International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Irrevocable Cryptographic Key generation from Multi-biometric images

G.Mary Amirtha Sagayee[A], S.Arumugam[B], B.Periyanayagi[A*] and G.S.Anandha Mala[C]

[A]Parisutham Institute of Technology & Science, Thanjavur
[B]Nandha Engineering College, Erode, India
[C]St.Joseph's College of Engineering, Chennai, India, Affiliated to Anna University, Chennai- Tamilnadu, India

Accepted 13 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

In recent times, generating cryptographic key from biometrics has gained huge attractiveness in research community due to its superior performance in security system. Objective of this research work is to generate tough and non- repeating cryptographic keys. In this paper, we have proposed non –repeating and irrevocable cryptographic key from biometric images. The proposed cryptographic method enhances security in Multibiometric authentication system with greater exactness and is more dependable way to recognize the person. In this system, ECC is used as the cryptosystem. The Elliptic curve generation expressly generated by using Genetic Algorithm. Genetic algorithm is a class of optimization algorithm. Many tribulations can be solved using genetic algorithm through genetic process of crossover and mutation. The objective of the GA is to enhance security through non repeating key and Digital signature. The proposed cryptography system leads to protect the multibiometric template and also provide authentication from irrevocable and nonrepeating key.

Keywords: *Multi biometric, Matrix Generation Algorithm, Genetic Algorithm, ECC, Key generation, Digital signature*

1. Introduction

Human identification leads to mutual trust that is essential for the proper functioning of society. With growing concerns about radical actions, defense breaches, and economic fraud, other physiological and behavioral human characteristics have been used for person identification. The individual characteristics, or biometric traits, include features such as face, iris, palm print, and voice. Multibiometric systems accumulate evidence from more than one biometric trait (e.g., face, fingerprint, and iris) in order to recognize a person. [Anil K. Jain]

The four most admired biometric modalities deployed today are face, fingerprint, iris and hand fingerprint (ten prints), for large-scale applications. While the mechanized border crossing in several countries (*e.g*. USA and Japan) require confirmation using fingerprints, the system in the United Kingdom is based on iris and the one in Australia is based on face. [Anil K. Jain]

The combination of different biometric modalities needs to be employed to ensure desired level of security and flexibility in some applications. Another advantage of multimodal systems is that they can potentially offer protection against spoof attacks as it is extremely difficult to spoof multiple modalities simultaneously. For protecting the biometric templates, a perfect cryptosystem is required to be flexible in the security mechanism as well as be able to render high secure performance. The security mechanism is described by authentication and authorization.[Nagar A, Nandhakumar]

Authorization is the duty of an authority. Authorization involves mainly the practice of providing admittance power to the users. Biometric authentication of every user can be used to enhance the security of the user environment. Authentication is the method of truly confirming that individuality of user. Biometric authentication system enhances the security of identification and verification system. The following Vulnerabilities occurred on the template of biometric authentication system due to attacks:

- The stored sample template may have a opportunity to replace by an imposter's template to gain unauthorized access.
- A intentional modification of an enrolled by an attacker.
- Abuse the user privacy by cross-matching the templates from associated databases.[Nagar A, Nandhakumar]

The biometric image security requires following characteristics,

○ The cryptosystem should be computationally secure.
○ The cryptosystem should be fast enough not to degrade system performance.
○ The security system should be flexible.
○ The security system is to avoid massive storage requirements.

Elliptic curve cryptography is new cryptography method. It is computationally difficult to hack and also it reduces

*Corresponding author **B.Periyanayagi** is a PG student the storage space. The parameters of the Elliptic curve are selected by genetic algorithm. The genetic process are crossover and mutation which produces the parameters without manual help.

