Enhancing the Security of Internet Banking using Iris Biometrics

AbhidaShende[1],Apurva Patil[2],PrachiPatole[3]

Students of PimpriChinchwad College Of Engineering,

Department of Computer Engineering,

Prof. Mrs. B Mahalakshmi
PimpriChinchwad College Of Engineering,

Department of Computer Engineering

Abstract— **Biometric recognition systems are nowadays playing important role in authentication field. The physiological features like Fingerprint and hand geometry, Iris, DNA, Palm print, Retina, face, Ear, etc. are used to differentiate between indivisuals. Among these iris is unique organ which can be used for secured authentication and avoids unauthorized access. Iris biometric systems are exposed to direct attacks consisting fake iris presentation to the sensor (a printed or a contact lenses iris image). Also there are other major issues involved while scanning iris, like occlusions caused by eyelids, spectacles, motion blur, presence of contact lenses, poor illumination, off-angle imaging, close-up of iris image, image taken from a longer distance and specular reflections etc. These issues highly affect the iris image quality.**

Internet banking is widely used nowadays. Almost every bank has got its own service of internet banking. Due to this the internet banking applications have become more complex. Collaborating two fields of biometrics and internet banking we can provide a more secure method to perform internet banking operations.

Index Terms— **Daugman algorithm, Segmentation, Normalization, Feature Extraction, Pattern Matching.**

I. Introduction

Online transaction has become a common trend now-a-days and security related to the same is becoming an issue. Authentication using passwords is vulnerable to attacks like hacking; hence by making use of biometric characteristics we can authenticate the person’s identity. Iris is a protected internal organ whose random texture is complex, unique, and very stable throughout life, it can serve as a kind of living passport or password that one need not to be remembered but can always be present. So Iris recognition is one efficient way of securing online transactions. Iris recognition system provides accurate, robust, fast, secure and user-friendly authentication solution. It protects personal identity of users by the acquisition, processing, analysis and comparison of iris patterns from their iris image.

The aim of this paper is to enhance the security of Internet Banking using iris biometrics, as secure authentication cannot be judged only on the basis of username and password as they can be guessed easily. Iris is an internal organ of an eye that is highly protected. It has random texture with high complexity. They are known for their uniqueness and stability throughout life.

The project aims to develop an application that will ask for the username, password as well as an iris image of the user, which the user should provide through his respective device camera. The application will pre-process the iris image and scan through the database for authentication. If the username, password and iris image matches with that in database then the user is authenticated.

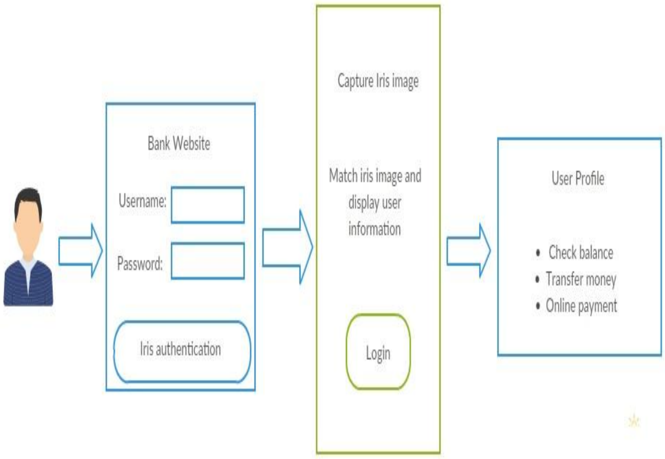


Figure 1. Internet Banking Application

II. Why the Iris?

1. Accurate and Reliable**:** Iris is more accurate than other biometrics in security. The iris pattern is distinctive and is not susceptible to theft.

2. Fast and Stable**:** Iris pattern is unique and is formed by age of 10 months, and remains stable throughout one’s life. Full

enrolment with instruction can take less than 2 minutes. Authentication takes less than 2 seconds.

3. Expandable, Scalable, and Flexible**:** Data templates require only 512 bytes of storage per iris. Large databases also do not compromise on search speed or degrade performance accuracy. It can be very easily inserted into already existing security systems and operates in standalone mode.

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

Table 1 : Biometric comparison List

III. Steps of Iris Recognition

Iris recognition process is basically divided into four important steps,

1. Localization – Calculation of inner and outer boundaries of iris from eye image. For localising iris, segmentation algorithm is used.

