



## Enhancing Security through Steganography by using Sudoku Puzzle and ECC Algorithm

<sup>1</sup>B.Chithra, <sup>2</sup>Depavath Harinath, <sup>3</sup>M.V.Ramana Murthy, <sup>4</sup>K.Ramesh Babu

<sup>1,3</sup>Dept. of Computer Science, Osmania University,

<sup>1,3</sup>Hyderabad, Telangana, India,

<sup>2</sup>Dept. of Computer Science, HRD Degree and PG College,

<sup>2</sup>Narayanaguda, Hyderabad, Telangana, India.

<sup>4</sup>Dept. of Mathematics, M.V.S.R Engineering College, <sup>4</sup>Nadergul, R.R. District, Hyderabad.

### Abstract:-

Now-a-days, data transmission becoming very important among us. There are many modes of transmission of data, but secured data transmission is an important thing what everyone needs, because everyone wants their data to transmit securely. But secured data transmission is still an important problem everyone is facing now-a-days. This paper illustrates image Steganography technique using Sudoku puzzle and ECC algorithm for secured data transmission. Image Steganography refers to the process of hiding the data into image, while ECC algorithm helps to convert the original data into secret code. In the proposed method, the image Steganography is done using Sudoku puzzle. So, this method not only hides the data, but it also converts the original data into secret code. Thus, by combining these two techniques the data will be more securely transferred by this approach. The proposed mechanism will be developed with the aid of the platform MATLAB.

**Keywords:-** Steganography, ECC algorithm, Sudoku Puzzle.

### 1. INTRODUCTION

Now-a-days, the most significant factors of information technology and communication has been the security of information [1]. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the

message secret [2] [3]. The prevalence of multimedia data in our electronic world exposes a new avenue for communication using digital Steganography [4]. Steganography, where the occurrence of communication is hidden, differs from cryptography, in which communication is evident but the content of that communication is inconspicuous [5] [6]. Steganography is the art and science of invisible communication [7]. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information [8] [10]. The term Steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image Steganography the information is hidden completely in images [9]. Steganography differs from cryptography in the sense that where cryptography focuses on possession of contents of a message secret, Steganography focuses on keeping the existence of a message secret [11] [12]. Steganography and cryptography are both ways to protect info from unwanted parties but neither technology alone is perfect and can be bargained. The most important stenographic techniques in digital images are proposed in [28]. The most general image formats on the internet are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and to a lesser extent the Portable Network Graphics (PNG) [15]. The difference between Steganography and Cryptography is that the cryptography attentions on keeping the contents of a message secret whereas Steganography focuses on keeping the

existence of a message secret [14]. Steganography and cryptography both are ways for protecting information from unwanted parties. Most of the techniques developed were set up to exploit the structures of these formats with some exceptions in the literature that use the Bitmap format (BMP) for its simple data structure [16]. Elliptic curve has a rich and beautiful history and mathematicians have studied them for many years. They have been used to solve a various types of problems [17]. The first use of elliptic curve in cryptography parlance was Lenstra's elliptic curve factorization algorithm which Inspired by this sudden unexpected application of elliptic curves in integer factorization in [18]. The principal attraction of ECC, compared to RSA, is that it appears to offer better security for a smaller key size, thereby reducing processing overhead. Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field [19] [20].

## 2. LITERATURE SURVEY

Shailender Gupta et al. [21] have proposed an information hiding scheme for the least significant bit Steganography along with cryptographic method. In this proposed scheme, the raw data was encrypted before embedding it into the image. This system makes use of Rivest, Shamir, Adleman (RSA) algorithm and the Diffie Hellman algorithm to encrypt the secret information. To provide higher security, the secret value is encrypted and then it was converted to binary form. Meanwhile, the image pixels were also converted to binary form and then the encrypted secret information was embedded into the image by an LSB encoder. Akhil Khareet al.[22] have proposed a system that allows user to transfer text messages securely by hiding them into a digital image file. This system was a combination of both Steganography and encryption algorithms and provides a strong backbone for its security. This system also proposed a framework for hiding the large volume of data in images while incurring minimal perceptual degradation. In this proposed method, Entropy thresholding (ET) and Selectively Embedding in Coefficients (SEC) were used to decide whether or not to embed the secret data into the image. This system was

