Secure Data Hiding using Elliptical Curve Cryptography and Steganography

Hemanta Kumar Mohanta
M. Tech, CST, GITAM University
Visakhapatnam, India

ABSTRACT
Now these days information are passing by internet. Hence the security of information has become a fundamental issue. Cryptography is the well-known technique to secure data over network. Steganography is the technique to hide the message in digital media. The elliptical curve cryptography is more secure than the existing cryptography models. This paper describes a proposed hybrid model using public key Elliptical Curve Cryptography (ECC) and Steganography. Which provide more security than a Single ECC or Steganography methods. The main aim of this project is to hide crucial information of internet users, military, different corporate sectors those which are frequently using public network for communication.

Keywords
Cryptography, Steganography, ECC, RGB, LSB, CNOT gate and PSNR

1. INTRODUCTION
The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of information hiding.

Cryptography is the process by which the data to be transmitted is hidden in a manner such that only the intended recipient can understand it. The initial data is called as plaintext and the encrypted data is called as cipher text. A key is used to hide the data [1]. There are different types depending on the number and way in which the keys are used.

There are two types of cryptographic techniques:

(i) Symmetric key cryptography

(ii) Asymmetric key cryptography

Symmetric Key Cryptography is actually the technique by which identical cryptographic keys are used for the purpose of both encryption and decryption. The receiver can get back original data by using the key. The symmetric key cryptography provides high data rates, usage as primitives to construct various cryptographic mechanisms and can be combined to produce stronger ciphers. The main fact here is that the security of data depends on the security of the key. So, care should be taken while exchanging keys between the sender and the receiver [2].

Symmetric cryptosystem have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will able to tap communication channels. So the only secure way of exchanging keys would be exchanging personally. Symmetric cryptosystem can't provide digital signatures that can't be repudiated [3].

Asymmetric key cryptography is the technique where two keys are used. One key is used to lock or encrypt the plaintext, and another to unlock or decrypt the cipher text. Neither key can do both the functions. One of these keys is published or made public and the other is kept private. This technique has comparatively slower data rate throughputs than the symmetric key technique [2].

Steganography is the art and science of hiding information such that its presence cannot be detected. A secret information is encoded in a manner such that the very existence of the information is concealed. Paired with existing communication methods, Steganography can be used to carry out hidden exchanges.

This proposed hybrid model is a combination of Elliptical curve cryptography (ECC) and Steganography. As per previous study, key size of ECC is very less in comparison to RSA [11]. The comparison between ECC and RSA algorithms are stated in table 1. Using Steganography we can send multiple messages inside a cover image. The proposed model is described in section 3 and the experimental result is in section 4.

Table 1. Comparison between ECC and RSA

ECC key size in bits	RSA key size in bits
106	512
112	768
132	1024
160	2048
210	3072
283	7680

2. RELATED WORK
2.1 Elliptical Curve Cryptography
Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields [13].

2.1.1 Different Operation on Elliptic Curve
Let E be the elliptic curve over finite field P over equation $y^2 = x^3+ax+b$ and satisfy $4a^3+27b^2 \neq 0 \pmod{p}$. The operations are point addition, point doubling and scalar multiplication.

2.1.1.1 Point Addition:
1. let $A(x_1,y_1)$ point ∞ is the point at infinite are in E(P)

$$A(x_1,y_1)+\infty = \infty + A(x_1,y_1) = A(x_1,y_1) . \quad (1)$$

2. let $A(x_1,y_1)$ and $B(x_2,y_2)$ are Two points and the resultant

point is $R(x_3,y_3)$ for all points in E(P)

$A(x_1,y_1)+B(x_2,y_2)=R(x_3,y_3)$

Where $x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2$, and $y_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3)-y_1$ (2)

2.1.1.2 Point Doubling

let $A(x_1,y_1)$ be the point in E(P) then

$2A=R(x_3,y_3)$

Where $x_3=\left(\frac{3x_1^2+a}{2y_1}\right)-2x_1$ and $y_3=\left(\frac{3x_1^2+a}{2y_1}\right)-(x_1-x_3)-y_1$ (3)

2.1.1.3 Point Subtraction

Let $A(x_1,y_1)$ and $B(x_2,y_2)$ are Two points and the resultant point is $R(x_3,y_3)$ for all points in E(P)

$R(x_3,y_3) = A(x_1,y_1) –B(x_2,y_2) = A(x_1,y_1) +\{– B(x_2,y_2)\}$

$= A(x_1,y_1) +B(x_2, –y_2)$

For any point $–A\ (x_1,y_1) = A(x_1, –y_1)$

2.1.1.4 Point Multiplication

Let A be any point on the elliptic curve (E). Then the operation multiplication of the point A is defined as repeated addition. kA = A+ A + ...k times.

