

# Design and Implementation of Spatial Domain Technique in Steganography Using RSA Encryption with Genetic Algorithm

*\* Jyoti Nanwal*

*\* Pooja Nanwal*

## Abstract

The usage of internet is increasing day by day and network security is becoming more important to us as the volume of data being exchanged is increasing. The data (i.e. secret data) transmitted by the sender can be detected, altered or modified in the network. In this paper, to prevent the data from being detected, we used modified Least Significant bit technique for hiding the data into bits of the image pixel and to prevent the data from being modified or altered, RSA encryption technique combined with Genetic algorithm was used as it would be very hard to break. We changed the least significant bit (LSB) to the nearest pixel according to the secret data bit so that it would be hard to find out the original message. In the present work, modified least significant bit embedding technique was used with genetic algorithm and encryption technique to get enhanced results or to get better results in terms of better security, image quality, PSNR ratio, and robustness. Encryption technique uses the concept of both public and private key to enhance the security level of the proposed work.

**Keywords:** Cryptography, data security, steganography

## I. INTRODUCTION

Steganography is related to hiding data so that one can't detect the presence of secret information, whereas in cryptography presence of data can be detected but obtaining the original message is hard as the data is present in encrypted form. Steganography is an art of hiding confidential data in the cover media so that intruder can't detect and alter the information to cause harm [1]. With cryptography we tried to improve the security level. If intruder detects the message he would see it in encrypted form. So, it would be of no use to him. A secure data transmission is made using cryptography and steganography. Combination of both these techniques resulted in creating a highly secured method for data communication [2]. The Application of Steganography can be Access Control System for Digital Content Distribution Confidential Communication and Secret Data Storing, e-Commerce, Protection of Data Alteration, Media, digital watermarking, database systems, etc..

In a steganography system there are two entities i.e. cover image and secret message. Cover Image is used for

data hiding. The message to be hidden is called the embedded message or the secret message. At transmitter side, these two are combined using one algorithm. Thus, presence of secret message cannot be recognized. This combination of cover image and secret data is termed as stego-message or stego-image [3]. Data type of cover message and stego message must be the same. With the help of figure 1 we can easily understand the flow.

## II. RELATED WORK

In order to transfer the data securely to the destination without any changes image steganography and cryptography using genetic algorithm and least significant bit technique is used. The sender selects an appropriate cover image in which the data is embedded. Data can be a text file which is first encrypted then converted into binary array of bits afterwards to embed it in the cover image. Steganography with cryptography assures security, capacity, and robustness for secure data transmission over the internet or network.

