International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 4 Issue 4 April 2018
ISSN (Online): 2455-4723

An Imporve Color Image Stgnography Using ECC Algorithm

Rekha yadav[1], Prof. Sumit Nigam[2]

[1]*M Tech Scholar, Computer Science and Engineering,SIMS, Indore 452001, India*

[2] *Prof. Sumit Nigam, Head of Department of Computer Science & Engineering,SIMS, Indore 452001, India*

Rekha.Yadav@Sims-indore.com , sumit.nigam@Sims-Indore.com

Abstract - **The main aim of the proposed work is to investigate about the data security technique. Therefore two major domains are concentrated for study cryptography and steganography. Both the techniques are much popular for securing data during different kinds of unsecured data communication scenarios. In addition of that both the techniques are low cost for implementation as well as maintenance. During investigation of this technique the steganographic techniques are not much secure due to most of the time LSB based steganography scenarios. Therefore the proposed work is intended to improve the security of traditional steganographic technique by incorporating the cryptographic technique too. Thus the proposed work introduced an ECC cryptographic technique for encrypting the message securely and then that is incorporated over the color image bit plane for 3 bits each. That process not much effect the actual color definition therefore the image quality is not changed. The implementation of the proposed concept is performed using dot net technology and their performance is computed. To evaluate the performance of the given system the MSE and PSNR is used for image quality parameters additionally for measuring the efficiency of the system time and space complexity is computed. According to the obtained performance the proposed technique is efficient and effective for secure steganographic scenarios..**

Keywords: ***Steganography, Image, Cryptography, AES, Data Security, LSB, Elliptic Curve Cryptography, Data Hiding***

1. INTRODUCTION

The current era is a computational age where most of information is communicated via internet or networks. Due to frequent usages of this public communication medium not all the communications are much secure. Banking information, army communication or some highly confidential information leakage is a key issue now in these days. In this context the data security in un-trusted network is a key area of study and new solution design. There are a number of effective solutions to provide such solution but either these are much resource complex or not much secure for confidential data exchange. Therefore a new technique is required to design for improving the security as well as the resource consumption for securing data in un-trusted communication channels.

In this context a new security model is proposed for design and implementation that is highly secure and efficient in terms of rapid data processing ability. Therefore a hybrid cryptographic concept by combining stegnography and cryptography is proposed for design and implementation. That technique first encrypt the data using an efficient and light weight cryptographic algorithm and then converted into the binary strings to incorporate the data into a digital image. That is performed on the basis of stegnographic concept. In this context first need to decide a efficient and secure cryptographic technique and LSB based stegnography is used for hiding data into an image medium.

2. PROPOSED WORK

The aim of the work is to design and implement a technique which is highly secure and efficient for short messages exchange. In this context a method is developed which is detailed in this chapter using methodology and the algorithm steps.

2.1) System Overview

As we know the cryptography and steganography both are the different techniques of data security. In cryptography the data is converted in another format which is not recognizable during normal processes. For recovering information from this technique need some kinds of keys or secrete pins on the other hand the steganography is also a processes of information security where the data is hide in another kind of message such as text, image or video. The information hidden in other data need to understand the pattern or need additional tricks to

be recovered. In this presented work the combination of steganography and cryptography is used to securing information. The advantage with this method of information security is their low cost of implementation and low cost during maintenance or changes.

The proposed work is intended to design and implement a secure steganographic technique that is not only secure data by hiding in any other form that also involve the cryptographic technique to strongly preserve the secrete message from attacker. The key advantage to do this is if an attacker identify the image contains some secrete message and recover the LSB from image then it is also secured by the cryptographic technique. In addition of that in order to use the private key encryption technique in this work the ECC (ecliptic curve cryptographic) algorithm is implemented. That algorithm self generate the key for encryption and decryption process. Therefore the method becomes more secure as compared to other steganographic approach. Therefore the proposed technique is combination of highly secure technique of steganography and cryptography. This section only the basic of the proposed technique is explained or overview is provided in next section the functional aspects of the system is described with utilized algorithm and processes.

2.2) Methodology

The proposed technique of steganography and cryptography is described using figure 2.1. The figure contains the different modules which are used to design the proposed working model. Additionally the detailed methodology of system design is also incorporated in this section.

