ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Implementation of Multi-Biometric Cryptosystem for Information Security using Elliptic Curve Cryptography

Bharti Kashyap[1], K. J. Satao[2]

M. Tech. Scholar, Computer Science and Engg, Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India[1]

Professor, Computer Science and Engg, Head Department of Information Technology & MCA, Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India[2]

Abstract: In current times, generation of cryptographic key from biometrics is more popular due to its enhanced security level. In this paper a method is proposed to generate unique keys for encryption and decryption of secret messages from biometric images. The keys are directly derived from the images and the captured images are not stored anywhere. Fusion of two or more biometric images increases security more as compared to single biometric feature. In this system, Elliptic Curve Cryptography algorithm is used as the cryptosystem and integrated with multi-biometric system for providing authentication in a secured way. Implementation of proposed system involves fusion of multi-biometric images, generation of Elliptic curve cryptographic parameters from that fused Image and generation of curve from generated parameters.

Keywords: Cryptographic key, Biometric, Elliptic Curve Cryptography, Multi-biometric, Elliptic curve parameters.

I. INTRODUCTION

Cryptography uses mathematics to encrypt and decrypt messages. It enables people to store or transmit sensitive information via insecure network. The main objective of cryptography is to provide security of information over the communication channel so that only the authentic user can be able to see or read the information. Cryptographic systems are divided into two different categories: Symmetric and Asymmetric cryptography (Public Key Cryptography). Both are used to protect flow of information over the communication channel. Symmetric Cryptography uses same key for encryption and also for decryption of message whereas Asymmetric Cryptography uses two different keys, public and private key for cryptographic process i.e. for encryption and decryption. Well-known asymmetric algorithms include DSA, RSA, ELGAMAL, ECC, etc.

In 1985, Neil Koblitz and Victor S. Miller independently proposed the concept of Elliptic Curve Cryptography. The first and probably most important reason is that Elliptic Curve Cryptography offers better security with a shorter key length than any other public-key cryptography [1]. The level of security achieved with ECC using a 160-bit key is equivalent to conventional public key cryptography (e.g. RSA) using a 1024-bit key [2]. The main advantages of using ECC key is shorter key lengths which is helpful especially in applications where limited memory resources are available because shorter key length requires less memory for key storage purpose. Wireless devices and smart cards present a good example for the constrained devices with limited resources.

The term Biometric consist of two Greek Words “Bios” which means life and “Metron” which means measurement. Biometric is defined as automatic system that uses measurable physical or behavioural characteristics to identify the identity of an individual. Some examples of Biometric features are Signature, Keystroke, voice, iris, finger print, face, ears, vein, palm, voice, etc. There are two important modalities of biometric identification viz.

1. Based on Physical Characteristics - It focuses on an individual physical pattern e.g. -Face, Hand, Iris, Fingerprint, etc.
2. Based on Behavioral Characteristics - It concentrates on an individual behavioral analysis e.g. -Typing, Keystroke, voice, etc.

Biometrics makes easier the task to remember textual user id and its associated passwords, which are used in different kind of applications e.g. - an identification system using biometrics such as: if user want to use the ATM without any Card, Claimed identity or PIN, in such condition The ATM scans user’s biometric feature like iris or thumb and determines who the user is and gives access to his/her money or the ATM scans user’s iris and uses it as a password to authenticate he/she is the right owner for use of the ATM and therefore gives authority for accessing his/her money. There is no need to remember the PIN number of ATM card.

In single biometric system a person is identified by a single biometric feature. This type of system depends upon

DOI 10.17148/IJARCCE.2015.4786

single feature of individual which suffers from spoof attack. Multi-biometrics overcomes the limitations imposed by single biometrics by using multiple biometric features. These systems are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. Multi biometric systems address the problem of non-universality and provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric feature of a legitimate user.

