

ECC Base point Generation using Finger print for Authentication and Message Encryption and Decryption using ECC

Dr. O.Srinivasa Rao¹, Dr. N.V.Ganapathi Raju², P.Sri Hari³

Associate Professor, CSE Department, UCEK, Kakinada, India¹

Professor, CSE Department, GRIET, Hyderabad, India²

M.Tech Student, CSE Department, UCEK, Kakinada, India³

Abstract: Biometrics refers to an automatic authentication of a person based on his physiological and/or behavioural characteristics. The usage of biometrics as a reliable means of authentication is currently emerging. This paper proposes a unique approach for generating base point of an elliptic curve using finger print of a person for authentication which is a prime parameter in Elliptic curve cryptosystem.

Keywords: Biometrics, Authentication, Fingerprint, ECC, Keys.

1. INTRODUCTION

Biometrics is the science of identification of humans by their characteristics. It refers to certain physiological or behavioural characteristic that is uniquely associated to a person. This trait is highly distinctive and can be utilized for distinguishing different individuals. The biometric can be categorized into two categories: physiological bio metrics and behavioural biometric [1].

Physiological biometrics refers to a person's physical attribute, such as fingerprint, face, and iris. [2]. the way people do things such as speaking (voice), writing (signature), typing (keystroke dynamics), and walking style (gait recognition) are known as behavioural bio metrics. [3]

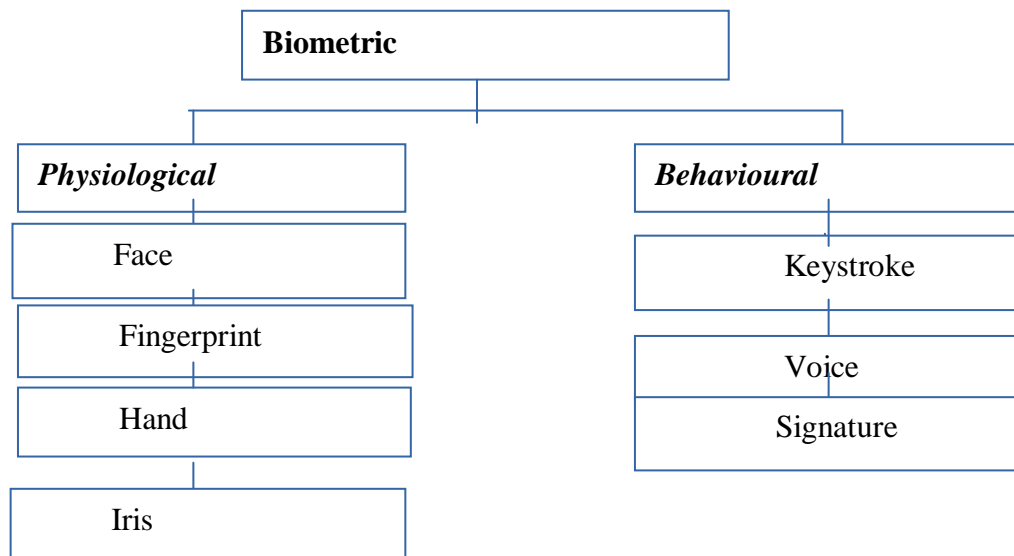


Fig1. Biometric characteristics

Biometrics and Crypto keys

Biometrics offers a natural and reliable solution to certain aspects of authentication by using semi- automated or fully-automated schemes to recognize individuals based on their biological characteristics. By using biometrics it is possible to establish an authentication[13] based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password. In traditional cryptosystems, user authentication is based on possession of secret keys [4]; the method fails if the keys are not kept secret (i.e., shared with non-legitimate users).

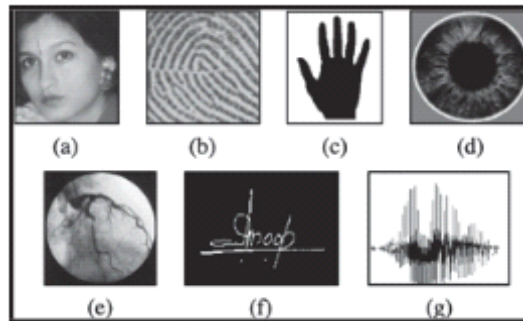


Fig. 2.Examples of biometric characteristics. (a) Face. (b) Fingerprint. (c) Hand geometry. (d) Iris. (e) Retina. (f) Signature. (g) Voice. From D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition

Further, keys can be forgotten, lost, or stolen and, thus, cannot provide non-repudiation [4][5]. Current authentication systems based on physiological and behavioural characteristics of persons known as biometrics, such as fingerprints, inherently provide solutions to above problems and may replace the authentication component of traditional cryptosystems [6].