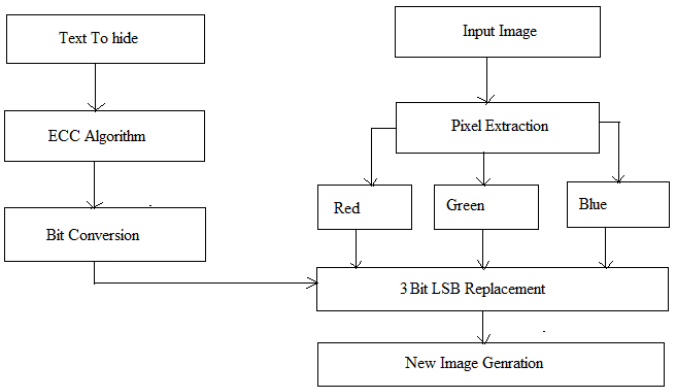


Figure 2.1 Proposed System Architecture

Text to hide: that is the initial input to the system in terms of the text message which is needed to exchange between two persons securely. The user (sender) first provides the message text as input to the system.

ECC Algorithm: input message is processed using the ECC (elliptic curve cryptographic technique). The ECC algorithm is asymmetric key encryption techniques which generate two keys namely one private key and second the public key. The encryption algorithm encrypts the data using public key and only the private key can decrypt the data. The ECC algorithm works on the following manner.

Suppose Q= public key

P= a point in curve

d= private key

M= original message

K= random number

Then, using above parameters we get the two cypher text blocks which are denoted using C_1 and C_2

$$C_1 = K.P$$

$$C_2 = M + KQ$$

The encryption process input file convert into byte array and then set x1, y1, x2, y2, for curve generation. Now get points on the curve and generate a random no. d from 1 to N. Calculate public key with the help of d and p and generate cipher text C1 and sequence of C2.

Using the above equations the message can be defined as:

$$M = C_2 - d * C_1$$

$$M = C_2 - KQ$$

At the network scenarios the cipher C_1 and C_2 is sanded on network and the recovery of the original message can be found using the below given expression.

$$M = C_2 - d * C_1$$

$$C_2 - d * C_1 = (M + KQ) - d * (K * p)$$

In next step

$$C_2 - d = M + KQ\, C_2 = M + KQ$$

$$M = M$$

Bit Conversion: the output of the previous step is a cipher text produced by ECC algorithm. This cipher text is read in terms of file bytes which are further converted into the bit format. After conversion of bytes into the bit the data is keep separate for hiding these generated bits into the image file.

Input Image: in this phase an additional color image is provided as input to the system. in color image each pixel of the image is defined using the three color combination thus

that can be presented using [R, G, B], where the colors values are varying between 0-255. Therefore for each pixel of the image can be represented using an individual bit plane.

The bit plane of a single color pixel is demonstrated using figure 2.2. Similarly for each color value a bit plane is prepared. Now for hiding the data into the image the LSB (least significant bits) are used.

3-Bit LSB: now the last bit of each color pixel is replaced with the data bits which are previously transformed into cipher to bits. Due to this last bit replacement the color definition is not much affected in actual color image and provides the low MSE error during quality of image test.

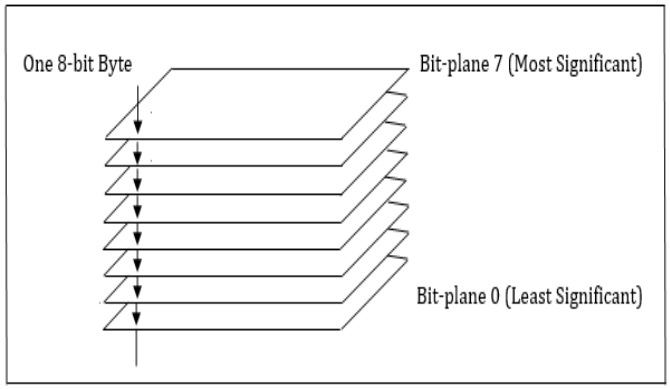


Figure 2.2 Bit Plane

New Image Generation: after bit replacement of color image the image is prepared to transmit in other end or receiver end.

This section describes the overall process of the proposed model in next section the model is described using algorithm steps.

