IMPLEMENTATION OF RECURSIVE METHOD IN IMAGE STEGANOGRAPHY

by

BHARATH SANAGASANI

PAVAN KUMAR UPPALA

Under supervision

of

Dr.Siamak Khatibi

Department of Applied Signal Processing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden.

Contact Information:

Author(s):
Bharath Sangasani
Address: Andhra Pradesh, India.
E-mail: bharath.sangasani@gmail.com.

Pavan Kumar Uppala
Address: Andhra Pradesh, India.
E-mail: pavank419@gmail.com.

Supervisor:
Dr. Siamak Khatibi
Blekinge Institute of Technology, Sweden
E-mail: siamak.khatibi@bth.se.

Examiner:
Dr. Sven Johansson
Blekinge Institute of Technology, Sweden
E-mail: sven.johansson@bth.se.

Department of Applied Signal Processing
Blekinge Institute of Technology
371 79 Karlskrona.

Internet	: www.bth.se
Phone	: +46 455 38 50 00
Fax	: +46 455 38 50 57

ACKNOWLEDGEMENTS

It gives us great immense joy in acknowledging **Dr.SiamakKhatibi** for his diligent support and extending the opportunity to pursue our master thesis under his immaculate supervision. We would like to thank **Mr.Sridhar Bitra** for providing valuable suggestions in the evolution of this thesis. We are indebted to our family and friends for their constant support those who helped us to complete this thesis.

This thesis is dedicated to our parents who stood beside us through thick and thin in making this thesis substantial.

CONTENTS

LIST OF FIGURES

TABLES

ABSTRACT

Nowadays steganographic techniques are with us and in everywhere because we are using information more and more and we need to have or transform the information as secure as possible. In these techniques we need to secure the information by encrypting (coding) and decrypting (decoding). In this thesis we propose a different coding procedure based on recursive methodology. We used image as medium for this steganographic technique. An image is splitted (coded) and merged (decoded) by recursive procedure. Our experiments show that the technique is applicable for both Gray Scale and Color images and also no need of providing a key security facility at the decoder end.

Keywords: Splitting, Encryption, Decryption, Recursive, Steganography.

1 INTRODUCTION

In today’s world there is a lot of advancement in technology especially in communication which is leading us to live a happy life and on the other side it is also leading us to live an insecure life due to exploitation of advanced technology in communication. Now exploitation has become the major criteria which should be solved. To solve this issue various techniques such as Cryptography, Watermarking, Steganography and some other different techniques have been developed. These techniques took various curves to refine it and they tried to prove themselves as the best, but due to over exploitation each and every method can be decoded. So we took exploitation as a challenge and also tried to develop a new technique under Steganography. We chose to develop a new technique under Steganography because it is one of the easy methods to encode but cannot be decoded easily.

Steganography is the art and science of hiding important information in such a way that only the specific person can retrieve the hidden information. The word Steganography has been evolved from a Greek word means “covered writing”. The word Stegano means “Covered or Protected” and Graphie means “writing” [1]. Steganography has various types of hiding information such as messages, images, audios, videos, etc., Steganography is being divided into three categories such as self-communication, one to one communication and one to many communications depending upon number of receiver’s. Steganography is applied in many ways in which some of them are implemented in day to day life without being noticed.

The Steganographic technique which we proposed is based on images. Digital images found in the internet can be used for different kinds of security threats. In this corporate world a mail carrying a single bitmap file can be enclosed with latest detailed secrets of a big Industry. Small image files can with-hold secrets of government or either latest military secrets. Due to that human vision system (HVS) is incapable of detecting minor changes in color patterns, taking this as an advantage original image files can be modified by adding either important text information or inserting different files into the pixels of an image without being detected.

In our thesis we proposed a new type of steganographic technique i.e., we are not introducing any text information or any files into the image but we worked on changing the original image information by splitting and shuffling the image into smaller pieces by introducing Recursive algorithm. We encrypted the image in such a way that the representation of the encrypted image should be as a noise and not look like an image. We also worked on reconstruction of this proposed technique using recursive algorithm.

1.1 MOTIVATION

The motivation behind this thesis is to find and design a unique encoding and decoding technique with the combination of different methods and algorithms to have a secure communication between the entities. The goal to design this thesis is not to use any cover medium like other available methods but to make totally different method i.e., the method should be in such a way that it should manipulate the decoder's and should not even be able to recognize that the file consists of an image or not and even should not be able decode the information by unauthorized people.

1.2 RELATED WORKS

Background Study

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files[1]. It is difficult for a normal person to see and understand an image which looks like noise. Many algorithms like LMS [2], [3], Lempel – Ziv Welch algorithm [4] have been developed for encoding and decoding using images. All introduced methods should be in such a way that both images should be of same size and pixel values even after encoding and decoding [4]. Several steganographic techniques have been evovled to increase the quality and intelligibility of hiding and retrieving the encoded data.

In previous methods many sophisticated steganographic techniques such as Canny edge Detection algorithm [5], LZW algorithm [6] etc.., have been used to increase the development of data hiding techniques. Some of the techniques follow few rules which would prefer to provide a serial or a key to the receiver to decode the encoded information [6]. Image segmentation techniques can be roughly classified into three types, namely, the histogram-based segmentation the neighborhood-based segmentation [7] and the physically-based segmentation methods [8, 9]. A new approach to design of a recursive image enhancer is introduced when the image is characterized statistically by its mean and correlation function [10]. There are some other techniques which look like steganography they are watermarking, cryptography and so on.., which have been widely used in hiding the data but these techniques reduce the quality of the input data due to rapid expansion of image acquisition and consumption and will provide a distorted output data [11].

Image partitions are risk combinational explosions due to two-dimensional nature of images [12]. The aim of an effective segmentation is to separate objects from the background and to differentiate pixels having nearby values for improving the contrast [13]. Extraction of the image should be done by calculating the most occurring pixel by same way as it has been embedded [14]. The pieces which are segmented should be in a confusing manner and mixing those segmented pieces recursively and then comparing the extracted secret image with the original secret image. Verifying whether the image has been altered by an intruder or not is also one of the categories which should be always checked [15]. Based on the difference between original intensity and the intensity of same pixel after embedding, adjustment has been made to minimize the impact of hidden data on the cover image, as final step of embedding [16]. Each and every algorithm works differently depending upon the type of image i.e., color or gray scale images [17]. A novel definition of histogram capacity curve taking into account the density distribution of histograms in the corresponding spaces is proposed and used to quantify the effectiveness of image descriptors and histogram dissimilarities in image retrieval application [18]. Image similarities are obtained through a weighted combination of overall similarity fusing global, semi-global and local region-based image level similarities [19]. Fibonacci Series follows as a mathematical necessity from the combination of an expanding apex and a suitable spacing mechanism for positioning new leave [20]. Correlation Coefficient is by far the most common index of the relationship between two variables [21].

1.3 CONTRIBUTION

We at first referred to more no. of papers on Steganography and got a general idea regarding the procedures of encoding and decoding. After that we studied about different types of algorithms used to encode and decode the data. In first session we tried to encode the image in a different way using block processing but that was not that reliable method to encode, so we tried to find out a new solution to make it more reliable and we found out a new algorithm known as recursive algorithm which is being implemented in other regions. To implement it we made more number of calculations to encode an image and to retrieve this as output also it takes more number of permutations and combinations are needed to be done so it is difficult for an unauthorized person to reveal the secret information which is being encoded. Splitting the image into different no. of pieces and to have a clear idea how we splitted the images in recursive method is a different technique implemented by us in image Steganography. Like other techniques we are not going to provide a key with the altered image.

1.4 AIMS AND OBJECTIVES

This thesis aims to create a different type of steganographic method by using recursive algorithm to split an image in different no. of pieces. Main goal of this thesis is to send information secretly such that an unknown person should be not able to extract the hidden information.

The objectives are as follows:

1. To understand how to create new technique in image Steganography using recursive algorithm.
2. To split an image into N no. of pieces using recursive algorithm.
3. To rearrange those splitted pieces and form the image which looks like a noise and should not provide any key to the receiver.
4. To the extract the hidden information using recursive algorithm.

1.5 RESEARCH QUESTIONS

1. How to use recursive algorithm in image Steganography?
2. How to split the image using recursive algorithm?
3. How to rearrange the huge vector which should look like noise but not as an image?
4. How to decrypt the image hidden using recursive algorithm?