2. Literature Survey

Biometric recognition provides validation of a person based on distinctive characteristics produced by the entity. Biometrics cannot be easily imitative, shared, dispersed and forgotten. The unimodal biometrics faced with variety of problems such as noise in sensed data, non-universality, inter class similarities and spoof attack. For these inconvenience and for improving the performance of the biometric system, different biometrics are integrated and formed the multimodal biometrics. The multimodal biometrics approaches afford suitable measures to resist against above mentioned problems. [Jagadeesan,.A.Dr. K.Duraiswamy]

Information security and Privacy is an important factor in the world. For achieving these factors, the researchers enter into the field of Biometric cryptosystem which combines the biometrics and cryptography. Based on biometric features, the cryptographic key is generated by the biometric cryptosystem. It provides the high security and privacy of the biometric template and also provides the secure authentication.[Lalithamani.N]

Cryptography is an important feature of computer and network security. In this project, the Elliptic curve cryptography is used as the biometric cryptosystem. The following passage discussed about ECC.

Elliptic curve cryptography is a new move toward and considered as an marvelous technique with low key size for the user. The intruders have a exponential time for breaking into the system. The elliptic curves have a rich and beautiful record; have been studied by mathematics for over a hundred years. In 1985, Public key cryptography was projected by Koblitz and Victor. They were separately estimated elliptic curve intend in cryptosystems.[Samta Gajbhiye, Monisha Sharma]

In 1990's ECC was consistence by a number of organizations such as IEEE,ANSI,NIST,ISO and it started receiving commercial reception. The choice of the type of elliptic curve was dependent on its field parameters, the finite field demonstration, elliptic curve algorithms for field arithmetic as well as elliptic curve arithmetic. [Tarun Narayan Shankar]

In 2000, an arithmetic finite field based elliptic curve was proposed by Daniel V. Bailey and Christof Paar in Elliptic curve Cryptography which discussed about arithmetic curve (i.e) point addition. [Yasser Salem Mohamed Ali]

In 2002, M.Bednara,M.Daldrup,J.Teich showed how an elliptic curve coprocessor based on the Montgomery algorithm for curve multiplication can be implemented using our generic coprocessor architecture. The ECC had highest strength per bit compared to other Public key cryptosystem.ECC gives the smaller key. It translated into savings in bandwidth, memory and Processing power. These were projected by Wendy chou.[Sravana Kumar.D]From the survey, ECC is the gifted aspirant for Public key cryptosystem. Its security has not been completely evaluated. Till research is going on elliptic curve cryptography by Certicom. The Certicom have generated different The ECC has been shown to have many advantages due to its ability to provide the same level of security as RSA using shorter key.

Genetic algorithm was proposed by Prof.John Holland. Genetic algorithm is the stochastic adaptive algorithm which gives the better solution for all problems. It has high search space and reproductive capacity.[Karel P. Bergmann]

Manisha Mehta was proposed a system for security with cancellable biometric. Here, the non-invertible key was generated by using Genetic process. This non-invertible key is not easy to hack.[Manisha Mehta]

Ankita agarwal was anticipated a encryption system with secret key. The secret key was formed by using genetic algorithm which gave a efficient encryption using genetic process of crossover and mutation.[Ankita agarwal]

Swati Mishra was created a non-repeating public key and private key in field of Public key cryptography. Here, Genetic process satisfied the uniqueness and better performance of public key cryptography. From the observation which increased the strength of keys and security.[Swati Mishra]

3. Proposed System

The proposed system provides secure authentication to incorporate multi biometric system with Elliptic Curve Cryptography that employs three modalities (i)Enrollment (ii)Verification (iii) Session key generation. In this method, selected portion of multi biometric images are fused into a single image and a curve is generated using ECC technique that employs secured domain parameters generated through Genetic Algorithm.

I) Enrollment:

In this system, users enter into the system with two ways. One is through biometric and another one is One time password. One time password is generated from the multibiometric template using ECC.

Biometric Traits:

Biometrics are extremely intricate to duplicate or forge and unfeasible to share. Biometric technologies are typically used to analyze human characteristics for security purposes.