Metrics Generation

RGB: In this we use text message for hiding information in image. Therefore we use 24 bit RGB color image can be allocated into three two dimensional matrix i.e. Red matrix, Green matrix and Blue matrix. These matrix can be viewed in figure 2.3

	1	2	3	4	5
▶	41	40	40	40	41
	233	233	233	233	234
	227	227	227	227	227
	224	225	225	225	225
	229	228	228	228	228
	226	227	227	227	227

(a) Red matrix

	1	2	3	4	5
▶	40	40	40	40	41
	233	233	233	233	234
	226	227	227	227	227
	225	225	225	225	225
	228	228	228	228	228
	227	227	227	227	227

(b) Blue matrix

	1	2	3	4	5
▶	41	40	40	40	41
	233	233	233	233	234
	226	227	227	227	227
	224	225	225	225	225
	228	228	228	228	228
	227	227	227	227	227

(c) Blue matrix

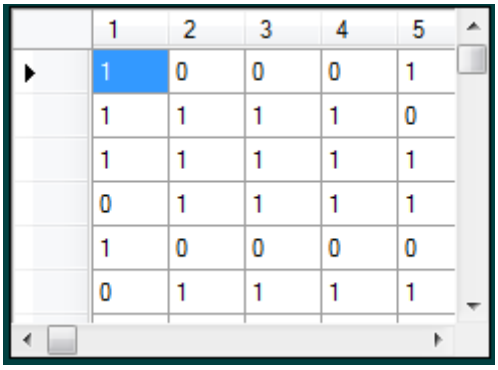
Figure 2.3: (a) (b) (c) For Red Green and Blue matrix

Data of each matrix can be represented by a decimal number between 0 to 255 Furthermore the value of each pixel can be represented by a binary number with 8 bit.

LSB RGB:

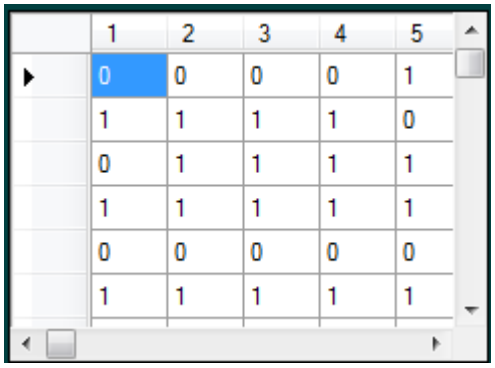
Then each component can take out the least bit from all pixels to compose the same size matrix which the value is 0 or 1, so that we can get the three matrix composed of the least

significant bit from Red matrix, Green matrix and Blue matrix. Figure 2.4 is the matrix composed of the least significant bit of Red Green and Blue matrix.



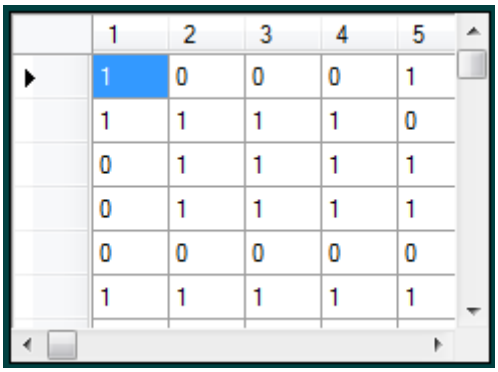
	1	2	3	4	5
▶	1	0	0	0	1
	1	1	1	1	0
	1	1	1	1	1
	0	1	1	1	1
	1	0	0	0	0
	0	1	1	1	1

(a) LSB Red



	1	2	3	4	5
▶	0	0	0	0	1
	1	1	1	1	0
	0	1	1	1	1
	1	1	1	1	1
	0	0	0	0	0
	1	1	1	1	1

(b) LSB Green



	1	2	3	4	5
▶	1	0	0	0	1
	1	1	1	1	0
	0	1	1	1	1
	0	1	1	1	1
	0	0	0	0	0
	1	1	1	1	1

(c) LSB Blue

Figure 2.4 (a) (b) (c) LSB (Red, Green, and Blue) matrix

2.3) Proposed Algorithm

This section provides the step processes involved in the proposed system of color image steganography. The encryption process is described using table 2.1.