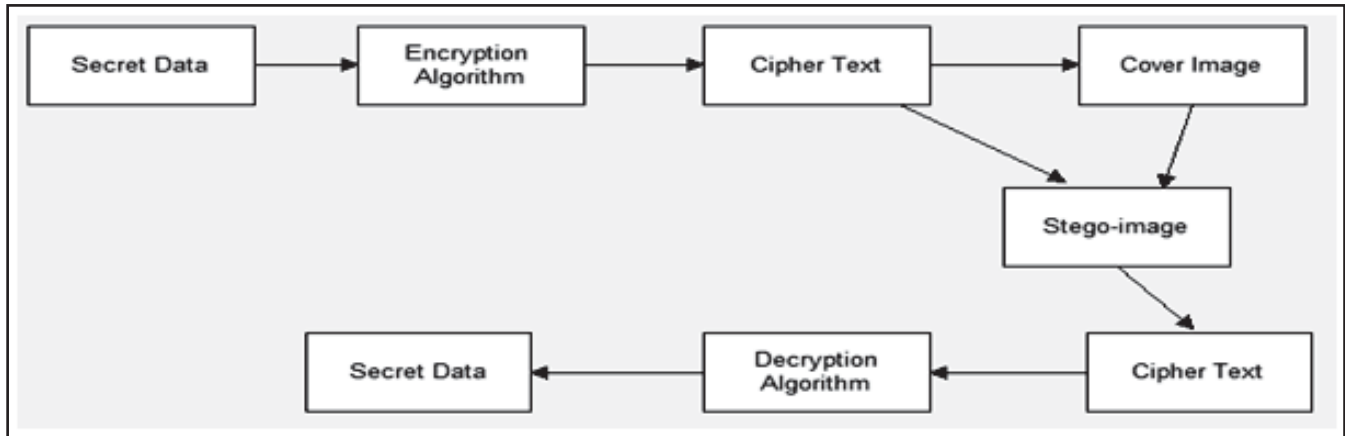
---

Manuscript received August 18, 2017; revised August 25, 2017; accepted August 27, 2017. Date of publication September 6, 2017.

\*J. Nanwal and P. Nanwal are with YMCA University of Science and Technology, Haryana, India - 121006.(email: nanwaljyoti1993@gmail.com, [pooja.nanwal02@gmail.com](mailto:pooja.nanwal02@gmail.com))

DOI: 10.17010/ijcs/2017/v2/i5/118806

Fig.1. Flow of the steganography and cryptography



### III. EMBEDDING

Modified Least significant bits (LSB) technique is chosen because it hardly distorts the image quality i.e. quality of cover image is hardly affected, capacity of hiding is good and it is also simple to implement. The human visual system can't find out the difference between the original image and the stego-image.

In modified LSB technique first we read the cover image file, then we break the message in bits which are called secret bits, instead of text message. We can either use an image or a video file. The secret data can be in text file or in binary form. If the secret data is in the text file then we have to convert it in binary value first and then it will be embedded into the cover image. Convert the image to matrix of pixels and then access the pixel value to convert it in binary after that access the LSB of the pixel [4]. Each secret bit is checked sequentially and embedded in the LSB of pixel of the cover image. It can be sequential or in randomised manner. Here we are modifying pixel to the nearest pixel according to the value of the secret data bit. Then finally we write the stego image.

At the receiver side stego-image is again converted in the matrix of pixel values. LSB of the pixel is accessed sequentially or in randomised manner, combining these bits to form bytes and bytes to form complete secret data. Retrieve bits and convert the set of eight bits into character to get the original form of the message i.e. text.

### IV. ENCRYPTION

For the encryption here we are using RSA algorithm given by Ronald Rivest, Adi Shamir, and Leonard Adleman which is based on public and private key

concept. In this algorithm two prime numbers are selected by using genetic algorithm which is far and large enough to break [5]. Human mind can't remember such large numbers, so it is hard to break the original message. It is a strong encryption technique with dual key concept i.e. public and private key. Sender encrypts the data by using public key and the receiver decrypts the data using a private key only. If the receiver does not have the private key, he is not the authenticated person and he will not be able to decode the original message. Hence, we are using this technique for the encryption of our data.

Receiver gets the stego-image, the image in which secret data is hidden in encrypted form and performs the reverse operation to extract the original message.

### V. PROCEDURE

In the proposed work there are two main entities that are basic requirements. These are: 1) Cover Image 2) Secret Data. Similar type of approach was also used by Dr. C.Immaculate Mary and P. Roshni Mol but with Caesar cipher algorithm for encryption and Diffie Hellman Key Exchange Algorithm, they also used the concept of Neural Key Generation [6]. Two entities that are feed for the Base algorithm are:

#### A. Base Algorithm - Modified LSB Technique

This base algorithm is a combination of steganography and cryptography. In steganography modified LSB technique is used, whereas, for cryptography RSA encryption algorithm is used. These are the steps of the proposed base algorithm:

**Step 1:** Read the cover image. This comes in the form of

matrix of decimal values. Then these decimal values are converted to binary values.

**Step 2:** Read the text message to hide. This will also be converted into binary bits so that further steps can be performed smoothly.