1.6 THESIS OUTLINE

The rest of the document is as follows. Chapter 2 provides the technical background of our thesis. Chapter 3 describes the experimental methodology, design and implementation. Chapter 4 describes the results and its analysis. Chapter 5 comprises of measurements. Chapter 6 comprises of conclusion and 7 comprises of future work.

2 TECHNICAL BACKGROUND

2.1 RECURSIVE METHOD

The word recursive itself means to repeat again and again. Recursion can be explained by taking an example of two mirrors placed opposite to each other in parallel. Then we can observe infinite number of illusions of the mirrors. This process of repeating outputs again and again is known as recursion. It is used to manipulate the input data in order to achieve a desired output. Due to using recursive there is one advantage and also a disadvantage i.e. if we are writing code for recursion in correct manner then it will finish with in finite loops and we can achieve good results. If we are not using recursive in a correct way then it leads to endless infinite loops and does not stop execution of the program. This functionality of infinite loops causes our system to hang or shut down.

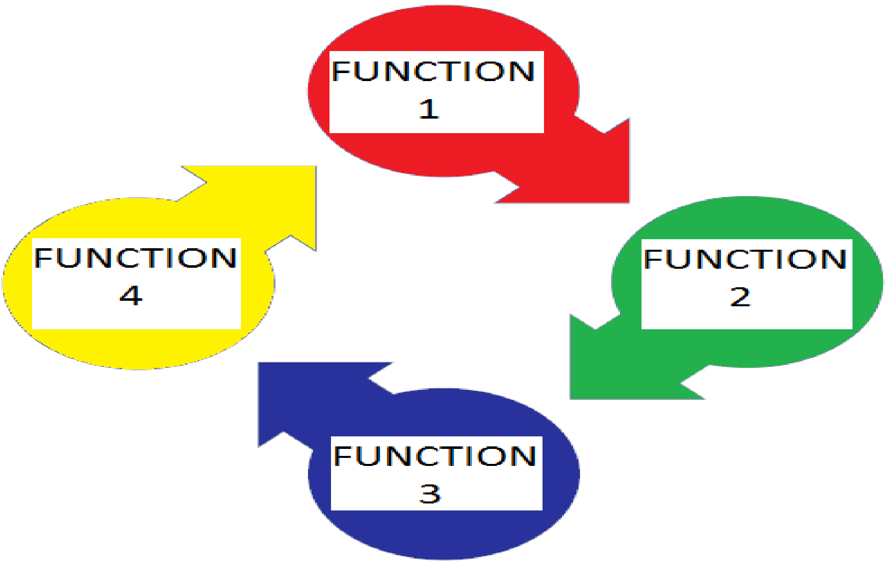


Figure1: Recursive method.

In our method e are using recursive in such a way that it have to call function into a function repeatedly to split the image into pieces in encryption. It is also used in decryption technique to club the splitted pieces into one huge matrix. We are using recursive function N number of times either to encrypt the image which should be hidden or even to decrypt the hidden data recursion is used n number of times.

Recursion is used in many different ways i.e., to solve huge problems by dividing it into small pieces. Recursive is commonly used in computer science, programming and mathematics. It is based upon large no. of permutations and combinations to solve a issue. Fibonacci series is the best example for recursion.

$F_1 = 1,\ F_2 = 1$

$F_n = F_{n-1} + F_{n-2}$

Fibonacci sequence is 1,1,2,3,5,8,13,21, 34……

2.2 Tree Method

Tree is a widely-used data structure which stores data with a set of linked nodes. The data structure is figure consists of nodes and edges are the links between them. Trees are usually used to represent data .As the trees contain the data; the node may contain a value or a condition or represent a separate data structure or tree of its own. In the tree each node contains any number of nodes .Each node contains a parent node. The node which doesn't have any child nodes is known as leaf nodes. If there is no kind of child node that means the tree is ended. In tree the height is calculated from the starting that is the very first node to the end of the tree (leaf).The height of the root is the height of the tree. Height can also represented as number of levels in the tree.

The tree contains number of nodes and a parental nodes and a child node. The starting of the node in tree is called as Root node. The root node is the main important one of the tree in which with this root node the tree will be starts. As this is the root node it doesn't have any parent node but it can have child node. By the starting of the root node all other nodes are reached from it by following edges and links. Generally trees are drawn in the plane and these are represented essentially uniquely in the plane so called plane trees.

Tree method

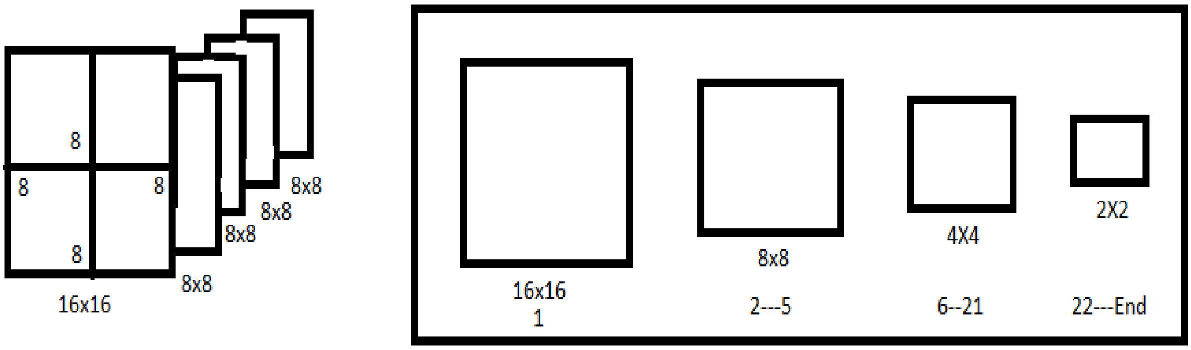


Figure 2: Basic Tree model

The above figure 2 shows how an image is being encrypted by splitting it into 4 pieces and those 4pieces are again being splitted N number of pieces in the form of nodes

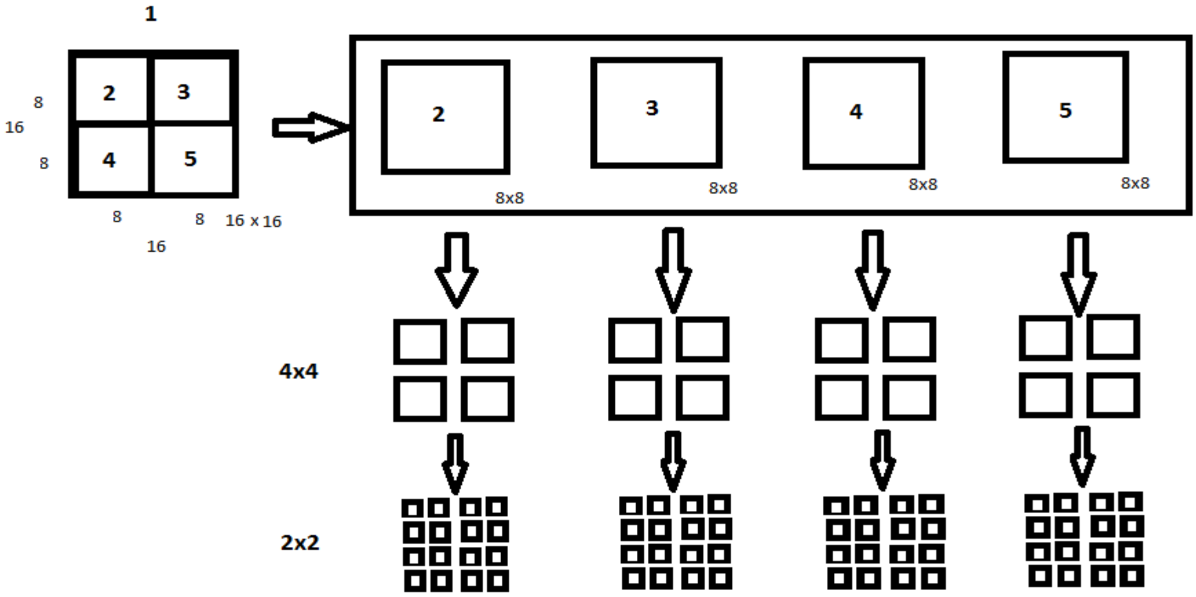


Figure 3: Method of splitting an image into small pieces

The above figure 3 shows the procedure of recursive way in the form of tree method that how an image is being splitted into N number of pieces.