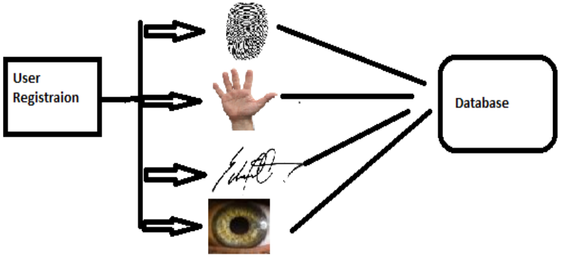

Fig.1. User Enrollment

During enrollment, biometric images are captured and related information stored on the database. The proposed system comprises Fingerprint, Hand geometry, signature

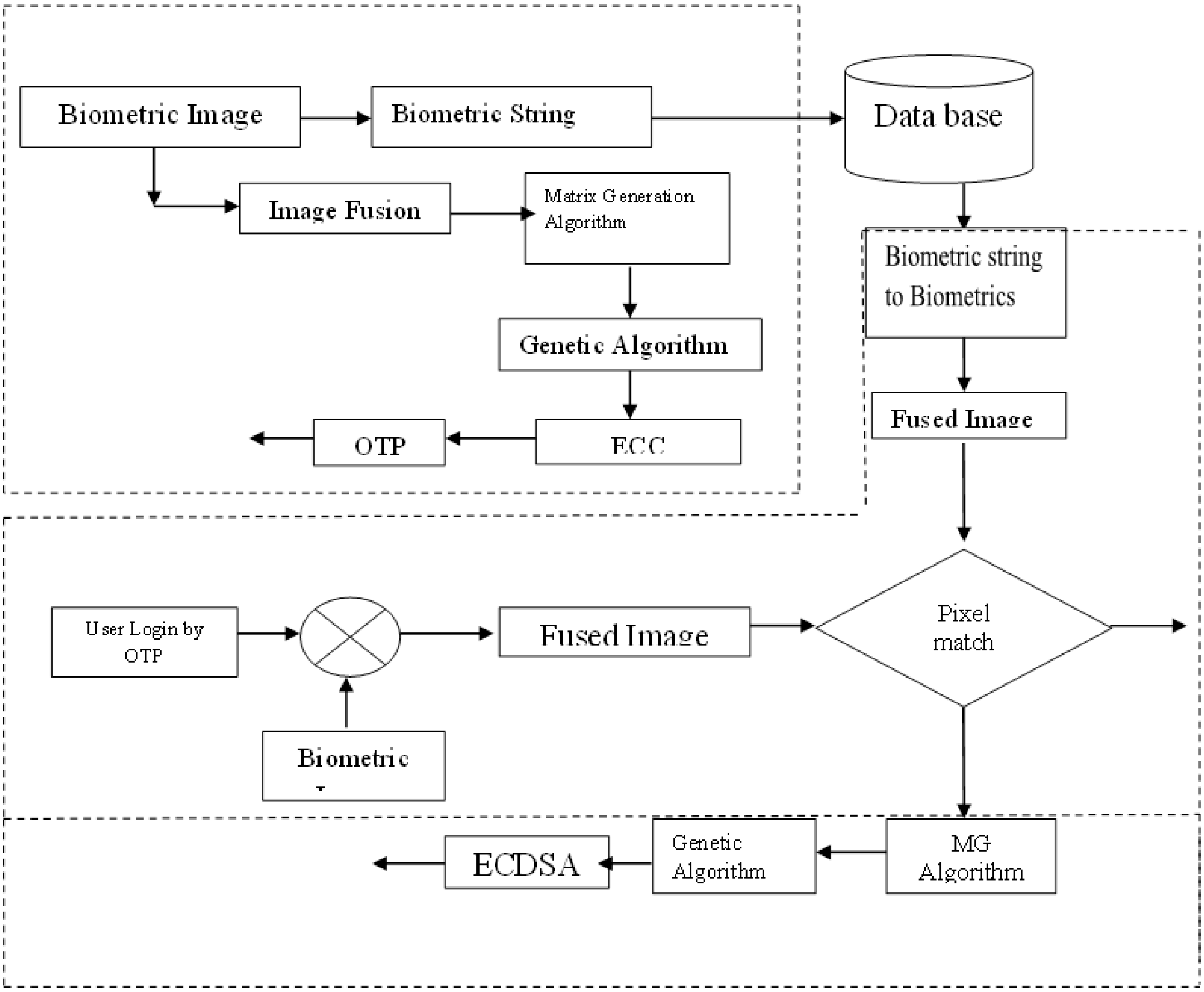

Fig.2. Proposed system Block Diagram

and Iris as biometric features. The biometric characteristics are converted into string and stored in the database. So, the hacker cannot be able to identify which biometric is stored in the database.

OTP Generation's:

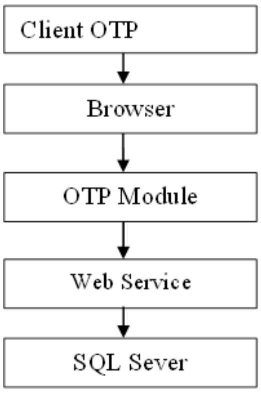

Fig.3.Flow diagram of OTP generation

The one time passwords are created multiple times based on the effective key generation which is generated by Elliptic curve cryptography. The sequence of OTP should be difficult to find which is unpredictable and irreversible.OTP generator is the self content tool. It needs two inputs: key and count. The count value increments on each time are made by given user. The input of the OTP is given by the ECC key. This OTP transferred to user mobile which is used as the user ID during biometric verification.

II) Verification:

During verification process, the user enters with OTP. After matching OTP, user login through biometric image. Then, the stored biometric string converted into biometric image. The biometric images are fused. Login images are also fused. Both fused images are verified by using pixel matching. If pixel matching is greater than 80% means, the verified image go to the next process of session key generation. Otherwise it stops the process.