Biometric cryptosystem is a method in which Biometric features are used to generate encryption keys to encrypt the secret message, which may refine the security of information. Due to the popularity of biometrics and cryptography, the information security is becoming as a common demand in all the application areas. In a biometric cryptosystem, there are no biometric images or templates stored in the central database, and the security is completely controlled by the user with his/her biometrics [5].

II. ADVANTAGES OF MULTI-BIOMETRIC CRYPTOSYSTEM

As compared with traditional single biometric system, multi biometric offer several advantages:

A. Improve accuracy**:** Combining the features obtained from different sources using an effective fusion scheme can significantly improve the overall accuracy of the biometric system. The presence of multiple sources also effectively increases the dimensionality of the feature space and reduces the overlap between the feature spaces of different individuals.

B. High Resistance to spoofing: Multi biometric systems are more resistant to spoof attacks because it is difficult to simultaneously spoof multiple biometric sources [6].

C. Noisy Data: The availability of multiple sources of information considerably reduces the effect of noisy data. If the biometric sample obtained from one of the sources is not of sufficient quality during a particular acquisition, the samples from other sources may still provide sufficient discriminatory information to enable reliable decision-making [7].

D. Multi biometric systems give anti-spoofing measures by devising it difficult for an intruder at the same time spoof the multiple biometric traits of a legitimate user [8].

III. RELATED WORKS

A system proposed by U. Mahalakshmi [9] provides secured authentication to integrate multi biometric system with Elliptic Curve Cryptography that employs two modalities (i) Fusion of fingerprint, face, iris and signature. (ii) Generating elliptic curve and key using Elliptic Curve Cryptography. In the proposed system, selected portion of multi biometric features are fused into a single image and a curve is generated using Elliptic Curve Cryptography based technique that employs secured domain parameters generated through Genetic Algorithm. A onetime password is also appended to the system to afford high authentication. The proposed algorithm was highly efficient against False Acceptance Rate and False Rejection Rate.

Xiangqian Wu [10] proposed a novel biometric cryptosystem based on the most accurate biometric feature i.e. Iris. In encryption phase, a quantified 256-dimension textural feature vector is firstly extracted from the pre-processed iris image using a set of 2-D Gabor filters. At the same time, an Error Correction Code is generated using Reed-Solomon algorithm. Then the feature vector is translated to a cipher key using Hash function. Some general encryption algorithms use this cipher key to encrypt the secret information. In decryption phase, a feature vector extracted from the input iris is firstly corrected using the Error Correction Code. Then, it is translated to the cipher key using the same Hash function. Finally, the corresponding general decryption algorithms use the key to decrypt the information. Experimental results demonstrated the feasibility of the proposed system.

Rashmi Singhal and Payal Jain [11] proposed a method by combing multiple sources of information system address, most of the problems encountered in mono-biometric systems. Depending upon the nature of application, there is a need to choose an suitable multi biometric system out of available ones. Further, the performance of the system improves if two or more physically uncorrelated traits are used. Efficiency of multi biometric system is highly dependent on the fusion technique employed.

Alok Kumar Vishwakarma [12] proposed Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme .This scheme based on the face and voice recognition to describe the authentication in real life. In this at first the Elliptic Curve Cryptography algorithm is applied on the voter's id as well as image and voice data. It is encrypted and hidden in an image using Steganography. After applying the Steganography it is very difficult for the hackers to identify that the image which is sent over the network contains any information. This kind of security provides the better authentication than any other method.

Nagar et al.[13] proposed the feature level fusion of multi biometric templates. For higher level security, the multiple traits of an individual are combined into a single secure sketch. There are three phases in this paper. First phase is to obtain biometric characteristics and convert to binary string, and in second phase is to combine the above biometric traits and third phase is securely sketch. Fuzzy vault and fuzzy commitments algorithms are used in this paper for decoding.