Tree method for Encryption

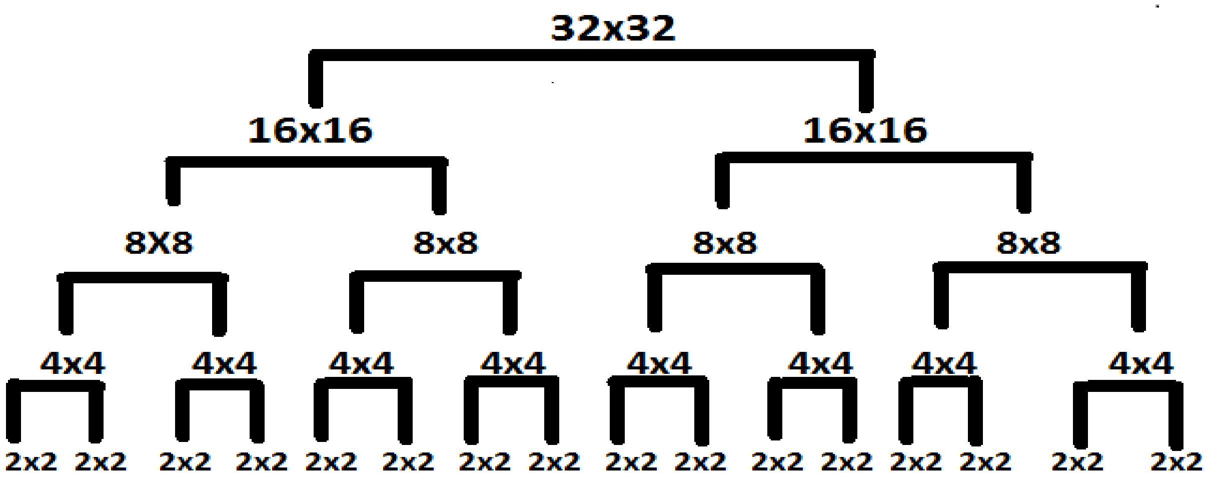

32x32
16x16
16x16
8X8
8x8
8x8
8x8
4x4
4x4
4x4
4x4
4x4
4x4
4x4
4x4
2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2

Figure 4: Tree method for Encryption.

The above figure 4 shows how an image is being splitted into pieces and encrypted in the form of tree method.

Tree method for Decryption

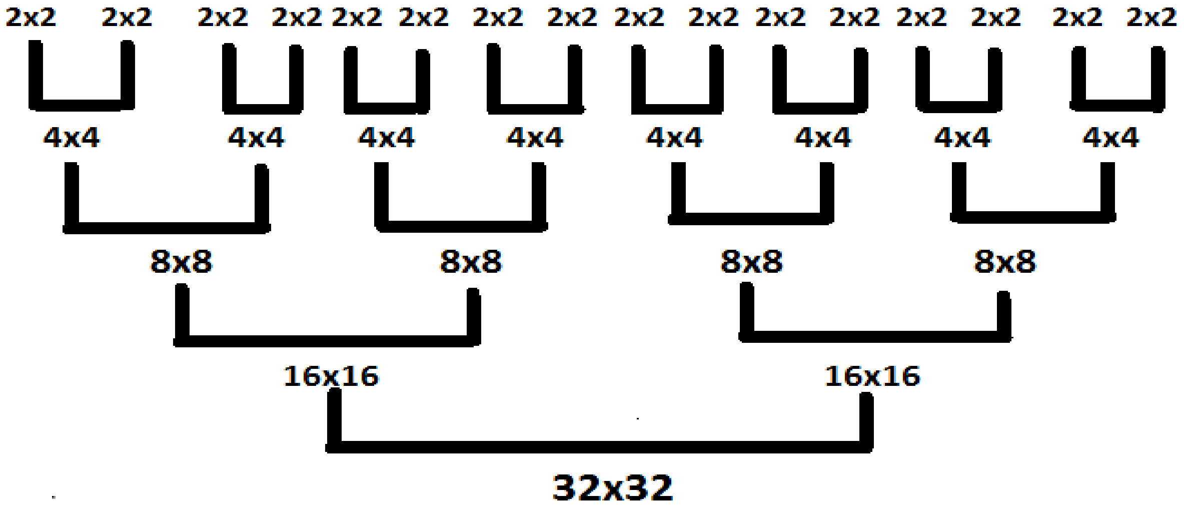

2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2 2x2
4x4
4x4
4x4
4x4
4x4
4x4
4x4
4x4
8x8
8x8
8x8
8x8
16x16
16x16
32x32

Figure 5: Tree method for Decryption

The above figure 5 shows how splitted pieces are being clubbed into pieces and decrypted in the form of tree method.

2.3 Reshape

In general cases reshape is used to transform one matrix into another matrix form which is not consider as a major role, but in our case reshape is a major command used for encryption and decryption of our images.

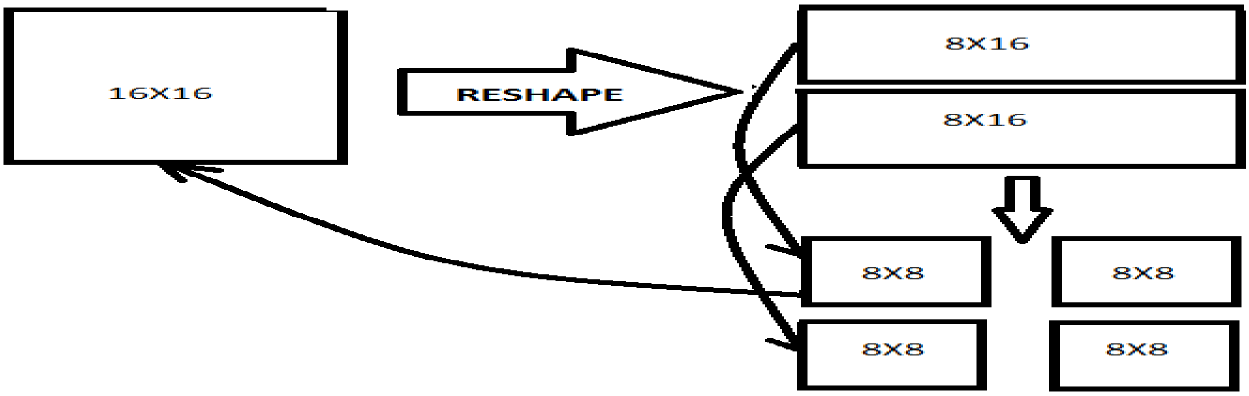


Figure 6: Block diagram of Reshape

Reshape is used in such a way that after each and every session of splitting of an image we are reshaping the matrices of splitted image. This process is done after splitting of an image,

Reshape is generally used for the changing the matrix. It is explained just as if we have two matrices A and B ,then the elements from A are taken in to B by reshaping i.e., if matrix A is 3-by-4 matrix then it is reshaped into a 2-by-6 matrix usually known as matrix B.

2.4 CORRELATION COEFFICIENT

Correlation Coefficient measures the degree of linear relationship between two variables. Two variables x and y are taken as input and to calculate the correlation coefficient CC(X,Y) the formula is derived the ratio between covariance of the two variables X and Y and the square root of the product of their X and Y variances.

$$\boldsymbol{CC(X,Y)} = \frac{\Sigma(\boldsymbol{X},\boldsymbol{Y})}{\sqrt{\Sigma(\boldsymbol{X},\boldsymbol{X})\Sigma(\boldsymbol{Y},\boldsymbol{Y})}} = \frac{\Sigma(\boldsymbol{X},\boldsymbol{Y})}{\sqrt{\boldsymbol{Var}(\boldsymbol{X}).\boldsymbol{Var}(\boldsymbol{Y})}}$$

Where $\Sigma(X, Y) = COV(X, Y)$

We use correlation coefficient to stop the iterations automatically until encryption of image is satisfied i.e., till the input image looks like noise. Since we know the procedure of encryption we are doing the exact reverse process in decryption to retrieve the encrypted image.