III) Session key generation:

The session key generation is one of the authentication methods. In this system, digital signature is generated from Elliptic curve points by using Elliptic curve Digital signature algorithm. The Digital signature algorithm provides a digital signature for the each session of the user login. Elliptic curve cryptography is a one of the cryptographic methods which produced by Matrix generation algorithm and genetic algorithm.

A. Elliptical curve Cryptography

Elliptic curve Cryptography is an asymmetric key cryptography by nature. ECC produces both Private and Public keys.ECC can be implemented in software and hardware. Software ECC implementation provide moderate speed, high power and have very restricted physical security with respect to key storage. Hardware implementation improves performance in terms of flexibility. The hardware implantation provides greater security and they cannot be modified read by the outside attacker.ECC has premier strength-per-bit compared to other Public key cryptosystems. The main advantage of the ECC is smaller key size. The smaller key sizes reduce bandwidth, memory and processing power and also reduce time. Elliptic curves generated in this cryptography. They are also named ellipses that are formed by quadratic curves. The standard form of the elliptic curve is described by

$$Y^2 = X^3+aX+b$$
$$4a^3 + 27b^2 \neq 0, x, y, a, b \in R$$

In this Cryptography schemes, elliptic curves over two finite fields are mostly used Prime field F_P and Binary fieldF_2^m.

