ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Randomly Carrier Detection based Data Hiding Using Two LSB Bits

Prof. Ram B. Joshi, Anuja T. Bhondve.

Ph.D Scholar, Dept. of Computer, JJT University, Rajasthan, India

M.E Student, Dept. of Computer, Indira college of Engineering and Management, SPPU, Pune, India

ABSTRACT: In this paper we present a Random Pixel Prediction approach to increase the security of the data hidden in a cover RGB image. Here we have used LSB insertion method that hides the bits of a secret message into the last two least significant of the pixels within a cover image. The pixels are selected by using a random number generator. It is commonly seen that the changes in the LSB cannot be detected due to noise that is presents in the digital images by the human visual system. The central idea of the proposed method is to increase security, embedding capacity as well as maintain quality of image. We have also explained the method that extracts the hidden message at the receiving end using a key. The main objective of the paper is to combine both the preferences and the resistance to the visual and statistical attacks for a large amount of the data to be hidden in a cover image.

KEYWORDS: Steganography, Least Significant Bit (LSB), RGB image, cover-image, stego-image, Random Pixel Prediction (RPP), key, PSNR, MSE.

I. INTRODUCTION

Steganography and cryptography are two different data hiding techniques. Steganography hides messages inside some other digital media. In the process a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using LSB insertion method.Data hiding ensures exclusive data access to class members and protects object integrity by preventing unintended or intended changes.Data hiding technique involves putting sensitive information in host image with minimum changes in the image. In most of data hiding techniques, image becomes more distorted and we are unable to retrieve its original format. The cover media are permanently distorted due to the data embedding. In sector such as military or medical it is necessary to retrieve original cover image without any loss of information.Data hiding technique involves putting sensitive information in host image with minimum changes in the image. In most of data hiding techniques, image becomes more distorted and we are unable to retrieve its original format. The cover media are permanently distorted due to the data embedding. In sector such as military or medical it is necessary to retrieve original cover image without any loss of information. There are different characteristics of data hiding technique such as: perceptibility, capacity, authentication, Security, Finger print and secret communication, [1] [2], Etc. that all can be achieved by using data hiding techniques. In data hiding technique the information is embedded into image, after that original image gets distorted and cannot be restored to its original format. With the help of (RDH)[4][5]it is possible to extract cover image as well as embedded message from the embedded image This technique is more needful in sensitive areas such as military , medical where recovery of original content is mandatory. Most of the proposed data hiding schemes are not based onpixel prediction and feature extraction.

II. RELATED WORK

A. INTEGER TRANSFORM TECHNIQUE:

There is a technique which hides the information into integer wavelet coefficient of an image is called integer transform technique. To overcome drawback of existing system and to maximize holding capacity of system, integer transform technique uses data hiding technique and optimum pixeladjustment algorithm. In image data is hidden in random order and for extraction of data sender and receiver both are having public key. This technique is available for gray scale images

DOI: 10.15680/IJIRCCE.2016. 0411181

only.

B. DIFFERENCE EXPANSION:

To overcome drawback of previous system, for difference expansion Yongjian Hu [7] uses the predicted image pixel error instead of the pixel-pair difference. The recovery process contains two steps of manipulations. First in the inner/embedded region, and then the embedded/hidden bit is extracted from it. Original pixel value is resumed in shifted regions. For difference expansion which is based on reversible data hiding, contains two parts, first part is used to convey secret message and second part hold binary location map and header file.

C. HISTOGRAM MODIFICATION:

In histogram modification technique [6], neighbour pixels are strongly correlated so there is difference is expected to be very close to zero so this difference is utilized rather than simple pixel value. To complete the data hiding and extraction process at the sending side, first scan the image in an inverse s-order and calculate the pixel difference d between pixels x-1 and xi. Is completes the data hiding and extraction process in which only one peak point is used. With same data hiding techniques we can achieve large hiding capacities as well. However without knowledge of peak points of every hiding pass recipients may not be able to retrieve the embedded message and the original.

