ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 1, July 2012

Enhancing Robustness of EC Cryptic Data using Forward Error Correction

Aanchal Aggarwal, Sunita Sangwan, Simerpreet kaur

Abstract: - With the explosion of networks and the huge amount of data transmitted along, the data content needs to be secured. Data encryption ensures security in open networks such as the Internet. With the fast development of cryptography research and computer technology, the cryptosystems such as of RSA and Diffie-Hellman require large number of bits so they became inadequate. The cryptosystem based on Elliptic Curve Cryptography is becoming the recent trend of public key cryptography. This paper presents the implementation of Elliptic Curve Cryptography by first transforming the message (text and image) into an affine point on the Elliptic Curve over the finite prime field. Here we illustrate the process of encryption of a text and image message and then a method for enhancing security using Forward Error Correction code for better error checking at the receiver side. This enables errors or noise added during transmission to be detected and corrected so that the receiver is receiving correct data and the received data matches with the sent data. Forward error correction is applied to progressive data to provide graceful degradation of text and image quality as packet losses increase.

Index Terms: **Convolutional Codes, Elliptic Curve Cryptography, Forward Error Correction, Viterbi Decoder.**

I. INTRODUCTION

With the popularity of computers and Internet, real time multimedia data is represented in digital forms to be transmitted on Internet. Digitized data can be texts, images, audios/videos. It is important to send the digital data securely. Cryptography is the science of converting data in non understandable form for the unintended viewers for securely transmitting messages between a sender and a receiver. The objective is to encrypt the message in a way such that an eavesdropper would not be able to read it. A cryptosystem is a system of algorithms for encrypting and decrypting the messages for this purpose Randomness is a key ingredient for cryptography. The cryptosystem requires the generation of a new random number each time a new message is encrypted. In traversing the network, a packet is sent from computer to computer until it arrives at its destination. However, when the number of packets sent exceeds transmission capacity, packets are discarded at random, causing loss of data and most likely decoding failure if the lost data are not retransmitted. Each packet can be assigned a unique sequence number, so it is known which packets are received and which are lost. In networks in which packets are discarded at random, there is no way to specify the importance of a particular packet. Usually, however, the data that we transmit vary in importance. Such a network strategy needs to quantify the importance of different chunks of data and, as channel conditions degrade, discard the least important data while retaining the most important data. In this paper, we describe the framework that signcrypts the text and image data and assigns unequal amounts of error correction to text and images that are compressed with an unmodified progressive algorithm and are transmitted over lossy packet networks without using feedback. Our scheme is modular in that we are using progressive algorithm and have graceful degradation of text and image quality with increasing packet loss rate.

OBJECTIVES

The aim of this paper is threefold.

1. To facilitate deployment of ECC [1] by completely specifying efficient, well-established, and well understood public-key cryptographic schemes based on ECC.
2. To increase the security of the transmitted data across the channel and ensuring correct decryption of data by the receiver using error correction scheme.
3. To compare the results of encoding and decoding of text and images for two cases:
   a) In the case where ECC is used without error correction code.
   b) In the case where Forward Error Correction is used Together with ECC.

II. PRINCIPLES OF ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) can be categorized as public cryptography with its many advantages over the other public cryptography. After it was first proposed by Koblitz and Miller [2]. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements. Elliptic curve is a plane curve defined by Weierstrass equation:

$$y2 + axy + by = x3 + cx2 + dx + e \quad (1)$$

If F is a field and a, b, c, d and e belong to F, number pair, (x, y), which is satisfied with the equation (1), is called a point on the curve. When the characteristic of equation (1) does not equal to 2 and 3, the equation can be simplified as follows:

$$y2 = x3 + ax + b, a, b \in F \quad (2)$$

For elliptic curves over prime fields GF(p) with p>3, the parameters a and b of equation (2) should satisfy

$$4a3 + 27b2 \neq 0 \bmod p \; . \quad (3)$$

The condition is required to ensure that the curve is smooth, and there are no points at which the curve has two or more distinct tangent lines. As the order of elliptic

