International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.119-124
http://dx.doi.org/10.14257/ijsia.2016.10.1.12

A Novel Iris Authentication Using ECDSA

Srinivasan Nagaraj[1] and Dr. G. S. V. P. Raju[2]

[1]*Asst. Professor, Dept. of CSE, GMRIT, GMR Nagar, RAJAM-532127, AP*
[2]*Professor, Dept. Of CS&ST, Andhra University, Vizag, AP.*
[1]*sri.mtech04@gmail.com*, [2]*gsvpraju2011@yahoo.com*

Abstract

The Cryptographic systems need a secret key or a random number must be necessarily tied to an individual through a unique identifier. This unique identifier definitely might exist a globally user id or biometric data [2]. In this paper we combined biometric with cryptography in which the intensity of each pixel of iris is changed into the elliptic curve and encrypted using ECC. The receiver end original image is recovered by using their decryption and authentication [8] is performed using ECDSA. The proposed technique is implemented for BMP images. We can enroll and add the number of images for authentication .It has been also performed more security if the image is recovered without being any side channel attack.

Keywords: *ECC, Iris Code, Encryption, Decryption*

1. Introduction

A Biometric is called as a distinctive, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Five of the most used physical biometric patterns analyzed for security purpose are fingerprint, hand, eye, face and voice. Biometric authentication of a person is highly challenging and complex problem. A significant research effort has gone into this area and a number of research works were published, but still there is an immense shortage of accurate and robust methods and techniques [4].

The Iris as a Biometrics:

Biometrics is mostly known as measurable physiological or behavioral features that can be used to verify the identity of an individual and the iris is an overt body that is existing for remote assessment with the aid of a machine vision system to do automated iris recognition. Iris recognition combines the fields of computer vision(cv) and pattern recognition(pr) and optics and statistical inference others .

These can be used as performance metrics for Iris Recognition Systems (IRS):

a. FAR or FMR (False accept rate or false match rate): The probability of the system wrongly matches the input pattern to a non-matching template data in the database. It is also used to compute the percent of invalid inputs wrongly accepted.

b. FRR or FNMR (False reject rate or false non-match rate): The probability of the system fails to find a match between the input pattern and a matching template. It computes the required percent of valid inputs from the incorrectly rejected inputs.

c. EER or CER (Equal error rate or crossover error rate): Both accept and reject error rate must be identical. The EER or CER value can be easily gained from the ROC curve. The EER is a method to match the accuracy of devices with various ROC curves values. In common, the device through the lowest EER is the most accurate.

ISSN: 1738-9976 IJSIA

d. Failure to enroll rate (FTE or FER): The rate at which attempts to create a template from an input is ineffective. It is frequently produced by short quality of inputs.

IRIS DATABASE'S USED: The accuracy of the iris recognition system (IRS) depends on the image quality of the iris images. Noisy and low quality images degrade the performance of the system. Some Iris image database available are: UBIRIS, CASIA, LEA, MMU and ICE database.

Now a day's so many advanced technologies have been established and however till today, it is very difficult to provide complete information security. So Cryptography acting as vital role for encrypting and decrypting the information and keep it top secret.

Cryptography is the division of information security which covers the learning of techniques and rules which secure data. It is widely used in intelligence and other areas like Wars as a tool for maintenance communications secret. But it is significant to remember that cryptography is necessary for secure communications, it is not sufficient by itself. There are specific security requirements which including:

• ***Authentication:*** *The method of verifying the identity of the user.*
• ***Privacy:*** *Ensure to facilitate no one can read the message except the correct receiver.*
• ***Integrity:*** *Received message does not modify from the original during transit is showed by this method.*
• ***Non-repudiation:*** *It is the method; the sender side has only sent this message.*

Elliptic Curve Cryptography (ECC):

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz (Koblitz 1987)and Victor Miller (Miller 1986)independently proposed the public key cryptosystems using EC cryptography and many scientists have studied the strength of ECC and improved techniques for its implementation. The Elliptic curve cryptosystem provides a smaller and faster public key cryptosystem [6].