Where k the integer in the field P.

2.1.2 The ElGamalcryptosystem [4] using an elliptic curve over F (p) or F (2^n)

A. Generating public and private keys

1. Bob chooses E (a, b) with an elliptic curve over F (p) or F (2^n).
2. Bob chooses a point on the curve, $e_1(x_1, y_1)$.
3. Bob chooses an integer d.
4. Bob calculate $e_2(x_2, y_2)$ =d × $e_1(x_1, y_1)$.Note that multiplication here means multiple addition of points.
5. Bob announce E (a, b), $e_1(x_1, y_1)$, and $e_2(x_2, y_2)$ as his public key;
6. Bob keeps d as his private key.

B. Encryption

1. Alice select P, a point on the curve, as her plaintext, P.
2. She then calculates a pair of points on the text as cipher texts:
   - I. C_1= r ×e_1
   - II. C_2= P + r ×e_2

C. Decryption

1. Bob after receiving C_1 *and* C_2 ,calculates P, the plaintext using the following formula.
   - P = C_2- (d× C_1)

2.2 Steganography

The simplest approach to hiding data within an image is called least significant bit (LSB) insertion [5][14]. For 24-bit true color image, the amount of changes will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Now suppose we want to hide the following 9 bits of data101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed) pixels:

10010101	0000110**0**	11001001
1001011**1**	0000111**0**	1100101**1**
10011111	00010000	11001011

The following formula provides a very generic description of the pieces of the steganographic process:

Stego-image = cover image + information

Information maybe text OR image etc.

2.2.1 CNOT Gate

CNOT gate is also called as Controlled not gate [7][12]. It comes under quantum computer. It is essential for constructing a quantum computer. Inside the CNOT gate, first qbit is control bit and the second bit is a target bit [7].

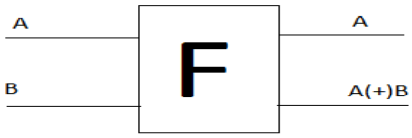

Figure 1: CNOT gate

Where, A be the control qbit, B be the target qbit, and (+) represents as EXOR. CNOT gate is completely different from the EX - OR gate. The EX-OR gate is irreversible gate, then the CNOT gate is reversible gate [7].

2.2.2 Wavelet Transformation

Wavelet compressions are two types lossless or lossy[12]. In lossless compression, the original data can be reconstructed from the compressed data, but in lossy compression the partial data can be reconstructed. Using wavelet transformation the data can be stored in less space, by doing so the memory space will be reduced and the data can be transferred easily [8]. Steps in wavelet compression: Load the image, perform wavelet decomposition of the image, and compress using fixed threshold.

2.2.3 Random Number Generators

Blum Blum Shub generator, is the pseudo random number generator [12]. By using this random numbers are generated. The formula has shown below [9],

$$X_{i+1} = (X_i)^2 \ mod\ n \quad (4)$$

Where, X_i is the seed, and n be the range.

The pseudo random bit generator is used for generating random numbers in cryptography. Seed, two large prime numbers, and the range is the inputs for the pseudo random bit generators. The mathematical formulae has shown below,

$$X_{i+1} = (PX_i + Q)^2 \ mod \ n \quad (5)$$

Where P, Q are two large prime numbers, X_i is the seed. n be the range.

2.2.4 Encryption Algorithm

The secret information may be in any form like text, image etc. is compressed by wavelet transforms [10]. The compressed text is converted into its corresponding ASCII value, next the ACSII is converted into its 8-bit binary value. By using Control NOT gate, the 8-bit binary value is encoded. Now these bits are ready to embedded into an image using LSB insertion. The encrypted message is ready to be embedded in the cover image. Before embedding the message, the image is converted into its corresponding pixel values. These values are arranged in the r × c matrix form, r and c represent rows and columns respectively. The bit of the secret information has to be embedded in the random positions in the cover image. To identify the random positions, Random number generator is used. Random numbers act like a key in this technique. Blum/blum/shub generator and Pseudo random generator are used to se1ect the random rows and columns respectively. Random numbers are generated by the generator, using the key (seed). Randomness will be varying from generator to generator. The randomness is achieved by padding the bits in the sequence. After selecting the random positions in the image (pixel values) now the secret message is embedded in the corresponding bits using the LSB insertion technique.