III.SYSTEM DESIGN

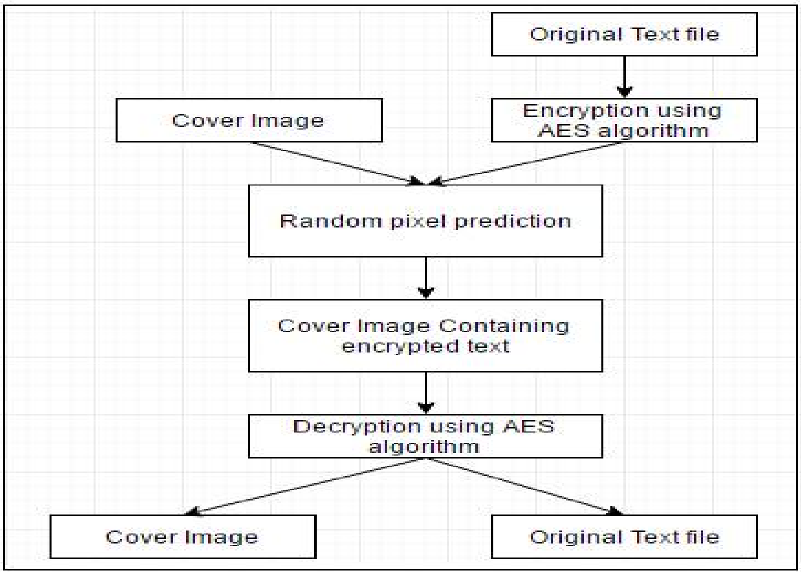

Original Text file
Cover Image
Encryption using AES algorithm
Random pixel prediction
Cover Image Containing encrypted text
Decryption using AES algorithm
Cover Image
Original Text file

Fig1: System design.

In our system, the original text file or the sensitive data is encrypted using the AES algorithm, then the encrypted data is embedded in cover image using random pixel prediction algorithm. Output of RPP is cover image containing information, so at the receiver end, for extracting information receiver should have the same algorithm. After receiving cover image the receiver will apply the same RPP algorithm to the cover image then he will get encrypted information. So for the original information, receiver need to decrypt the data using AES decryption. Here system ensures double security. First at both end, algorithm should be same and even if hacker got the algorithm, he will able to only get information in encrypted format which will be of no use. So for extraction of original information, sender and receiver both should have the same algorithm as well as both should have the same key. Quality of image is calculated using the PSNR and the histogram.Peak signal-to-noise ratio (PSNR) is a measure of the "noise" in a signal relative to the peak intensity. In PQA, PSNR is a referenced measurement, which means that PQA calculates the results by comparing the frames of image being acquired with a "golden" reference image stream. When comparing the two images, PSNR is calculated by taking the mean squared error (MSE) between the pixel intensities and taking the ratio of the maximum possible intensity to the result of the calculation. PSNR is often used with monochrome images, where the intensity is represented by a single value. However, PQA calculates PSNR on color (RGB) images by first averaging the red, green, and blue color intensities to create a generic average image. PSNR is then calculated on the average image. The result is a single-point metric (one result per frame) represented in dB. Typical values for an image with 8-bit color depth may fall between 30 dB and 50 dB and, in general, a higher PSNR value corresponds to a better quality image. However, the PSNR result is unbounded and the range of the results will vary with different images. To use PSNR as a test of image quality, it is recommended that you perform testing to see the typical and expected values for your test signal, in order to set meaningful test limits for PSNR. If you select the multipoint metric result for PSNR, PQA shows a difference spectrum histogram for each frame. The histogram represents the frequency of differences in intensity between the two compared images. If the images are the same, the difference in intensity is zero, and the histogram will show a single spike at 0 (meaning that all pixels in the frame fall in this category). If, for example, one image is darker than the other, then the whole histogram will be shifted to one side (asymmetrical). PSNR measurements can only be performed with NI Picture Quality Analysis, not with NI image Measurement Suite (VMS). Additionally, for new PQA configurations, NI recommends using the structural similarity index measurement (SSIM). SSIM is more robust and returns a result bounded from 0 (no match) to 1 (perfect match), unlike the unbounded and variable result from PSNR.