mainly used for applications that require high-volume embedding with robustness. Pasumarthy Saradha et al. [23] have proposed a scheme for improving data hiding capacity using Sudoku puzzle in color images. The main idea of the scheme was to use a Sudoku puzzle, in which every value corresponds to a pixel pair (red, blue) of the image mapped with the secret by replacing a pair of one pixel of two colors. This scheme was proposed to improve the visual quality of the stegoimage and to improve the average hiding capacity of the image to 4 bpp (bits per pixel). This scheme makes use of 24 bit of any type of image and modifies 16 bit of each pixel. The Sudoku solution was used as a reference matrix for both embedding and extracting the secret data into and from the image. Hui-Lung Lee et al. [24] have proposed a maze base steganographic system. In this proposed method, the maze game was used as a carrier media for concealing the secret data. This proposed scheme considered multi-path rather than considering the solution path alone to gain more embedding capacity. This scheme first generates a perfect maze using HKMG algorithm. Subsequently, it chooses some cells as the start cells and one cell as the common end one, of the multi-paths. The secret data are embedded in the Embeddable cells in the perfect maze. Laxman Tawade et al. [25] have proposed an efficient data hiding scheme using secret reference matrices. The data was hidden in 8 bit grayscale image using 256 X 256 matrix which was constructed by using 4 x 4 table with unreported digits from 0~15. The proposed method was to improve the holding capacity of cover image and increase the complexity to crack the Secret Reference Matrix (SRM). They also proposed a new spatial domain data hiding scheme by using a secret reference matrix (SRM) for data embedding and extraction. VikasTyagi et al. [26] have proposed a steganographic method using Least Significant Bit (LSB) along with a cryptographic algorithm. The symmetric cryptographic algorithm was used for encryption of the secret message. This algorithm uses random size of the key. After converting the information into secret code or encrypted form it was patched into the image. For patching the secret data, the least significant bit of the image was used. Emad T. Khalaf et al. [27] have proposed a robust Steganography

technique based on LSB matching. In this scheme, the secret data were concealed in the image based on LSB insertion and RSA encryption technique. The key of the proposed technique was to encrypt the secret data. Then the encrypted data was converted into a bit stream and divided it into a number of segments. The cover image is also divided into the same number of segments. Each segment of data was compared with each segment of the image to find the best match segment, in order to create a new random sequence of segments to be inserted into the cover image.

### 3. SUDOKU MATRIX

Sudoku puzzles and their variants have become extremely popular in the last decade, and can now be found daily in most major U.S. newspapers. Sudoku was popularized in 1986 by the Japanese puzzle company Nikoli, under the name Sudoku, meaning “single number”. A standard Sudoku is a logic-based, combinatorial number-placement puzzle consisting of a 9 by 9 grids. Here we define a Sudoku Matrix as an X by X matrix with the numbers from 1 to N with the constraints that X is a square number and N = X, such that each number occurs exactly once in each row, exactly once in each column and exactly once in each block. The following Figure 1 shows an example of a Sudoku puzzle and its solution in figure 2, when X = 9. We call the solution of the Sudoku puzzle a Sudoku matrix.

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Figure.1: Sample Sudoku puzzle

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5

3	4	5	2	8	6	1	7	9
---	---	---	---	---	---	---	---	---

Figure 2: Solution to sample Sudoku puzzle (Sudoku matrix)

## 4. IMAGE STEGANOGRAPHY USING ECC ALGORITHM AND SUDOKU PUZZLE

### 4.1. ECC Algorithm

Initial process in this technique is encrypting the secret data using an effective cryptographic algorithm. Here, encryption of the user’s secret data is done using the most secure Elliptic Curve Cryptography (ECC) algorithm. The efficiency of a cryptographic algorithm is based on the complex mathematical operations it performs which are not easy to solve. ECC is a public key cryptographic algorithm where the cryptographic operations are described over an elliptic curve  $y^2 = x^3 + ax + b$  Where  $4a^3 + 27b^2 \neq 0$ . Based on the values of a and b different elliptic curves are generated and all the points (x, y) that satisfy the above equations lie on the elliptic curve. Public key cryptography is a cryptographic system where all users taking part in the communication makes use of a public key and a private key. Only the public key is known to all users and private key is known only by that particular user. In ECC the public key is any point on the curve and it is obtained by multiplying generator point G along with private key. Private key is any random number. As mentioned above, the security and secrecy of a cryptographic algorithm lies in the complex mathematical operations it performs. Similarly the efficiency of ECC lies in elliptic curve Discrete Logarithm Problem. The main operation of ECC is point multiplication which involves both point addition and point doubling.

#### 4.1.1. ECC over a Prime Field Fp

By foundation, the elliptical curve operations are very slow. But a cryptographic algorithm must be fast in computation to make it more efficient. So, the operations of the elliptic curve cryptographic algorithm are defined over two finite fields (i) Prime Field and (ii) Binary Field. For our implementation, we have used the ECC over prime field Fp. The equation for elliptic curve over Fp is given by eq (1).

$$y^2 \text{ mod } p = x^3 + ax + b \tag{1}$$

Where,

$$4a^3 + 27b^2 \text{ mod } p \neq 0 \quad (2)$$

and the value of  $p$  is chosen such that there are large number of points on the elliptic curve to make the cryptographic algorithm more secure.