3 EXPERIMENTAL METHODOLOGY

This section describes regarding evaluation of algorithms in encryption, decryption and software tools which were used in our steganographic technique. This section consists of explanation of two experimental setups, one for encryption and the other for decryption.

3.1 ALGORITHM USED

There are different types of algorithms used by different steganographic to make their encryption robust. Most of different types of image steganographic techniques uses LSB algorithm. Only slight changes were made to the algorithms and some “ADD ON’s” will be made to propose a new technique.

But in our proposed technique we used a new different kind of algorithm i.e., Recursive algorithm which is never used in steganographic techniques. Recursive algorithm is nothing but calling a function inside the function repeatedly while execution of a program. This can be explained clearly by taking example of 2 mirrors, in which both the mirrors are placed parallel and facing opposite to each other. Then we can observe that infinite number of images can be seen in both the mirrors. This process of continuous iterations is called as recursion. Recursive algorithm gives the exact result only when the program written for recursive is correct otherwise if a program is written in wrong way it leads infinite number of loops that may cause to hanging crashing of operating systems, making system busy…, etc.

3.2 ENCRYPTION

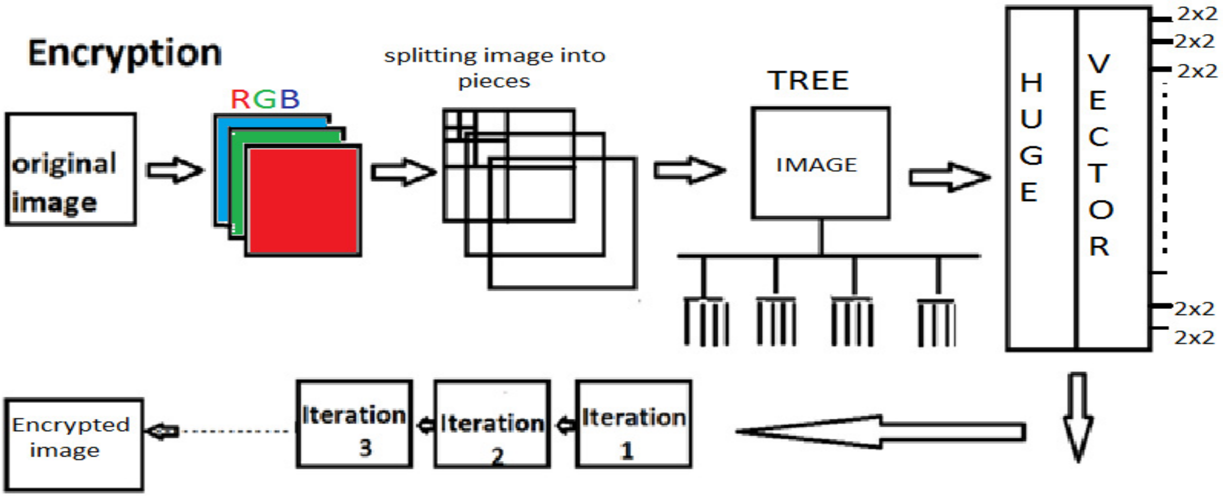


Figure 7: Block diagram of encryption technique using recursive method.

In first step we are writing a core function which divides the image into 2 halves and then reshaping it. Then again it is being divided into 4 pieces and then assigning a value to them. So that by doing this now we are having 5 nodes. The main image is the 1st node and when the image is splitted into 4 pieces then 2nd, 3rd ,4th and 5th nodes will be formed. Now the output of the 1st function which we are having is 5 nodes.

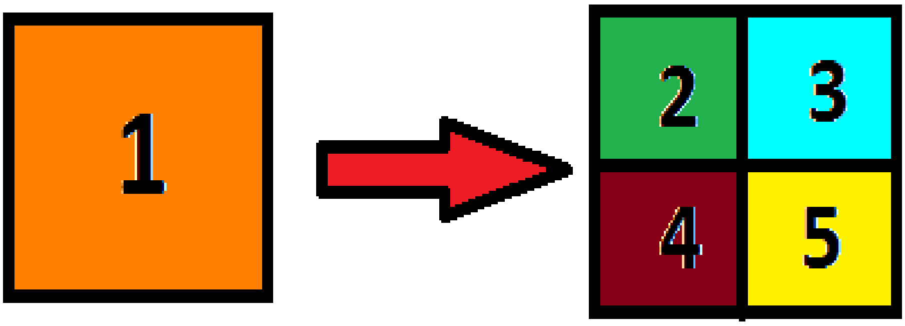


Figure 8: Reshaping of a matrix.

In second step we are again writing a function which takes output of 1st function as input. The 4 splitted nodes 2, 3, 4 and 5 will be taken as input. Now each node is again splitted into 4 sub nodes in that way at the end we get a result of 16 nodes and each node is being assigned with a value. Now we consider 16 nodes as inputs and again split them into each into 4 pieces. The result which we acquire is 64 new nodes and then again those are splitted into 4 pieces. In this process we are making a tree data structure for all nodes which are presented. This process will come to an end when we assign a value to stop the iteration. The value which we gave to stop the iteration is that each and every block should have a 2x2 matrix with its value assigned. By the end of this process we will have typical output containing splitted image of different no. of 2x2 matrices with values assigned. This process of calling a function again and again until the expected result is acquired without any infinite loop is known as recursion. For an input image given we get an output of different sets of sub matrices and huge vector .this vector values will be assigned. This process of dividing one matrix into 4 matrices and 4 matrices into 16 matrices and continuing it until we get 2x2 matrices is known as tree method. As soon as the splitted file is formed a value is assigned to that piece of image this process of assigning a value to the newly splitted pieces of image is known as indexing.

In third step we are repeating the above two process for a color image. We are making iterations for all three channels in a color image (RGB channels) and extracting the output of each channel as different number of 2x2sets of matrix

In the final step we will give image as an input. Then the width, height and channels are being calculated. Since the given input is a color image it will be having 3 stages. For the 3 channels R, G and B all the three steps above explained will be performed and we will have specific output which consists of different number of 2x2 matrices. We then reshape the splitted image pieces so that they form a different kind of shape which cannot be understood by an un authorized person. To make the output more reliable we again took the output as input and performed same process repeatedly using an iterative loop. So that the output which we get will look like a noise, so that an unauthorized person cannot understand that there is any information is provided in the noise. This noise output will be sent to the receiver in the network.

Therefore by acquiring an output which looks like a noise our encryption technique is successfully done.

3.3 DECRYPTION

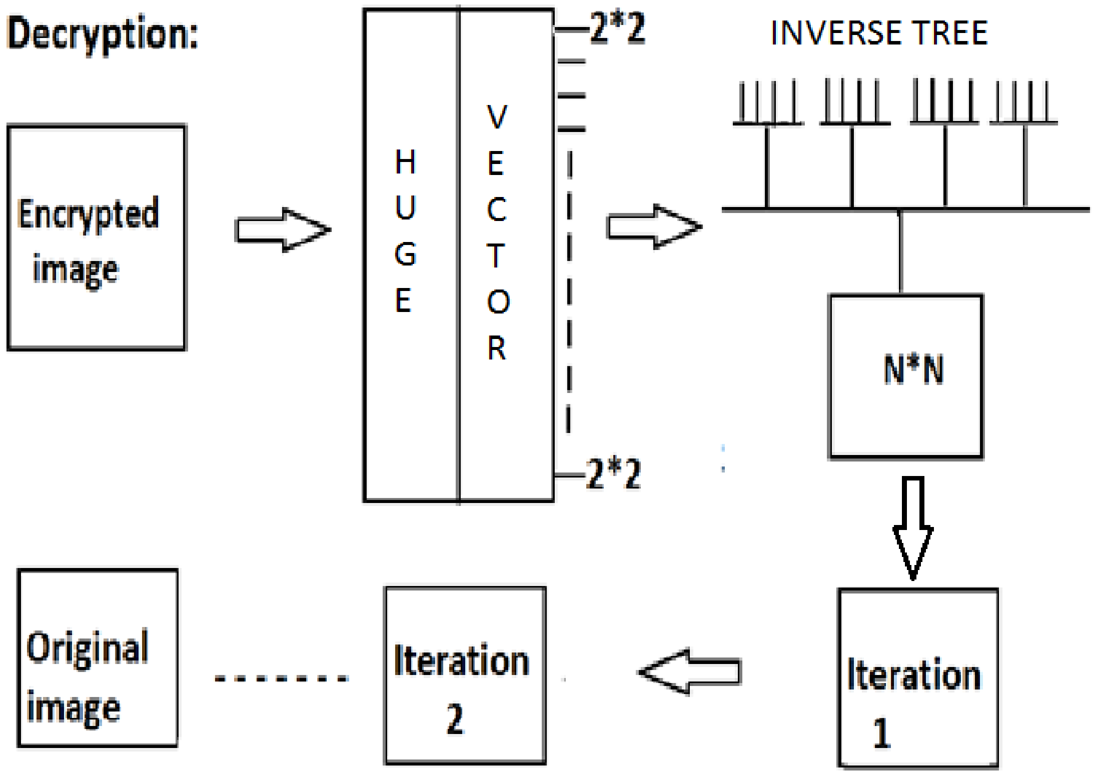


Figure 9: Block diagram of decryption technique using recursive algorithm.