IV. PSEUDO CODE

Random Pixel Prediction:

Random Pixel Prediction algorithm involves embedding of information into image and stegoanalysis reveals thepresence of data. This is technique for random pixelprediction which is based on randomizing the sequenceof cipher bits. First we calculate measure of all possiblerandom sequences of cipher bits and then select one ofrandom sequence which is close to image.Random sequences are generated by computing sequencewhich is based on seed pixel, and then with the helpof this random sequence of cipher bits, information isembedded into cover image. These technique is prioritizebecause it does not contain one-to-one mapping betweena given cipher text and a Cover image, and for cryptographyanalysis, even if successful attack on encryptionsystem, attacker need to get information of seed which ishelp to generate this random sequence.

Step 1)

- Determine the length of the encrypted data (n).
- Choose a cover image where it has more pixels than n+p,where n is the length of encrypted data and p is the length needed to embed the encrypted information of string
- Set initial value of seed pixel.
- Choose pixel randomly and Segment that pixel into three blocks, each of 8 bits.
- Take one block and consider it as m.

Step 2) Calculate pixel prediction (PP) bit length (m) such that 2m>n.

Step 3) Consider an m-bit length and represent the same in binary notation (one indicates bit location is tabbed and zero indicates otherwise)

Step 4)

Each bit of permuted encrypted data is embedded in to the last two least significant bits of pixel bytes of the cover image for which the suitability is above the threshold. If suitability is below the some fixed threshold.

Step 5)

- Using this (PP,seed) generates random permutation of f1,2,...ng as f11,f12,...lng.
- Permute the encrypted data using the permutation obtained above, to obtain a Permutation string

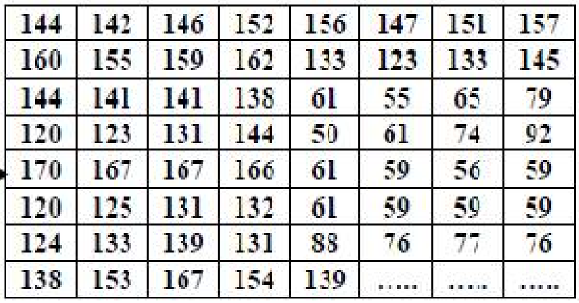
Step 6) Output of RPP is stego image containing information in encrypted format.

Least Significant Bit

Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. Like all stenographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer.The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s).This minimizes the variation in colors that the embedding creates. For example, embedding into the least significant bit changes the color value by one. Embedding into the second bit-plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding. Steganography avoids introducing as much variation as possible, to minimize the likelihood of detection. In a LSB embedding, we always lose some information from the cover image. This is an effect of embedding directly into a pixel. To do this we must discard some of the cover's information and replace it with information from the data to hide.LSB algorithms have a choice about how they embed that data to hide. They can embed lossless, preserving all information about the data, or the data may be generalized so that it takes up less space.The cover image and secret data are passed as an input to the system, which is illustrated by fig 2, then over a cover image system performs RPP to embed secret data into the image.

Embedding operation shown in Algorithm 1 and to locate the exact position of pixel to store data shown in Algorithm 2 Least significant bit is the simplest form of steganography method in use, and therefore it is most vulnerable among all methods available. In this method embedding process consists of sequential substitution of each Least Significant Bit (LSB-1) of image pixel for bit message. The following steps illustrate that how this (LSB-1) isused to hide the secret data ”A” in cover image named as”Mansoura.bmp ”.