### A. Point Multiplication

The point multiplication is the main operation of ECC algorithm. In this operation a point on the curve is multiplied with another scalar value to obtain a new point.  $kP = Q$  (3) where  $k$  is the scalar and  $P$  is a point on the curve. This point multiplication can be achieved only by performing two other main operations namely the point addition and point doubling.

### B. Point Addition

Point addition is the process of adding two points on the elliptic curve to obtain another point on the same elliptic curve. Let  $J$  and  $K$  be two points on elliptic curve such that

$$J = (X_J, Y_J) \text{ and } K = (X_K, Y_K)$$

These two points are added to obtain another point  $L$  on the same elliptic curve.

$$L = J + K \quad (4)$$

Where  $L = (X_L, Y_L)$ , then

$$X_L = (S^2 - X_J - X_K) \text{ mod } p$$

$$Y_L = (-Y_J + S(X_J - X_L)) \text{ mod } p$$

$S = ((Y_J - Y_K) / (X_J - X_K)) \text{ mod } p$ ,  $S$  is the slope of the line through  $J$  and  $K$ .

### C. Point Doubling

In point doubling, a point on the elliptic curve is added to itself to obtain another point on the same elliptic curve. Let  $J$  be a point on the elliptic curve such that  $J = (X_J, Y_J)$ , where  $Y_J \neq 0$ , and it is added to itself in order to obtain another point  $L$  on the elliptic curve. It is given by  $L = 2J$  (5)

Where  $L = (X_L, Y_L)$ , then

$$X_L = (S^2 - 2X_J) \text{ mod } p$$

$$Y_L = -Y_J + S(X_J - X_L) \text{ mod } p$$

$$S = ((3X_J^2 + a) / (2Y_J)) \text{ mod } p$$

In ECC over prime field, the elements of the prime field are the numbers between 0 and  $p-1$ . Also the domain parameters for this ECC over prime field  $F_p$  constitute the coordinates  $a$ ,  $b$ , generator point  $G$ , prime number  $p$  and the order of elliptic curve  $n$ . The main advantage of using this ECC as the cryptographic algorithm is its key size which is small and constant. A 160 bit key used in ECC is considered to be as strong as 1024 bit key used is RSA cryptographic

algorithm.

### 4.1.2. Encryption via Elliptic Curve Cryptography(ECC)

This section briefs about the process of encrypting user information using elliptic curve cryptography. In ECC, we randomly select a basic point  $P_i$  that satisfies eq.1 mentioned in previous section. To perform encryption on the given message (ex. Password), we need to select a private key  $P_k$  which is a randomly selected integer less than  $p$  and we generate a public key  $u_k = P_k * P_i$ . The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

**Cipher Generation:** The steps involved in generating the cipher are,

#### Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. Consider 'm' has the point 'M' on the curve 'F'. Randomly select 'h' from  $[1 - (p-1)]$ . Two cipher texts will be generated let it be  $C_1, C_2$

$$C_1 = h * P_i \quad (6)$$

$$C_2 = M + h * u \quad (7)$$

### 4.2. Genetic Algorithm

The Genetic Algorithm (GA) is an optimization strategy based on the Darwinian evolution process [13]. Genetic algorithms (GAs) are computer programs that mimic the processes of biological evolution in order to solve problems and to model evolutionary systems. Genetic algorithms (GAs) are a promising heuristic approach to finding nearoptimal solutions in large search spaces [Dav91, Gol89, Hol75].

Standard Genetic Algorithm (SGA):

- (1) Generate initial population;
- (2) while number of generations not exhausted do
- (3) for 1 to Population Size do
- (4) Randomly select two chromosomes and apply the crossover operator;
- (5) Randomly select one chromosome and apply mutation operator;
- (6) End for
- (7) evaluate all the chromosomes in the population and perform selection;
- (8) End while
- (9) Report the best chromosome as the final solution. Similarly, to select the best pixels from the cover image for embedding the secret value



(eg. PIN, Passwords, Private keys), optimization using the GA technique is deployed in the Sudoku matrix. Instead of chromosomes, it selects the pixel values in digital image and makes changes by embedding the cipher using Sudoku matrix.

**4.3. Image Steganography using Sudoku Matrix**

1. Create a tile matrix ('Z') by obtaining Sudoku puzzle solution and subtracting 1 from all the fields in the puzzle (Fig. 4). The initial puzzle contained data values ranging from 1 to 9. After subtracting the values will range from 0-8.