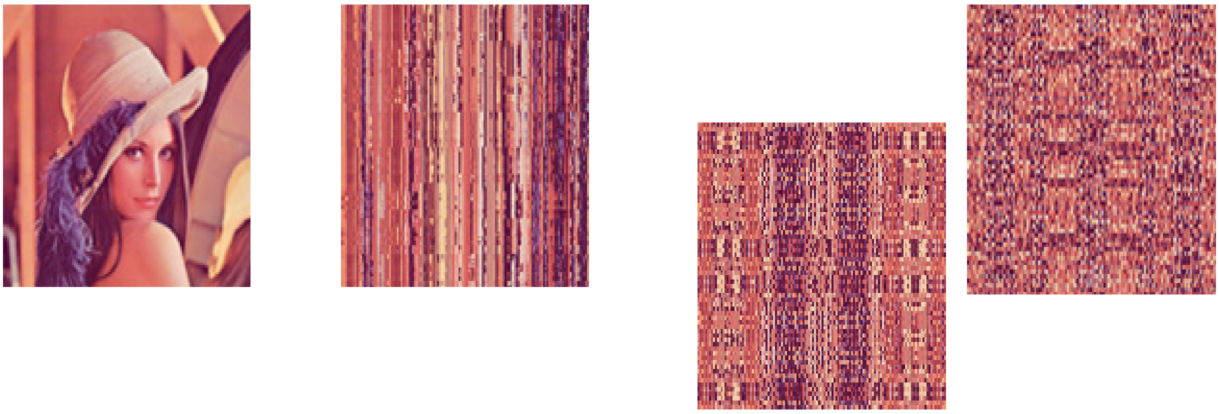
Decryption of this method is done by rearranging and clubbing of all the splitted pieces. But in general case we cannot decrypt if we don't know the how the file is encrypted. It is easy to decrypt a file which has encoded sequence or order. But in our case our file is encrypted in such a way that it looks like a noise and also there is no sequence or order to decrypt the image. The only way to decrypt our image is we should know how our image is encrypted.

In first step we receive an input image which looks like noise but it is combination of different no. of 2x2 matrices without any sequence. We will first reshape the input and take first 4 different matrices. According to the encryption sequence we segmented the image first into four pieces that was basic core for us. The exact reverse process should be done i.e., to make decrypting technique we have to make a core such that clubbing of four segmented pieces into one. Clubbing four 2x2 matrices into one 4x4 matrix. This should be written in a function so that it should be easy for us to call another function.

In second step we take input of 4 different 4x4 matrices and we club them into one to become one 8x8 matrix. This process will be done in a recursive way by clubbing different sets of matrices again and again i.e., we are calling a function into another function until all the matrices are clubbed to become one huge matrix. This process of clubbing different sets of matrix into on matrix is known as inverse tree method. We are doing an extra version in our encryption i.e., after encryption of image for one time we are again taking the encrypted output as input and making 2nd version of encryption and acquiring the output again. The next step is that we again taking the 2nd version output again into input. We are doing this again and again until we are satisfied with our encrypted output. These output versions can be done N different times using N no. of iterations. Since we know one version of extraction of the encrypted image, it is not enough to extract the image because in encryption N no. of versions are being done to encrypt the image. So to extract the original image one version of extraction should be repeated again and again to get the original image. The same way as encrypted image, we also have to make N no. of iterations of the extracted output to get the original image.

4 RESULTS

4.1 ENCRYPTION

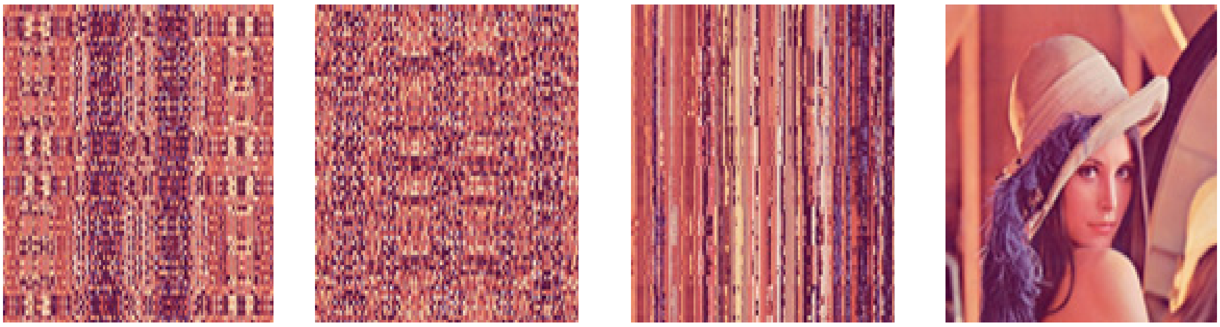


Original image 1st Iteration 2nd Iteration Encrypted image

Figure 10: Encryption procedure with images

The above figure 10 comprises of the steps of encryption. From the above results we can observe how an image is being encrypted using recursive algorithm in the form of iterations. These iterations are being done automatically using the correlation coefficient.

4.2 DECRYPTION



Encrypted Image Ist Iteration 2nd Iteration Decrypted Image

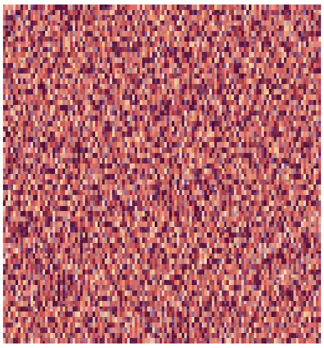
Figure 11: Decryption procedure with images

From the above figure 11 we can see the decryption procedure of the encrypted image using recursive method. These iterations are being done automatically using the correlation coefficient until we get the original image as output.

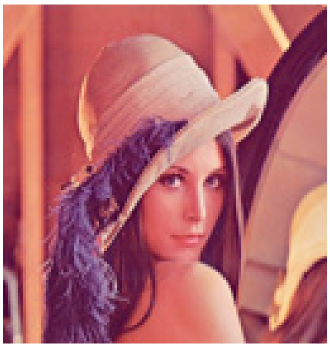
4.3 OUTPUT FOR DIFFERENT SET OF IMAGES

The results shown below are the regarding data set of different images which were used for descriding the experimental methodology which has been explained in the section 3. In the below images different set of images has been taken as input and the second image is the encrypted format of the input images. Encrypted image has been taken as input and then decryption procedure has been applied on it to retrieve the output image same as the input image which has been encrypted.