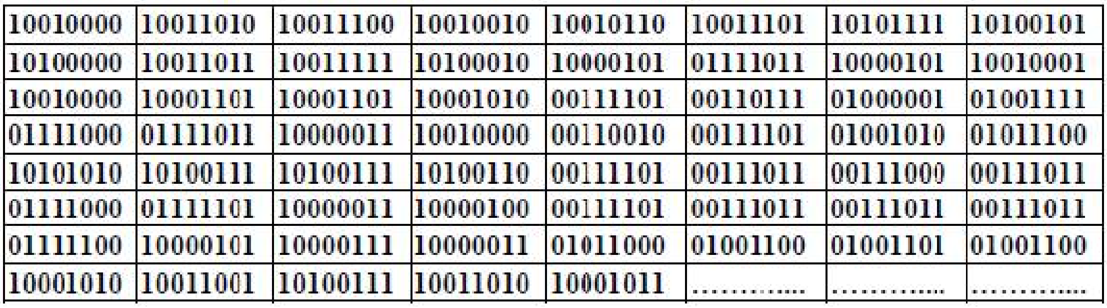
1) This step includes converting the data from decimal to binary.



144	142	146	152	156	147	151	157
160	155	159	162	133	123	133	145
144	141	141	138	61	55	65	79
120	123	131	144	50	61	74	92
170	167	167	166	61	59	56	59
120	125	131	132	61	59	59	59
124	133	139	131	88	76	77	76
138	153	167	154	139	.....	.....	.....

2) This step includes reading the Cover image ”Mansoura. “bmp” as shown in following fig:

3) This step converts the Cover Image from decimalformat to binary format.

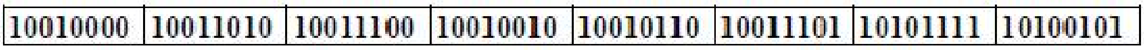


10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101
10100000	10011011	10011111	10100010	10000101	01111011	10000101	10010001
10010000	10001101	10001101	10001010	00111101	00110111	01000001	01001111
01111000	01111011	10000011	10010000	00110010	00111101	01001010	01011100
10101010	10100111	10100111	10100110	00111101	00111011	00111000	00111011
01111000	01111101	10000011	10000100	00111101	00111011	00111011	00111011
01111100	10000101	10000111	10000011	01011000	01001100	01001101	01001100
10001010	10011001	10100111	10011010	10001011	....	....	....

Table 1: Binary data.

4) This step includes conversion of byte code into bits. Thus [10000001] is divided into 8 bits.

5) In this step, take first eight byte of original data.



10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101

Table 2: Single row considered for conversion.

6) In this step, replace the least significant bit by one bit of the data to be hidden.

- Take the first byte of original data from the cover Image.

1	0	0	1	0	0	0	0

- It's very first bit of the data to be hidden:
- Then replace the least significant bit:

7) Repeat this process of replacing for all bytes of cover Image: - And finally the cover image before and after steganography is shown in figure.