B. Elliptic Curve over Prime field Fp

Many Cryptosystems frequently involve the use of algebraic groups. A group is a set of elements with custom – defined arithmetic operation on those elements. For elliptic curve groups, these operations are defined geometrically. Cryptographic applications require fast and precise arithmetic. Elliptic curves are not ellipses. An elliptic curve has an underlying field can be created on $F_{p.}$ a and b variables choosing from the field of $F_{p.}$ The elliptic curve includes all points (X,Y) which satisfy the elliptic curve equation modulo P**.**

$Y^2 mod\ P = X^3 + aX + b\ mod\ p$ has an underlying field of F_p if a and b are in $F_{p.}$

C. Matrix Generation Algorithm

Matrix generation is one of the new algorithms for generating Prime number of ECC. The Fused Multibiometric Image gives as the input of the Matrix generation algorithm. This Algorithm automatically generates the prime number for Elliptic Curve generation.
Step1: Choose fixed points in the fused image
Step2: Extract RGB values from fixed points in the fused image
Step3: The extracted RGB values doubled.
Step4: From doubling process, 8×8 matrix generated.
Step5: In matrix, the values are added row by row.
Step6: From the resultant values, smallest number has chosen.
Step7: The first consecutive Prime number has chosen from smallest number.

D. Genetic Algorithm

Genetic algorithms (GAs) are a group of optimization algorithms. Many tribulations can be solved by genetic algorithms throughout modeling a simplified adaptation of genetic process This new method was applied to the applicant type of information i.e. images. Genetic algorithm is encouraged by natural evaluation.

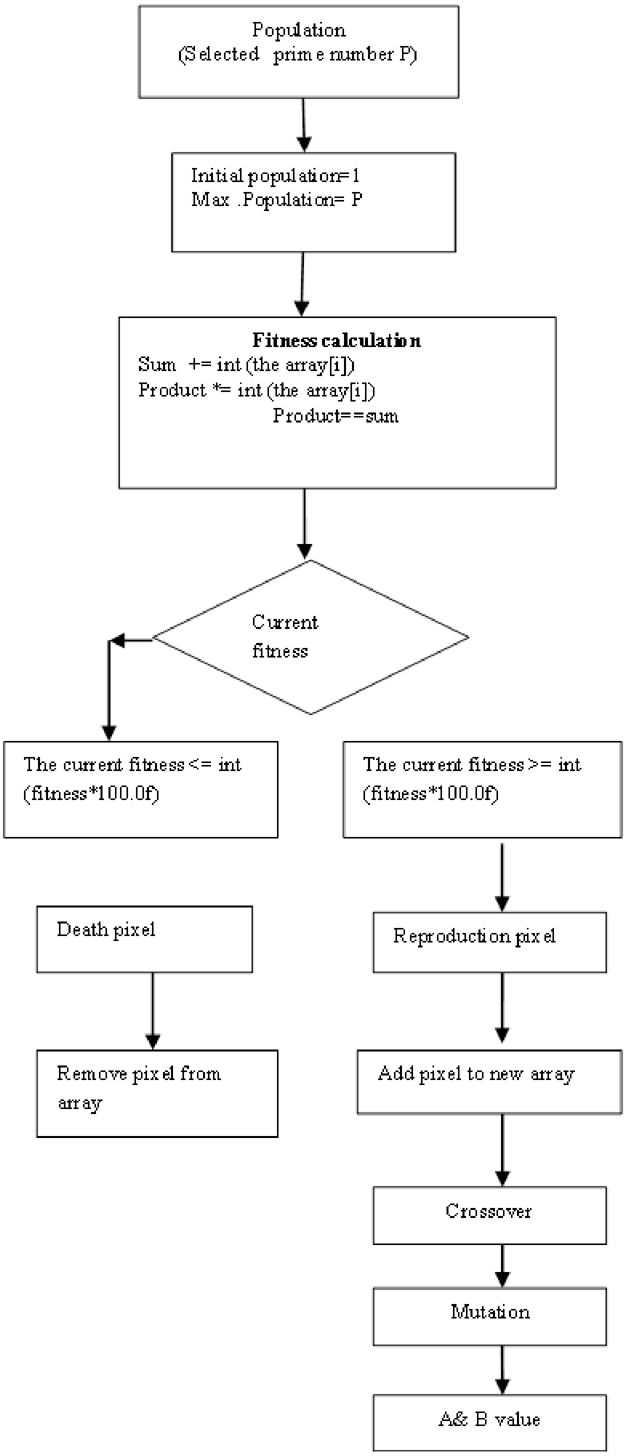

Fig.4. Flow diagram of Genetic Algorithm

Generally, Genetic algorithm has the following steps,

- Population
- Fitness selection
- Reproduction
- Elitism

1. Population

Population is the maximum value of the prime number. That is, maximum number of pixels.