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 1, July 2012

curves is 3, there must be the third point on the elliptic curves if a line has two intersection points with an elliptic curve. The points on the elliptic curve form an addition group, an Abel group. The addition rule of two points is explained in the following way. Suppose two points P and Q are on the elliptic curve and P is not equal to Q, first we draw a line passes these two points, then compute the intersection point T of the line and the curve, after this, draw a line passing point T, which is paralleling Y coordinate, finally compute the intersection point R of the line and the curve, and point R is the very result we want, that is to say, R = P+Q. If P is equal to Q, first of all, we draw a tangent line of the curve at point P, then compute the intersection point T of the line and the curve, after this, draw a line passing point T, which is paralleling Y coordinate, finally, compute the intersection point R of this line and the curve, and point R is the very result we want to compute, and that is to say, R = 2P. The computing procedure is demonstrated as follows.[3]

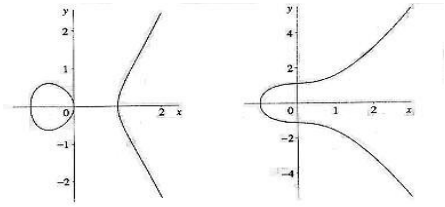

Fig 1. Elliptic Curves of y2=x3-x, y2=x3+x/4+5,

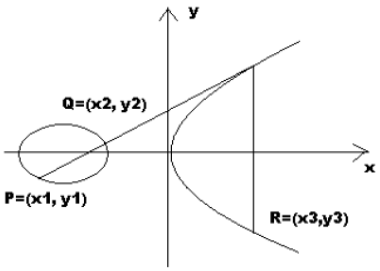

Fig 2. Point Plus on an Elliptic Curve

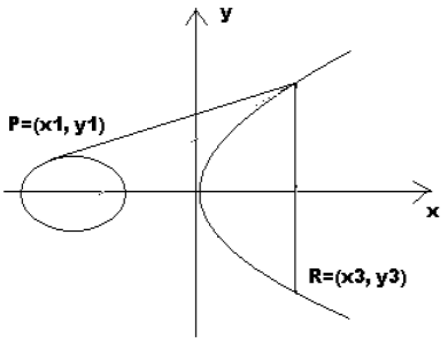

Fig 3. Point Double on an Elliptic Curve

III. LITERATURE SURVEY

A paper named "Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications" studied the encryption and decryption of the text with simple example and the work is extended to the image applications.. [4]

A paper named "Implementation of elliptic curve cryptography on text and image" studied application of Elliptic Curves over finite fields for traditional key exchange and encryption of text. It has implemented both and proposed a scheme for encryption of images..[5]

A paper named "Fast Scalable Implementation of Elliptic Curve Cryptosystem on NIST Prime Field" has studied carefully the principles of Elliptic Curve Cryptosystems, and the file of FIPS Federal Information Processing Standards, published at 2000 January 27. It is about Digital Signature Standard (DSS) published by U.S. Department of Commerce/National Institute of Standards and Technology.. [6]

A paper named "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography" was implemented in which each character in the message is represented by its ASCII value. Each of these ASCII value is transformed into an affine point on the EC, by using a starting point called Pm [7] .

IV. RESEARCH METHODOLOGY

First the implementation of the text and image based cryptosystem has been done by performing encryption and decryption using keys. Then some enhancements to the code are done by adding Error checking and correcting code like Forward error correction code. In the previous works of elliptic curve cryptography over text and image messages, the noise factor was not taken into consideration, but it is a major factor in security of signcrypted message. The encrypted message will not decrypt or will be received with changes if noise in the channel of transmission [8] is introduced .We illustrate this procedure in the fig 8.

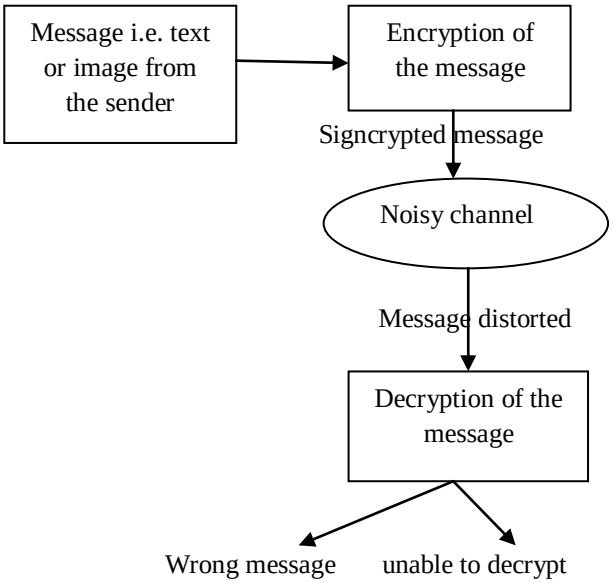

Fig 4. Block Representation of Noisy Channel Transmission of Message

The research will include enhancing the security of Elliptic Curve encrypted data. The basic programmes are:

1. Key generation
2. Encryption

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 1, July 2012

3. Error Correction
4. Decryption

The technique that is being used for enhancing the security is the Forward Error Correction scheme which is both a parity checker and corrector [9] which automatically removes noise from the code and returns the accurate code to the receiver for decryption and tries to give 100% accurate result.

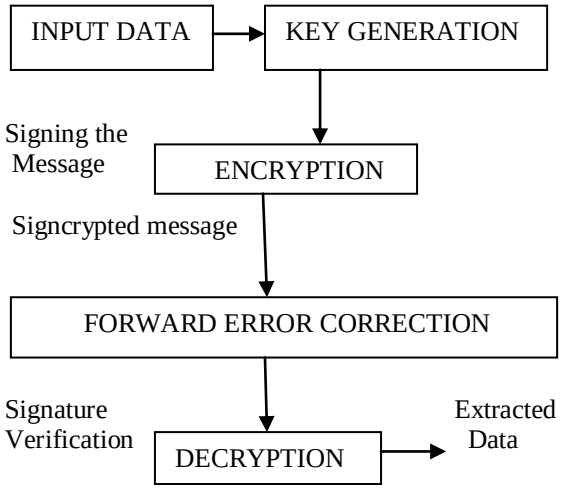

Fig 5. Block Representation of the Proposed Work

In this work Convolutional encoder and Viterbi decoder are being used.

A. Viterbi Algorithm

A Viterbi algorithm [10] consists of the following three major parts:

1. **Branch metric calculation** – calculation of a distance between the input pair of bits and the four possible "ideal" pairs ("00", "01", "10", "11").
2. **Path metric calculation** – for every encoder state, calculate a metric for the survivor path ending in this state (a survivor path is a path with the minimum metric).
3. **Traceback** – this step is necessary for hardware implementations that don't store full information about the survivor paths, but store only one bit decision every time when one survivor path is selected from the two.

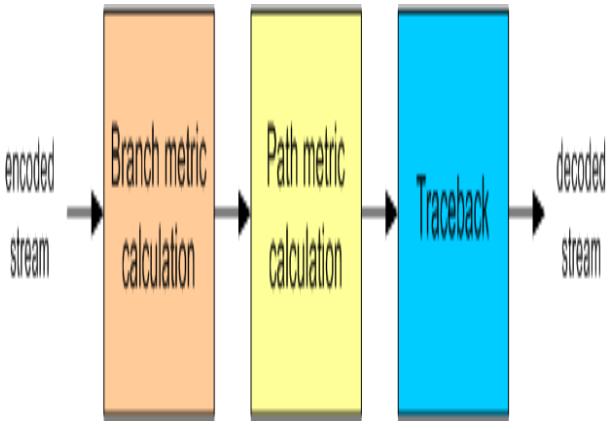

Fig 6. Viterbi Decoder Data Flow

B.Tool Used

Matlab 7.6 is used for the implementation of the work. Matlab is an ideal tool for simulating digital communication systems. This tool provides an easy scripting language and excellent data visualisation capabilities [11].

