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].

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>
<thead>
<tr>
<th>ECC key size in bits</th>
<th>RSA key size in bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>106</td>
<td>512</td>
</tr>
<tr>
<td>112</td>
<td>768</td>
</tr>
<tr>
<td>132</td>
<td>1024</td>
</tr>
<tr>
<td>160</td>
<td>2048</td>
</tr>
<tr>
<td>210</td>
<td>3072</td>
</tr>
<tr>
<td>283</td>
<td>7680</td>
</tr>
</tbody>
</table>

2. RELATED WORK
2.1 Elliptic 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 $4a^3+27b^2\neq 0 (mod\ p)$. The operations are point addition, point doubling and scalar multiplication.

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

   $A(x_1,y_1)+\infty = \infty + A(x_1,y_1) = A(x_1,y_1)$. (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 \( E(P) \)

\[
A(x_1,y_1)+B(x_2,y_2)=R(x_3,y_3)
\]

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

(2)

2.1.1.2 Point Doubling

Let \( A(x_1,y_1) \) be the point in \( E(P) \) then

\[
2A=R(x_3,y_3)
\]

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

(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 \( E(P) \)

\[
R(x_3,y_3) = A(x_1,y_1) - B(x_2,y_2) = A(x_1,y_1) + [-B(x_2,y_2)]
\]

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. \( kA = A + A + \ldots \ldots + k \) times.

Where \( k \) the integer in the field \( P \).

2.1.2 The ElGamalCryptosystem [4] using an elliptic curve over \( F(p) \) or \( F(2^k) \)

A. Generating public and private keys

1. Bob chooses \( E(\mathbf{a, b}) \) with an elliptic curve over \( F(p) \) or \( F(2^k) \).
2. Bob chooses a point on the curve, \( e_1(x_1, y_1) \).
3. Bob chooses an integer \( d \).
4. Bob calculate \( e_2(x_2, y_2) = d \times e_1(x_1, y_1) \). Note that multiplication here means multiple addition of points.
5. Bob announce \( E(\mathbf{a, b}) \), \( e_1(x_1, y_1) \), 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. \( c_1 = r \times e_1 \)
   II. \( c_2 = P + r \times e_2 \)

C. Decryption

1. Bob after receiving \( c_1 \) and \( c_2 \) calculates \( P \), the plaintext using the following formula:

\[
P = c_2 - (d \times c_1)
\]

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:

\[
\begin{align*}
10010101 & \quad 00011101 & \quad 11001001 \\
10010110 & \quad 00011110 & \quad 11001010 \\
10011111 & \quad 00010000 & \quad 11001111
\end{align*}
\]

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:

\[
\begin{align*}
10010101 & \quad 00011110 & \quad 11001001 \\
10010111 & \quad 00011110 & \quad 11001011 \\
10011111 & \quad 00010000 & \quad 11001111
\end{align*}
\]

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

\[\text{Stego-image} = \text{cover image} + \text{information}\]

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](image)

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],

\[
X_{i+1} = (X_i)^2 \mod n
\]

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,

\[ X_{i+1} = (PX_i + Q)^2 \mod n \]  

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 ASCII 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 be 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 \( r \times c \) 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 select 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 reverse 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. PROPOSED MODEL

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 \( \infty \) is also in the curve. The abelian subgroup of \( E(F_p) \) generated by \( p \) is

\[ P = \{(x, y, 2P, 3P, \ldots, (n-1)P)\} \]

#### 3.1 Key Generation

**Input:**

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

**Output:**

Public key \( Q \) and private key \( d \).

1. Select \( d \in [1, n - 1] \)
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 \( C_I \), Stego key

1. Represent the message ‘\( m \)’ as a point \( M \) in \( E(F_p) \).
2. Select \( K \in \mathbb{Z}[1, n] \).
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 \( (C, I) \)

#### 3.3 Decryption

**INPUT:**

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

**OUTPUT:** (message \( m \), image \( I \))

1. Extract \( I \) from \( C \).
2. Extract \( C_1, C_2 \) from \( I \).
3. Compute \( M = C_2 - d \times C_1 \) and compute \( m \) from \( M \).
4. 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](image-url)
3.4 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, e1(x_1, y_1):
   let(1,5)
3. Bob chooses an integer d. Let d = 3
4. Bob calculate e2(x_2, y_2) = d × e1(x_1, y_1). Note that multiplication here means multiple addition of points:
   e2(x_2, y_2) = (20, 3)
5. Bob announce E = (a, b), e1(x_1, y_1), and e2(x_2, y_2), p as his public key; E(4, 20), e1(1, 5), e2(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)

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 = C2 - d × C1
Consider the above example

Table 4: Decryption process of the example

<table>
<thead>
<tr>
<th>(C1, C2)</th>
<th>C2 - d × C1</th>
<th>P</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>(c, k)</td>
<td>(13, 23) - 3 × (4, 19)</td>
<td>(24, 22)</td>
<td>h</td>
</tr>
<tr>
<td>(g, w)</td>
<td>(3, 28) - 3 × (17, 19)</td>
<td>(15, 27)</td>
<td>e</td>
</tr>
<tr>
<td>(l, 0)</td>
<td>(10, 4) - 3 × (6, 12)</td>
<td>(10, 25)</td>
<td>l</td>
</tr>
<tr>
<td>(p, t)</td>
<td>(2, 6) - 3 × (3, 1)</td>
<td>(10, 25)</td>
<td>l</td>
</tr>
<tr>
<td>(d, x)</td>
<td>(5, 7) - 3 × (20, 3)</td>
<td>(5, 22)</td>
<td>o</td>
</tr>
</tbody>
</table>

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.
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 x n monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

\[
MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} [I(i,j) - K(i,j)]^2
\]

The PSNR is defined as:

\[
PSNR = 10 \log_{10} \left( \frac{MAX^2}{MSE} \right) = 20 \log_{10} \left( \frac{MAX}{\sqrt{MSE}} \right)
\]

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.

Table 3. PSNR table

<table>
<thead>
<tr>
<th>Cover image size(pixel)</th>
<th>input</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text(bytes)</td>
<td>Image(pixel)</td>
<td></td>
</tr>
<tr>
<td>800x600</td>
<td>84</td>
<td>294x184</td>
</tr>
<tr>
<td>800x600</td>
<td>168</td>
<td>294x184</td>
</tr>
<tr>
<td>800x600</td>
<td>168</td>
<td>256x256</td>
</tr>
<tr>
<td>800x600</td>
<td>848</td>
<td>256x256</td>
</tr>
<tr>
<td>800x600</td>
<td>2539</td>
<td>256x256</td>
</tr>
</tbody>
</table>

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 violation.

6. ACKNOWLEDGEMENT

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

7. REFERENCES