2. Fitness selection

```
Sum  += int (the array[i])
Product *= int (the array[i])
 (Product==sum) →Current fitness

The current fitness <= int (fitness*100.0f) → Death fitness
The current fitness >= int (fitness*100.0f)–-> Reproduction fitness
    Death fitness pixel removed from the array
    Reproduction pixel added to the array
```

3. Generation of new parents

Then generate the new population array
Reproduction array creates the new generation.

4. Crossover

Set crossover point
From the new generation, Parent genes are generated. Then parents are crossover for generating new baby genes.

```
babyGene1 = GeneDads[i]).Crossover(GeneMoms[i]);

babyGene2=(GeneMoms[i]).Crossover(GeneDads[i]);
```

5. Mutation

If the new population genes don't satisfy the following condition, the baby genes are mutated.

```
TheSeed.Next(100)<(int)(kMutationFrequency * 100.0))
aGene.Mutate()
```

6. Elitism

Elitism is performed to retain *e* percentage of the fittest gene in the previous population in the new population. The retained genes replace the weakest genes in the new population. The genetic algorithm runs for g generations for every chunk, hence a total of $g \times d$ generations.

After these natural genetic processes of Crossover and Mutation, the algorithm gives the best pair. This pair are taken as the a & b for ECC. The a & b values have substituted in the elliptic curve equation. Elliptic curve points generated over the Prime field. The genetic processes end after six generation. The genetic process increases the strength of the key.

4. Test results

The Elliptic curve points have been taken from different dataset. Here, multiple biometric images have been used for image fusion and Elliptic curve cryptography. For a single person, the multiple biometric is difficult to collect and test. We need different sensor system and modalities for collecting different biometric for a person. So, It takes more cost, complexity and time. For reducing capturing time and complexity of the sensor, I have chosen the multiple fingerprint CASIA dataset. Because, It is easy to collect and test.

The Elliptic curve points have been taken from the CASIA Multiple fingerprint dataset. The curve points are depends on a & b parameter. From the test results, each user's prime numbers have been selected automatically from the fused image. These prime numbers are large and it is the max population size of the genetic algorithm. Prime number, A&B and Elliptic curve points are observed from model and shown in the table.1. The prime numbers have been created automatically by using MG algorithm which gives the maximum prime field for Elliptic curve. The A&B values satisfied the condition of non-singular curve. The non-singular curve is difficult to hack. So, it reduces the spoofing attack.

Table2. Shows test result of key generation. For each user it creates an unique and non-repeatable keys based on the elliptic curve parameters. If the keys are non-repeatable means, it is unique also. These keys are irrevocable also. Because, the elliptic curve points are not easy to predict. Table.3 shows a different A&B for a single user in different login time. In genetic algorithm, genetic process provided the diverse value of A&B. The crossover and mutation is doing their main role in GA. After sixth generation only it gave value of A&B parameter. So, each generation the parent genes have been changed and also it gave a different offsprings also. Finally, it produced A &B value with satisfaction of non-singular condition. Crossover and mutation produced different for each login time of a user.

If the attacker wants to read the original template, it needs keys. Here, the keys are computationally infeasible to revoke. So, it maintains confidentiality of biometric system. It reduces the spoofing and cross matching attack.