C. Generation of Points for Elliptic Curve

Table I. Set of Sample points on Elliptic Curve for text message

(0,1)	(34,5)	(21,25)	(21,12)
(25,0)	(25,0)	(6,36)	(6,1)
(1,15)	(1,22)	(24,14)	(24,23)
(26,18)	(26,19)	(8,15)	(8,22)

Table II. Set of Sample Points on Elliptic Curve for Image Message

(34,5)	(17,26)	(35,18)	(35,19)
(2,13)	(2,23)	(27,8)	(27,29)
(19,16)	(19,21)	(36,6)	(36,31)
(11,14)	(11,23)	(33,9)	(33,28)

A. Calculation Of Bit Error Rate

The formula for error rate calculation is as given below :

$$Error\ rate = (Total\ bits - error\ bits)\ /Total\ Bits * 100$$

Where, Total Number of bits = 336
Total number of characters = 42

Error rate calculation without error correction code

Table III. Representation of Error Bits and Bit Error Rate With 1% Error

Error Bits (1% error)	Character Error
4	2
9	4
2	2
5	4
5	3
Mean=5 **BER**=98.6%	Mean=.3

Table IV. Representation of Error Bits and Bit Error Rate With 2% Error

Error Bits (2% error)	Character Error
10	4
11	8

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 1, July 2012

5	4
9	9
12	11
Mean=9.4 **BER**=97.4%	Mean=7.2

Error rate calculation with error correction code

Table V. Representation of Error Bits and Bit Error Rate With 1% Error

Error Bits (1% error)	Character Error
3	1
7	2
0	0
5	1
1	1
Mean=2 **BER**=99.4%	Mean=.8

Table VI. Representation of Error Bits and Bit Error Rate With 2% Error

Error Bits (2% error)	Character Error
8	2
11	2
3	1
2	1
0	0
Mean=3.1 **BER**=99.1%	Mean=1

V. TEXT ENCRYPTION AND DECRYPTION

The message to be encrypted is encrypted using the points on elliptic curve and then the message is sent over the noisy channel to the receiver. The results of decryption are compared and lesser error in message is found at the same noise level after introducing error correction code together with elliptic curve cryptography.

A. Result of Text Encryption and Decryption With Noise Added Without Error Correction Code

Text message to be encrypted sent over the channel to the Receiver Encryption Encrypted message Decryption Decrypted message with error due to noise added