Fu et al.[14] proposed a method of multi biometric cryptosystem, by binding the multiple features of biometrics to cryptography. There are two levels of combining,

DOI 10.17148/IJARCCE.2015.4786

i.e. combining at the biometric level and combining at the cryptographic level. Shannon entropy is used to afford security. Accuracy and efficiency are also evaluated and it was compared with other systems.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptosystems can be viewed as elliptic curve analogues of the older discrete logarithm (DL) cryptosystems in which the subgroup of Zp is replaced by the group of points on an elliptic curve over a finite field. The mathematical basis for the security of elliptic curve cryptosystems is the computational intractability of the elliptic curve discrete logarithm problem (ECDLP)[15]. An elliptic curve E over Zp is defined in the Cartesian co-ordinate system by an equation of the form:

$$y^2 = x^3 + ax + b \qquad (1)$$

where a, b ε Zp, and $4a^3 + 27b^2 \neq 0 \pmod p$, together with a special point O, called the point at infinity. The set E(Zp) consists of all points (x, y) ε Zp, which satisfy the Equation 1, together with O. Each value of a and b gives a different elliptic curve. The public key is a point on the curve and the private key is a random number. The public key is obtained by multiplying the private key with a generator point G in the curve.

Let p be a prime number. The finite field Fp called a prime field, is comprised of the set of integers {0,1,2,….,p-1} with the following arithmetic operations:

A. **Addition**: If a, b ϵ Fp, then a+b=r, where r ϵ [0,p-1] is the remainder when the integer a+b is divided by p and r is known as addition modulo p.

B. **Multiplication**: If a, b ε Fp, then a.b=s, where s ϵ [0,p-1] is the remainder when a.b is divided by p and s is known as multiplication modulo p.

C. **Inversion**: If a is a non-zero element in Fp, the inverse of a modulo p, denoted by a^{-1}, is the unique integer c ϵ Fp, for which a.c =1.

Elliptic Curve Cryptography provides several advantages over other cryptographic system:

A. It provides greater security in shorter key length.

B. It provides effective and compact implementations for cryptographic operations requiring smaller chips.

C. It is mostly suitable for machines having low bandwidth, low computing power, less memory.

D. It has easier hardware implementations.

V. HASHING ALGORITHM

The term Hashing means transformation of any length of strings into a fixed length value or key. The output of Hash function is called as Hash value or Hash code. The one-way hashing algorithm takes variable-length of data even thousands or millions of bits and produces a fixed-length output. Currently, there are several different hashing algorithms such as LM, MD5, SHA-1, and SHA-2. They can be used in different applications like digital signatures, message authentication, etc. It is impossible to recreate the input data from its hash value alone.

Message Digest algorithm 5 (MD5)

MD5 hashing algorithm was created in 1991 by Ronald Rivest (an MIT professor), as a successor to MD4[16]. MD5 starts by adding the entering data to result in a fixed length. Then, it takes the data in 512-bit blocks, each of these blocks is divided into sixteen 32-bit sub-blocks. Next, each of these sub-blocks is used to affect the 128-bit state variable. It is used in the algorithm in which there are four 32-bit variables such as 'a', 'b', 'c' and 'd'. These variables go through four different nonlinear functions. The fourth step (the final state) a, b, c, d are added to the original entries in this step of the algorithm. After processing all the data, the 128-bit state variable remains.

VI. GENERATION OF KEYS AND ELLIPTIC CURVE PARAMETERS

In this paper we are using finger print and Iris features of senders' and receivers' for generating secret keys, then the keys are used in Elliptic Curve Cryptography to provide network security while sending the information from sender to receiver and vice versa.

First of all, fingerprint and iris features are extracted and then fusion of both images produces a single fused image of fixed size. To generate private key, take the fused of the user and generate its hash value by the help of MD5 cryptographic hash function [17]. This resultant hash value is the private key of the user. Suppose this value is d_A for user A and d_B for user B.

Now generation process of public key in elliptic curve cryptosystem with the help of generated biometric private key is as follows:-

Step1: Both user choose the same large prime 'p' and the elliptic curve parameter 'a' and 'b' such that :

$$y^2 \bmod p = (x^3 + ax + b) \bmod p;$$
$$\text{where, } 4a^3 + 27b^2 \neq 0.$$

Step 2: Now choose any one point G(x, y) from this elliptic curve. This point is called the generator point of the curve.