In this work for the purpose of the encryption and decryption using elliptic curves we consider the equation of the form

$$Y2 = x3+ax+b$$

Elliptic Curve Domain Parameters are D = (q, FR, a, b, G, n)
q: prime power, that is q = p or q = 2m, where p is a prime
FR: Field representation: It represents field elements $\in$ Fq
a, b: field elements, they specify the equation of the elliptic curve E over Fq,
y2 = x3 + ax + b
G: A base point represented by G= (xg, yg) on E (Fq)
n: Generated Prime number.

2. Proposed Method of Implementation

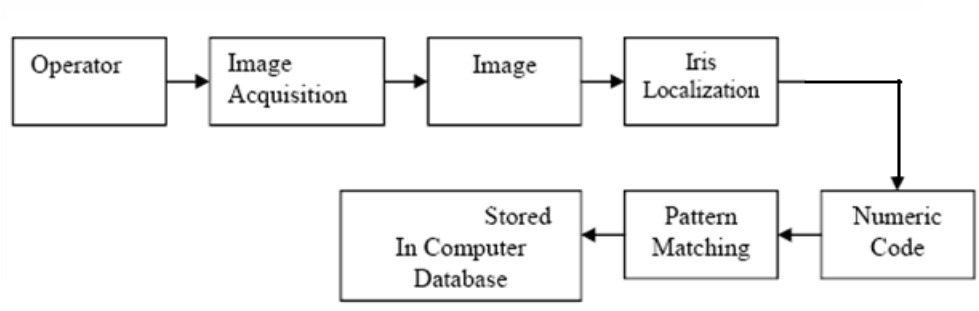

Figure 1. Block Diagram of Proposed Method

Iris Localization:

a. Pupil Detection
- Threshold
- Edge Detection
- Circular Hough transform

b. Iris Detection

Thresholding: The pupil area is acquired after thresholding the input image. The pupil is the darkest portion of the eye.
Edge Detection: Obtained using canny edge detection method.

Circular Hough Transform: It is used to convert a set of edge points in the image space into a set of accumulated votes in a parameters space. The array elements contain the highest number of votes present in the shape for every edge pixel find the center point.

$XC=XP-r \times \cos\theta$
$YC=YP-r \times \sin\theta$

Where Xp , Yp are location of edge points.

$r \in [r\ min\ r\ max]$.The center point(ct) is calculated.

The accumulating array incremented by 1 for calculating the center point pt.

New Point [XC, YC] = New Point[XC, YC]+1

The pt of maximum value is accumulated [New Points] denoted as circular centre with r radius.

Iris Detection: Concentric circles of various radii are drawn from pupil center. The intensities which lie over the perimeter of the circle are added up. Among the added circles the one with max modification in intensity with respective previous drawn circle is the outer iris outer boundary.

Iris Normalization: The annular ring transformed to rectangular ring. Localization of iris from image delineates the annual portion from remaining part of the image. The co-ordinate system is closed by unwrapping the iris from Cartesian co-ordinate their polar equivalent.

$$I(x(\rho,\theta), y(\rho,\theta)) \rightarrow I(\rho,\theta)$$

with

$$x_p(\rho,\theta) = x_{p0}(\theta) + r_p * \cos(\theta)$$
$$y_p(\rho,\theta) = y_{p0}(\theta) + r_p * \sin(\theta)$$
$$x_i(\rho,\theta) = x_{i0}(\theta) + r_i * \cos(\theta)$$
$$y_i(\rho,\theta) = x_{i0}(\theta) + r_i * \sin(\theta)$$

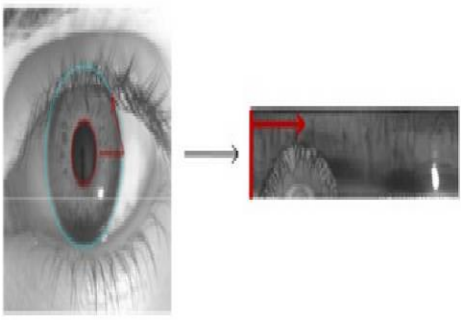

Figure 2. Iris Co-Ordinates

3. Implementation

Proposed Algorithm: This algorithm first converts an image into binary and then map.