6	5	1	7	4	8	2	5	9
9	3	8	2	5	6	1	7	4
2	4	7	3	1	9	8	6	5
3	2	4	1	9	7	6	5	8
5	7	6	4	8	3	9	2	1
8	1	9	5	6	2	3	4	7
4	6	2	8	7	1	5	9	3
7	8	3	9	2	5	4	1	6
1	9	5	6	3	4	7	8	2

Figure.3. Sudoku solution

5	4	0	6	3	7	1	4	8
8	2	7	1	4	5	0	6	3
1	3	6	2	0	8	7	5	4
2	1	3	0	8	6	5	4	7
4	6	5	3	7	2	8	1	0
7	0	8	4	5	1	2	3	6
3	5	1	7	6	0	4	8	2
6	7	2	8	1	4	3	0	5
0	8	4	5	2	3	6	7	1

Figure.4. Tile matrix

2. Generate Reference Matrix ('T') - Replicate the tile matrix on both axes to create a matrix of size 256 x 256. The reference matrix, T is then consisting of an n×n tiling of copies of Z, where n = floor (256/9) + 1. The overflowing fields are ignored and T is truncated to 256×256 matrix. (Fig. 5)

3. Data embedding: Convert the cipher text obtained from ECC algorithm to base-9 numeral system. So that the cipher text is taken as:

$$C = C_1, C_2, C_3, \dots, C_E$$

Where, E is the number of converted secret digits

		$G_{i+1}$																					
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...	253	254	255
$G_i$	0	5	4	0	6	3	7	1	4	8	5	4	0	6	3	7	1	4	8	.....	5	4	0
	1	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	.....	8	2	7
	2	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	.....	1	3	6
	3	2	1	3	0	8	6	5	4	7	2	1	3	0	8	6	5	4	7	.....	2	1	3
	4	4	6	5	3	7	2	8	1	0	4	6	5	3	7	2	8	1	0	.....	4	6	5
	5	7	0	8	4	5	1	2	3	6	7	0	8	4	5	1	2	3	6	.....	7	0	8
	6	3	5	1	7	6	0	4	8	2	3	5	1	7	6	0	4	8	2	.....	3	5	1
	7	6	7	2	8	1	4	3	0	5	6	7	2	8	1	4	3	0	5	.....	6	7	2
	8	0	8	4	5	2	3	6	7	1	0	8	4	5	2	3	6	7	1	.....	0	8	4
	9	5	4	0	6	3	7	1	4	8	5	4	0	6	3	7	1	4	8	.....	5	4	0
	10	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	.....	8	2	7
	11	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	.....	1	3	6
	12	2	1	3	0	8	6	5	4	7	2	1	3	0	8	6	5	4	7	.....	2	1	3
	13	4	6	5	3	7	2	8	1	0	4	6	5	3	7	2	8	1	0	.....	4	6	5
	14	7	0	8	4	5	1	2	3	6	7	0	8	4	5	1	2	3	6	.....	7	0	8
	15	3	5	1	7	6	0	4	8	2	3	5	1	7	6	0	4	8	2	.....	3	5	1
	16	6	7	2	8	1	4	3	0	5	6	7	2	8	1	4	3	0	5	.....	6	7	2
	17	0	8	4	5	2	3	6	7	1	0	8	4	5	2	3	6	7	1	.....	0	8	4
..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	.....	..	..	..	
253	5	4	0	6	3	7	1	4	8	5	4	0	6	3	7	1	4	8	.....	5	4	0	
254	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	.....	8	2	7	
255	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	.....	1	3	6	

Figure.5. Reference matrix (T)

4. Carrier image used for this method is an RGB image. We will use values of 2 channels, R and

G, from each pixel to map coordinates in Reference matrix. New values of R & G for

mapping in matrix will be obtained as:

$$R = (R\%9) + 9 \tag{8}$$

$$G = (G\%9) + 9 \tag{9}$$

This will be paired as  $(G_i, G_{i+1})$ , where  $G_i = R$  and  $G_{i+1} = G$ . These R and G values will be pointed in the reference matrix as the values in matrix also lie in same range. Since reference matrix is generated by a Sudoku puzzle, any value between 0 to 8 can be located within movement of two positions from any block in matrix.

**5. Candidate elements:** Three candidate elements are selected to obtain minimum deviation Distance for new values of  $i G$  &  $1 i+ G$ . The minimum deviation for any value from a given position in Sudoku will lie on horizontal axis within a distance of 9 blocks or as a best case,

within surrounding blocks. For example (Fig. 6), suppose value to be concealed is 2 and coordinates pointed by R & G of a pixel in cover image are 13,8. The location is obtained in reference matrix and vertical, Horizontal and block values are marked. Now look for 2 in all the 3 candidates (CEH, CEV and CEB) and obtain minima of the distances. The cover pixel R & G values will be modified with minimum distortion candidate element. These three candidates are named and selected as:-