Biometric cryptosystems[7],[15]are similar to password based key generation systems as they are used to secure cryptographic key or to directly generate cryptographic key from biometric features.

Fingerprints are the most widely used parameter for human identification amongst all biometrics. Fingerprint comprises a set of minutiae. A ridge in fingerprint is defined as a single curve segment and a valley is the region between two adjacent ridges. The collective set of ridge endings and bifurcations form the minutiae. The minutiae can be of different types including dots ,islands, ponds or lake, spurs ,bridges and crossovers. The orientation of the minutiae uniquely identifies a fingerprint. This feature has been exploited to generate a unique code for an individual. The code is further modified to obtain a base point of an Elliptic Curve Cryptography [11].[12].

2. FINGERPRINT PROCESSING: FINGER PRINT OF AN HUMAN BEING IS PROCESSED AS FOLLOWS

2.1 Histogram Equalization

Histogram equalization [8] increases the contrast of images. In this technique the basic idea is to map the gray levels based on the probability distribution of the input gray levels. Histogram Equalization transforms the intensity values of the image as given by equation

$$S_k = T(r_k) = \sum_{r_j} P_r(r_j) = \sum_{j=1}^k n_j / n \text{ for } j=1..k.$$

Where S_k is the intensity value in the processed image corresponding to intensity r_k in the input image and $p_r(r_j) = 1, 2, 3, \dots, L$ is the input fingerprint image intensity level.



Fig1. sample fingerprint image Fig 2.After Histogram Equalization

2.2 Binarization

Binarization [9] is to transform the 8-bit Gray fingerprint image with 0-value for ridges and 1 value for each pixel. Typically, the two colours used for a binary image are black and white, though any two colours can be used. The colour used for the object in the image is the foreground colour while the rest of the image is the background colour.

2.3 Morphological Operation

Structure of an image or form of an is obtained by using Morphological Operation [10]. It used to obtain identification of objects or boundaries within an image. The primary morphological functions are erosion, dilation, hit or miss.

Morphological operations are performed on binary images where the pixel values are either 0 or 1. Binary morphological operators are used on binarized fingerprint image to remove spurs, bridges, line breaks etc. A process called thinning is also applied to reduce thickness of lines. It is a process particularly used for skeletonisation.

2.4 Minutiae points' extraction

The binary image is thinned such that a ridge is only one pixel wide. Among all fingerprint features minutia point features with corresponding orientation maps are unique enough to discriminate amongst finger print robustly; the minutiae feature representation reduces the complex fingerprint recognition problem to a point pattern matching problem. The minutiae are extracted [11] from the enhanced, thinned and binary image. One of the minutia extraction techniques is crossing number.

2.4.1 Crossing Number

It uses the skeleton image where the ridge flow pattern is eight-connected. The local neighbourhood of each ridge pixel in the image is scanned out using a 3x3 window.

Table 1. A 3x3 neighbourhood

p ₄	p ₃	p ₂
p ₅	P	p ₁
p ₆	p ₇	p ₈

The crossing number (CN) value is then computed as follows

$$CN = 0.5 \sum_{i=1}^8 |P_i - P_{i+1}| \text{ for } i=1 \dots 8 \text{ Where } P_9 = P_1$$

It is defined as the half the sum of the differences between pairs of adjacent pixels in the eight neighbourhood. Using the properties of CN as mentioned below, ridge pixel can be classified as ridge ending, bifurcation or non-minutiae point

Table 2. Properties of Crossing Number

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

After obtaining the minutiae points of a fingerprint of a human being, are used to find a base point of an elliptic curve using the following algorithm.