Table 2.1 Proposed Algorithm

Input: Message to encrypt M, Cover image I

Output: Steganographic Image I_s

Process:

1. $T = readTextMsg(M)$
2. $E_t = ECC.Encrypt(T)$
3. $B_N = E_t.Convert2Bits$
4. $[row, col]readImage(I)$
5. $for(i = 1; i < row; i++)$
    a. $for(j = 1; j < col; i++)$
        i. $P_{i,j} = LSB.replace(B_j)$
    b. $end\ for$
6. $end\ for$
7. $I_s = ReconstructImage(P)$
8. Return I_s

3. RESULT ANALYSIS

After successfully implementation of the proposed image steganography technique, performance of proposed algorithm is evaluated on different file size. The performance of the secure image steganography of cryptography is implemented techniques is given using the following given parameters.

3.1) Time Consumption

The amount of time required to process the selected proposed algorithm is known as time consumption. The evaluation of time usage is demonstrating using cryptography concept in figure 3.1 and table 3.1. In this diagram the X axis shows the file size (in terms of KB-kilobytes) of images used for experiments and the Y axis shows the amount of time consumed for estimation of required time.

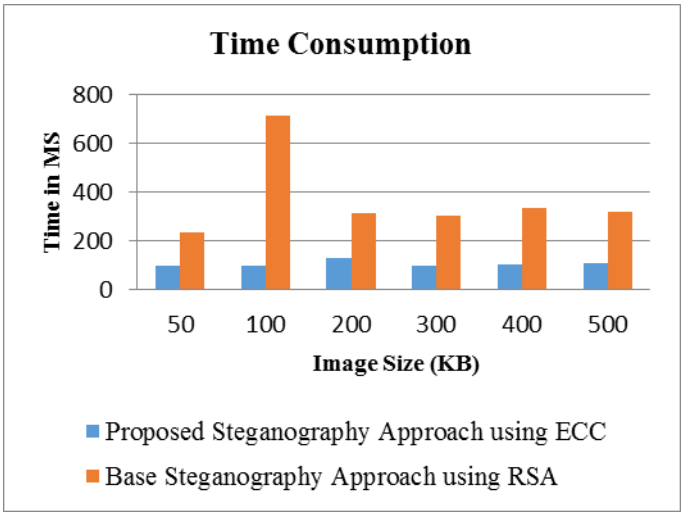


Figure 3.1 Time Consumption

In this bar graph, we have been plotted different file size values for depiction of output variation. Blue line represents the proposed steganography approach for different experimental scenario, where orange line shows the base approach of text hide. Moreover, with increasing size of data the time consumption of the proposed approach is increases. Therefore the proposed technique is more efficient and accurate for hiding data into image file a as compared to base RSA method.

Table 3.1 Time Consumption

Image Size (File size in KB)	Proposed Steganography Approach using ECC	Base Steganography Approach using RSA
50	101	238
100	101	716
200	130	312
300	101	305
400	105	336
500	110	320

3.2) Memory Consumption

The amount of main memory required to execute the implemented proposed algorithm is termed as space (memory) complexity. The figure 3.2 and table 3.2 shows the performance of the developed hide text in to image steganography algorithm. For results demonstration of both approaches the X axis shows the different data file size in KB respective to be performed experiments and the Y axis shows the memory consumption during encryption in terms of kilobytes.