User	Prime Number	A & B	EC Points
User1	967	9,-1	(-1,-2)(-1,2)(2,-4)(2,4) (3,-6)(3,6)
User2	769	7,-7	(2,-1)(2,1)(5,-11)(5,11) (9,-27)(9,27)
User3	619	4,9	(1,-3)(1,3)(2,-5)(2,5) (5,-13)(5,13)(10,-33)(10,33)
User4	569	6,-5	(-3,0)(0,-3)(0,3)(1,-2) (1,2)(4,-7)(4,7)
User5	521	2,-8	(-3,-2)(-3,2)(0,-2)(0,2) (3,-2)(3,2)
User6	1151	7,9	(-2,-3)(-2,3)(-1,-3)(-1,3) (3,-3) (3,3)
User7	593	5,7	(-3,-1)(-3,1)(1,-1)(1,1)(2,-1) (2,1)
User8	601	7,-7	(-1,1)(-1,1)(1,-3)(1,3)(4,-9) (4,9)(11,-37)(11,37)
User9	809	2,-5	(1,-3)(1,3)(2,-5)(2,5)(5,-13) (5,13)(10,-33)(10,33)
User10	593	6,-5	(0,-2)(0,2)(3,-7) (3,7)(6,16)(6,-16)

Table.1. Elliptic Curve Points from Multibiometric Image

User	Prime Number	A & B	Key Generation
User1	967	9,-1	TOYHDWWOWPBHSGL
User2	769	7,-7	OWSTJVUDZPBAPGTW
User3	619	4,9	XWAUHJZZMFNTXHEY
User4	569	6,-5	ETPPELLCKLGAIEHMR
User5	521	2,-8	BWSFSSRFRZTSYTTKT
User6	1151	7,9	WFZMNJZIJXWXWDV
User7	593	5,7	MRVNBKVNDIEBOSI
User8	601	7,-7	VZQKSKGNIWIXARPM
User9	809	2,-5	QUAHJARMSHBUVE
User10	593	6,-5	BATGSIEZVTURUIPZ

Table.2. Key generation from Multibiometric Image

User11	Login Time T1	Login Time T2	Login Time T3	Login Time T4
A & B value	(8,1)	(6,4)	(7,-7)	(2,9)

Table.3. A& B value for single user in different login time

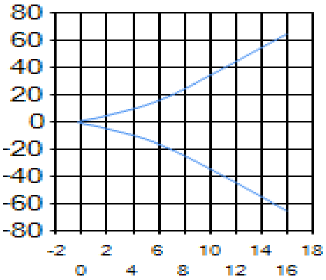

Fig.5.Elliptic curve - User11 (8,1)

5. Digital Signature

I) Signature Generation:

In this system, Elliptic curve digital signature algorithm has been used for generating digital signature. In this algorithm, the hash has found for string of biometric image. Then, take the signature for string image.

e= elliptic curve points
P=kG ; R= eP
r = X co-ordinate of (R)

P is the any one point of the elliptic curve. k is an integer between [1,n-1].G is the base point of the elliptic curve. Then, R is calculated from the elliptic curve points. r is the signature which digitally generated by the curve points. This signature can be used as the session key for different applications.

II) Signature Verification:

During verification also, the signature has been generated using Elliptic curve.
W= ekG
W=e P
v=X_1 coordinate (W)

if r & v are equal means, the signature has validated. Then authentication provided to the authorized person. The authorized person has been validated by the signature. But, signature generated from authorized biometric of a person.

Conclusion

The proposed work analyses the Elliptic curve cryptography and genetic algorithm. Prime Number have been generated automatically by Matrix generation algorithm. The best pair of a & b values have been generated from prime number by using genetic algorithm. The a& b has to be used in the Elliptic curve equation as elliptic curve parameters. It generates the Optimized elliptic curve. This curve improves a security of the authentication system. For enhancing authentication, the identification code has been created. The identification code is One time password which is generated from EC. Before image verification, OTP is entered in the verification Module. Then, Image has been verified using pixel matching. ECC have been generated the non repeating key for each user by using genetic algorithm. This non repeating key is more difficult to reverse and revocable. Key should be changed in each login time of user. ECC makes an attractive cryptosystem. It makes an irrevocable key for every user. This system achieves the maximum security through the above process without degrading biometric image performance.

