Iris Recognition for Person Identification using RSA Algorithm
Ms. Y. Elakkiya1  Ms. V. Girija2 Ms. B. Aktharunisa Begum3
1,2,3Department of Computer Applications
1,2,3IFET College of Engineering

Abstract—In biometrics, human being needs to be identified based on some characteristic physiological parameters. A wide variety of recognition schemes is used to either confirm or determine the identity of an individual requesting their services. In this work, we present various approaches to generate a unique and more secure cryptographic key from iris template. The iris images are processed to produce iris template or code to be utilized for the encryption and decryption tasks. A fuzzy vault refers to a biometric cryptosystem that can be used to effectively protect private keys and to release them only when legitimate users enter their biometric data. Distance metric such as hamming distance is used for the template matching identification process. Experimental results demonstrate the feasibility of the various systems and it shows that, R-S cryptographic algorithm can obtain a higher security with a low false rejection or false acceptance rate comparing to other techniques, and we would like to introduce this technique in adhar card.

Key words: Iris Localization, Edge Detection

I. INTRODUCTION
With communications among people constantly increasing nowadays, how to recognize people’s identity has become an essential problem. The traditional methods such as keys, certificates, passwords, etc, can hardly meet the requirements of identity recognition in the modern society. Biometrics, which means biological features based identity recognition, has provided a convenient and reliable solution to this problem.

Iris based identity recognition is one of the most important parts of biometrics due to its various advantages, such as preciseness and no need of direct contact with the testis. According to some comparative research, the error rate of iris recognition is the lowest one among all the biometrics approaches till date.

Many users are skeptical of the use of such a technology due to wearers of eyeglasses, contact lenses, or sunglasses. However, the recognition system is able to perform right through glasses or lenses since they do not interfere with the process. There is no need for a customer to take off their glasses in order to be identified quickly and accurately.

Iris recognition technology was designed to be less intrusive than retina scans, which often require infrared rays or bright light to get an accurate reading. Scientists also say a person’s retina can change with age, while an iris remains intact. And no two blueprints are mathematically alike, even between identical twins and triplets. During the course of examining large number of files, anatomists and ophthalmologists have noted that the detailed pattern of an iris, even the left and the right iris of a single person, seem to be highly distinctive.

II. FIVE STEPS IN IRIS RECOGNITION

A. Segmentation:
The image is cleaned up and a circular Hough transform is used to isolate the inner and outer iris boundaries. Advance the algorithm to ensure the inner boundary is within 20-90% of the outer boundary. Automatically choose the iris and pupil boundary radii.

B. Iris Localization:
In this stage, we should determine an iris part of the image by localizing the position of the image derived from inside the limbus (outer boundary) and outside the pupil (inner boundary), and finally convert the iris part into a suitable representation. Because there is some obvious difference in the intensity around each boundary, an edge detection method is easily applied to acquire the edge information.

C. Edge Detection:
It is used to find complex object boundaries by marking potential edge points corresponding to places in an image where rapid change in brightness occurs. After edge points have been marked, they can be merged to for lines. Edge detection operators are based on idea that edge information in an image is found by looking at the relationship of a pixel with its neighbors. In other words, edge is defined by discontinuity in gray values. An edge separates two distinct objects.

D. Normalization And Feature Encoding:
Basic rubber mapping need to account for pupil and iris boundaries not being quite concentric. Fully implement rubber sheet mapping - converting the disc of the iris to a rectangular matrix. Remove occlusions - the eyelashes, the eyelids, specular reflections.

E. Matching:
Planning to extract an iriscode which maximizes differences. Perhaps using Principle Components Analysis, or potentially a choice of several algorithms.