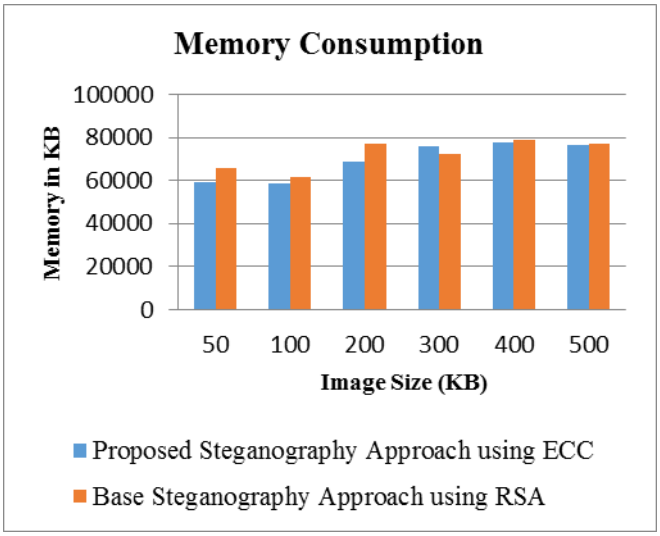


Figure 3.2 Memory Consumption

In order to show the performance of proposed and base algorithm in figure 3.2 where blue line is used for proposed steganography approach of hide text into image and orange line show for base RSA approach. According to the given results most of the time the memory consumption is much stable for and many time it varies whenever we increases the data size. In addition of that the space complexity of the algorithms are increases with the increasing size of experimental images. Therefore the proposed algorithm is much adoptable due to constant memory consumption. For more clear performance we included tabular form of all output values in table 3.2.

Table 3.2 Memory Consumption

Image Size (File size in KB)	Proposed Steganography Approach using ECC	Base Steganography Approach using RSA
50	59348	65732

100	58604	61520
200	68668	77004
300	75800	72248
400	77623	78654
500	76558	77015

3.3) Mean Square Error (MSE)

The mean squared error (MSE) of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss.

In this figure 3.3 and 3.3 table, depiction of mean square error of input data images for proposed and base method. The Mean Square Error is defined as the square of the difference between the pixel values of the original image and the Stego image and then dividing it by size of the image.

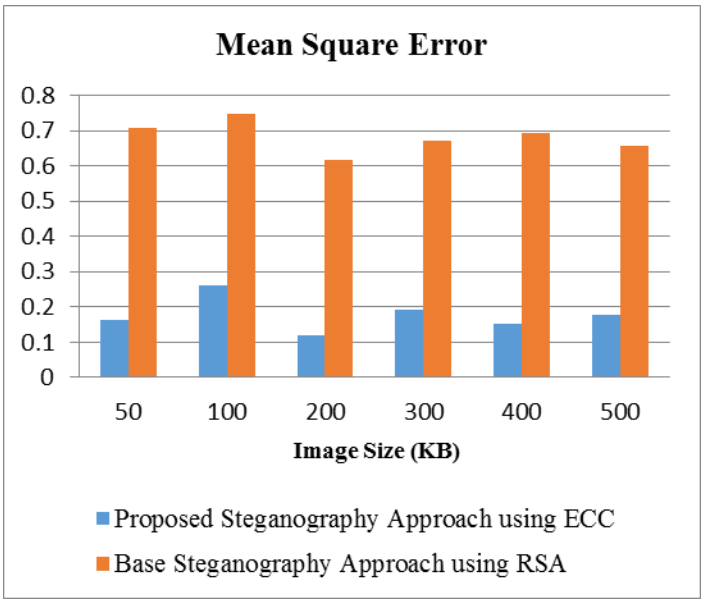


Figure 3.3 Mean Square Error

The proposed image steganography technique show while X-axis depicts different data size and Y-axis shows the error in percentages. The lower value of Mean Square Error (MSE) signifies lesser error in the Stego image in other words better quality.

Table 3.3 Mean Square Error

Image Size (File size in KB)	Proposed Steganography Approach using ECC	Base Steganography Approach using RSA
50	0.1618	0.7061
100	0.2609	0.7490
200	0.1198	0.6167
300	0.1933	0.6715
400	0.1533	0.6939
500	0.1771	0.6581

3.4) PSNR (Peak Signal to Noise Ratio)

The PSNR measures the peak signal-to-noise ratio between two images. This ratio is often used as a quality measurement between the original and a compressed image. Higher the PSNR means better the quality of the compressed or reconstructed image. The PSNR value can be calculated as:

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right)$$

Peak signal to noise ratio of the proposed techniques for image steganographic is given using figure 3.4 and table 3.4. In this diagram the X axis shows the experimental file size and the Y axis shows the obtained PSNR ratio. The blue line shows the proposed image steganography technique. The amount of computed PSNR is fluctuating with the image quality therefore that is not depends on the image size that is depends on the quality of image.