2. Normalization **-** Iris of different individuals are different and it is captured in different size. Also for the same person iris image size may vary because of the variation in darkness, brightness and other factors. Iris image is converted from Cartesian coordinate system to Polar system. The process os called as iris wrapping.

3. Feature encoding – Iris structure is very unique and abundant in information. A feature vector is formed from the various representations of the iris images. This feature vector consists of the ordered sequence of features extracted.

4. Matching **-** Hamming Distance techniques is used to find threshold value for classification of feature vectors.

The process of segmentation influences the performance of iris recognition systems highly. Segmentation is used to locate the correct iris boundary in an eye. It removes the occlusion of eyelashes, eyelids, pupil, noises and reflection present in iris region from images. Thus it must be accurate as well as correct. The efficiency of segmentation algorithm depends on the quality of iris image. Segmentation process becomes difficult when noise is present in image. The inaccuracy in segmentation process decrements the recognition rate. Therefore, segmentation algorithm should give high performance.

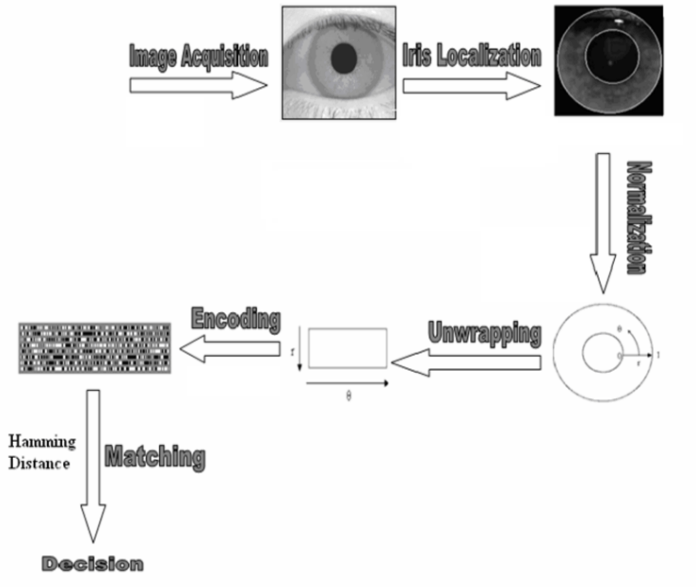


Figure2. Iris Recognition Process

The performance results are based on error rates: False Acceptance Rate (FAR) and False Rejection Rate (FRR); and the overall accuracy. The percentage accuracy based on FAR and FRR of the implemented algorithms is shown in Table 2

Algorithm	FAR/FRR	Accuracy %
Avila	0.03/2.08	97.89
Li Ma	0.02/1.98	98.00
Tisse	1.84/8.79	89.37
Daugman	0.01/0.09	99.90

Table 2 : Performance of Algorithms

Hence Daugman algorithm gives the best performance in comparison to other algorithms.

IV. Daugman's Algorithm

Daugman's algorithm is based on applying an integro-differential operator to find the iris and pupil contour. The equation is as follows:

$$\max(r,x_o,y_o)\left|G_\sigma(r)*\frac{\partial}{\partial r}\oint_{r,x_o,y_o}\frac{I(x,y)}{2\pi r}ds\right| \qquad (1)$$

Equation1 : Daugman's Integro-Differential Equation

Where:

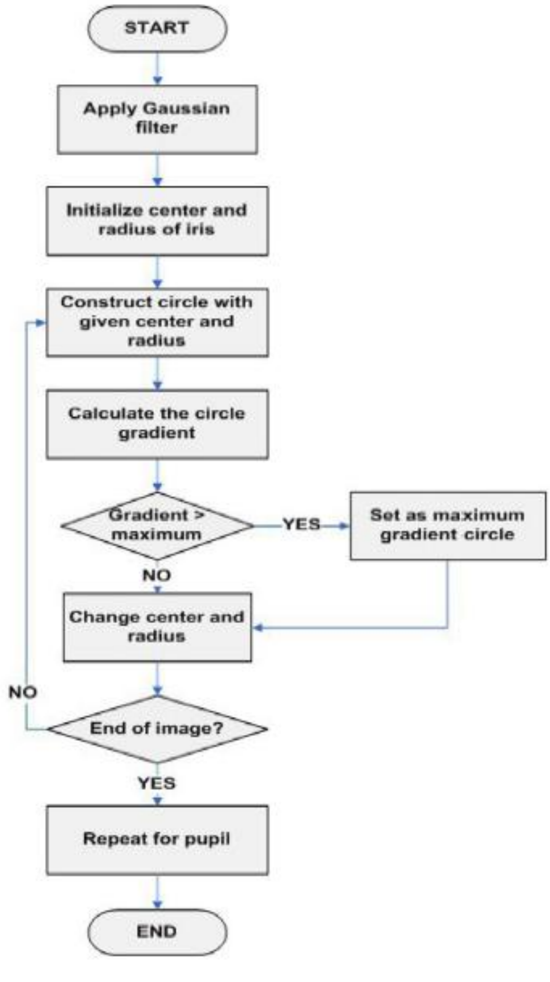
x_0 , y_0, r_0 : the center and radius of coarse circle (for each of pupil and iris).