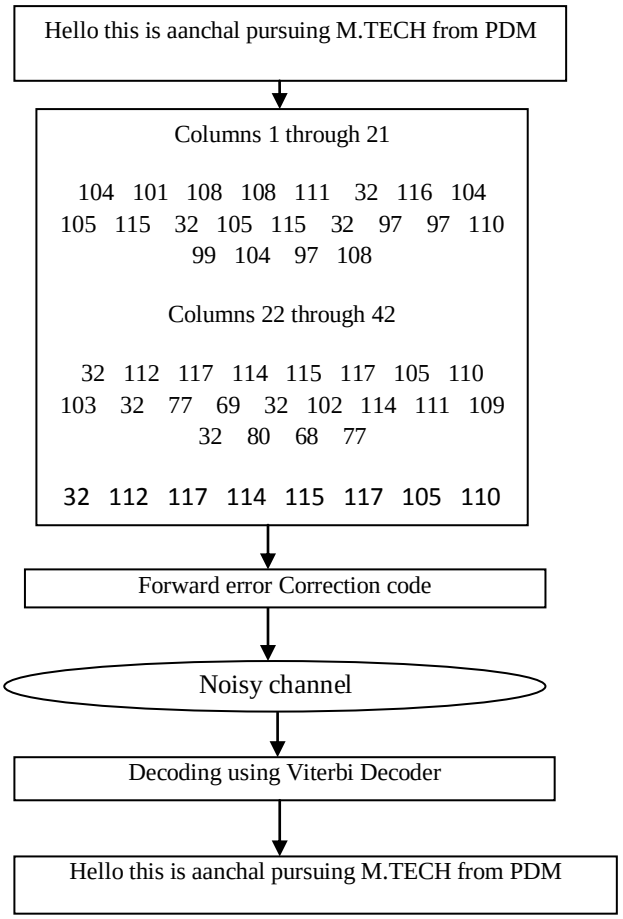

Fig 7. Text Cryptography without Error Correction Code

B. Result of Text Encryption and Decryption With Error Correction Code

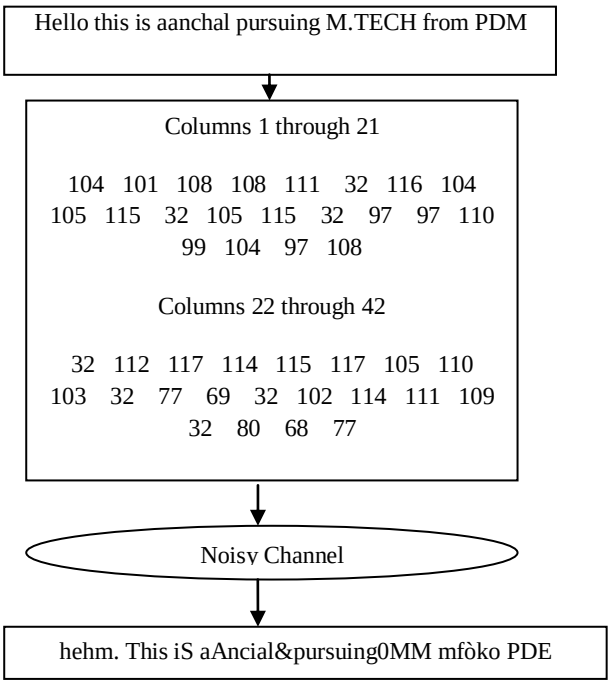

Fig 8. Text Cryptography without Error Correction code

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 1, July 2012

Text message to be encrypted sent over the channel to the Receiver Encryption Encrypted message Channel encoder Decryption Decrypted message without error

VI.IMAGE ENCRYPTION AND DECRYPTION

In our work we have performed encryption and decryption of text and image .Here we give a brief description of the image signcryption. The image is selected and first it is transformed into a black and white image over the finite fields [12] and then it is signcrypted using the points on the elliptic curve .The image is hidden after the sender sends it over the network and then the key exchange takes place between the sender and receiver so that the intended receiver can easily decrypt the image, we illustrate this procedure with a pictorial view of the snapshots from our work as follows.

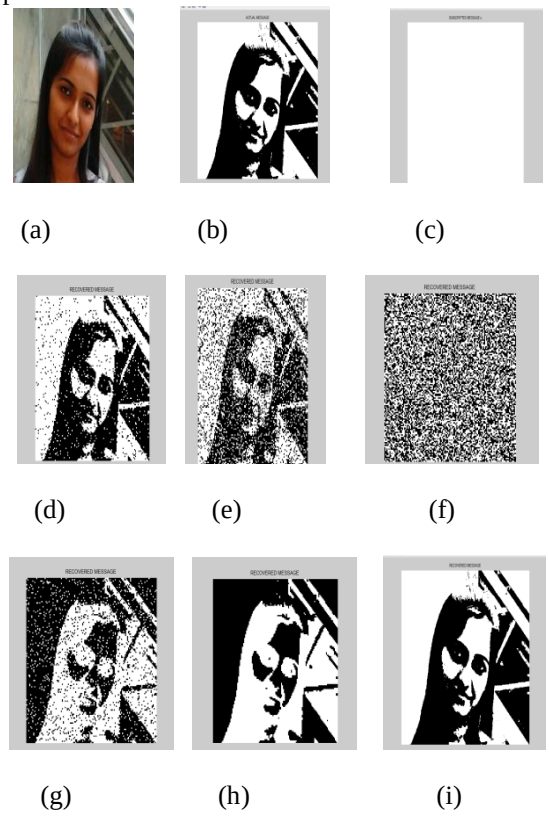

Fig 9. Representation Of Image Encryption and Decryption (A) Actual Image (B) Black and White Conversion Of Actual Image (C) Signcrypted Image (D),(E),(F),(G),(H) Recovered Distorted Images Without Error Correction Code With 2% ,4%,5%,9%,10% Noise (I) Recovered Actual Image With Error Correction Code Without Noise.

VII. NEED FOR ERROR CORRECTION

Whenever we pass the message over the network then some amount of packet loss or change of message is possible due to noise .So in such cases we need to provide some measures to recover the original message ,so that the actual message is not lost or a different message is not received at the receiver side .For this we are proposing forward error correction mechanism over the encrypted message which works over a large domain of the field of elliptic curve and provides checking and correcting of the message ie. Text or image upto a certain extent suitable to the environment of the signcryption and tries to provide accurate results.