Table 3.4 PSNR Values

Image Size (File size in KB)	Proposed Steganography Approach using ECC	Base Steganography Approach using RSA
50	56.0407	49.6417
100	53.9656	49.3858
200	57.3439	50.2299

300	55.2682	49.8602
400	57.3215	50.6551
500	55.8932	49.5531

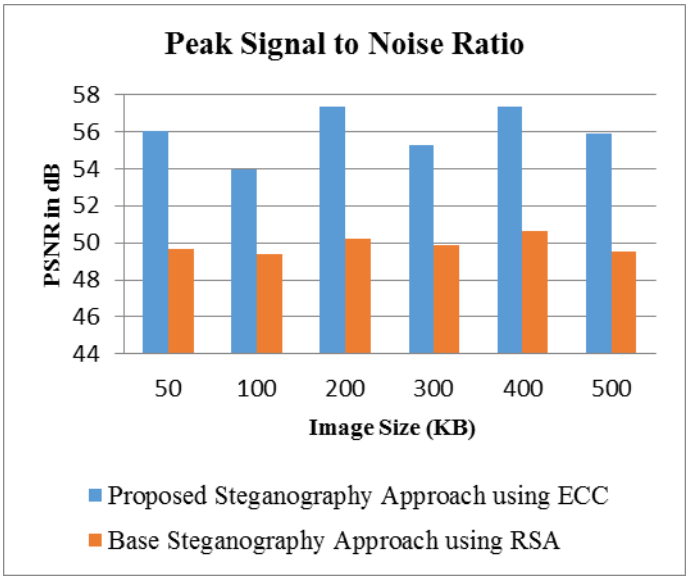


Figure 3.4 PSNR

3.5) Normalized Absolute Error (NAE)

Normalized Absolute Error is a measure of how far is the referenced image from the original image. Large value of NAE indicates poor quality of the image. This quality measure can be expressed as follows:

$$NAE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(|A_{ij} - B_{ij}|)}{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{ij})}$$

The original cover image A sized $m \times n$ and the Stegno image B sized$m \times n$, and A_{ij} and B_{ij} are pixel located at the $i_{t\square}$ row and the $j_{t\square}$ column of images A and B, respectively.

The above given figure show the normalized absolute error of the implemented proposed approach. In this graph, blue bar indicate our method for a given input. Additionally, X-axis depict different image size and Y-axis plotted values of different execution of different images. For more clear, we add tabular form of plotted values. Hence, A higher NAE value shows that image is of poor quality.

Table 3.5 NAE Values

Image Size (File size in KB)	Proposed Steganography Approach using ECC
50	0.12983
100	0.13276
200	0.17326
300	0.18897
400	0.24797
500	0.27789

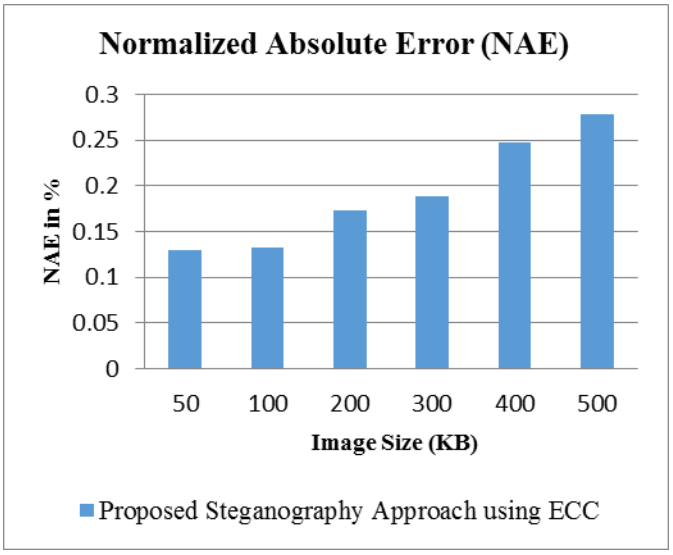


Figure 3.5 Normalized Absolute Error

3.6) Maximum Difference (MD)

MD (Maximum Difference) provides the maximum of the error signal (i.e. difference between the processed and reference image). It is obtained by measuring the distortion between the original and the fused image. MD is defined as follows:

$$MD = \text{Max}\,(|A_{ij} - B_{ij}|)$$

$$\text{Where } i = 1, 2, 3, \ldots\ldots m. j = 1, 2, 3, \ldots\ldots n.$$
$$A = \text{Original Image}, B = \text{Referenced Image}$$