Step3: Compute $P_A = d_A * G(x, y)$

This P_A is called the public key of user A. To generate public key of user B same operation can be performed with the help of biometric private key of user B.

In proposed methodology, multiple biometric features such as Fingerprint and Iris are taken for secured authentication of user. Fig 1.1 shows the system architecture. In this system, biometric features are resized into fixed size image and then gray scaled. After that, they are fused into a single image which is used for generating elliptic curve parameters and also secret keys i.e private keys of users.

DOI 10.17148/IJARCCE.2015.4786

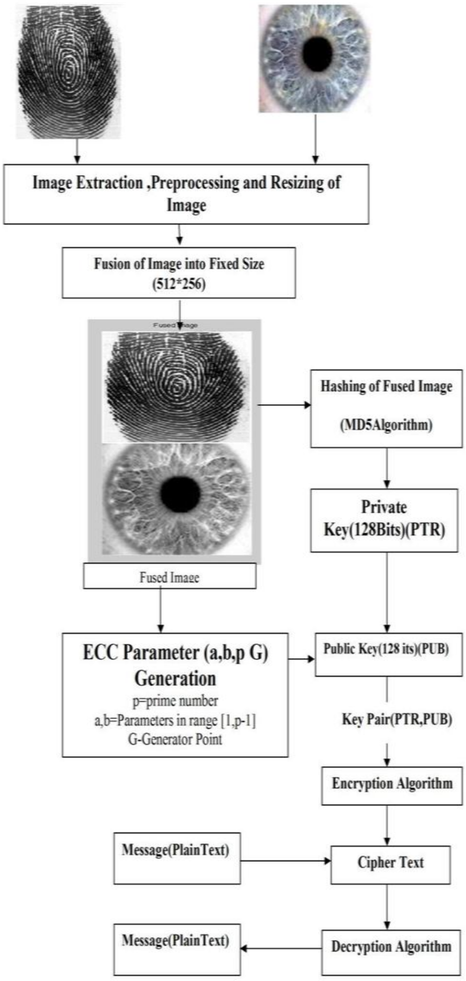
Image Extraction ,Preprocessing and Resizing of Image
Fusion of Image into Fixed Size (512*256)
Fused Image
Fused Image
Hashing of Fused Image (MD5Algorithm)
Private Key(128Bits)(PTR)
ECC Parameter (a,b,p G) Generation
p=prime number
a,b=Parameters in range [1,p-1]
G-Generator Point
Public Key(128 its)(PUB)
Key Pair(PTR,PUB)
Encryption Algorithm
Message(PlainText)
Cipher Text
Message(PlainText)
Decryption Algorithm

Fig1. Multi-Biometric Cryptosystem Architecture

Fused image is given as input to MD5 algorithm to generate the hashed value of it, which gives the private key. This private key is used to generate the public key for the same user. A matrix is formed by randomly selecting some fixed 10 points from fused image, which is used to generate ECC parameters. The intended message is mapped with the ECC curve, and with the help of key pair (Private Key, Public Key) encryption and decryption operations are performed.

VII. ALGORITHM

Following are the major steps in Multi biometric Encryption Technique-

Step1:-**Extraction of Multi biometric samples:**

Fingerprint and Iris are extracted from sources for further processing.(Let S1-Fingerprint,S2-Iris or Fingerprint).

Step2:-**Preprocessing**

a) Gray scaling of both the images from RGB to Gray Scale using Matlab Function rgb2gray().
b) Resizing of each sample into fixed size image (say 256*256).
c) Both the images are merged to obtain fused image of size 512*256.

Step3:-**Parameter Generation (P, a & b)**

A. Prime Number P :

a) Find any 10 values from the fused image and store in a variable (Say fp).
b) Find the sum of selected 10 values: s=sum (fp).
c) Generate prime numbers associated with s
(Using Matlab Function primes(s) : PS=primes(s)).
d) Find maximum value from that generated prime number: P=max (PS).