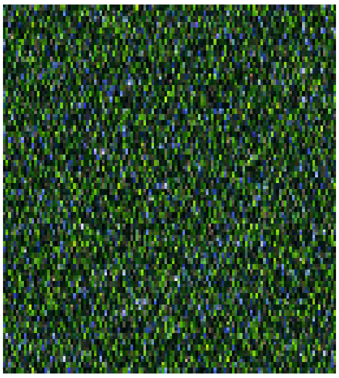
Input image

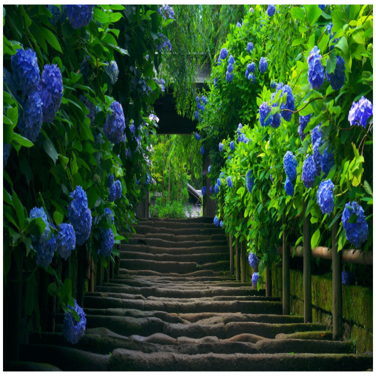


For 1st image



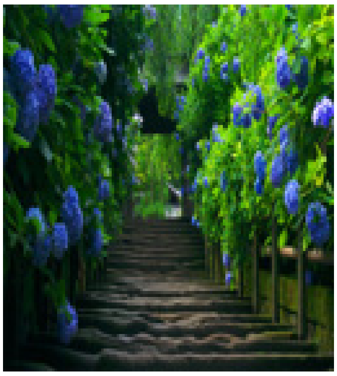
output image





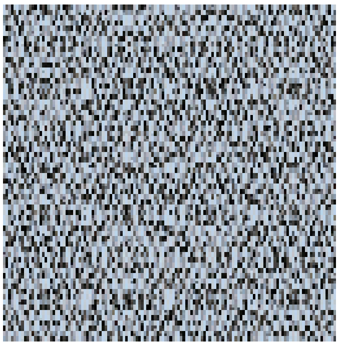
Input image

For 2nd image

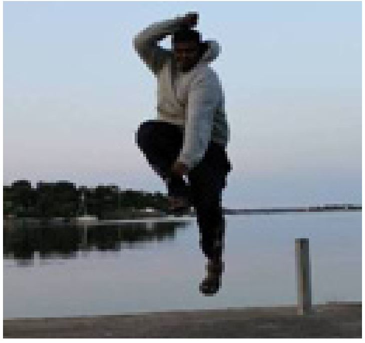


output image

Input image

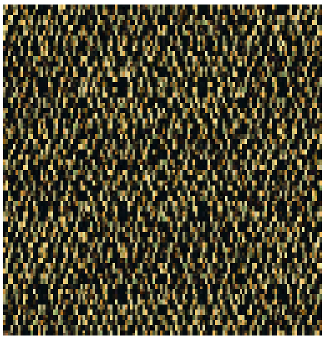


For 3rd image

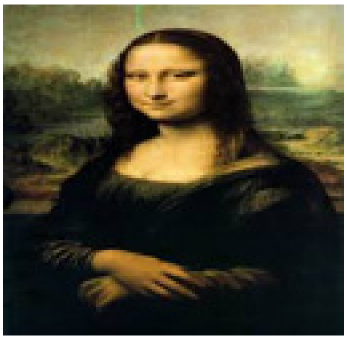


output image

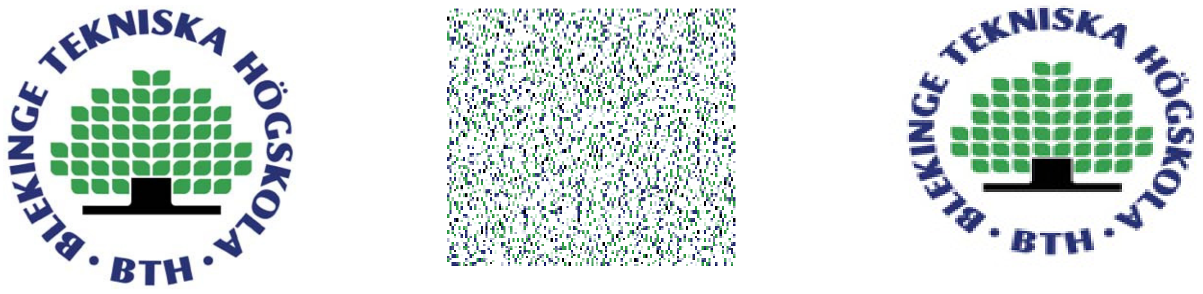
Input image



For 4th image



output image



Input image For 5th image output image

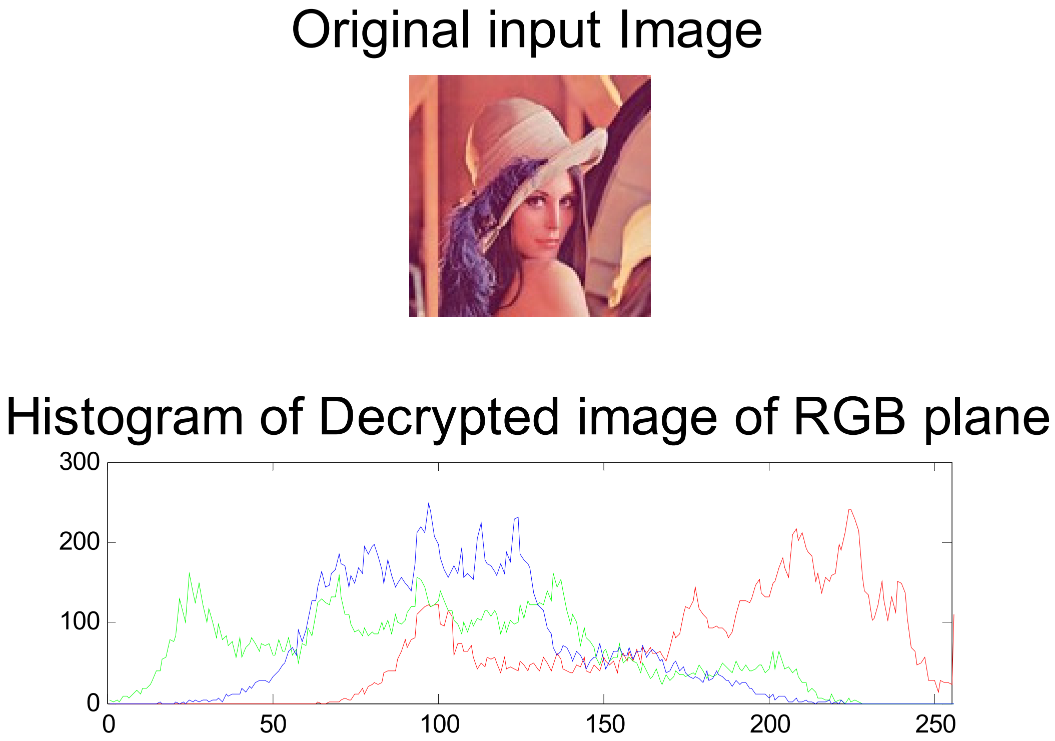
Figure 12: Data set different images of used in Experimental Methodlogy

From figure 12 i.e dataset of different images we can observe that encrypted image is no more looking like an image but it looks like some kind of noise and there is no difference between output image compared to input. We also can observe how an image is splitted into small pieces which cannot be recognized by an unauthorized person that there is some infromation or image related to confidential issue and even we can see the decrypted image which has been clubbed by different no. of splitted pieces of an image.

5 MEASUREMENTS

5.1 MEASUREMENTS OF INPUT IMAGE

Lena.jpg image has been taken as input image for testing the algorithm. The below plot consists of histogram of input image which consists envelope of all three channels i.e, Red, Blue and Green channels. Histogram of this original input image has been taken for having knowledge about how much the image has been degraded when the image is being encrypted as well as when the encrypted image is degraded.



Original input Image

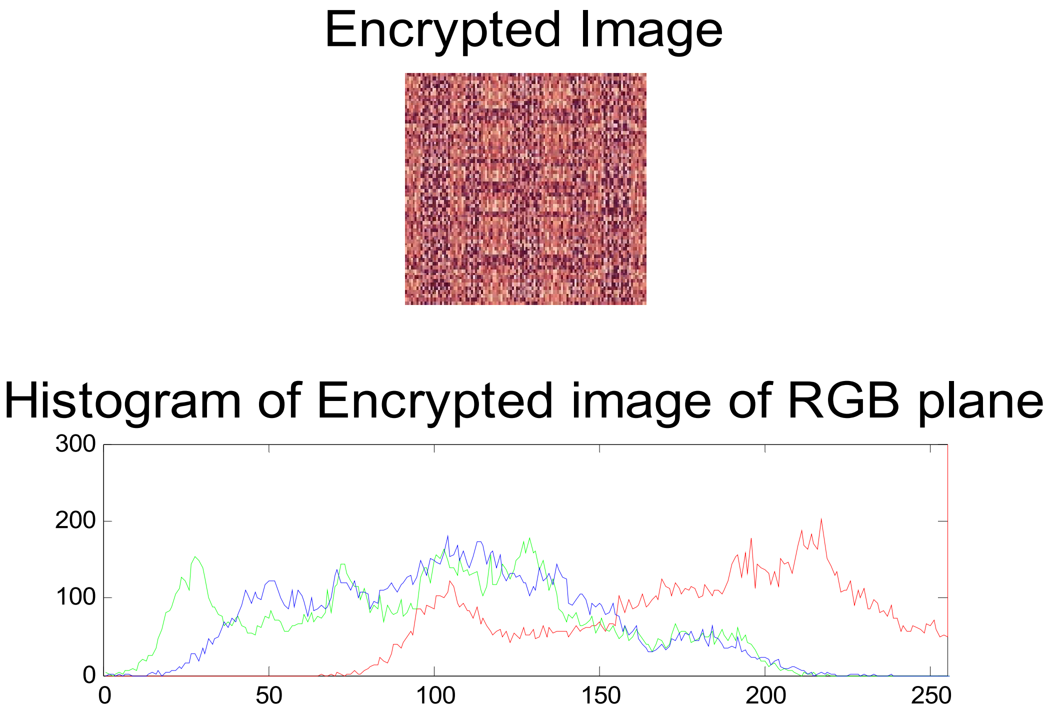
Histogram of Decrypted image of RGB plane

