Protocol for Secure Iris Authentication Framework using Cryptography

Mrs.Swati A. Jadhav

Abstract- Data encryption is the key role in current and future technologies. Many public key cryptography algorithms were presented depending on a specific mathematical problem. It is desired to communicate data with high security over insecure network. Due to sensor technology biometrics has lead to rising concerns about the network security, privacy, trust issues and accuracy. Hence, securing biometric template in public network is great challenge. Because once it is compromised or stolen it cannot be revoked. In order to provide remote biometric authentication these systems incorporated with cryptography and primarily focused on template security, revocability, privacy, accuracy. The system is secure in the sense that the biometric are going to use is encrypted using Elliptic curve cryptography (ECC). Proposed system is based on client server architecture in that server is secure. Experimental result shows encryption time using ECC 256-bit key size for iris authentication.

Index Terms: *ECC, Template Security, Privacy, Segmentation, Normalization,SVM.*

1. INTRODUCTION

Nowadays large number of people makes high demand for online e-learning, e-government, gaming, social networks, money transfer, knowledge sharing, bank account access etc. which is essential part for our future. To maintain security of these systems is very essential part while sending large amount of confidential data over public networks. Among the available different authentication methods like token or password of an individual, biometric authentication is often presented as a promising solution for computer security. Since from 1985, many researchers put focus on development in cryptography area and biometric security. The capabilities of cryptographic algorithm such as of AES, DES, RSA,DSA,RC4 and Diffie-Hellman are not enough due to the requirement of large number of bits. The cryptosystem based on Elliptic Curve Cryptography(ECC) is becoming the recent trends of current public key cryptography [5].

Swati A.Jadhav is currently pursuing Masters in Computer Engineering from MCERC ,Nasik, University of Pune,India. E_mail:swatijadhav.jadhav@gmail.com.

In biometric authentication system attacks on biometric template compromises the security of biometric. So various cryptographic algorithms have been proposed to achieve the security services such as privacy, secure Authentication, Confidentiality, Non-Repudiation. At present, various types of cryptographic algorithms provide high security over public network. To improve the strength of these security algorithms, a new security blind authentication protocol for remote authentication is designed using combination of iris features.

Public acceptance of biometric systems has a critical impact on their success due to their potential misuse of biometric data. Unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Therefore it is illegally acquired by an attacker, not only the security of the system is at risk but the privacy and the security of the user may be compromised forever too. So granting template security is one of the most important issues in practical. The need of protecting user

sensitive information locally and performing secure user authentication remotely become more increasing.

1.1Bio-Cryptography

Bio-Cryptography is emerging as a powerful solution to provide template security which can combine the advantages of conventional cryptography and biometric security. Cryptography is the science of converting data in non understandable form for the unintended viewers, for securely transmitting messages. A cryptosystem is a system of algorithms for encrypting and decrypting the messages for this purpose [2]. The conventional security system uses password or security key for authentication; but those password and security key can be easily stolen by the theft. One solution to overcome these issues, biometrics encrypted using ECC to secure

Algorithm security lifetimes	ECC key Size
Through 2010 (min. of 80 bits)	Min.: f=160
Through 2030 (min. of 112 bits)	Min.: f=224
Beyond 2030 (min. of 128 bits)	Min.: f=256

Table 1: NIST recommended key length[15]

the system. From ECC key is generated which is more secure than other techniques.

However, cryptography has its own drawbacks like sometimes an attacker may obtain the cryptographic key via an illegal ways and then act as an authentic user. A lot of work done by researcher on various encryption algorithm [4] (AES, DES, 3DES, Diffie-Hellman, RSA,RC4, DES, Blowfish) to protect confidential data from unauthorized access. Currently a few work done by researcher on elliptic curve cryptography to provide biometric security and privacy. The use of Elliptic Curves (EC) in public key cryptography was independently proposed by Koblitz and Miller in 1985 [8] and since then, an enormous amount of work has been done on ECC. Since from 2000, researcher perform work on ECC combine with biometric features (iris,fingerprint,face) to provide network security and secure authentication. However some author observe ECC based security offers a similar level of security that can be achieved with shorter keys than existing methods which are based on the difficulties of solving discrete logarithms over integers or integer factorizations. [10]