	0	1	2	3	4	5	6	7	8	9	$G_{i+1}$									253	254	255
0	5	4	0	6	3	7	1	4	8	5	4	0	6	3	7	1	4	8	.....	5	4	0
1	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	.....	8	2	7
2	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	.....	1	3	6
3	2	1	3	0	8	6	5	4	7	2	1	3	0	8	6	5	4	7	.....	2	1	3
4	4	6	5	3	7	2	8	1	0	4	6	5	3	7	2	8	1	0	.....	4	6	5
5	7	0	8	4	5	1	2	3	6	7	0	8	4	5	1	2	3	6	.....	7	0	8
6	3	5	1	7	6	0	4	8	2	3	5	1	7	6	0	4	8	2	.....	3	5	1
7	6	7	2	8	1	4	3	0	5	6	7	2	8	1	4	3	0	5	.....	6	7	2
8	0	8	4	5	2	3	6	7	1	0	8	4	5	2	3	6	7	1	.....	0	8	4
9	5	4	0	6	3	7	1	4	8	5	4	0	6	3	7	1	4	8	.....	5	4	0
$G_i$ 10	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	.....	8	2	7
11	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	.....	1	3	6
12	2	1	3	0	8	6	5	4	7	2	1	3	0	8	6	5	4	7	.....	2	1	3
13	4	6	5	3	7	2	8	1	0	4	6	5	3	7	2	8	1	0	.....	4	6	5
14	7	0	8	4	5	1	2	3	6	7	0	8	4	5	1	2	3	6	.....	7	0	8
15	3	5	1	7	6	0	4	8	2	3	5	1	7	6	0	4	8	2	.....	3	5	1
16	6	7	2	8	1	4	3	0	5	6	7	2	8	1	4	3	0	5	.....	6	7	2
17	0	8	4	5	2	3	6	7	1	0	8	4	5	2	3	6	7	1	.....	0	8	4
...	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	.....	..	..	..
253	5	4	0	6	3	7	1	4	8	5	4	0	6	3	7	1	4	8	.....	5	4	0
254	8	2	7	1	4	5	0	6	3	8	2	7	1	4	5	0	6	3	.....	8	2	7
255	1	3	6	2	0	8	7	5	4	1	3	6	2	0	8	7	5	4	.....	1	3	6

Figure.6. Candidate elements. (CEH, CEV and CEB)

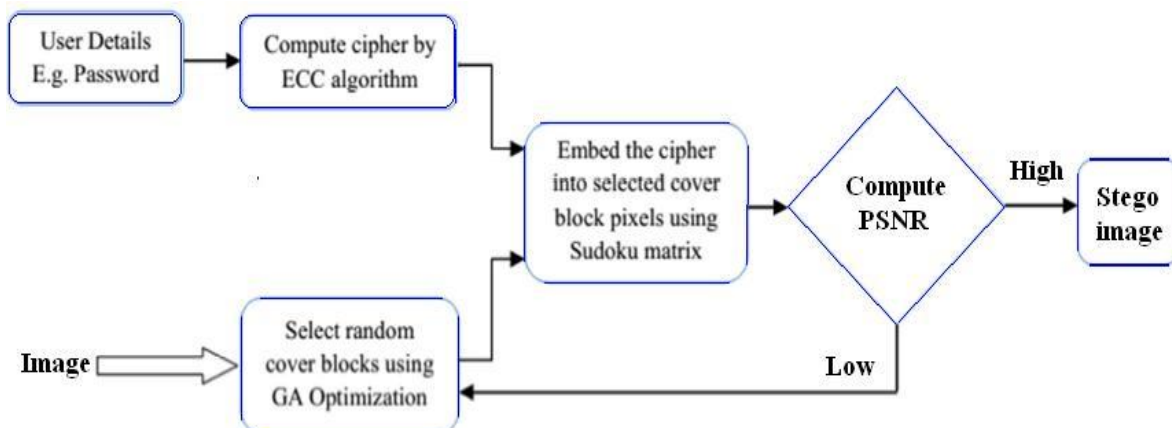


Figure.7. Structure of proposed secure data transmission using ECC algorithm and Sudoku matrix

**a. Horizontal (CEH)**

If  $G_{i+1} > 3$  and  $G_{i+1} < 252$ ,  
 then  $G_i = G_i \% 9 + 9$ ,  $G_{i+1} = G_{i+1} \% 9 + 9$  and  
 $CE_H = \{T(G_i, G_{i+1}-4) \text{ to } T(G_i, G_{i+1}+4)\}$   
 (10)

i.e. Select the surrounding 9 block horizontal line with the pointed location  $(G_i, G_{i+1})$  at mean.