2.2.5 Decryption Process

Decryption is the repeal process of the encryption process[10]. After receiving the stego image, the receiver will convert the image into its corresponding pixels (matrix form). With the help of Key (seed) the receiver will be generating the random number using the random generators to identify in which positions the bits have been embedded. After getting the pixel positions, applying reverse LSB insertion technique will give the encoded bits. Applying the Control NOT gates on the encoded bits, the compressed text is retrieved. By applying wavelet, transformation technique (decompression) the original secret information is retrieved.

3. PROPOSEDMODEL

In the proposed model elliptic curve parameters are(p, E, P, n,) where p is the prime number F_p denoted as field of integers modulo p. E is the elliptic curve over F_p is defined by the equation $y^2=x^3+ax+b$ where (a,b) are the real numbers over F_p and satisfy $4a^3+27b^2 \neq 0$ (mod p). The point infinity ∞ is also in the curve. The abelian subgroup of $E(F_p)$ generated by p is

P={∞, *P,2P,3P,……(n-1)P*}

3.1 Key generation

Input:

Elliptic Curve Domain parameters (p, E, P, n,)

Output:

Public key Q and private key d.

1. Select $d \in_R [1, n-1]$
2. Select $e_1(x_1, y_1)$.
3. Compute $e_2(x_2, y_2) = d \times e_1(x_1, y_1)$
4. Q = $\{e_1, e_2, E\}$
5. Return(Q, d)

3.2 Encryption and LSB Embedding

INPUT:

Elliptic Curve Domain parameters (p, E, P, n), public key Q, Plaintext m, message image I, Cover image C.

OUTPUT: Stego-image CI, Stego key

1. Represent the message 'm' as a point M in E (F_p).
2. Select $K \in_R [1, n-1]$.
3. Compute $C_1 = k \times e_1(x_1, y_1)$
4. Compute $C_2 = M + k \times e_2(x_2, y_2)$.
5. RGB cover image=C.
6. Hide (C_1, C_2) into I using LSB Steganography.
7. Hide I into C using Steganography.
8. Return (CI)

3.3 Decryption

INPUT:

Elliptic Curve Domain parameters (p, E, P, n), Private key d, stego-image CI, stego key.

OUTPUT: (message m, image I)

1. Extract I from CI Extract C_1, C_2 from I
2. Compute $M = C_2 - d \times C_1$ and compute m from M
3. Return (m, I)

3.4 Background work

Consider the elliptical curve is $y^2 = x^3 + 4x + 20$ over finite field F_{29}

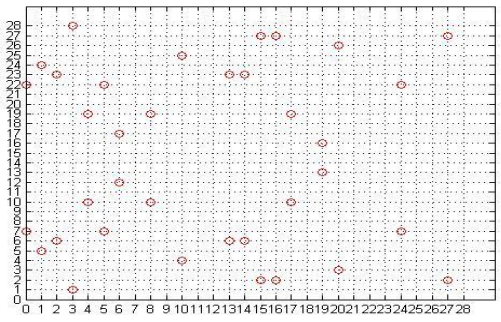

Figure 2. Points on the curve $y^2 = x^3 + 4x + 20$ mod 29

Points are[(∞),(1,5),(4,19),(20,3),(15,27),(6,12),(17,19), (24, 22),(8,10),(14,23),(13,23),(10,25),(19,13),(16,27),(5,22)(3,1),(0,22),(27,2),(2,23),(2,6),(27,27),(0,7),(3,28),(5,7),(6,2),(19,16),(10,4),(13,6),(14,6),(8,19),(24,7)(17,10),(6,17),(15,2),(20,26),(4,10),(1,24),(20,3)]

Table 2: Different points in elliptical curve mask different characters.