G (r) σ : Gaussian function.

Δ r : the radius range for searching for.

I(x, y): the original iris image.

G (r) σ is a smoothing function, the smoothed image is then scanned for a circle that has a maximum gradient change, which indicates an edge. This algorithm is implemented in two steps, first is to get the iris boundary and other is to get the pupil boundary. There is common chance of the illumination problem lies inside the pupil, which is a perfect circle with very high intensity level (nearly pure white). Therefore, we face the max gradient circle problem related to illumination. So the pupil radius to be set should be minimized. Another problem is determining the pupil boundary, the maximum change should occur at the edge between the very dark pupil and the iris, which is relatively darker than the bright spots of the illumination. Hence, one should take care when scanning the image, a very bright spot value could deceive the operator and can result in a maximum gradient. This leads to failure in localization of the pupil.


START
Apply Gaussian filter
Initialize center and radius of iris
Construct circle with given center and radius
Calculate the circle gradient
Gradient > maximum
YES
Set as maximum gradient circle
NO
Change center and radius
NO
End of image?
YES
Repeat for pupil
END

Flow Diagram showing Daugman's algorithm.

Once the iris is localized the next step is to normalize it. Normalization transforms the iris region into fixed dimensional image. This image will used for comparison purpose. The Daugman's 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]. It actually converts the Cartesian coordinates to Polar coordinates. The Cartesian coordinates (x,y) are converted to Polar coordinates (r,ϴ).

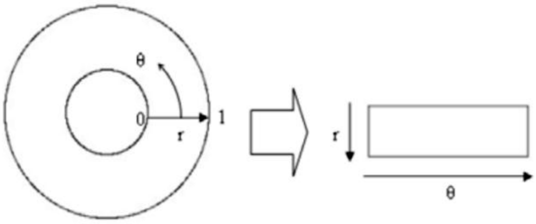


Figure3. Daugman's rubber sheet model

The model of representing the normalized polar coordinates which are obtained from Cartesian coordinates of iris image (x,y) is given by

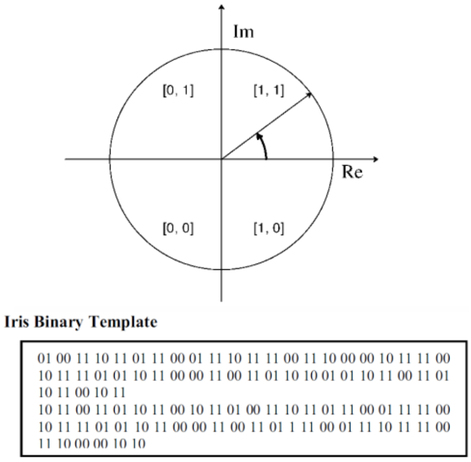
$$
\begin{aligned}
&I(x(r,\theta),y(r,\theta)) \rightarrow I(r,\theta)\\
&\text{with}\\
&x(r,\theta)=(1-r)x_p(\theta)+rx_l(\theta)\\
&y(r,\theta)=(1-r)y_p(\theta)+ry_l(\theta)
\end{aligned} \tag{2}
$$

Equation2. Converting from cartesian to polar coordinates

Where I(x, y) is the iris image, (x, y) are the Cartesian coordinates, (r, ϴ) are the corresponding normalized polar coordinates, and xp , yp and xl , yl and are the coordinates of the pupil and iris boundaries along the ϴ direction.