**b. Vertical (CEV)**

If  $G_i > 3$  and  $G_i < 252$ ,  
 then  $G_i = G_i \% 9 + 9$ ,  $G_{i+1} = G_{i+1} \% 9 + 9$  and  
 $CE_V = \{T(G_i-4, G_{i+1}) \text{ to } T(G_i+4, G_{i+1})\}$  (11) i.e.  
 Select the surrounding 9 block vertical line with the pointed location  $(G_i, G_{i+1})$  at mean.

**c. Boxed (CEB)**

If  $G_i < 252$  and  $G_{i+1} < 255$  then compute -

$$A_o = \lfloor G_i / 3 \rfloor \times 3, B_o = \lfloor G_{i+1} / 3 \rfloor \times 3 \quad (12)$$

And Select surrounding box edging on  $A_o$  and  $B_o$ . i.e. Select the blocks around the pointed location  $(G_i, G_{i+1})$ .

Now the modified values are obtained and if the secret messages were embedded into cover block by changing their values, the PSNR should be high to obtain high quality image. The PSNR can be found by using the formula

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE} \text{ dB} \quad (13)$$

Where, MSE is the mean square error between the original image and the stego image. The MSE is defined as follows:

$$MSE = \frac{1}{V \cdot W} \sum_{i=0}^{V-1} \sum_{j=0}^{W-1} (R_{ij} - R'_{ij})^2 + \sum (G_{ij} - G'_{ij})^2 + \sum (B_{ij} - B'_{ij})^2 \quad (14)$$

RGB value of original and stego images pixels respectively.  $V \cdot W$  gives number of all pixels present in a image. A larger PSNR indicates that the quality of the stego image is closer to the original one. Normally human's eyes find it hard to distinguish between the distortions on a stego image compared to original image when its PSNR value is greater than 30 dB Similarly, the PSNR of each modified cover block is calculated. Then using GA evolutionary optimization algorithm, a new set of cover blocks is selected and the secret messages are embedded. This process continues until the fitness, i.e., PSNR becomes high. Finally when the optimal blocks for embedding secret message are found, the index values of those blocks are embedded.

**4.4. Image and Information Recovery**

At the receiver side, the following steps are performed to recover the secret message.

- First, on the stego image, select the modified cover blocks by the referring the index value
- Second, by referring the reference matrix, the secret digits are obtained using the modified R & G pixel values
- Then extract the secret digits from the reference matrix and compute their binary values and then the ASCII values to retrieve the encrypted cipher.
- Decrypt the cipher by using the equation  $M = C_2 - pk * C1$  to obtain the original message.

**5. RESULT AND DISCUSSIONS**

The proposed secure technique using ECC and Sudoku matrix technique is implemented in the working platform of MATLAB version 2013. The given input information is encrypted by ECC and the secret message is embedded in the input image. The sample image used for this implementation is shown in figure 8.























**Figure(8.) Sample Input Cover Image**

























**Figure( 9.) Stego-Image**









The performance of this proposed method is analyzed by embedding the secret messages into images and their PSNR values and noise correlation are demonstrated in table 1. Also the proposed method is compared against the existing method which is shown in table.2















Message	Cover Images	Stego-Images	Retrieved Image PSNR value	Retrieved Image PSNR Value
SO			87.8786	SO
ME			88.5481	ME
MY			89.3399	MY
US			89.0905	US
WE			88.3133	WE
BYE			86.0493	BYE
YOU			86.4768	YOU
SIX			86.9511	SIX
OUT			86.4768	OUT
LAW			86.9511	LAW









































FIND			84.8683	FIND
HANG			85.0802	HANG
LOCK			84.973	LOCK
OKAY			84.8683	OKAY
GOAL			84.5687	GOAL
HELLO			83.2475	HELLO
ARRAY			84.1111	ARRAY
BASIC			83.2475	BASIC
POINT			83.2475	POINT
TURBO			84.6663	TURBO
@ # 1 2 \$			83.1769	@ # 1 2 \$

% 5 6 # @			83.4665	% 5 6 # @
^&*123			82.7757	^&*123
\$#+^&*			83.1769	\$#+^&*
#58974*			81.2331	#58974*

**Table.1. Performance Results of Proposed Technique**

Message	Cover Images	Stego-Images	Retrieved Image PSNR value	Retrieved Image PSNR value
SO			86.7872	SO
ME			84.8683	ME
MY			87.4835	MY
US			85.5378	US
WE			84.3798	WE
BYE			83.6972	BYE

YOU			85.0802	YOU
SIX			83.8581	SIX
OUT			83.9408	OUT
LAW			84.2884	LAW
FIND			82.4676	FIND
HANG			82.1799	HANG
LOCK			82.8401	LOCK
OKAY			83.1769	OKAY
GOAL			83.2475	GOAL
HELLO			81.5104	HELLO
ARRA Y			82.1799	ARRAY