B. ECC Parameter a and b
Parameter a and b are calculated using generated prime number P by using following steps.

a) Find the difference between S(sum of 10 values) & Prime number P: A=S-P.
b) Find uniformly distributed pseudorandom number of 1(rand (1)).
c) Multiply two above calculated Numbers and increment it.

Encryption Algorithm:

Suppose user ‘A’ wants to send a message to user ‘B’. First task in this system to encode the plaintext message to be sent as a point Pm(x, y). It is the point Pm that will be encrypted as a cipher text and subsequently decrypted. After mapping of points[18] with message on elliptic curve, they can encrypt the message by following steps :

Step1. Suppose User A encodes the message m as Pm=(x,y).
Step 2.User A take his private key from his multi-biometric fused image, suppose it is k.
Step 3. User A compute the k*G.
Step 4. User A compute the Pm+k*Pub, P_B is the public key of user B and Pm is the message.
Step 5. User A take the Cm=(k*G, Pm+k*P_B) as a cipher text
Step 6. User A can send this cipher text to User B.

Decryption Algorithm:

For data decryption we have to perform following steps :
Step1. User B takes the first point of the encrypted message.

Step 2.User B now compute d_B*k*G.
Step 3.User B then subtracts it with his second point.
Step 4.Thus user B compute Pm :

$$m+k*Pb-db*k*G=Pm-k(Prk_b*G)+kPub = Pm-kPub+kPub =Pm$$

Step 5.The message Pm is the required message of User B which is sent by User A.

VIII. RESULTS AND CONCLUSION

Several tests were conducted on many iris and fingerprint images, and these resulted in different domain parameters and private keys for each image. MD5 is used to produce the output digest from the fused image of fingerprint and Iris, which is considered as the seed for the parameters obtained in this study and Elliptic curve algorithm, is used for encryption and decryption of message.

This system is implemented using MATLAB (R2009a) on the window operating system. The various elliptic curve point operations over GF(P) like addition, multiplication, inversion, parameter generation, key generation, encryption and decryption are tested over implemented system.

Keyword	**Parameters**	**Values**
ECC Parameters	P	**7057**
	A,B	**2,3**
	G	**2916 4335**
Keys	Private Key	**219156166bdada660033ea89f19f3ef4**
	Public Key A	**5840c76d4a9c5c69222f872b7e125540**
	Public Key B	**6e273782349b244a313899de92ce260a**
Encryption and Decryption using ECC	Plain Text	**Hiii this is message to encrypt**
	Encrypted Text	**ee90dc44eb4a7f5f66c09c31dce01e93**
	Decrypted Text	**Hiii this is message to encrypt**

Table 1**.** Sample ECC parameters and Outputs

IX. FUTURE SCOPE

The implemented method has generated private key from fused image and also elliptic curve parameters to find the elliptic curve and public key associated with the user. This method can further be developed to generate the digital signature by using ECDSA (Elliptic curve digital signature Algorithm) and can also be merged with Steganography.

REFERENCES

[1] S. Mohammadi, S. Abedi, "ECC based Biometric Signature: A new approach in electronic banking security", in International Symposium on Electronic Commerce and Security (ISECS 07), pp.763-766, 2008.

[2] H.X.Mel,Doris Baker,Cryptography Decrypted,Addision-Wesley, Edition 2011. N. Koblitz,"Elliptic Curve Cryptosystem",Mathematics of Computation, no. 48,pp. 203-209,1987.

[3] G. Mary Amirtha Sagayee, S Arumugam, and G.S.Anandha Mala(2013), Biometric Encryption using Enhanced Finger Print Image and Elliptic Curve,IJCSNS , VOL.13 No.7, July 2013:106-113.