**Step 3:** Encrypt message using RSA cryptography technique.

**Step 4:** Keys are generated using the combined approach of Genetic Algorithm and RSA encryption algorithm.

**Step 5:** Get the encrypted data. Convert the data from decimal to binary.

$[Message] \xrightarrow{\text{Dec to Binary}} [1000001]$

**Step 6:** Break the byte to be hidden into bits.

$[10000001] \xrightarrow{\text{is divided into 8 bits}} [10000001]$

**Step 7:** Find the length of the secret data or message.

**Step 8:** Find the Least Significant Bit for each pixel of the cover image. This can be done by taking modulus of the pixel with 2.

**Step 9:** Compare the LSB bit of each pixel with the secret data bits. The LSB insertion technique is done based on two conditions.

**Condition 1:** If LSB bit equals zero and secret data bit equals one, 1 is added to each and every pixel of the cover image

**Condition 2:** If LSB bit equals to one and secret data bit equals to zero, 1 is subtracted from each and every pixel of the cover image.

**Step 10:** The hiding process is guided by a key entered by the user. The modified image is the stego image with the secret data in it.

**Step 11:** The reverse process is done for extracting the secret data from the stego image.

**Step 12:** Secret data bits are finally converted to text format. After a call to decryption algorithm, the hidden message is retrieved.

## B. RSA algorithm

For the encryption of secret data, RSA algorithm has been used. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. Here RSA algorithm is combined with genetic algorithm for the automatic calculation of two large prime numbers [5]. RSA involves a public key and private key. The public key is used to encrypt messages and private key is used by receiver for decryption. Steps of algorithm are given below:

Step 1: Call Genetic Algorithm to find two prime numbers  $p$  and  $q$  which are sufficiently large.

Step 2: Calculate  $n = p * q$

Step 3:  $n$  is the modulus for the public key and the private keys

Step 4: Calculate the totient :  $\Phi(n) = (p-1)(q-1)$  .

Step 5: Choose an integer  $e$  such that  $1 < e < \Phi(n)$ , and  $e$  is co-prime to  $\Phi(n)$  i.e.  $e$  and  $\Phi(n)$  share no factors other than 1;

$\gcd(e, \Phi(n)) = 1$

Where ' $e$ ' is released as the public key exponent

Step 5: Compute  $d$  to satisfy the congruence relation  $de = 1 \pmod{\Phi(n)}$  i.e.  $de = 1 + k\Phi(n)$  for some integer  $k$  . where ' $d$ ' is kept as the private key exponent

The public key is made of the modulus  $n$  and the public (or encryption) exponent  $e$  .(used at Sender). The private key is made of the modulus  $n$  and the private (or decryption).

## Genetic Algorithm

To obtain the optimized result, RSA algorithm is combined with the genetic algorithm [7]. Steps of genetic algorithm is given below:

**Step 1:** Randomly generate initial population as follows:


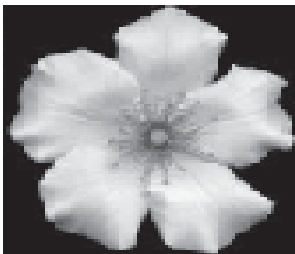

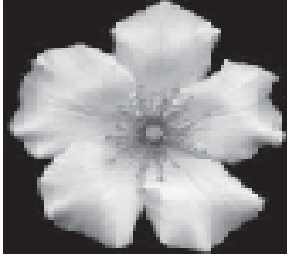

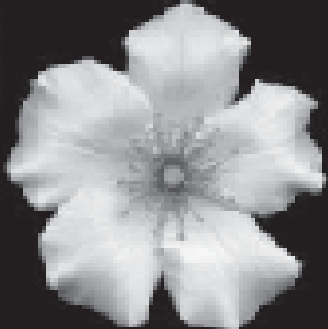
No. of chromosomes = 15

Length of chromosome = 8

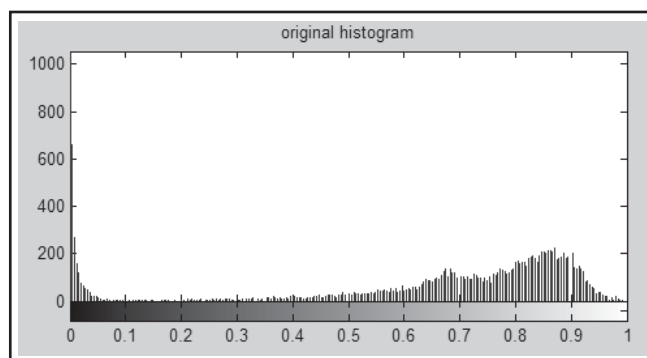
Type of chromosome = Binary

**Step 2:** Evaluate individuals for fitness.

**TABLE I.**  
**RESULTS ON THE BASIS OF IMAGE QUALITY**

| Technique Name   | Original Image   | Stego-image   |
|--|--|---|
| LSB technique  |   |   |
| Pseudo-random<br>LSB substitution<br>technique   |   |   |
| Proposed results :-<br>Modified LSB with<br>RSA encryption<br>using genetic<br>algorithm |  |  |

**Fig. 2. Histogram of the original image**



Fitness function:

- A chromosome is more fit if distant from its neighbors.
- This ensures the selection of two prime numbers which are far apart.

**Step 3:** Select more fit individuals for crossover.

**Step 4:** Crossover is 2-point crossover with a rate of 80%.

**Step 5:** Mutation randomly flips a bit in chromosomes and make next population.

**Step 6:** Repeat steps 2 to 5 till 50 rounds of iteration.

Here, all these algorithms are used to accomplish the proposed work.

## VI. RESULTS AND DISCUSSION

Results were taken on the basis of various factors that are:

- Comparison of quality of the original image and the stego-image
- Comparison of Histograms
- Comparison of PSNR ratio

Here comparison of LSB, Pseudo random LSB and proposed algorithm are done. These comparisons (i.e. comparisons of LSB and pseudo random LSB steganography techniques) were also done by Dhall et.al [7] in their findings during the year 2015.

### A. Results on the basis of picture/image quality

Image quality of the images is hardly affected. Image quality also depends upon the length of secret data. Comparison of three techniques is shown in table I.

### B. Results on the basis of histograms

The histogram of the original image is given in fig. 2.

### C. Results on the basis of PSNR ratio

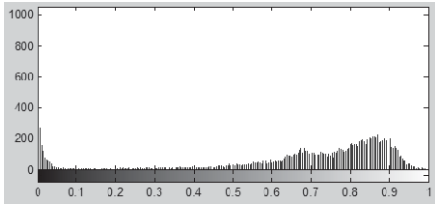
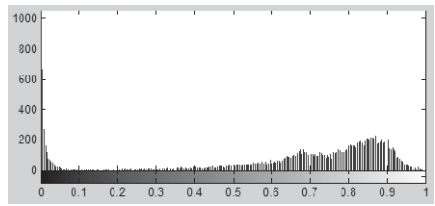
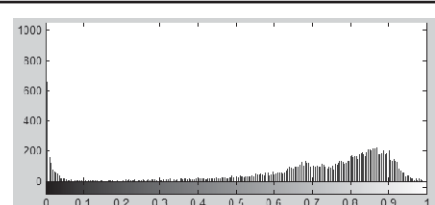
Spatial domain techniques having signal to noise ratio [6 - 8] are shown in table III.

### D. Results on the basis of time complexity

Time complexity is the time taken by the algorithm to execute. It will vary according to the size of image. Here 128 bit image is used. The time complexity of LSB is less

as compare to pseudo-random LSB technique. The results corroborate the findings of Dhall et.al.(2015) (7). Modified LSB technique with genetic algorithm and RSA algorithm takes more time than other two algorithms because of its complexity as shown in table IV.