BASIC			82.2359	BASIC
POINT			81.8066	POINT
TURBO			81.416	TURBO
@ # 1 2 \$			81.656	@ # 1 2 \$
% 5 6 # @			80.57	% 5 6 # @
^&*12 3			81.4629	^&*123
\$#+^& *			80.7265	\$#+^&*
#58974 *			80.0971	#58974*

**Table.2. Performance Results of existing Technique**

The table.1 and table.2 shows the results of the proposed and existing method. By analyzing the results of table.1 and table.2, we can clearly see that the PSNR values of the table.1 are very high compared to the PSNR values of table.2. From the results, we can clearly identify that PSNR value of the proposed method shows good value. The PSNR values are taken for 20 pure text messages and 5 numbers with characters for the existing and the proposed method. From this input given to the image, we can clearly identify that proposed method performs better than the existing method. So the proposed image Steganography using ECC and Sudoku matrix method performs better than the existing image

Steganography using Sudoku matrix method alone. Thus, the image Steganography using ECC and Sudoku matrix method with the combination of GA optimization technique has increased the PSNR value to a greater extent. Thus, the proposed ECC and Sudoku matrix technique performs well for secure data transmission.

## CONCLUSION

Nowadays, secure data transmission become more important. Even though, there are many biometric authentications to restrict the unauthorized users, a more trusted system was needed to make the security appropriate for



logical access. Therefore, this paper depicts a secure technique by integrating a cryptographic technique and a steganographic technique. By making use of ECC for encrypting the user data, this technique has used the most secured cryptographic algorithm. The main advantage of using ECC is its small key size. Also for embedding the cipher into cover image, the Sudoku matrix is used with the help of GA algorithm. Thus, the data will be more securely transferred by embedding the cipher into an image. Hence this technique can be used for the purpose of security in data transmission where security is under great threat.

## REFERENCES

- [1] Kavitha, Kavita Kadam, Ashwini Koshti and Priya Dughav, "Steganography Using Least Significant Bit Algorithm", International Journal of Engineering Research and Applications, Vol. 2, No. 3, pp. 338-341, May-Jun 2012.
- [2] P. Mohan Kumar and D. Roopa, "An Image Steganographic Framework with Improved Tamper Proofing", Asian Journal of Information Technology, Vol. 6, No. 10, pp.1023-1029, 2007.
- [3] Samir Kumar Bandyopadhyay and IndraKanta Maitra, "An Alternative Approach of Steganography using Reference Image", International Journal of Advancements in Technology, Vol. 1, No. 1, pp. 95-102, 2010.
- [4] Lisa M. Marvel, Charles G. Boncelet, and Charles T. Retter, "Spread Spectrum Image Steganography", IEEE Transactions on Image Processing, Vol. 8, No. 8, pp. 1075-1083, August 1999.
- [5] Chandramouli R., Hoboken NJ and Memon N., "Analysis of LSB based image Steganography techniques", In proceedings of International Conference on Image Processing, Vol. 3, pp. 1019-1022, 2001.
- [6] Avcibas I., Memon N. and Sankur, B., "Image steganalysis with binary similarity measures", In proceedings International Conference on Image Processing, Vol. 3, pp. 645-648, 2002.
- [7] Benjamín Barán, Santiago Gómez and Víctor Bogarín, "Steganographic watermarking for documents", In proceedings of the 34th Annual Hawaii International Conference on System Sciences, pp. 1-10, 2001.
- [8] Khosravi Sara, Abbasi Dezfoli Mashallah and Yektaie Mohammad Hossein, "A New Steganography Method Based on HIOP (Higher Intensity of Pixel) Algorithm and Strassen's Matrix Multiplication", Journal of Global Research in Computer Science, Vol. 2, No. 1, pp. 6-12, 2011.
- [9] Masoud Nosrati, Ronak Karimi, Hamed Nosrati and Ali Nosrati, "Embedding stego-text in cover images using linked list concepts and LSB technique", Journal of American Science, Vol. 7, No. 6, pp. 97-100, 2011.
- [10] Pallavi Khare, Jaikaran Singh and MukeshTiwari, "Digital Image Steganography", Journal of Engineering Research and Studies, Vol. 2, No. 3, pp. 101-104, 2011.
- [11] Rajarathnam Chandramouli, Mehdi Kharrazi and Nasir Memon, "Image Steganography and Steganalysis: Concepts and Practice", Digital Watermarking, Vol. 2939, pp. 35-49, 2004.
- [12] Veerraju Gampala, Srilakshmi nuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering, Vol. 2, No. 3, pp. 138-141, July 2012.
- [13] B. R. Rajakumar, "Static and Adaptive Mutation Techniques for Genetic algorithm: A Systematic Comparative Analysis", International Journal of Computational Science and Engineering, Vol. 8, No. 2, pages: 180-193, 2013.
- [14] Huaiqingwang and Shuozhong wang, "Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, Vol. 47, No. 10, pp. 76-82, 2004.
- [15] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKeivitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Vol. 90. No.3, pp.727-752, 2010.
- [16] Kamlesh Gupta and Sanjay Silakari, "ECC over RSA for Asymmetric Encryption: A Review", International Journal of Computer Science Issues, Vol. 8, Issue 3, No.2, pp. 370-375, May 2011.
- [17] A.V.N.Krishna, "Probabilistic Encryption Based ECC Mechanism", International Journal of Advancements in Technology, Vol. 2, No. 2, pp. 257-268, 2011.
- [18] C. Sajeev and G. Jai sArul Jose, "Elliptic Curve Cryptography Enabled Security for Wireless Communication", International Journal