[4] A. Burnett, F. Byrne, T.Sowling, and A.Duffy. A Biometric Identity Based Signature Scheme. Applied Cryptography and Network Security Conference, Columbia University, New York, USA, 2005.

[5] Bo Fu, Simon X. Yang, Senior Member, IEEE, Jianping Li, and Dekun Hu,2009,Multibiometric Cryptosystem: Model Structure and Performance Analysis,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, DECEMBER 2009:4(4), 867-873

[6] Ross A (2007) An Introduction to Multibiometrics, Proceedings of the 15th European Signal Processing Conference (Poznam, Poland)

[7] Nagar A, Nandhakumar K et al. (2012). Multibiometrics cryptosystem based on feature level fusion, IEEE Transaction on Information Forensics and Security, vol 7(1), 255–268.

[8] Juels A, and Wattenberg M (1999). A fuzzy commitment scheme, Proceedings of the Sixth ACM Conference On Computer and Communications Security, Singapore, 28–36.

[9] Mahalakshmi U. andShankar Sriram V. S. ,2013,An ECC Based Multibiometric System for Enhancing Security,Indian Journal of Science and Technology.6(4):4298-4305.

[10] Xiangqian Wu, Ning Qi, Kuanquan Wang, David Zhang ,2008,A Novel Cryptosystem based on Iris Key Generation,IEEE.:53-57.

[11] Rashmi Singhal and Payal Jain, "multi-biometric systems: secure security systems"in IJREAS Volume 2, Issue 2 (February 2012), ISSN: 2249-3905.

[12] Vishwakarma A.K. ,Kumar A.,2011, A Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme International Journal of Technology And Engineering System:2(1),8-12.

[13] Nagar A, Nandhakumar K et al. (2012). Multibiometric cryptosystem based on feature level fusion, IEEE Transaction on Information Forensics and Security, vol 7(1), 255–268.

[14] Fu B, Yang S X et al. (2009) Multibiometric cryptosystem: Model structure and performance analysis, IEEE Transactions on Information Forensics Security, vol 4(4), 867–882.

[15] Certicom ECC Challenge. 2009. Certicom Research.

[16] Jesper, J. The Most Misunderstood Windows Security Setting of All Time. TechNet Magazine. Retrieved on 2007-01-08., 2006.

[17] Anoop MS, Elliptic Curve Cryptography, An implementation tutorial, Tata Elexsi Ltd, Thiruvananthapuram, India.

[18] O. S. a Rao."Efficient mapping method for elliptic curve cryptosystems". International Journal of Engineering Science and Technology, Vol. 2, no. 8, pp. 3651-3656, 2010.

BIOGRAPHIES

Ms. Bharti Kashyap received the B.E. Degree from, Chhattisgarh Swami Vivekananda Technical University Bhilai (C.G.), India, in Computer Science & Engineering in the year 2011. She is currently pursuing M. Tech. Degree in Computer Science & Engineering from Chhattisgarh Swami Vivekananda Technical University Bhilai (C.G.), India. Her research areas include Cryptography, Image Processing etc.

Prof. K. J. Satao is Professor of Computer Science & Engineering and Head of Information Technology and MCA Department at Rungta College of Engineering & Technology, Bhilai, and Chhattisgarh State, India. He has obtained M.S. degree in Software Systems from Birla Institute of Technology and Science, Pilani, Rajasthan State, India in 1991. He has published 60 Papers so far in various reputed National & International Journals, Conferences, and Seminars. He is Ex. Dean of Computer & Information Technology faculty in Chhattisgarh Swami Vivekananda Technical University, Bhilai, India (A State Government University). He is Ex. member of the Executive Council and the Academic Council of the University. He is a member of the Computer Society of India and the Indian Society for Technical Education. He has worked in various Engineering Colleges for about 28 Years and has about 4 Years industrial experience as well. His areas of research include Operating Systems, Editors& IDEs, Information System Design & Development, Software Engineering, Modeling & Simulation, Operations Research, etc.

DOI 10.17148/IJARCCE.2015.4786