Figure 13: Input image of lena.jpg and Histogram of input image

In the above figure 13 we can observe that lena.jpg has been taken as input and the histogram shows the Red, Blue and Green plane of the input image used and the plot is regarding histogram is of the input image which has been taken as input. Finally by having histogram of input image and concerned decrypted image is to see the difference between original image and decrypted image.

5.2 MEASUREMENTS OF ENCRYPTED IMAGE

The image which has been shown is the encrypted image of Lena.jpg which has been taken as input image and when tested with the Recursive algorithm and then image has been encrypted. The below plot consists of histogram of Encrypted image which consists envelope of all three channels i.e, Red, Blue and Green channels. By plotting the histogram of encrypted image we can observe difference between original image and encrypted image. We also can trace how much image has been degraded by observing both the histogram of this original input image and encrypted image.



Encrypted Image

Histogram of Encrypted image of RGB plane

Figure 14: Encrypted Input image and Encrypted Histogram

From figure 14 we can observe that it looks like noise but it does not look like that its has components of an image and the measurements shown below are the regarding histograms of Encrypted image which were used for describing the experiment and its function about how image has been Encrypted.

The statistics of an image when an image is being encrypted are the correlation coefficient has been varied for four times for being encrypted i.e., the correlation coefficient for first time was 87, for second time it was 19, for third time it was 17 and then finally it was satisfied for fourth time at -23 and then Contrast of image is [4.4121 4.46623], Homogenity is [0.5189 0.5071], Entropy E1 was 7.7549 and varied at E3 to 7.7193 and time elapsed for the encrypting the input image was 16.145364 seconds.

5.3 MEASUREMENTS OF DECRYPTED IMAGE

The image which has been shown is the Decrypted image of Lena.jpg. Encrypted image has been taken as input for retrieving the Decrypted image. Decryption of Encrypted image is done by using the Inverse Recursive algorithm which is exatly replica of the Recursive algorithm. The below plot consists of histogram of Decrypted image in which it consists envelope of all three channels i.e, Red, Blue and Green channels.

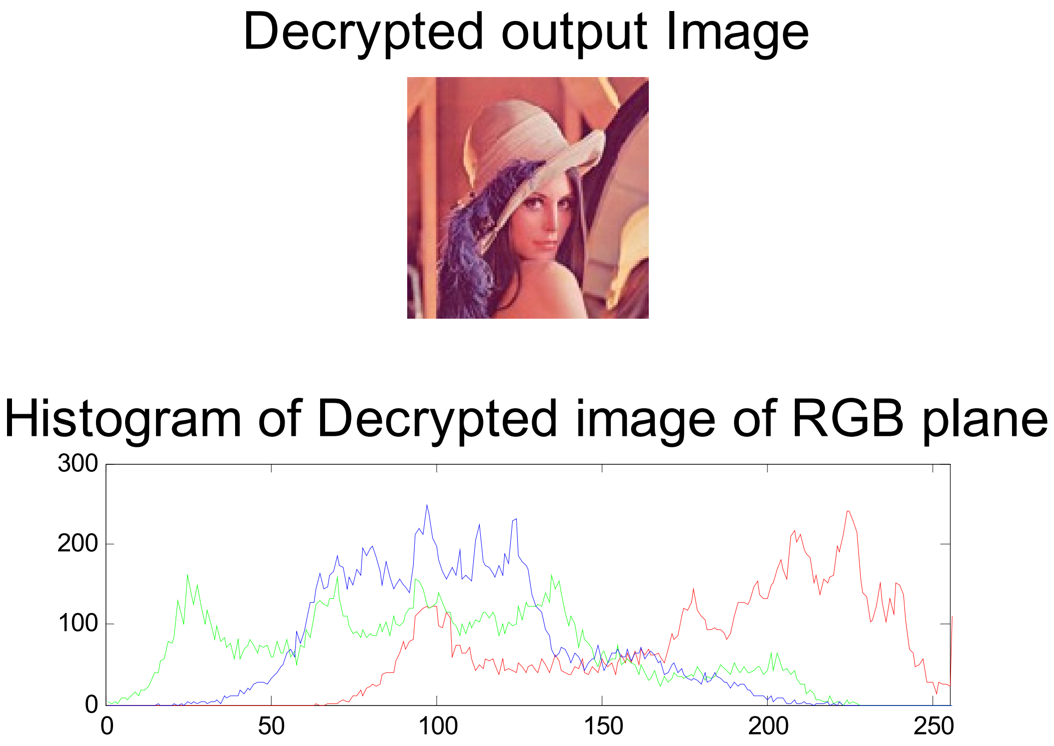


Figure 15: Decrypted Output image and Decrypted Histogram

From figure 15 we can observe that it is similar to input Lena.jpg we cannot find any difference between Input image and Decrypted image through our naked eye but we can be observe the difference only in the histogram since there will be a slight degradation of image since it took part in Encryption and Decryption techniques.

The statistics of an image when an image is being decrypted are the correlation coefficient has been varied for four times for the image to be decrypted i.e, the correlation coefficient for first time was 17, for second time it was 19, for third time it was 87 and then finally it was satisfied for fourth time at -34 and then Contrast is [2.5795 2.6096], Homogeneity is [0.6392 0.6338], there is no variation in E1 and E3 to 7.7830 it maintained same at both times and time elapsed for the encryption was 16.361157seconds.

From the above measurements i.e., from figure 14, figure 15 and figure 16 we can observe that a Lena.Jpg image is taken as input image to be encrypted. Since our encryption ratio is high while decrypting the image we can observe some difference in histogram of Input image and Decrypted image. We can also observe the value of Correlation coefficient how it is being degraded according to encryption or decryption of the image. Encryption and Decryption are being done according to the iterations of correlation coefficient.

We also calculated the distance of each image i.e, distance between input image and Encrypted image and as well as input image and Decrypted image. By checking the distance between input image and Decrypted image we can verify if there is any change in input image after the Encryption and Decryption process is being applied to an image.

Name of the image	Input image vs Encrypted image (Distance)	Input image vs Decrypted image (Distance)
Lena.jpg	13.53	0
Pawan.jpg	5.98	0
Bth.jpg	27.42	0
Nature.jpg	66.84	0
Images.jpg	5.22	0

Table 1: Distance’s between Input image, Encrypted image and Decrypted image

The above table 1 consists of table which clearly measures the distance of all the images which have been used as data set for implementing the Encryption and Decryption procedure on these images. The distance between original input, Encrypted and Decrypted image has been calculated by using Bhattacharya distance [19] method of comparing the histograms of different types of images. 1st block of the table consists of name of the images which have been taken as Input, 2nd block consists of distance between Input image and Encrypted image, by observing reading in the table we can observe some difference between Input image and Encrypted image and that is because due to the recursive method of encryption where the components of images are being splitted into different no. of pieces and the 3rd and final block consists of the distance between Input image and decrypted image where we can clearly observe that there is no difference between Input image and Decrypted image since all the splitted pieces of the image are being again re-ordered into same form by using inverse recursive algorithm to obtain Decrypted image same as Input image.

5.4 TOOL USED

The software tool which we used is MATLAB R2013A in Intel core I5 with 4 GB RAM.