3. ALGORITHM

1. Read the input Fingerprint Image.
2. Binarize the image.
3. Thin the Binarized image (Image Skeletonization).
4. Find all minutiae points (ridge points).
5. Add all minutiae points. $(\sum X, \sum Y, \sum \square)$
6. Reduce the three dimensional minutiae coordinates to two dimensional coordinates (newx, newy) i.e. $newx = (\sum X / \sum \square)$ and $newy = (\sum Y / \sum \square)$.
7. $nex = newx \% p$ and $ney = newy \% p$.
8. Find the nearest point on the elliptic curve to the point (nex, ney) and name it as G.
9. Do the encryption and decryption using G as Generator.

Once, the base point is obtained, we can encrypt and decrypt any messages using elliptic curve crypto system. The following section, explain the elliptic curve cryptosystem briefly.

4. ELLIPTIC CURVES OVER FINITE FIELD (ZP)

For elliptic curves over Z_p , we use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through $p-1$, for some prime number p , and in which calculations are performed modulo p [14].

$$y^2 \text{ mod } p \equiv (x^3 + ax + b) \text{ mod } p$$

Example:

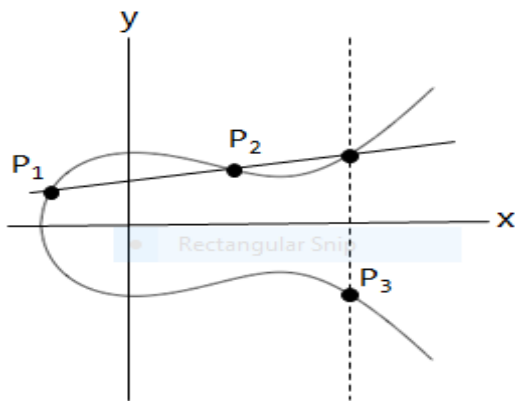
For the given $a=1, b=1$, and $p=79$, the points of the elliptic curve are

(0,1),(0,78),(2,13),(2,66),(3,30),(3,49),(5,17),(5,62),(6,12),(6,67),(11,0),(14,28),(14,51),(15,28),
(15,51),(16,20),(16,59),(18,20),(18,59),(20,11),(20,68),(21,35),(21,44),(23,5),(23,74),(25,3),(25,76),
(26,12),(26,67),(27,35),(27,44),(28,16),(28,63),(29,18),(29,61),(30,31),(30,48),(31,35),(31,44),
(43,36),(44,38),(44,31),(46,22),(46,57),(51,29),(51,50),(53,20),(53,59),(56,0),(59,33),(59,46),(60,16),(60,63),(61,39),(61,40),
(64,12),(64,67),(65,12),(65,67),(70,12),(70,67),(71,21),(71,58),(78,0).

Elliptic curve arithmetic is defined as follows

4.1 Point Addition

Let $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ are two points on the elliptic curve E . The sum P_3 is defined as: First draw a line through P and Q , this line intersects the elliptic curve at a third point. Then the reflection of this point of intersection about x -axis is P_3 which is the sum of the points P_1 and P_2 .



Define for two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ in the Elliptic curve

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{for } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{for } x_1 = x_2 \end{cases}$$

• Rectangular Snip

Then $P+Q$ is given by $R(x_3, y_3)$:

$$\begin{cases} x_3 = \lambda - x_1 - x_2 \\ y_3 = \lambda(x_3 - x_1) + y_1 \end{cases}$$

4.2 Point Doubling:

Doubling is adding the point to itself. First draw the tangent line to the elliptic curve at P which intersects the curve at a point. Then the reflection of this point about x -axis is R .

4.3 Point Multiplication:

Let P be any point on the elliptic curve (K). Then the operation multiplication of the point P is defined as repeated addition. $kP = P + P + \dots + P$ (k times).