After successful conversion to polar coordinates feature encoding process is done. The implementation of feature encoding is done using 1D Log Gabor wavelets which convolutes the normalized iris pattern. The normalized polar coordinates are in 2D pattern. This 2D pattern are broken up into number of 1D signals, and then these 1D signals are convolved with 1D Gabor wavelets. The rows of the 2D normalized pattern are taken as the 1D signal; each row corresponds to a circular ring on the iris region. The output of filtering should be free from the influence of noise. For this the intensity values at known noise areas are set to the average intensity of surrounding pixels. This will prevent the output from the influence of noise. The output of filtering is then phase quantized to four levels with each filter producing two bits of data for each phase. The output of phase quantization is

chosen to be a grey code, so that when going from one quadrant to another, only 1 bit changes.



```
01 00 11 10 11 01 11 00 01 11 10 11 11 00 11 10 00 00 10 11 11 00
10 11 11 01 01 10 11 00 00 11 00 11 01 10 10 01 01 10 11 00 11 01
10 11 00 10 11
10 11 00 11 01 10 11 00 10 11 01 00 11 10 11 01 11 00 01 11 11 00
10 11 11 01 01 10 11 00 00 11 00 11 01 1 11 00 01 11 10 11 11 00
11 10 00 00 10 10
```

Figure4. Phase quantization and Iris binary template

The final step is of pattern matching. The pattern matching is done using the hamming distance formula. Thus, when comparing two iris images, their corresponding binary feature vectors are passed to a function responsible of calculating the Hamming distance between the two. The maximum Hamming distance that exists between two irises belonging to the same person is 0.32.

$$HD=\frac{1}{N}\sum_{i=1}^{N} X_I \otimes Y_I$$

For differentiating between two iris images of same person can be determined by following parameters.

If HD <= 0.32 decide that it is same person

If HD > 0.32 decides that it is different person

V. Conclusion

Banks must protect sensitive data, avoid a security breach and prevent unauthorized access. Even a single instance of unauthorized access to secure data can cause significant loss of business and reputation. Documents classified as ‘top secret’, ‘secret’ and ‘confidential’ demand high level security scanning and clearance. Banks must ensure that sensitive data is accessible only to authorized persons.

In traditional security systems, access to documents can be secured with, limited network access and at the document level via passwords for documents and encryption of data. Password protection and encryption techniques do not guarantee data security. In addition, it does not ensure that the person is authorized to access information.

Biometric technology offers enhanced security while being convenient to use. It guarantees that information is accessed only by authorized persons. The security system offers a reliable method for authenticating users. It is robust solution to meet the stringent requirements of restricted access for top secret information. Significantly, it reduces frauds and minimizes password administrator costs. When biometric technology goes mainstream, banks can use biometrics in every transaction requiring the authentication of identity. Iris recognition is one of the most accurate security systems to identify a unique user,promptly and conveniently. Iris biometrics will emerge as an effective strategy to protect information, safeguard privacy and prevent fraud. Iris biometric system can be deployed in all areas to minimize unauthorized access and consequently business risks.

REFERENCES

[1] Safe as bank: Iris Scan Biometrics for Secure Data Access, Secure confidential data for banks with cutting edge safety net- Mohan Kumar, Rakhi Agrawal, Dhruv Chauhan

[2] Cătălin LUPU * , Vasile-Gheorghiță GĂITAN * , Valeriu LUPU **,”Security enhancement of internet banking applications by using multimodal biometrics”,IEEE 2015

[3] Ana F. Sequeira, Juliano Murari and Jaime S. Cardoso,”Iris liveness detection methods in the mobile biometrics scenario”,IJCNN 2014

[4] Kamal Hajari, Kishor Bhoyar,”A Review of Issues and Challenges in Designing Iris Recognition Systems for Noisy Imaging Environment”,ICPC 2015

[5] Oleg V. Komogortsev, Alexey Karpov and Corey D. Holland, “Attack of Mechanical Replicas: Liveness Detection With Eye Movements”,IEEE 2015

[6] John Daugman,”How Iris Recognition Works”,IEEE 2004

[7] VanajasRoselin.E.Chirchi,Dr.L.M.Waghmare,E.R.Chirchi, ”Iris Biometric Recognition for Person Identification in Security Systems”,International Journal of Computer Applications (0975 – 8887) Volume 24– No.9, June 2011

[8] Dr. Mohamed A. Hebaishy, Poster: Optimized Daugman’s Algorithm for Iris Localization, NARSS