**TABLE II.**  
**RESULTS ON THE BASIS OF HISTOGRAM**

| Technique  | Histogram of the stego image   |
|--|--|
| LSB  |   |
| Pseudo-random LSB substitution technique                                     |   |
| Proposed results :- Modified LSB with RSA encryption using genetic algorithm |  |

**TABLE III.**  
**RESULTS ON THE BASIS OF PSNR ratio**

| Image Size | LSB   | Pseudo-Random LSB | Modified LSB with RSA encryption using genetic algorithm |
|------------|-------|-------------------|--|
| 64x64      | 62.72 | 63.36             | 79.03  |
| 128x128    | 68.9  | 69.09             | 81.6   |
| 189x194    | 70.28 | 70.92             | 83.78  |

**Fig.3. Comparison of PSNR ratio**

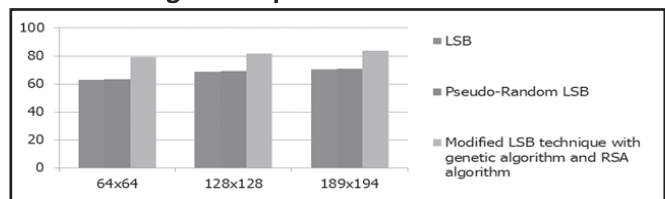


TABLE IV.  
RESULTS ON THE BASIS OF TIME TAKEN

| Technique | LSB       | Pseudo-random LSB | Modified LSB with RSA encryption using genetic algorithm |
|-----------|-----------|-------------------|--|
| Time      | 32.178212 | 42.231421         | 49.142567  |

## VII. CONCLUSION AND FUTURE WORK

The findings of present paper are based on the combination of steganography and cryptography in LSB technique. RSA encryption algorithm has increased the security level. Other encryption technique can be easily cracked by using some combinations but RSA algorithm is based on prime number which are far enough. This has improved the security level very much. PSNR ratio and time has been increased. This paper presents genetic algorithm which is used for automatic calculation of prime numbers which are large and far enough. Genetic algorithm has also given optimal results.

The method used in this study was implemented in the spatial domain and has achieved better results on the evaluation measures. This was tested on various images to get different aspects.

Further work is suggested on neural network instead of using Genetic algorithm. Further compression techniques can also be combined.

## REFERENCES

- [1] R. Jain and N. Kumar, "Efficient data hiding scheme using lossless data compression and image Steganography," *Int. J. of Eng. Sci. and Technol.*, vol. 4, no. 8, pp. 283-241, 2012.
- [2] D. Bloisi and L. Iocchi, "Image based Steganography and cryptography," *Comput. Vision Theory and Appl.*, vol. 1, pp. 127-134, 2014.
- [3] F. M. Shelke, A. A. Dongre, and P. D. Soni, "Comparison of different techn. for Steganography in images," *Int. J. of Application or Innovation in Eng. & Manage.*, vol. 3, no. 2, pp. 171-176, 2014.
- [4] C. A. Oluwakemi, S. A. Kayode, and J. O. Ayotunde, "Efficient data hiding system using cryptography and Steganography," *Int. J. of Appl. Inform. Syst.*, vol. 4, no. 11, pp. 6-11, 2012.
- [5] A. Kumar and R. Sharma, "A secure image Steganography based on RSA Algorithm and Hash-LSB technique," *Int. J. of Advanced Res. in Comput. Sci. and Software Eng.*, vol. 3, no. 7, pp. 1448-1454, 2013.
- [6] C. I. Mary and P. R. Mol, "An effective approach for hiding encrypted messages with neural key using LSB image Steganography," *Int. J. of Innovative Technol. and Res.*, vol. 4, no. 2, pp. 2832-2835, 2016.
- [7] S. Dhall, B. Bhushan, and S. Gupta, "An in-depth anal. of various Steganography techn.," *Int. J. of Security and its Appl.*, vol. 9, no. 8, pp. 67-94, 2015.

### About the Authors



**Jyoti Nanwal** received her M.Tech. (with specialization in networking) from YMCA University of Science and Technology, Faridabad, India. She completed her B.Tech from Manav Rachna College of Engineering, Faridabad, India. Her area of interest is networking.



**Pooja Nanwal** received her M.Tech. (with specialization in networking) from YMCA University of Science and Technology, Faridabad, India. She completed her B.Tech from Manav Rachna College of Engineering, Faridabad, India. Her area of interest is networking.