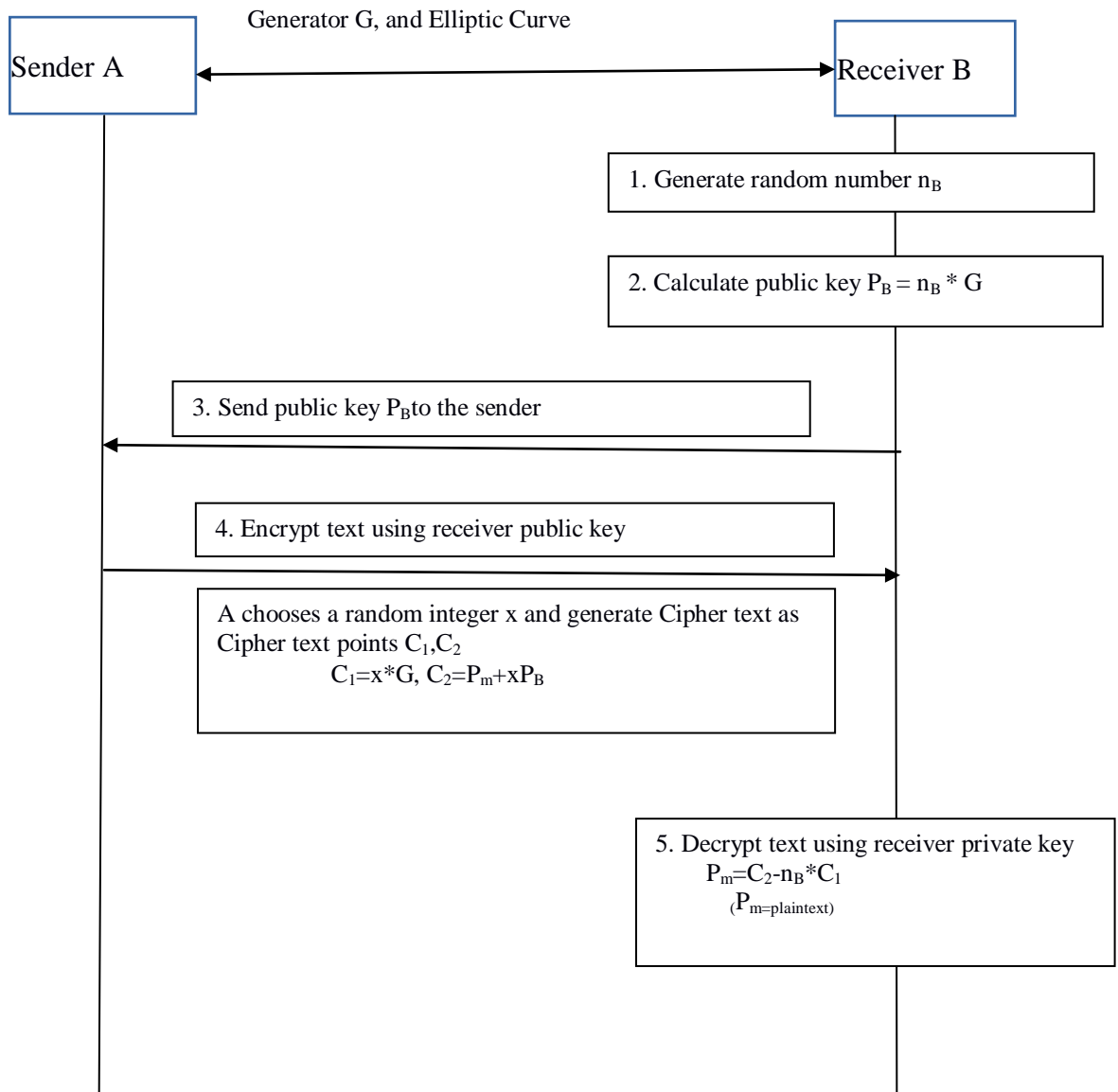
4.4 Point Subtraction:

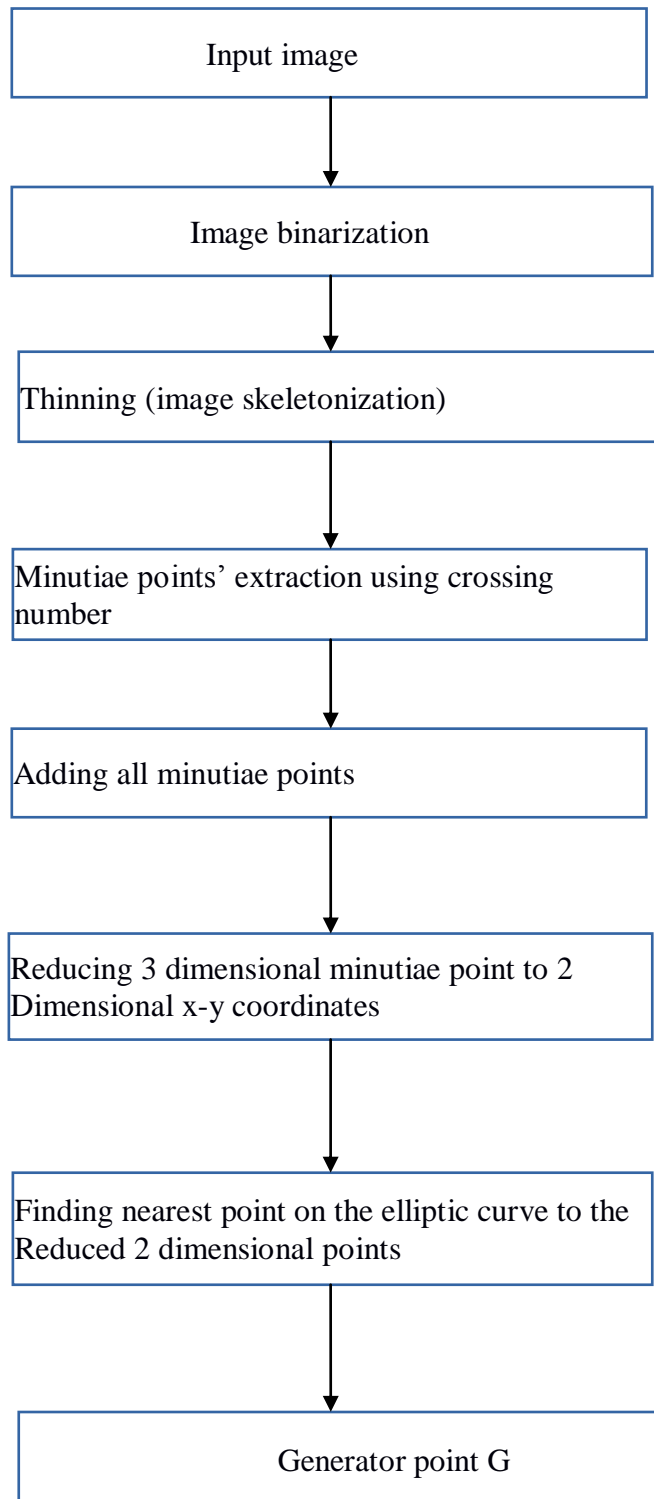
Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ are two points on the elliptic curve E . The subtraction R is defined as Addition of the points $P(x_1, y_1)$ and $Q(x_2, -y_2)$.

4.5 Elliptic Curve Encryption and Decryption

1. Every character on plaintext message m to be mapped as an x - y point P_m on the elliptic curve.
2. For encryption/decryption we require a point generator point G (which is generated by fingerprint of an authenticated user in this case), random number x and an elliptic group $E_p(a, b)$ parameters need to be known to both sender and receiver..
3. Each user A selects a private key n_A and generates a public key $P_A = n_A * G$.
4. To encrypt and send a message P_m to B , A chooses a random positive integer x and produces the cipher text C_m consisting to the pair of points $C_m = \{xG, P_m + xP_B\}$.
5. To decrypt the cipher text, B multiplies the first point in the pair by B 's secret key and subtracts the result from the second point






$$= P_m + xP_B - n_B(xG) = P_m + x(n_BG) - x(n_BG) = P_m$$



5. FLOWCHART

The overall process is shown in the following flow chart. The sample results of above process is shown in the table 1 and also output of the program is shown in Figure1

Table1

Image	Minutiae co-ordinates	New co-ordinates (nex,ney)	Mapped point on elliptic curve $y^2 \text{ mod } 79 = (x^3 + x + 1) \text{ mod } 79$
1.png 	(113,132,0.8502)	(53,76)	(53,75)
2.png 	(92,146,0.9581)	(17,73)	(20,68)
3.png 	(113,136,0.8570)	(53,1)	(53,4)
4.png 	(105,129,0.8653)	(42,71)	(47,67)
5.png 	(108,140,0.879)	(44,1)	(36,2)