2. ECC BACKGROUND

At the time of its implementation, ECC were considered unpractical by researcher due to its strong mathematics. ECC able to provide the following security services:

- Confidentiality
- Authentication
- Non-repudiation
- Network security

The most important difference between ECC and other conventional cryptosystems is that for a well-chosen elliptic curve, the best method currently known for solving the ECDLP is fully exponential. It also means that ECC keys have much fewer bits than Integer Factorization Problem (IFP) and Discrete Logarithms Problem (DLP) based applications. ECC keys take much more effort to break compared to RSA and DSA keys[18]. Due to this, many people believe that ECDLP is basically harder than the other two problems. ECC proposes equivalent security with smaller key sizes, compared to RSA, which results in faster computations, reduced power consumption, as well as savings in memory space and bandwidth.

3. RELATED WORK

In this section various existing biometric template protection scheme are reviewed and compares their

advantages and limitation related with template security, privacy, revocability and matching of biometric. The aim of these proposed system is able to design a secure authentication framework for biometric with cryptography. Elliptic Curves (EC) in public key cryptography was independently proposed by Koblitz and Miller in 1985 [8] and since then, an enormous amount of work has been done on elliptic curve cryptography.

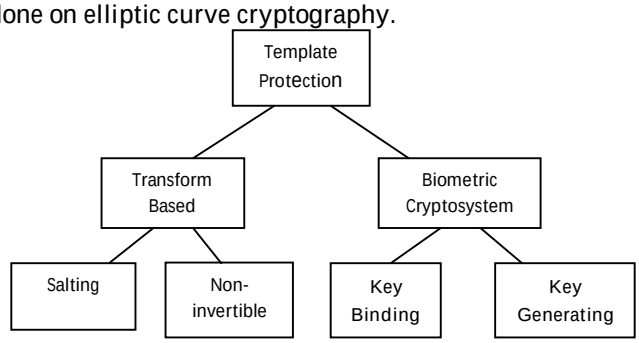


Fig 1: Template Protection Scheme by Jain et.al

3.1 Salting

Kong et al. [9] do a detailed analysis of the current bio-hashing based on biometric approaches. They conclude that the zero equal error rate (EER) reported by many papers is obtained in carefully, set experimental conditions and unrealistic under assumptions from a practical view point.

3.2 Noninvertible Transform

In this approach a trait specific noninvertible function on the biometric template to secure it. Robust hashing and cancelable biometric [13] fall in this category to replace a leaked template, while reducing the amount of information revealed through the leak. Privacy is not maintained in this approach.

Boult et. al. [9] extended the above approach to stronger encryption, and proposed an encrypted minutia representation and matching scheme of fingerprints. In which a Bio-token consists of the encrypted integer part and the increment information in plain. Its drawback is making compromised between security and accuracy.

3.3 Key Binding

Juels and Sudan [10] proposed a cryptographic construction called fuzzy vault. The general idea is to hide the cryptographic key in a scrambled list which is composed of genuine fingerprint features and fabricated chaff features. It lacks in diversity and revocability.

C. Soutar et al. [11] proposed a key-binding algorithm using correlation-based fingerprint matching method. In the algorithm, a cryptographic key extracts only limited features and the corresponding user's fingerprint image are bound at the enrollment stage.

3.4 Key Generaing

Fuzzy extractor is a type of key generating approach designed by researcher Y.Dodis [12] to convert noisy data. The Secure Sketch generates public help data which are related to the input but does not reveal biometric information. Mannish Upmanyu et.al.[16] proposed blind authentication protocol using biometric features and public key cryptography (RSA).