∞	1,5	4,19	20,3	15,27	6,12	17,19
a	b	c	d	e	f	g
24,22	8,10	14,23	13,23	10,25	19,13	16,27
h	i	j	k	l	m	n
5,22	3,1	0,22	27,2	2,23	2,6	27,27
o	p	q	r	s	t	u
0,7	3,28	5,7	6,2	19,16	10,4	13,6
v	w	x	y	z	0	1
14,6	8,19	24,7	17,10	6,17	15,2	20,26
2	3	4	5	6	7	8
4,10	1,24	20,3				
9	space	.				

3.4.1 Key generation

For elliptic curve $y^{2} = x^{3} + 4x + 20$ over finite field F_{29}

1. Bob chooses E (a, b) with an elliptic curve over F_p a =4, b=20,p=29
2. Bob chooses a point on the curve, $e_1(x_1, y_1)$.

   let(1,5)
3. Bob chooses an integer d. Let d = 3
4. Bob calculate $e_2(x_2, y_2)$ =d × $e_1(x_1, y_1)$.Note that multiplication here means multiple addition of points.$e_2(x_2, y_2)$=(20,3)
5. Bob announce E (a, b), $e_1(x_1, y_1)$, and $e_2(x_2, y_2)$, p as his public key;E(4,20),e_1(1,5),e_2(20,3)
6. Bob keeps d as his private key.

3.4.2 Encryption

INPUT :(cover image C, image I, message 'm')

OUTPUT: (stego object CI)

1. Alice selects P, a point on the curve, as her plaintext, P. EXAMPLE Message=hello P1=(24,22),P2=(15,27),P3=(10,25),P4=(10,25), P5=(5,22)
2. She then calculates a pair of points on the text as cipher texts:

   III. $C_1 = r \times e_1$

   IV. $C_2 = P + r \times e_2$

Table 3: Encryption process of above example

points	r	$C_1 = r \times e_1$	$C_2 = P + r \times e_2$	(C_1, C_2)
h=P1(24,22)	2	(4, 19)	(13, 23)	(c, k)
e=P2(15,27)	6	(17, 19)	(3, 28)	(g, w)
l=P3(10,25)	5	(6, 12)	(10, 4)	(f, 0)
l=P4(10,25)	15	(3,1)	(2,6)	(p ,t)
o=P5 (5,22)	3	(20, 3)	(5, 7)	(d, x)

3. Separate all C1, C2 and make array of

   C1* ∈{$C1_1$, $C1_2$, $C1_3$……}

   C2* ∈{$C2_1$, $C2_2$, $C2_3$……} respectively.
4. Embedded C1* and C2* into the image I
5. Choose one cover image C
6. CI = Embedded I into C

3.4.3 Decryption

INPUT: stego-object, stego key

OUTPUT: message 'm'

To extract the cipher text and image from stego object ,the stego key is used that used to construct a stego object.

To get the text message from cipher text we use private key that is

$M = C_2 - d \times C_1$

Consider the above example

Table 4: Decryption process of the example

(C_1, C_2)	$C_2 - d \times C_1$	P	M
(c, k)	(13, 23) – 3 × (4, 19)	(24, 22)	h
(g, w)	(3, 28) – 3 × (17, 19)	(15, 27)	e
(f, 0)	(10, 4) – 3 × (6, 12)	(10, 25)	l
(p ,t)	(2,6) – 3 × (3,1)	(10,25)	l
(d, x)	(5, 7) – 3 × (20, 3)	(5, 22)	o

Output message m = (hello)

4. EXPERIMENTAL RESULT

The above stated hybrid method was applied to the message as shown in figure (3).The cover image used for this process is shown in figure (4). Total process of the entire method is shown in figure (5).

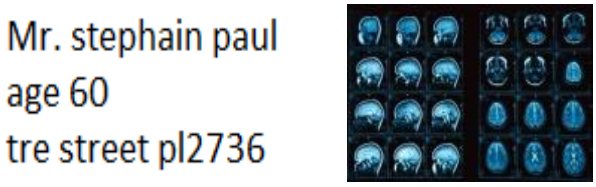

Figure 3. Patient information and brain MRI scan

Figure 4. Cover image (animal.jpg)