VIII. DISCUSSIONS & CONCLUSION

In this research, an Elliptic Curve Cryptosystem is proposed together with an Error correction which corrects the error from noisy data. The encryption and decryption of the text and image is demonstrated. For the text applications, each character in the message is represented by its ASCII value. First the encryption process is applied, and then to recover the information from the encrypted version, we apply the decryption process of ECC. Lastly by using the discrete logarithm concept, it is possible to evaluate the ASCII value and thereby recover the plaintext. Hence the keys are transformed over the EC field for both encryption and decryption. This promises to afford maximum security from intruders and hackers. Convolutional encoding and decoding [13] with Viterbi decoder is used for error correction of the encrypted message i.e. Text and image. Thus a better degree of encryption and decryption with Elliptic curve cryptography and better error correction is achieved with Forward error correction code. The work can be extended in future for video files and some different coding schemes can be used which could provide more accurate results.

ACKNOWLEDGMENT

The authors are grateful to the P.D.M College of engineering for extending all the facilities and constant encouragement for carrying out this research work.

REFERENCES

[1] Charles Wang, Dean Sklar, Diana Johnson (Winter2001/2002).Coding". Crosslink—The Aerospace Corporation magazine of advances in aerospace technology (The Aerospace Corporation) 3 (1). "How Forward Error-Correcting Codes Work".

[2] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, volA8, 1987, pp.203 -209.

[3] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, Software Implementation of Elliptic Curve Cryptography over Binary Fields,2000,http://citeseer.ist.psu.edu/hankerson00software.html

[4] S.Maria Celestin Vigila1and K. Muneeswaran2 "Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications", International Journal of Network Security, Vol.14, No.4, PP.240-246, July 2012.

[5] Mrs. Megha Kolhekar and Mrs. Anita Jadhav "implementation of elliptic curve cryptography on text and image", International Journal of Enterprise Computing and Business Systems ISSN (Online): 2230-8849 Vol. 1 Issue 2 July 2011.

[6] Guicheng Shen and Bingwu Liu, "Research on "Fast Scalable Implementation of Elliptic Curve Cryptosystem

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 1, July 2012

on NIST Prime Field", ©2011 IEEE.

[7] S.Maria Celestin Vigila1, K. Muneeswaran' "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography", ©2009 IEEE.

[8] G.M. Davis, J. M. Danskin, and X. Song, "Joint source and channel coding for Internet image transmission," in Proc. ICIP, vol. 1, Sept. 1996, pp. 21–24.

[9] Shu Lin, Daniel J. Costello, Jr. (1983). Error Control Coding: Fundamentals and Applications. Prentice Hall. ISBN 0-13-283796-X.

[10] Viterbi Algorithm for Decoding of Convolutional Codes – By core technologies.

[11] Christos Xenophontos: A Beginner's Guide to MATLAB Department of Mathematical Sciences.

[12] B.Sklar: "Digital Communication", Pearson's Publication, Edition 2.

[13] H. D. Lin and D. G. Messerschmitt, "Algorithms and architectures for concurrent Viterbi decoding," in Proc. IEEE Int. Conf. Commun., Jun. 1989, pp. 836–840.

AUTHOR'S PROFILE

Aanchal Aggarwal completed the B.Tech. Degree in Computer Science and Engineering in 2010 from Rajasthan technical University and currently pursuing M.Tech. Degree in Computer Science and Engineering from M.D.U (Rohtak). Presently Assistant Professor in the Department of Computer Science, P.D.M College of Engineering, Bahadurgarh, Rohtak. The research interest includes Cryptography and Network Security, Wireless Networks and Information Hiding.

Sunita Sangwan, completed the B.Tech. Degree in Computer Science and Engineering in 2003 from M.D.U (Rohtak) completed M.Tech. Degree in Computer Science and Engineering in 2008 from M.D.U (Rohtak).. Presently Assistant Professor in the Department of Computer Science, P.D.M College of Engineering, Bahadurgarh, Rohtak.

Simerpreet kaur completed the B.Tech. Degree in Computer Science and Engineering in 2005 from M.D.U (Rohtak), completed M.Tech. degree in Computer Science and Engineering in 2010 from M.D.U (Rohtak). Presently Assistant Professor in the Department of Computer Science, P.D.M College of Engineering, Bahadurgarh, Rohtak.