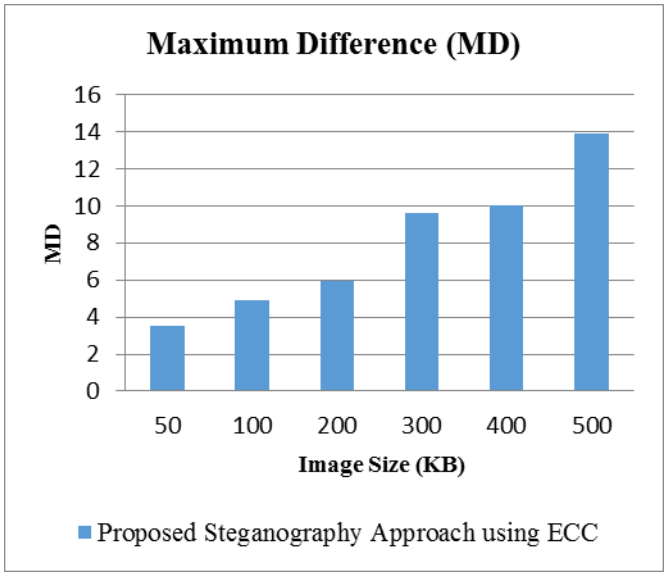


Figure 3.6 Maximum Difference

In this graph, we demonstrate performance of the maximum difference of the images. For the performance of image quality we take two input images i.e. original image and referenced image. Proposed steganography approach is implemented successfully for given images which is ensure for security during message exchange. The values of maximum difference is increasing whenever we are increasing image size respectively. Hence, higher the value of the maximum difference, the poorer the quality of the image.

Table 3.6 MD Values

Image Size (File size in KB)	Proposed Steganography Approach using ECC
50	3.50402
100	4.88608
200	5.93022
300	9.58614
400	10.0056
500	13.89533

3.7) Normalized Cross Correlation (NCC)

NCC (Normalized Cross Correlation) measure shows the comparison of the processed image and reference image. NCC is expressed as follows:

$$NCC = \sum_{i=1}^{m}\sum_{i=1}^{n}\frac{(A_{ij}XB_{ij})}{{A_{ij}}^2}$$

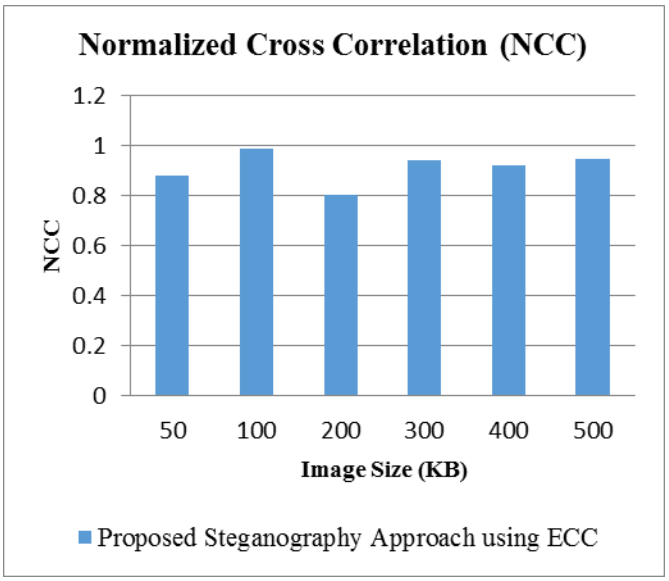


Figure 3.7 Normalized Cross Correlation

Normalized cross-correlation, which can efficiently handle image pairs with significant rotation and scale changes. Figure 3.7 show the depiction of the normalized cross correlation which is based on pairs on images. In this graph, X-axis show different image size and Y-axis show performance of NCC. Blue bar demonstrated performance of proposed steganography approach. The parameter of this approach i.e. NCC is producing values approximately to near of each other of variation of image size. Therefore, we can say that NCC of different file size is approx. similar. Tabular value are also listed this parameter.

Table 3.7 NCC Values

Image Size (File size in KB)	Proposed Steganography Approach using ECC
50	0.87833
100	0.98702
200	0.80507

300	0.93998
400	0.92401
500	0.94495

4) CONCLUSION AND FUTURE WORK

The main objective of the proposed LSB based steganography is to provide high degree of security during message exchange. Therefore a method is proposed and implemented. This chapter includes the conclusion of the conduced work in this context additionally the future scope of the work is also submitted.