1. A square grid of required size is constructed by taking the binary data from source file. We are taking into account a grid of 64 X 64 and stuffing with 0 if needed.
2. As the image is now seen as a grid of 64 X 64, every pixel of this image is first mapped on the elliptic curve by applying the function gen-point (a, b, p).
3. Next the pixels are encrypted using ECC.

Generation of nonnegative integer points from (0,0) to (p,p) in Ep : Genpoint (a,b,p)

{ For x=0;
While(x<=p)
{ Y 2 =(x3 +ax+b) mod p If y2 is a perfect square in GF(p)
Output(x,sqrt(y)), (x-sqrt(y))
x++; } }

Encryption steps for A:

PmI=aPm // a: Intensity value from the image grid // Pm: random point on EC

PB=nB * G
// G is the base point of EC
// nB is the private key
CipherText={kG,PmI+k*PB}

Decryption steps for B:

Let us say kG is the first point and PmI + k*PB be the second point .

nBkG = nB * first point;
Calculate PmI = PmI + kPB- nBkG;
An attacker must compute k given G and kG, which is assumed hard.
Calculating the Pm value from PmI by using discrete logarithm

3.1. Implementation of Proposed Algorithm:

For mapping the image of an Elliptic Curve (EC), The following steps are executed:

1. Assume the following elliptic curve Y 2 mod p =(x3 +ax+b) mod p
Let as assume a=2 , b=3, p=263.Here a ,b are trace values and then the following points are plotted on the elliptic curve(EC).

Table 1. Points Generation

X	Y
60	215
61	243
102	173
144	228
175	83

3.2. Iris Authentication using Iris Template:

ECDSA Key Generation - The user A follows these steps:

1. Select a random integer b ϵ [2, s-2]

2. Compute M= b*a
3. The public and private keys are (G, a, s, M) and b.

ECDSA Signature Generation -The user A signs the message D using these steps:

1. Select a random integer b ϵ [2, s-2]
2. Compute M = b*a = (x1, y1) and r = x1 mod s
If x1 ϵ GF (2D), x1 is represented as a binary number.
3. If r = 0 then move to step 1.
4. Compute ks-1 mod s
5. Compute t = ks - 1 (H (D) + br) mod s.
Here H is the secure hash algorithm SHA
6. If t = 0 go to step 1.
7. The Signature for the message D is (r, t)

ECDSA Signature Verification - The User B Verifies A's Signature (r, t) on the message D by applying the following steps:

1. Compute c = t-1 mod s and H (D)
2. Compute u1 = H (D) c mod s and u2 = rc mod s
3. Compute u1 * a + u2 * M = (x0, y0) and v = x0 mod s
4. Accept signature if v = r.