6.png 	(106,157,0.96)	(33,8)	(32,4)
7.png 	(91,126,0.9130)	(21,59)	(18,59)

Figure1

```
adding all minutiae points
109,147,0.9167920666165611
newx:40,newy:3
minimum distance:4
minimum distance point or generator point G:(36,2)
private key of B:1
public key of B:(36,2)
random number x:20
```

```
public key Received: (36,2)
random no x:20
enter plain text to encrypt
qsdrewxc
point Pm:(28,63)
points xG,pm+xpB:(31,35)(72,58)
point Pm:(3,30)
points xG,pm+xpB:(31,35)(54,54)
point Pm:(33,42)
points xG,pm+xpB:(31,35)(47,67)
point Pm:(16,20)
points xG,pm+xpB:(31,35)(33,42)
point Pm:(54,54)
points xG,pm+xpB:(31,35)(2,13)
point Pm:(40,50)
points xG,pm+xpB:(31,35)(2,66)
point Pm:(5,62)
points xG,pm+xpB:(31,35)(47,12)
point Pm:(72,58)
points xG,pm+xpB:(31,35)(18,59)
```

```
point decrypted:(28,63)
point decrypted:(3,30)
point decrypted:(33,42)
point decrypted:(16,20)
point decrypted:(54,54)
point decrypted:(40,50)
point decrypted:(5,62)
point decrypted:(72,58)
```

6. CONCLUSION

Since the Generator Point obtained for a person finger print is Unique, so that we can authenticate encryption and decryption process of ECC. By using this method we can provides strong authentication to the data transfers.

REFERENCES

[1]. Biometrics and Biostatistics. <http://www.omicsonline.org/jbmbshome.php> 08.Biometrics for network security Paul Reid, 2004 b y Pearson education.

[2]. Anil k. Jain, fellow, IEEE, Arun Ross, member, IEEE," Biometrics: A Tool for information security" IEEE Transactions on information forensics and security. VOL.1.No.2.June 2006.

[3] AshwiniR.Patil,Mukesh A Zaveri,"A Novel Approach for Fingerprint Matching using Minutiae",IEEE Fourth Asia International Conference on Mathematical/Analytical Modelling and computer Simulation,2010.

[4] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall College, 2006.



- [5] U. Uludag, "Secure biometric systems," PHD thesis, Michigan state university, 2006.
- [6] Uludag.U,Pankanti.S.Prabhakar.S,Jain.A.K"Biometric cryptosystems: issues and challenges "Proceedings of IEEE, Vol 92, No.6, Pp 948-960, 2004
- [7] F Chafia ,CSalim and B Fraid ," Biometric crypto system for authentication" International Conference on Machine and Web Intelligence ,Pp434 -438,2010
- [8] A Jagadeesan, Dr K.Duraiswamy "Secured Cryptographic key generation from multimodal Biometrics:Feature Level Fusion of Fingerprint and Iris" in International Journal of computer science and information security,Vol 7,No 2,February 2010.
- [9] C Nandini and B.Shylaja "Efficient Cryptographic key generation from fingerprint using symmetric hash functions" in International Journal of Research and reviews in Computer Science. Vol 2,No 4 ,August 2011,ISSN:2079-2557.
- [10]. Erden,S.S., Yanik,T.Kog,G.K.:Fast finite Field multiplication In:C.K.Kog(ed).Cryptographic Engineering chapter 5.Springer(2009)
- [11]. RoliBansal,PritiSehgal,PunamBediin"Minutiae Extraction from fingerprint images- a Review" on International journal of computer science issues,vol 8,issue 5,no 3,September 2011.
- [12]. R.SashankSinghvi,SP. Venkatachalam and others in "Cryptography Key Generation using Biometrics".
- [13]. Yusupov S. Yu, Medetov S.K. in "Application of Biometric Methods in Cryptography.
- [14]. O. SrinivasaRaoet. al. / International Journal of Engineering Science and Technology Vol. 2(8), 2010, 3651-3656.
- [15] Rupam Kumar Sharma,generation of Biometric Key for use in DES", International Journal of Computer Science Issues (IJCSI) in volume 9 issue 6, November 2012, ISSN (Online):1694-0814