Recently work done on template security mostly focus on key generation and key binding approach. Although there are many encryption algorithms available among them RSA public key cryptography is widely used for authentication. Because it offers large key size and complex calculation for large prime thus gives better security. In 1986 Victor Miller and N. Koblitz introduces "Elliptic Curve Cryptography" technique as an alternative to established public-key systems such as DSA and RSA. The ECC has a smaller key size which offers the same security strength as the RSA. So ECC is preferable for constraint specified devices where small memory, low

computational power and less time are expected such as smart card, portable devices, RFID etc. Since mobile devices have limited CPU, power and network connectivity ECC is especially useful.[13]

Elliptic Curve Cryptography (ECC) is a public-key cryptography system [10], in which a key pair is selected so that the problem of deriving the private key from the corresponding public key is equivalent to solve a computational problem that is believed to be intractable.

In general, the keys are protected by user passwords, which will compromise the integrity of sensitive data due to poor selection of the password by the user. Combining biometric with cryptography could be the solution by generating deterministic bit sequences for generating a reliable key. But it is essential to generate the key with minimum possibility of uncertainty due to poor image quality [17].

4. EXISTING SYSTEM

In existing system biometric is combined with public key cryptography such as RSA. Due to it's large key size RSA require large time for encryption thus increases computation time and key generation time. Also number of features is fixed for biometric key generation. Only black and white images are tested for verification of protocol

5. PROPOSED SYSTEM

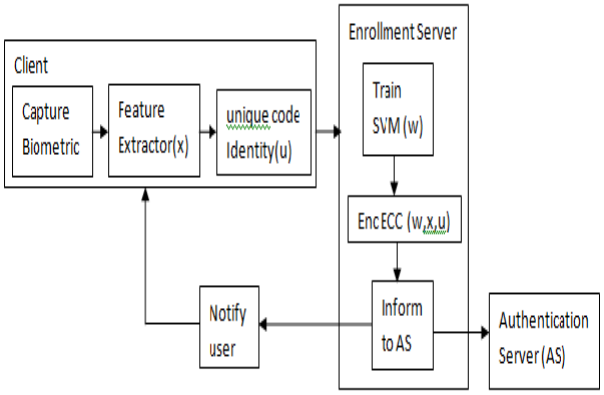


Fig 2: Enrollment

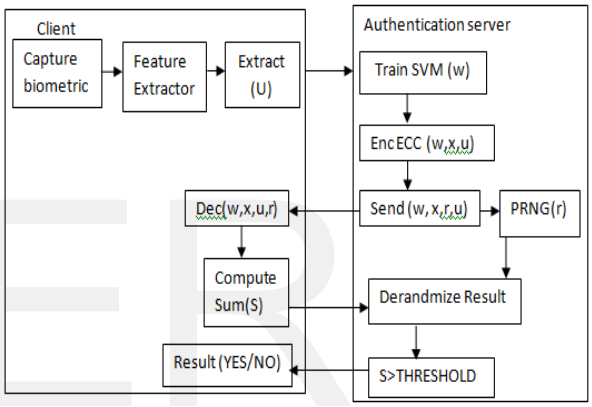


Fig 3: Authentication

5.1 Security Strength For Proposed System

For a bio-cryptosystem, not only the cryptographic information, e.g. the key, but also the biometric data should be protected against attacks. Proposed method is secure against client side attacks,brute force attack due to large key size etc.

Algorithm 1: Authentication
1. Load biometric image.
2. Feature extracted.
3. Train SVM for matching
4. Server send encrypted parameter to client for decryption.
5. Client compute sum of product(SOP)
6. Send SOP to server and generate random number
7. Server derandomizes result to obtain final result and compared with threshold for authentication.

- Enrollment

During the enrollment, the client sends samples of her biometric to the enrollment server, who trains a classifier for the user. The trained parameters are encrypted and sent to the authentication server, and notify to the client.

Algorithm 2: Enrollment
1. Load biometric image.
2. Feature extracted.
3. Apply ECC encryption on template
4. Train SVM
5. Encrypt SVM parameter
6. Inform to server about registration
7. Server sent message back to client

- CLIENT MODULE:

1.Authentication module:

This module is to register the new users and previously registered users can enter into system.

2. Blind encryption:

Blind in the sense that it reveals only the identity, and no additional information about the user or the biometric data. In this module biometric data with the message to be encrypted using ECC.

3. Encrypted data forward:

Data forwarding is a process of transferring data in a secure network. Server is only able to open the file because it has the original key and biometric data, after his verification the file could be decrypted.

