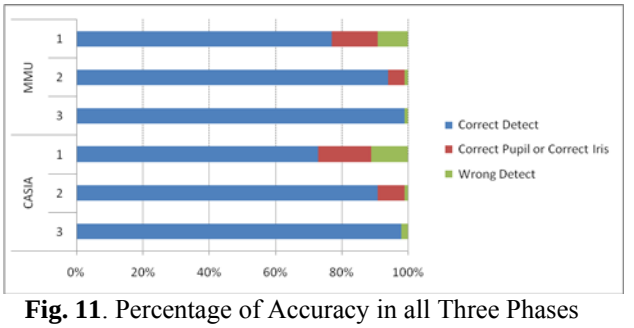

Fig. 11. Percentage of Accuracy in all Three Phases

As shown in Fig. 12, with high quality images, auto detection produces encouraging results. On the other hand poor iris images need user-intervention to increase the rate of correct iris and pupil detection.

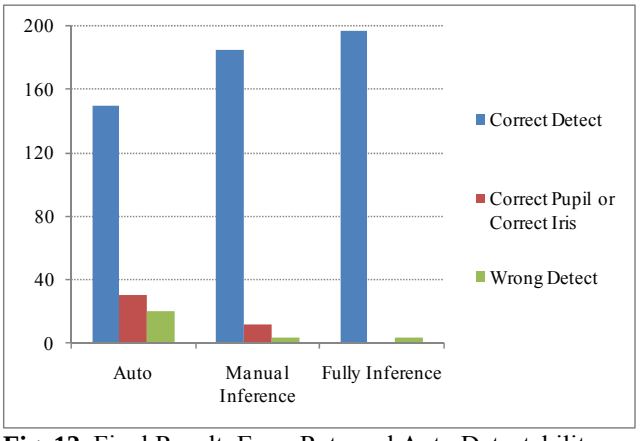

Fig. 12. Final Result, Error Rate and Auto Detectability

3. CONCLUSION AND FUTURE WORKS

As we have shown in the previous section, the poor image quality is due to the presence of shadow especially in corners that contribute to the wrong detection of center point. Another potential problem is associated with luminosity in some images that hinder the detection process. A further problem is due to the irregular image dimension. To overcome the above problems, we can either use more than one image or incorporate an intelligent technique to automatically adjust the associated parameters for correct detection. Another challenging problem that we encounter during the normalization stage is the effect of eye lashes towards the iris. We do not have to perform the noise removal if both iris and eye lashes have similar colors. In this case noise is indicated by the presence of eye lashes. However, we need to remove the noise from the iris, if iris and eye lashes have different colors. The noise will affect the accuracy of the template generated from a normalized iris in our next venture.

4. ACKNOWLEDGMENT

This project was supported by the research project at Islamic Azad University, Bardsir Branch.

REFERENCES

[1] Anderson R.J.; **"Security Engineering: A Guide to Building Dependable Distributed Systems"**. New York: Wiley, (2001)

[2] Barros, J, French, J and Martin, W.; **"Indexing Multi-Spectral Images for Content-Based Retrieval"**, University of Virginia Technical Report, CS-94-40, (1994)

[3] Barros, J., French, J. *et al.*; **"System for Indexing Multi-Spectral Satellite Images for Efficient Content-Based Retrieval"**, Storage and Retrieval for Image and Video database, SPIE Vol. 2420, pp. 228-237, (1995)

[4] Barry C. and Ritter N.; **Database of 120 Grayscale Eye Images**. Lions Eye Institute, Perth Western Australia.

[5] Anoop Ms; **"Public key Cryptography-applications Algorithms and Mathematical Explanations"**. India: Tata Elxsi, (2007)

[6] Boles W. and Boashash B. **"A Human Identification Technique Using Images of the Iris and Wavelet Transform"**, *IEEE Transactions on Signal Processing*, Vol. 46, No. 4, (1998)

[7] Burt P. and Adelson E. **"The Laplacian Pyramid as A Compact Image Code"**. *IEEE Transactions on Communications*, Vol. 31, No. 4, (2004)

[8] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. Kumar; **"Biometric Encryption Using Image Processing",** *in Proc. SPIE Optical Security and Counterfeit Deterrence Techniques II, R. L. van Renesse*, Ed., Vol. 3314, No. 1, (2006)