6. CONCLUSION

In this thesis work the proposed method is to use recursive algorithm in image steganography and make encryption in more robust form so, tried to encrypt an image in such a way that the encrypted image looks like pure noise but not even single portion of it looks like an image and not even a security key is provided to retrieve the encrypted information. To verify our encryption we tried to decrypt the encrypted image through available online software's but none of them were able to decrypt our encrypted image.

Decryption of the encryption technique has also been implemented since it is very much necessary for revealing the encrypted image to the authorized user and also made sure to receive the output image as clear as input image.

This is a trivial example accomplished by implementing an image steganographic technique using recursive algorithm but it goes far beyond by using more no. of algorithms by implementing them in more different kind of steganographic techniques.

7. FUTURE WORK

There is a lot of scope to do in this method i.e.., when we are encrypting an image there is a degradation of image due to high compression ratio. There is also another work regarding size of the input image i.e., if image size is too high then it exceeds the recursion limit which is leading to hanging the system or being in busy state.

More research also can be done to find more different techniques like these for not allowing the unauthorized people to access the information which is very much confidential.

Not only recursive algorithm many other algorithms can be used and tried to make more different types of image steganographic techniques.

8. BIBLIOGRAPHY

1. Das, R.; Tuithung, T., "A novel steganography method for image based on Huffman Encoding," *Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference*, pp.14,18, 30-31 March 2012
doi: 10.1109/NCETACS.2012.6203290
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203290&isnumber=6203266 Jan, 2013.
2. Almohammad, A.; Ghinea, G., "Image Steganography and Chrominance Components," *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference,* pp.996, 1001, June 29 2010-July 1 2010
doi: 10.1109/CIT.2010.183
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5578486&isnumber=5577816 Apr, 2013.
3. Hong-Juan Zhang; Hong-Jun Tang, "A Novel Image Steganography Algorithm Against Statistical Analysis," *Machine Learning and Cybernetics, 2007 International Conference*, vol.7, pp.3884, 3888, 19-22 Aug. 2007
doi: 10.1109/ICMLC.2007.4370824
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4370824&isnumber=4370780 Jan, 2013.
4. Jayachandran, M.; Manikandan, J., "SAR Image Compression Using Steganography," *Advances in Computer Engineering (ACE), 2010 International Conference,* pp.203, 206, 20-21 June 2010.
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5532846&isnumber=5532798. March, 2013.
5. Jiantao Zhou; Au, O.C.; Xiaopeng Fan; Wong, P.H.-W., "Secure Lempel-Ziv-Welch (LZW) algorithm with random dictionary insertion and permutation," *Multimedia and Expo, 2008 IEEE International Conference,* pp.245, 248, June 23 2008-April 26 2008.
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4607417&isnumber=4607348
March, 2013.
6. En-Jung Farn; Chaur-Chin Chen, "A jigsaw puzzle based secret key exchange scheme," *Machine Learning and Cybernetics, 2008 International Conference on* , vol.6, no., pp.3067,3071, 12-15 July 2008
doi: 10.1109/ICMLC.2008.4620935
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4620935&isnumber=4620933. Feb 2013
7. Geman, Stuart; Geman, D., "Stochastic Relaxation, Gibbs Distributions, and the Bayesian Restoration of Images," *Pattern Analysis and Machine Intelligence, IEEE Transactions*, vol.PAMI-6, no.6, pp.721, 741, Nov. 1984
doi: 10.1109/TPAMI.1984.4767596.

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4767596&isnumber=4767587. Feb 2013.

8. Healey, G., "Segmenting images using normalized color," *Systems, Man and Cybernetics, IEEE Transactions*, vol.22, no.1, pp.64, 73, Jan/Feb 1992
doi: 10.1109/21.141311.
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=141311&isnumber=3792. Feb 2013.
9. Jianqing Liu; Yang, Y.-H., "Multi resolution color image segmentation," *Pattern Analysis and Machine Intelligence, IEEE Transactions*, vol.16, no.7, pp.689, 700, Jul 1994
doi: 10.1109/34.297949.
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=297949&isnumber=7384. July 2013.
10. Nahi, N.E.; Franco, C., "Recursive Image Enhancement--Vector Processing," *Communications, IEEE Transactions on*, vol.21, no.4, pp.305, 311, Apr 1973
doi: 10.1109/TCOM.1973.1091662
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1091662&isnumber=23793. July 2013
11. C.Brain Atkins, Nicholas P.Lyons, Xuemei Zhang, Daniel R. Tretter, Template," Blocked Recursive Image Composition", MM 08 proceedings of the 16th ACM international conference on multimedia, 821-824. 2008.
URL: http://dl.acm.org.miman.bib.bth.se/citation.cfm?id=1459496 Oct, 2013.
12. Long Zhu; Yuanhao Chen; Yuan Lin; Chenxi Lin; Yuille, A., "Recursive segmentation and recognition templates for image parsing," *Pattern Analysis and Machine Intelligence, IEEE Transactions*, vol.34, no.2, pp.359,371, Feb. 2012
doi: 10.1109/TPAMI.2011.160
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6107465&isnumber=6107461 June, 2013
13. S.Arora; J.Acharya; A.Verma; Prasanta K.Panigrahi, "Multilevel threshold for image segmentation through fast statistical recursive algorithm" *Pattern Recognition Letters*, Volume 29, Issue2, 15 January 2008, Pages 119–125.
URL:
http://www.sciencedirect.com.miman.bib.bth.se/science/article/pii/S0167865507002905
June, 2013.
14. Saha, A.; Halder, S.; Kollya, S., "Image steganography using 24-bit bitmap images," *Computer and Information Technology (ICCIT), 2011 14th International Conference*, pp.56,60, 22-24 Dec. 2011
doi: 10.1109/ICCITechn.2011.6164873

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6164873&isnumber=6164770 Aug, 2013.

15. Thiyagarajan,P.; Aghila,G.; Prasanna Venkatesan,V.(2010).Dynamic pattern Based Image Steganography. *Journal of computing, 2*(18), 1-9.Retrieved from:http://arxiv.org/ftp/arxiv/papers/1206/1206.2583.pdf Sept, 2013
16. Mandal, J.K.; Sengupta, M., "Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF)," *Emerging Applications of Information Technology (EAIT), 2011 Second International Conference* ,pp.298,301, 19-20 Feb. 2011
 doi: 10.1109/EAIT.2011.24
 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5734971&isnumber=5734894 Aug, 2013.
17. Huili Zhao; Guofeng Qin; Xingjian Wang, "Improvement of canny algorithm based on pavement edge detection," *Image and Signal Processing (CISP), 2010 3rd International Congress* , vol.2., pp.964,967, 16-18 Oct. 2010
 doi: 10.1109/CISP.2010.5646923
 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5646923&isnumber=5646712 Aug, 2013.
18. BRUNELLI, R., AND MICH, O. 2001.Histograms analysis for image retrieval. *Pattern Recognition*, vol. 34, 8, 1625–1637.
 URL: http://www.sciencedirect.com.miman.bib.bth.se/science/article/pii/S0031320300000546 Feb,2015.
19. Rahman, M.M.; Desai, B.C.; Bhattacharya, P., "A Feature Level Fusion in Similarity Matching to Content-Based Image Retrieval," *Information Fusion, 2006 9th International Conference on*, vol., no., pp.1,6, 10-13 July 2006
 doi: 10.1109/ICIF.2006.301664
 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4085950&isnumber=4042156 Feb, 2015.
20. Hutan Ashrafian, Thanos Athanasiou, Fibonacci Series and Coronary Anatomy, Heart, Lung and Circulation, Volume 20, Issue 7, July 2011, Pages 483-484, ISSN 1443-9506, http://dx.doi.org/10.1016/j.hlc.2011.02.008.
 URL: http://www.sciencedirect.com/science/article/pii/S1443950611000898 Mar, 2015.
21. Onwuegbuzie, A., Daniel, L., & Leech, N. (2007). Pearson Product-Moment Correlation Coefficient. In Neil J. Salkind, & K. Rasmussen (Eds.), *Encyclopedia of Measurement and Statistics.* (pp. 751-756). Thousand Oaks, CA: Sage Publications, Inc. doi: http://dx.doi.org.miman.bib.bth.se/10.4135/9781412952644.n338 Mar, 2015.