- on Computer Science and Engineering, Vol. 02, No. 06, pp. 21872189, 2010.
- [19] Don Johnson, Alfred Menezes and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", International Journal of Information Security, Vol. 1, No. 1, pp. 36-63, 2001
- [20] Neal Koblitz, Alfred Menezes and Scott Vanstone, "The State of Elliptic Curve Cryptography", Designs, Codes and Cryptography, Vol. 19, pp. 173-193, 2000
- [21] Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", International Journal of Modern Education and Computer Science, Vol. 6, pp. 27-34, June 2012
- [22] Akhil Khare, Meenu Kumari and Pallavi Khare, "Efficient Algorithm for Digital Image Steganography", Journal of Information, Knowledge and Research in Computer Science and Applications, Vol. 1, No. 1, pp. 1-5, October 2010.
- [23] Pasumarthy Saradha and Bala Swamy, "Improving Image Data Hiding Capacity Scheme using Sudoku Puzzle in Color Images", International Journal of Engineering Research and Applications, Vol. 2, No. 3, pp. 2741-2744, May-June 2012.
- [24] Hui-Lung Lee, Chia-Feng Lee and Ling-Hwei Chen, "A Perfect Maze Based Steganographic Method", The Journal of Systems and Software, Vol. 83, No. 12, pp. 2528-2535, July 2010.
- [25] Laxman Tawade, Rajshree Mahajan and Chandan Kulthe, "Efficient & Secure Data Hiding Using Secret Reference Matrix", International Journal of Network Security & Its Applications, Vol. 4, No. 1, pp. 43-50, January 2012.
- [26] Vikas Tyagi, Atulkumar, Roshan Patel, Sachin Tyagi and Saurabh Singh Gangwar, "Image Steganography using Least Significant Bit with Cryptography", Journal of Global Research in Computer Science, Vol. 3, No. 3, pp. 53-55, March 2012.
- [27] Emad T. Khalaf and Norrozila Sulaiman, "A Robust Data Hiding Technique based on LSB Matching", World Academy of Science, Engineering and Technology, Vol. 58, pp. 117-121, 2011.

[28] Shubhi Gupta, P.S. Gill Awakash Mishra and Abhishek Dwivedi, "A Scheme for Secure Image Transmission Using ECC over the Fraudulence Network", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 4, pp. 67-70, April 2012.

[29] Depavath Harinath et. al., "Cryptographic Methods and Performance Analysis of Data Encryption Algorithms in Network Security" in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 5, Issue 7, July 2015.

### Author Profile

**Depavath Harinath**, received the Bachelor of Science degree in computerscience from New Noble Degree college, Affiliated to Osmania University, Hyderabad, Telangana, India in 2008 and received Master of Computer



Applications degree from Sreenidhi Institute of Science and Technology, an autonomous institution approved by UGC. Affiliated to JNTU, Hyderabad, Telangana., India in 2012. Now working as Lecturer in Computer Science in HRD Degree and PG college, Affiliated to Osmania University, Narayanaguda, Hyderabad, Telangana, India. Having three years of experience in teaching and already published many manuscripts in different international journals. Research fields includes Computer Networks and Network Security.

**Prof. M. V. Ramana Murthy**, Professor in department of mathematics and computerscience, Osmania University, since 1985. Obtained Phd degree from Osmania University in 1985 and visited many a countries across the globe in various capacities and participated in many academic programs. Research fields includes computational plasma, Artificial Neural Networks, and Network securities.



**Mrs B. Chithra**, Asst .Professor in department of mathematics and computer science, Osmania University, Hyderabad. She has Worked as Associate Professor (dept. of



Computer Science) at St. Ann's college for women, for about fifteen years and published a paper in one of the reputed International Journals. Research interest includes Network Security.

**K.Ramesh Babu**, received his Ph.D in 2012



from Osmania University for the thesis entitled “ Estimation of target position from noisy radar data using kalman filter”. Presently working at M.V.S.R Engineering College, Nadergul as Asst. Professor in mathematics. The research areas includes Theoretical computer Science.