[9] Noh S., Pae K., Lee C. and Kim J. **"Multiresolution Independent Component Analysis for Iris Identification"**. *International Technical Conference on Circuits/Systems, Computers and Communications*, Phuket, Thailand, (2002)

[10] Clancy T., Kiyavash N., and Lin D. **"Secure Smartcard-based Fingerprint Authentication,"** *in Proceedings ACM Multimedia 2003 Workshop on Biometric Methods and Applications, Berkeley, USA*, (2003)

[11] Clancy T.C., Kiyavash N., and Lin D.J., **"Secure Smart Card-Based Fingerprint Authentication",** *ACM SIGMM Workshop Biometrics Methods and Application (WBMA)*, (2003)

[12] Connie T., Teoh A., Goh M., and Ngo D. **"Palmhashing: A Novel Approach for Cancelable Biometrics",** *Information Processing Letters*, Vol. 93, No. 1, (2005)

[13] Duagman J., Anderson R. and Hao F. **"Combining Crypto with Biometrics Effectively''** *IEEE Transactions on Computers*, Vol. 55, No. 9, (2006)

[14] Ferguson N., Schneier B. **"Practical Cryptography''**. Wiley. ISBN 0-471-22357-3, (2003)

[15] Field D.; **"Relations between The Statistics of Natural Images And The Response Properties of Cortical Cells"**. *Journal of the Optical Society of America*, (2005)

[16] Goh A. and Ngo C.; **"Computation of Cryptographic Keys"** *Lecture Notes in Computer Science*, Vol. 2828, (2003)

[17] Goh A. and Ngo D.C. L.; **"Computation of Cryptographic Keys from Face Biometrics",** *Proc. Int'l Federation for Information Processing 2003*, pp. 1-13, (2003)

[18] Hao F. and Chan C.W.; **"Private Key Generation from On-Line Handwritten Signatures",** *Information Management & Computer Security*, Vol. 10, No. 2, pp. 159-164, (2002)

[19] Hao F., Anderson R., and Daugman J. **"Combining Cryptography with Biometrics Effectively"**, *University of Cambridge Computer Laboratory, Tech.* Rep, (2005)

[20] Juels A. and Sudan M. **"A Fuzzy Vault Scheme"**, *Proc. IEEE Int'l Symp. Information Theory*, (2002)

[21] Kass M., Witkin A., Terzopoulos D. **"Snakes: Active Contour Models"**, *International Journal of Computer Vision*, (2005)

[22] Katz J., Lindell Y.; **Introduction to Modern Cryptography**, CRC Press. ISBN 1-58488-551-3, (2007)

[23] Lee T. **"Image Representation Using 2d Gabor Wavelets"**. *IEEE Transactions of Pattern Analysis and Machine Intelligence*, Vol. 18, No. 10, (2006)
[24] Lim S., Lee K., Byeon O. and Kim T. **"Efficient Iris Recognition through Improvement of Feature Vector and Classifier"**. *ETRI Journal*, Vol. 23, No. 2, Korea, (2001)
[25] Ma L., Wang Y. and Tan T. **"Iris Recognition Using Circular Symmetric Filters"**. *National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences*, (2002)
[26] Chinese Academy of Sciences–Institute of Automation. Database of 756 Grayscale Eye Images. http://www.sinobiometrics.com Version 1.0, (2003)
[27] O'Gorman L., **"Seven Issues with Human Authentication Technologies"**, AutoID, (2002)
[28] CASIA iris image database, in http://www.sinobiometrics.com, Chinese Academy of Sciences Institute of Automation.
[29] MMU iris image database, in http://pesona.mmu.edu.my/~ccteo, Multimedia University.
[30] Prabhakar S. , Pankanti S., Jain A. K. **"Biometric Recognition: Security and Privacy Verification Competition"** *in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada*, pp. 744-747, (2003)
[31] Soutar C., Roberge D., Stoianov A., Gilroy R., and Vijaya Kumar B.V.K. **"Biometric Encryption"**, *ICSA Guide to Cryptography, McGraw-Hill*, (1999)
[32] Soutar C., Roberge D., Stoianov A., Gilroy R., and Kumar B. V. **"Biometric Encryption Using Image Processing"**, *in Proc. SPIE Optical Security and Counterfeit Deterrence Techniques II, R. L. van Renesse,Ed.*, Vol. 3314, No. 1. SPIE, pp. 178–188, (1998)