4.1) Conclusion

The data security is a major concern in these days communication. Everyone is well understood the security and the techniques of securing data. Therefore any high confidential data exchange in normal network is a concern of network and data security. In this presented work the main aim is to study to secure data in un-trusted environment of data communication. In various applications such as security agencies and their communications are need to be prevented from any kind of attack and mislead. Therefore by motivation of this different cryptographic and stegnography techniques are studied and a new technique is presented in this work.

The basic motive of this presented study is to explore the techniques of cryptography and color image stegnography for improving the security to communicate sort secret messages. Therefore first the data or message to be hiding is taken as input to the system and for encryption of data ECC (elliptic curve cryptography) is used. After encryption of data that is converted into the binary format. In order to hide data and transmit to the receiving party the stenographic technique is used. Thus a color image is accepted as input to the system and this color image LSB is used to hide the data. In this work the 3bit LSB stenography is used to hide the data. The key advantage of color image is their ability to hide large amount of data in their pixel definition because each pixel is defined using three color composition and a small change in these three definition in last bits are not effect much in the actual image definition.

The implementation of the proposed color image stegnographic technique using ECC algorithm is performed in visual studio technology. Additionally for computing the complexity of the implemented cryptographic system time and space complexity is computed that is reported in table 4.1. In addition to that how accurately the pixels of image modified and recovered is described using MSE and PSNR parameters which are also included in this table by their mean values.

Table 4.1 Average Performance

S. No.	Performance factors	Proposed model	Traditional model
1.	Memory utilization	69433.5 KB	72028.83 KB
2.	Time requirements	108 MS	371.166 MS
3.	MSE	0.1777	0.68255
4.	PSNR	55.98	49.88
5.	NAE	0.19178	-
6.	MD	7.96789	-
7.	NCC	0.91322	-

The performance of the proposed stegnographic model demonstrates it is efficient, secure and effective for hiding short messages on the image data. In this context the proposed technique outperform respectively to the traditional technique.

4.2) Future work

The proposed work is a fusion of cryptography and stegnography for enhancing the security of data during communication. In this context a model is proposed and implemented successfully. In near future the following future extension is possible for more improvement.

1. Include some additional encoding scheme and/or compression technique to reduce the amount of data hiding by which the PSNR of image can improved more
2. Explore the techniques beyond the LSB based data hiding process to make more stronger techniques for stegnography.
3. Include the technique to secure messages by utilizing some authentication approach before recovery of messages.

REFERENCES

[1] Zhou, Xinyi, et al. "An improved method for LSB based color image steganography combined with cryptography", 2016 IEEE/ACIS 15th International

Conference on Computer and Information Science (ICIS), 2016.

[2] Clerk Maxwell, "Digital image representation", available online at: http://pippin.gimp.org/image_processing/chap_dir.htm

[3] Sadoon Hussein Abdullah, "Steganography Methods and some application (The hidden Secret data in Image)", available online at: http://www.iasj.net/iasj?func=fulltext&aId=37681

[4] N. Provos, "Probabilistic Methods for Improving Information Hiding", CITI Technical Report 01-1, January 31, 2001

[5] A. Cheddad, J. Condell, K. Curran, P.M. Kevitt, Digital image steganography: survey and analysis of current methods, Signal Process, 90 (2010), PP.727–752.

[6] H. Wang, S. Wang, Cyber warfare: Steganography vs. steganalysis, Communication ACM 47 (2004) PP.76–82.

[7] R an Isbell, "Steganography: Hidden Menace or Hidden Saviour", Steganography White Paper, 10 May 2002.

[8] Muhalim Mohamed Amin "Information Hiding Using Steganography", ethesis, Universiti Teknologi Malaysia, 2003.

[9] Komal Patel and Sumit Utareja, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Applications (IJCA), Volume 63– No.13, February 2013.

[10] Sumeet Kaur, Savina Bansal, and R. K. Bansal, "Steganography and Classification of Image Steganography Techniques", International Conference on Computing for Sustainable Global Development, IEEE 2014

[11] R. Popa,"An Analysis of Steganographic System", The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.

[12] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[13] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.c.