In addition recent medical advances such as refractive surgery, cataract surgery and cornea transplants do not change iris’ characteristics. In fact, it is impossible to modify the iris without risking blindness. And even a blind person can participate. As long as a sightless eye has an iris, that eye can be identified by iris recognition.
F. Overview of Backend Design:

III. SEVEN STEPS TO PROCESS:

IV. SURVEY

A. Hough Transform:
The Hough transform is a standard computer vision algorithm that can be used to determine the parameters of simple geometric objects, such as lines and circles, present in an image. The circular Hough transform can be employed to deduce the radius and centre coordinates of the pupil and iris regions. An automatic segmentation algorithm based on the circular Hough transform is employed by Wildes et al., Kong and Zhang, Tisse et al., and Ma et al. Firstly, an edge map is generated by calculating the first derivatives of intensity values in an eye image and then thresholding the result. From the edge map, votes are cast in Hough space for the parameters of circles passing through each edge point. These parameters are the centre coordinates \( x_c \) and \( y_c \), and the radius \( r \), which are able to define any circle according to the equation

\[
A \text{ maximum point in the Hough space will correspond to the radius and centre coordinates of the circle best defined by the edge points. Wildes et al. and Kong and Zhang also make use of the parabolic Hough transform to detect the eyelids, approximating the upper and lower eyelids with parabolic arcs, which are represented as;}
\]

Taking only the vertical gradients for locating the iris boundary will reduce influence of the eyelids when performing circular Hough transform, and not all of the edge pixels defining the circle are required for successful localisation. Not only does this make circle localisation more accurate, it also makes it more efficient, since there are less edge points to cast votes in the Hough space.

There are a number of problems with the Hough transform method. First of all, it requires threshold values to be chosen for edge detection, and this may result in critical edge points being removed, resulting in failure to detect circles/arcs. Secondly, the Hough transform is computationally intensive due to its ‘brute-force’ approach, and thus may not be suitable for real time applications.

B. Eyelash and Noise Detection:
Kong and Zhang present a method for eyelash detection, where eyelashes are treated as belonging to two types, separable eyelashes, which are isolated in the image, and multiple eyelashes, which are bunched together and overlap in the eye image. Thus, if a resultant point is smaller than a threshold, it is noted that this point belongs to an eyelash. If the variance of intensity values in a small window is lower than a threshold, the centre of the window is considered as a point in an eyelash. The Kong and Zhang model also makes use of connective criterion, so that each point in an eyelash should connect to another point in an eyelash or to an eyelid. Specular reflections along the eye image are detected using thresholding, since the intensity values at these regions will be higher than at any other regions in the image.

V. IRIS CODE CONSTRUCTION AND ENTROPY MEASURES

A. The IRIS Code:
The 2-D Gabor filters used for iris recognition are defined in the doubly dimensionless polar coordinate system \((r, \theta)\) as one can see from the definition, Eq.6, both the real and imaginary numbers are used, so resulting image projections are complex. The real parts of the 2D Gabor filters are slightly adjusted through truncation to give them zero volume, and hence no DC response, so that computed iris code bits do not depend upon the strength of illumination. (The imaginary parts of the filters have no DC response because of odd symmetry.) The parameters \(\alpha\) and \(\beta\) co-vary in inverse proportion to \(\omega\) to generate a self-similar, multi-scale wavelet family of 2D frequency-selective quadrature filters with constant logarithmic bandwidth, whose locations, specified by \(\theta_0\) and \(r_0\), range across the zones of analysis of the iris.

Each bit, \(h_i\), in an iris code is regarded as a coordinate of one of the four vertices of a logical unit square in the complex plane (Figure 11). It is computed by evaluating the sign of both the real and imaginary parts of the quadrature image projections from a local region of the iris image, \(I(\rho, \phi)\), onto a particular complex 2D Gabor filter:
Iris Recognition for Person Identification using RSA Algorithm
(IJSRD/Vol. 3/Issue 02/2015/498)

This means that a single complex 2D Gabor filter (eq.6), has a particular set of size and position parameters ($r_0$, $\theta_0$, $\alpha$, $\beta$, $\omega$) in the dimensionless iris domain ($r$, $\theta$), and that it performs a coarse phase quantization of the local texture signal by approximating it as one vertex ($h_{Re}, h_{Im}$) of the logical unit square associated with this filter through conditionals (eq.7-10). The iris code has a length of 256 bytes, or 2048 bits.

B. Bitwise Entropy and IRIS Variation

An important property of the iris recognition system, is that there are independent variation in iris detail, both within a given iris and as well across the human population. Any systematic correlations in iris detail across the population would undermine the uniqueness of an iris code. As well, any systematic correlations within an iris would reduce its statistical complexity, or dimensionality, hence also undermine its uniqueness.