ECC is an ideal for key distribution and management that provides authentication and data integrity. During verification it will not degrade the original image. It achieves the performance of the secure biometric image template.

References

Anil K. Jain, Ajay Kumar (2010.) , Biometrics of Next Generation: An Overview, Springer

Ankita Agarwal (April2012), Secret Key Encryption Algorithm Using Genetic Algorithm, International Journal of Advanced Research in Computer Science and Software Engineering

Beng.A, Jin Teoh and Kar-Ann Toh (June 2008), Secure biometric key generation With biometric helper , in proceedings of 3rd IEEE Conference on Industrial Electronics and Applications, pp.2145-2150, Singapore.

Curve Cryptosystems, RSA Security,13 Dec. 2004. RSA Laboratories.

ECC Cryptography Tutorial, Certicom,13 Dec. 2004.

Jain A, Nandakumar Ket,el(2005), Score normalization in Multimodal Biometric systems, the Journal of pattern recognition society, Vol 38,(2270-2285)

Jagadeesan.A., Dr. K.Duraiswamy (Feb2010), Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris on International Journal of computer science and information security,vol.7.

Karel P. Bergmann, Renate Scheidler (2008), Cryptanalysis using Genetic Algorithms,*GECCO'08,* July 12–16, Atlanta, Georgia, USA.

Lalithamani.N., Dr.K.P.Soman (March2009.), An effective scheme for generating Irrevocable cryptographic key from cancelable fingerprint template on International Journal of computer science and Network Security, Vol.9.

Matthew K. Monaco, Color Space Analysis for Iris Recognition, Lane Department of Computer Science and Electrical Engineering (2007) M.Maniroja and Sudhir Sawarkar, Biometric Database Protection using Public key Cryptography, IJCSNS

Manisha Mehta (Nov-Dec-2011.), A Genetic Based Non-Invertible Cryptographic Key Generation From Cancelable Biometric in MANET, IJCAT, vol2

Nagar A, Nandhakumar and Anil.K.Jain (2012), Multibiometric Cryptosystem Based on feature level fusion, IEEE.

Ola M. Aly 1, Hoda M. Onsi , Gouda I. Salama , Tarek A. Mahmoud (Nov2011), A multimodal biometric recognition system using feature fusion based on PSO On International Journal of Advanced research in computer and Communication Engineering,vol.2.

Ross A (2007), An Introduction to Multibiometric, proceedings of the 15th European, Signal Processing Conference.

RashiBais,K.K.Mehta (June2012), Biometric Parameter based cryptographic key Generation on International journal of Engineering and advanced Technology, vol.1.

SEC1: Elliptic curve Cryptography (2000), Certicom Research, Available from http://www.secg.org/ collateral/sec1_final .Pdf

SujimangalamM., M.Karnan, R.Sivakumar (May 2013), Generating cryptosystem for Multimodal biometrics based on feature level fusion on International journal of computer science and management system, vol.2

Samta Gajbhiye, Monisha Sharma (Dec2011.), A survey Report on Elliptic Curve Cryptography on International Journal of Electrical and Computer Engineering, Vol.2.

Sravana Kumar.D., CH. Suneetha., Chandrasekh.AR (Jsn 2012.), Encryption of data using Elliptic curve over finite fields son International journal of Distributed and Parallel system,vol.3

Tarun Narayan Shankar and G.Sahoo (April/May2009), Cryptography with Elliptic Curves on International Journal of Computer science and Applications,Vol.2.

Yasser Salem Mohamed Ali, Implementation of Elliptic Curve Cryptography using biometric features to enhance security services.

Swati Mishra, Siddharth Bali (May2013.), Public Key Cryptography Using Genetic Algorithm, (IJRTE),Vol2