- SERVER MODULE:

1. Biometric verification:

In this process biometric data compare with whole database data using the matching technique in this matching depend on the each pixel of image.

2.Blind decryption:

In this module client side encrypted message is to be decrypted using key.

- SVM Classifier:

SVM is unsupervised learning machine in pattern and image classification. It is designed to separate of a set of training images two different classes, (x1, y1), (x2, y2), ..., (x_n, y_n) where xi in Rd, d-dimensional feature space, and yi in {-1,+1}, the class label, with i=1……n. SVM builds the optimal separating hyper planes based on a kernel function (K). All images, of which feature vector lies on one side of the hyper plane, are belong to class -1 and the others are belong to class +1. The decision boundaries are directly derived from the training data set by learning method.

The SVM maps the inputs into a high-dimensional feature space through a selected kernel function. Then, it constructs an optimal separating hyper-plane in the feature space. The dimensionality of the feature space is determined by the number of support vectors extracted from the training input. It estimates the optimal boundary in the feature space by combining a maximal margin strategy with a kernel method; this process is called a kernel machine.

- SVM Kernel Function:

In SVM dot products may be computed easily in terms of the variables by defining them in terms of a kernel function $K(x,y)$. If $K(x,y)$ becomes small as y grows further away from x, each term in the sum measures the degree of closeness of the test point x to the corresponding data base point x_i. In this way, the sum of kernels above can be used to measure the relative nearness of each test point to the data points originating in one or the other of the sets to be discriminated.

$$K(\mathbf{X}_i,\mathbf{X}_j)=\begin{cases}\mathbf{X}_i\cdot\mathbf{X}_j & \text{Linear}\\ (\gamma\mathbf{X}_i\cdot\mathbf{X}_j+C)^d & \text{Polynomial}\\ \exp(-\gamma|\mathbf{X}_i-\mathbf{X}_j|^2) & \text{RBF}\\ \tanh(\gamma\mathbf{X}_i\cdot\mathbf{X}_j+C) & \text{Sigmoid}\end{cases} \quad \text{.....(1)}$$

Where , $K(\mathbf{X}_i,\mathbf{X}_j)=\phi(\mathbf{X}_i)\bullet\phi(\mathbf{X}_j)$ that is, the kernel function, represents a dot product of input data points

mapped into the higher dimensional feature space by transformation ϕ.

6 IRIS FEATURE EXTRACTION PROCESS

1) Graying

In this colored image is converted in gray-pattern. Method of converting an image in gray color is by selecting two appropriate numbers that are indicated to two upper and lower thresholds (L,U).

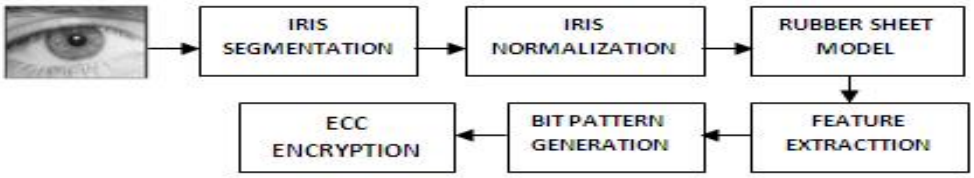


Fig 4: IRIS Key Generation Process

2) Segmentation

The success of segmentation depends on the imaging quality of eye images. Persons with darkly pigmented irises will present very low contrast between the pupil and iris region if imaged under natural light, making segmentation more difficult. The segmentation stage is critical to the success of iris recognition.

1: EDGE DETECTION

For edge detection here sobel operator in which gradient is calculated. The gradient is simply the derivative of the local image values. An edge in the original image would correspond to a higher value in the gradient image. Using a gradient image hough transform decreases computation time significantly since only points that correspond to actual edges are used in the computation.

2: THRESHOLDING

The edge and the image we have a mixture of black, gray and white values. In order to maintain the feasibility we will consider one threshold value. All the values above that threshold will be considered white and all those below as black. Thus a pure black and white image is obtained.