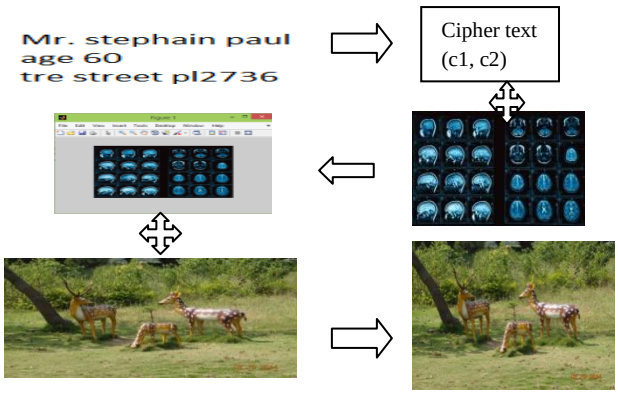

Figure5. Total process of proposed model

The cover image is the main image in which the hidden information will be embedded. The resultant image is the stego image which is the same type of image as the cover image. To measure the quality of stego image, Peak Signal-to-Noise Ratio (PSNR) is calculated. PSNR is a statistical measurement used for digital image or video quality assessment [6]. PSNR is most easily defined via the mean squared error (MSE) which for two m×n monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - k(i,j)]^2 \qquad (6)$$

The PSNR is defined as:

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20\ \log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right) \qquad (7)$$

Larger PSNR indicates better quality of the image or in other terms lower distortion. The larger the PSNR value the smaller the possibility of visual attack by human eye.

Table 3 Represent the PSNR value after embedding different size of input data and image into cover image.

Table5. PSNR table

Cover image size(pixel)	input		PSNR
	Text(bytes)	Image(pixel)	
800x600	84	294x184	56.3741
800x600	168	294x184	56.3747
800x600	168	256x256	55.5312
800x600	848	256x256	55.5314
800x600	2539	256x256	55.5310

5. CONCLUSION

The proposed model introduced above is a combination of cryptography and Steganography. The goal of the technique is to put the unauthorized person in a difficult position to determine the presence of information. The dual security makes the information more secure. With this model any one can easily send multiple information to the receiver using public network. This model is very useful for defense, corporate, banking, communication and different government portals where information exchange is more crucial. The data hiding capacity in audio and video is more than image, so in future using audio or video steganography and cryptography huge amount of data will transmit in public network without security violence.

6. ACKNOWLEDGEMENT

The author would like to thank Ms. J. Hyma, assistant professor, cse department, GITAM University, for various help and guidance.

7. REFERENCES

[1] M. M Amin, M. Salleh, S .Ibrahim, M.R.K atmin, and M.Z.I.Shamsuddin, Information Hiding using Steganography, National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003 IEEE.

[2] S Ushll , G A SathishKumal, K Boopathybagan,A Secure Triple Level Encryption Method Using Cryptography and Steganography, 20 II International Conference on Computer Science and Network Technology, 978-1-4577-1587-7/111$26.00 ©20111EEE, December 24-26, 2011

[3] X. Zhang and S. Wang, Steganography using multiple-base notational system and human vision sensitivity, IEEE Signal Process. Lett., vol.12, no. I, pp. 67-70, Jan. 2005.

[4] BehrouzA.Forouan, Debdeep Mukhopadhyay, 2nd edition Cryptography and network security, McGraw Hill Education, pp.295-296

[5] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, A New Approach for LSB Based Image Steganographyusing Secret Key987-161284-908-9/11/$26.00 2011 IEEE

[6] M. Hossain, S.A. Haque, F. Sharmin, Variable RateSteganography in Gray Scale Digital Images Using Neighborhood Pixel Information, Proceedings of 200912th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.

[7] Controlled NOT gate, From Wikipedia, http://en , wikipedia . org/wiki/Controlled_NOT _gate .

[8] Ivan W. Selesniek "Wavelet Transforms A Quick Study", Physies Today magazine, üetober, 2007.

[9] "Blum Blum Shub", From Wikipedia, http://en.wikipedia.org/wiki/Bluffi_Bluffi_Shub

[10] R Praveen Kumar, V Hemanth, MShareef, Securing Information Using Sterganoraphy, 2013 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013]

[11] Ipsita sahoo , SEMINAR REPORT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS http://www.facweb.iitkgp.ernet.in/~isg/ICTSEMINAR/REPORT-Ipsita.pdf

[12] M Venkteswara Reddy, M Lakshman Naik, Securing Information Using Steganography, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[13] Darrel Hankerson, Alfred Menezes, Scott Vanstone, Guide to elliptic curve cryptography, springer

[14] Ahaiwe J. Document Security within Institutions Using Image Steganography Technique, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064