The following diagram shows a study where the variation among the code bits was tracked both across bit location (128 locations for each code) within the code, and as well across a population of 592 different iris codes. It is sampled from all parts of the iris code.

The figure shows us the probability for a set bit, and that there is more or less equal probability for the bits to be in the different code bit locations. The probability for each code bit location is close to one half (measured of the mean of the means of the probabilities). This shows us the independent variations in the iris patterns that exists not only between features in one iris, but also across the human population. All in all one can say about the iris code that it is very close to a maximum entropy code ($P_j = 1/n$).

VI. HAMMING DISTANCES:

The Hamming distances would be a binomial distribution with $p = 0.5$ and $N = 2048$ (hence a peak around 1024). Adding the 2D Gabor filters, the new distributed Hamming distances would have a distribution of $p = 0.5$ and $N = 506$, where all of the bits in the iris code are without any correlations. This is the theory, the measured distribution of Hamming distances, generated from 2064 comparisons between unrelated pairs of iris codes is as shown in figure 6 below.

Here the mean is $\mu = 0.497$ and the standard derivation is $\sigma = 0.038$. This distribution of Hamming distances is equivalent to a binomial process with $N = 173$ Bernoulli trials per run and $p = 0.5$, which as it turns out corresponds to about 173 independent binary degrees of freedom remaining in a 2048-bit iris code (this number varies in each measure, and is often closer to 250 as mentioned before). This means that the probability of two irises having the same iris code by chance in these distributions, is in the order $10^{-173}$.

So far in this chapter, we have seen the Hamming distributions between unrelated iris codes, but there still remains the problem of determining at what Hamming Distance a sampled iris code should be considered an authentic, or an imposter. As mentioned in section 4.2, there are a lot of factors that can make one image of an iris different from another of the same iris. The following figure models the Hamming Distance measured for 9.1 million eyes to the right and to the left the Hamming Distance of 7070 different pairs of same-eye images at different times, under different conditions, and usually with different cameras.
Hysteresis is used to track errors. In his paper, Canny followed a list of criteria to improve current methods of edge detection. The first and most obvious is low error rate. It is important that edges occurring in images should not be missed and that there be no responses to non-edges. The second criterion is that the edge points be well localized. In other words, the distance between the edge pixels as found by the detector and the actual edge is to be at a minimum. A third criterion is to have only one response to a single edge. This was implemented because the first 2 were not substantial enough to completely eliminate the possibility of multiple responses to an edge.

Based on these criteria, the Canny edge detector first smooths the image to eliminate noise. It then finds the image gradient to highlight regions with high spatial derivatives. The algorithm then tracks along these regions and suppresses any pixel that is not at the maximum (nonmaximum suppression). The gradient array is now further reduced by hysteresis. Hysteresis is used to track along the remaining pixels that have not been suppressed. Hysteresis uses two thresholds and if the magnitude is below the first threshold, it is set to zero (made a nonedge). If the magnitude is above the high threshold, it is made an edge. And if the magnitude is between the 2 thresholds, then it is set to zero unless there is a path from this pixel to a pixel with a gradient above T2.

B. The Hough Transform:

The Hough transform is a method that, in theory, can be used to find features of any shape in an image. In practice it is only generally used for finding straight lines or circles. The computational complexity of the method grows rapidly with more complex shapes.

Assume we have some data points in an image which are perhaps the result of an edge detection process, or boundary points of a binary blob. We wish to recognise the points that form a straight line.

The representation of a line is given by

\[ ax \cos \theta + y \sin \theta = r \]

where \( r \) is the distance of the line from the origin and \( \theta \) is the angle between this perpendicular and the x-axis. Our parameter space is now in \( \theta \) and \( r \), where

\[ 0 \leq \theta \leq 2\pi \]

and \( r \) is limited by the size of the image.

As before, peaks in the accumulator array mark the equations of significant lines.