4. Result

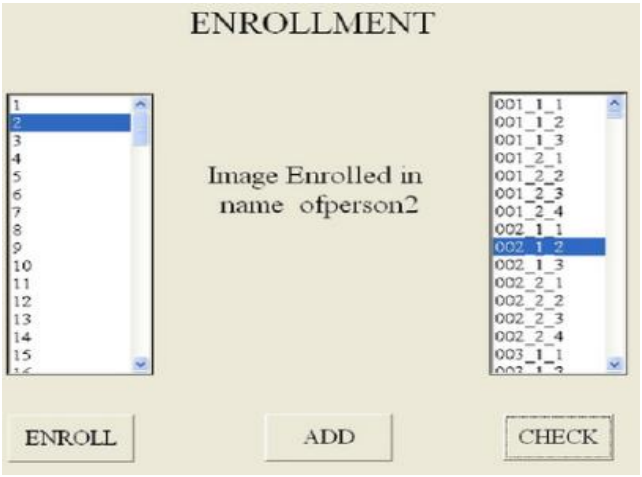

Figure 3. Enrollment Screen

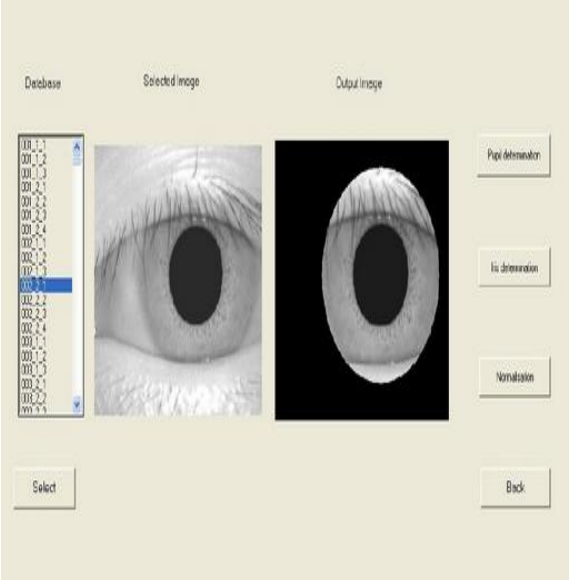

Figure 4. Iris Recognition

5. Conclusion

The attractiveness of ECC, with respective to RSA, it is more security for a smaller key size, reducing processing overhead. The advantage which includes higher speeds, lower power consumption, storage efficiencies, and smaller certificates. Iris technology grows less expensive, always been an exceptionally accurate one and it could very likely unseat a large portion of the biometric industry. The proposed technique is implemented for BMP images. In this work, we implemented, the intensity of each pixel is transformed into the elliptic curve and encrypted using ECC. At the receiver size original image is recovered by using their decryption and authentication is performed using ECDSA [8]. It has been observed that the original image is recovered from the encrypted image and We can enroll and add the number of images for authentication .Future work includes Attacks on the biometric sensor/Acquisition device Examples of such attacks are spoofing biometric live features by using artificial presented to and accepted by the sensor and Attacking on the biometric reference data. This only leads to loss of privacy for the respective person or to further attacks, if the intercepted data is subsequently actively re-introduced to the subsystem.

References

[1] J. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 15, no. 11, **(1993)**, pp. 1148 – 1161.
[2] J. Daugman, United States Patent No. 5,291,560 (issued on March 1994)." Biometric Personal Identification System Based on Iris Analysis", Washington DC: U.S. Government Printing Office**, (1994)**.
[3] J. Daugman, "The Importance of Being Random: Statistical Principles of Iris Recognition", Pattern Recognition, vol. 36, no. 2, pp 279-291.
[4] R. P. Wildes, "Iris Recognition: An Emerging Biometric Technology", Proc. of the IEEE, vol. 85, no. 9, **(1997)**, pp. 1348-1363.
[5] Y. Zhu, T. Tan, and Y. Wang, "Biometric Personal Identification Based on Iris Patterns", ACTA AUTOMATICA SINICA, no. 1, **(2002)**.
[6] R. P. Wildes, "Iris Recognition: An Emerging Biometric Technology", Proc. of the IEEE, vol. 85, no. 9, **(1997)**, pp. 1348-1363.
[7] Y. Zhu, T. Tan and Y. Wang, "Biometric Personal Identification Based on Iris Patterns," ACTA AUTOMATICA SINICA, no. 1, **(2002)**.
[8] Anderson, Ross and H. Feng. "Combining Crypto with Biometrics Effectively". IEEE, 2005.
[9] R. Arian. " An efficient Iris Authentication". IEEE-**(2009)**.