3: CIRCULAR HOUGH TRANSFORM

The transform is computed by taking the gradient of the original image and accumulating each non-zero point transformed image correspond to the centers of circular features of the given size in the original image. Once a peak is detected and a circle 'found' at a particular point, nearby points are excluded as possible circle centers to avoid detecting the same circular feature repeatedly.

3) Normalization

Normalization is used to standardize the intensity values in an image by adjusting the range of grey level values so that it lies within a desired range of values which is fixed. The normalization process produces iris region, which have the same constant dimensions,

Daugman's rubber sheet model used to find fixed iris radius and angle [10]. Moreover this rectangular representation of the iris breaks the no

DB NAME	160-BIT (ms)	256-BIT (ms)
MMU IRIS	406	547
COLOR IRIS	437	609
CASIA IRIS	375	468
UB IRIS	328	953
REALIMAGE	407	516

Table 1: Encryption time using 160 and 256 bit

eccentricity of the iris and the pupil. The θ (θ Є [0; 2π]) parameter and dimensionless radious ϱ (ϱ Є [0; 1]) parameter describe the polar coordinate system. Thus the following equations implement:

$$\begin{cases} x_p(\theta) = x_{p0}(\theta) + r_p * \cos(\theta) \\ y_p(\theta) = y_{p0}(\theta) + r_p * \sin(\theta) \end{cases}$$

$$\begin{cases} x_i(\theta) = x_{i0}(\theta) + r_i * \cos(\theta) \\ y_i(\theta) = y_{i0}(\theta) + r_i * \sin(\theta) \end{cases}$$

……..(3)

Where rp and ri are respectively the radious of the pupil and the iris, while ($x_{\varrho}(\theta)$, $y_{\varrho}(\theta)$) and ($x_i(\theta)$,$y_i(\theta)$) are the co-ordinates of the pupillary and limbic boundaries in the direction h.[21]

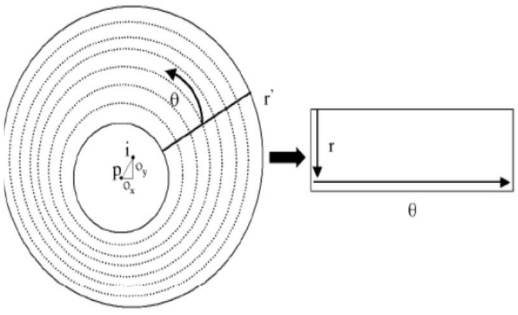
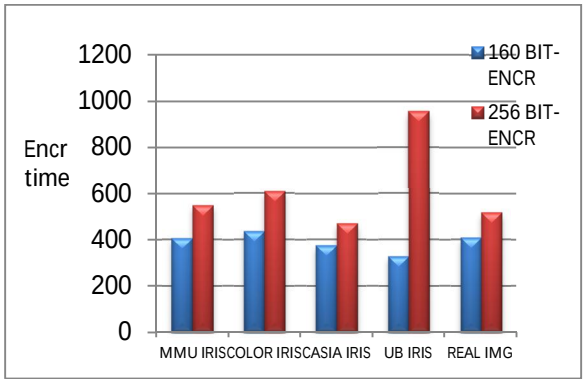


Figure 5: Normalization of Iris

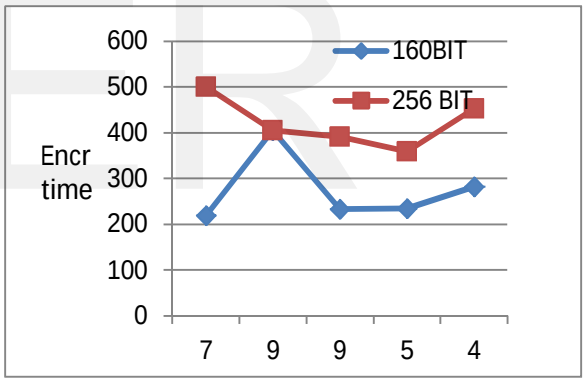
4) Bit Pattern Generation

Since an individual iris region contains features with high degrees of freedom, each iris region will produce a bit-pattern which is independent to that produced by another iris, on the other hand, two iris codes produced from the same iris will be highly correlated.