In theory any kind of curve can be detected if you can express it as a function of the form

\[ f(x, y) = 0. \]

For example a circle can be represented as

\[ (x - a)^2 + (y - b)^2 - r^2 = 0. \]
One then has to work in $n$ dimensional parameter space (three dimensional space for a circle). This model has three parameters: two parameters for the centre of the circle and one parameter for the radius of the circle. If the gradient angle for the edges is available, then this provides a constraint that reduces the number of degrees of freedom and hence the required size of the parameter space. The direction of the vector from the centre of the circle to each edge point is determined by the gradient angle, leaving the value of the radius as the only unknown parameter. Thus, the parametric equations for a circle in polar coordinates are

$$x = a + r \cos \theta$$

and

$$y = b + r \sin \theta.$$  

Solving for the parameters of the circle we obtain the equations

$$a = x - r \cos \theta$$

and

$$b = y - r \sin \theta.$$  

Now given the gradient angle $\theta$ at an edge point $(x,y)$, we can compute $\cos \theta$ and $\sin \theta$. Note that these quantities may already be available as a by-product of edge detection. We can eliminate the radius from the pair of equations above to yield

$$b = a \tan \theta - x \tan \theta + y.$$  

Then the Hough Transform algorithm for circle fitting can be described as follows.

VII. ENCRYPTION AND DECRYPTION

Encryption is the act of encoding text so that others not privy to the decryption mechanism (the "key") cannot understand the content of the text. Encryption has long been the domain of spies and diplomats, but recently it has moved into the public eye with the concern of the protection of electronic transmissions and digitally stored data. Standard encryption methods usually have two basic flaws: (1) A secure channel must be established at some point so that the sender may exchange the decoding key with the receiver; and (2) There is no guarantee who sent a given message.

Public key encryption has rapidly grown in popularity (and controversy, see, for example, discussions of the Clipper chip on the archives given below) because it offers a very secure encryption method that addresses these concerns.

A. RSA Algorithm:

The RSA algorithm can be used for public key encryption. The 3 basic steps of this algorithm are: 1.Key Generation algorithm 2.Encryption 3.Decryption.Key Generation Algorithm1.Generate two large random primes, $p$ and $q$, of approximately equal size such that their product $n = pq$ is of the required bit length, e.g. 1024 bits. 2.Compute $n = pq$ and $(p-1)(q-1)$.

1) Choose an integer $e$, $1 < e < \phi$, such that $gcd(e, \phi) = 1$. 4.Compute the secret exponent $d$, $1 < d < \phi$, such that $ed = 1 \pmod{\phi}$.

5.The public key is $(n, e)$ and the private key is $(n, d)$.

The values of $p$, $q$, and $\phi$ should also be kept secret. $n$ is known as the module is known as the public exponent $e$ and the private exponent $d$ is known as the secret exponent or decryption exponent.

b. Encryption

Sender A does the following:

2) Obtains the recipient B’s public key $(n, e)$.

2. Represents the plaintext message as a positive integer $m$. 3. Computes the ciphertext $c = m^e \pmod{n}$. 4. Sends the ciphertext $c$ to B.

c. Decryption

Recipient B does the following:

3) Uses his private key $(n, d)$ to compute $m = c^d \pmod{n}$. 2. Extracts the plaintext from the integer representative $m$.

B. Circle Fitting Algorithm:

1) Quantise the parameter space for the parameters $a$ and $b$.

2) Zero the accumulator array $M(a,b)$.

3) Compute the gradient magnitude $G(x,y)$ and angle $\theta(x,y)$.

4) For each edge point in $G(x,y)$, increment all points in the accumulator array $M(a,b)$ along the line

$$b = a \tan \theta - x \tan \theta + y.$$  

5) Local maxima in the accumulator array correspond to centres of circles in the image.

VIII. CONCLUSION

Thus the problem of live-tissue verification is done through this project by giving eye as an input. The reliability of any biometric identification depends on ensuring that the signal acquired and compared has actually been recorded from a live body part of the person to be identified and is not a manufactured template. Distance metric such as hamming distance is used for the template matching identification process. Experimental results demonstrate the feasibility of the various systems and it shows that, R-S cryptographic algorithm can obtain a higher security with a low false rejection or false acceptance rate comparing to other techniques.

BIBLIOGRAPHY


[8] Iridian Technologies. Iris Recognition Basics, science behind the technology. 10, June 2012, pp 121-128