7 Result



Graph1:Encryption time for various datasets



Graph 2: Key generation time for iris using 160-256 bit

DB NAME	160-BIT (ms)	256-BIT (ms)	No.of feature
MMU IRIS	219	500	7
COLOR IRIS	406	406	9
CASIA IRIS	234	391	9
UB IRIS	235	359	5
REALIMAGE	282	553	4

Table 2:Key generation time and iris feature

7.CONCLUSION

In this system very strong encryption schemes have been used in order to provide more security and the accuracy can be achieved by means of matching algorithms. The system won't reveal about biometric details of the person to the database in the same way client does not know what is happening in the server. The real identity of the person is hence not revealed to the server, making the protocol, completely blind.ECC is strongest concept having higher security level than RSA and it is easy to use. Result shows encryption time using ECC 160 and 256 bit key length. Also it is expected that, ECC offers a better performance in public key cryptosystem (PKC). Hence the result processing becomes faster and there is quite difficult for hackers and crackers to break key or capture biometric template because it is encrypted.

In future ECC used in

- Wireless mobile authentication
- Multiple server authentication
- WSN or RFID
- Dynamic warping for variable length feature
- Biomedical images for security

REFERENCES

[1] A. K. Jain et.al, "Biometric Template security", EURASIP J. Adv. Signal Process. 2008.

[2] A. Teoh, D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, Nov. 2004.

[3] Kai Xi et.al "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment",Security and communication networks, Issue paper,2010.

[4] R. L Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", MIT Laboratory for Computer Science and Department of Mathematics, ACM 0001-0782178/0200-0120.

[5] Arun kumar et.al., "A Comparative Study of Public Key Cryptosystem based on ECC and RSA", IJCSE, ISSN : 0975-3397, Vol. 3 No. 5 May 2011.

[6] Yasser Salem Mohamed Ali, "Implementation of Elliptic Curve Cryptography using biometric features to enhance security services", Master of Comp.Science, Thesis, pp.17-38,July 2009.

[7] A.L.Jeeva et.al "Comparative analysis of performance efficiency and security measures of some encryption algorithms",IJERA,Vol. 2, Issue 3, pp.3033-3037 ,May-Jun 2012.

[8] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, pp. 203-209,

[9] A. Kong, K. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants", Pattern Recognition., vol. 39, no. 7, pp.1359–1368, July 2006.

[10]A. Juels and M. Sudan, "A fuzzy vault scheme," Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237–257, 2006.

[11]Kevin W. Bowyer et.al, "Image understanding for iris biometrics: A survey", ELSEVIER, Computer Vision and Image Understanding 110, 281–307,2008.

[12] M. Savvides and B. V. Kumar, "Cancellable biometric filters for face recognition", Int. Conf. Pattern Recognition (ICPR), vol. 3, pp. 922–925,2004.

[13] S. Maria Celestin Vigila and K. Muneeswaran,"Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications", International Journal of Network Security, Vol.14, No.4, PP.236-242, July-2012.

[14] Ion TUTANESCU, Constantin ANTON, "Elliptic Curves Cryptosystems Approaches", Int. Conf. on Information Society (i-Society 2012).

[15] Kamlesh Gupta, Sanjay Silakari, "ECC over RSA for Asymmetric Encryption: A Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011

[16] Kulwinder Singh et.al., "Fingerprint Feature Extraction",IJCST Vol. 2, Issue 3, September 2011.

[17] Maneesh Upmanyu et.al, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", IEEE Trans, Information Forensics and Security, Vol. 5, No. 2, June 2010.

[18] G. Mary et.al, "Biometric Encryption using Elliptic Curve", (IJRRCS), ISSN: 2079-2557 ,Vol. 2, No. 5, October 2011 .

[19] Jithra Adikari, "Efficient Algorithms for Elliptic Curve Cryptography",university of calgary,p_hd thesis,2011.

[20] Christel-loïc TISSE1, "Person identification technique using human iris recognition", Advanced System Technology, STMicroelectronics ZI Rousset – 13106 Rousset Cedex, France.