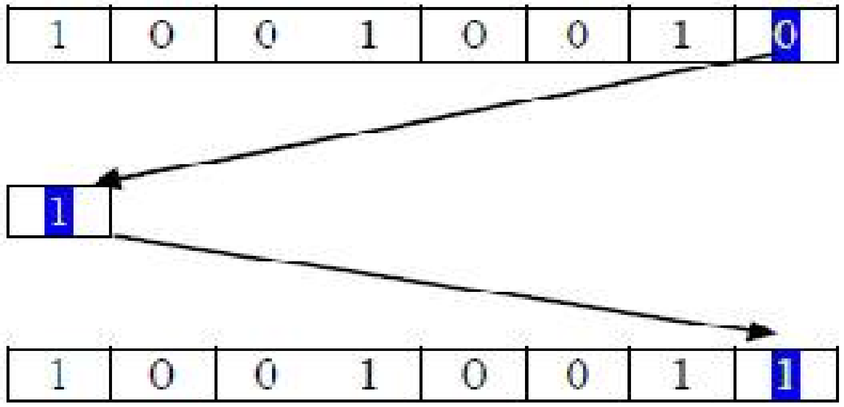


Fig 2: LSB Working

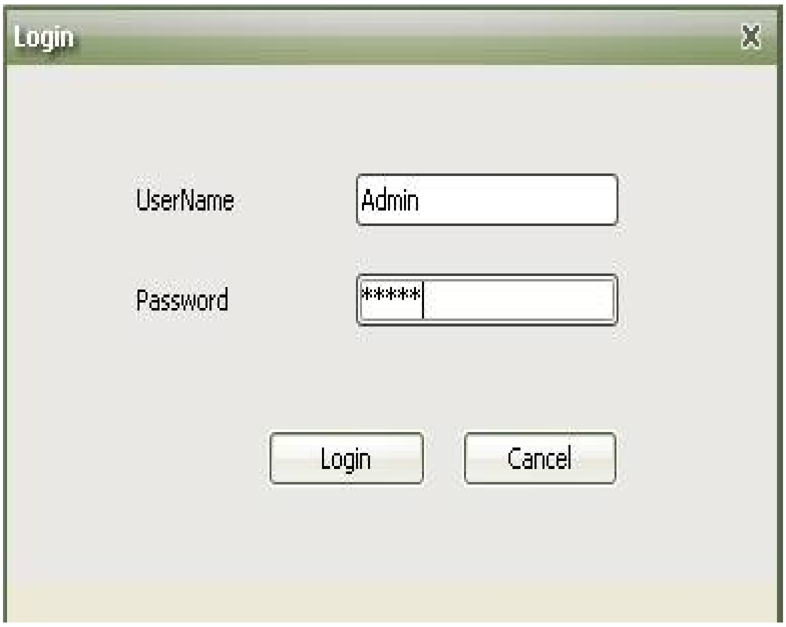
Fig3: Cover image before steganography.

Fig 3, illustrate that cover image before embedding data. So we can take this image for reference and after embedding data we can check the images quality through the PSNR and histogram.

Fig 4: Cover image after steganography.

Fig 4, shows that cover image after data encryption and embedding. In this image we have first encrypt the data using AES algorithm and then we have embedded data into image using RPP and LSB technique. This image should ensure that the quality of image should contain minimum of difference. So that attacker will not able to identify that this is stego image.

V. SIMULATION RESULTS



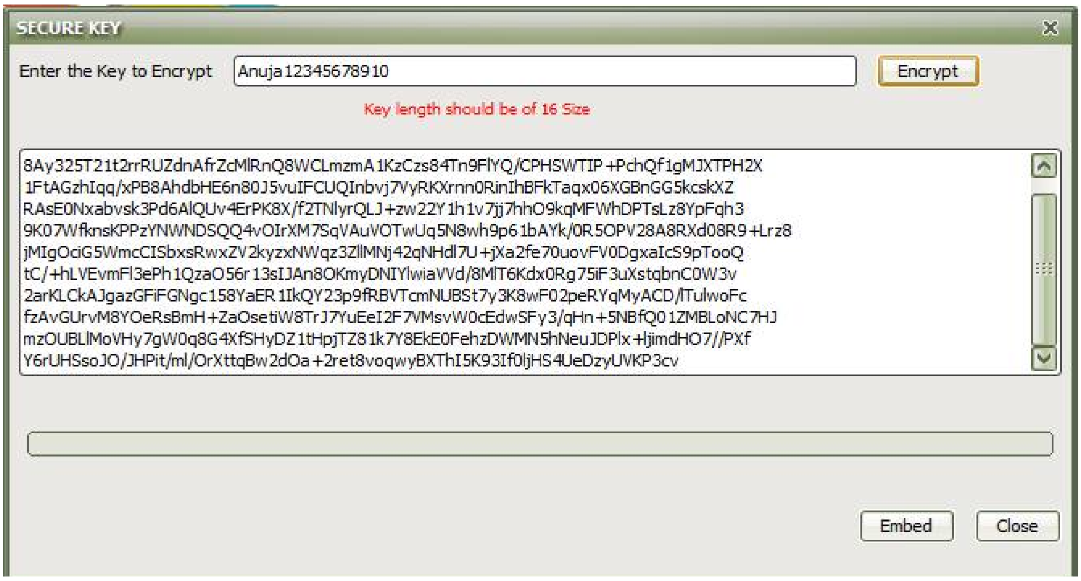
Login

UserName Admin

Password *****

Fig 5: login.

Fig 5, illustrates that login screen, this is for authentication so that authenticate user only access to data. No other user will enter into system.



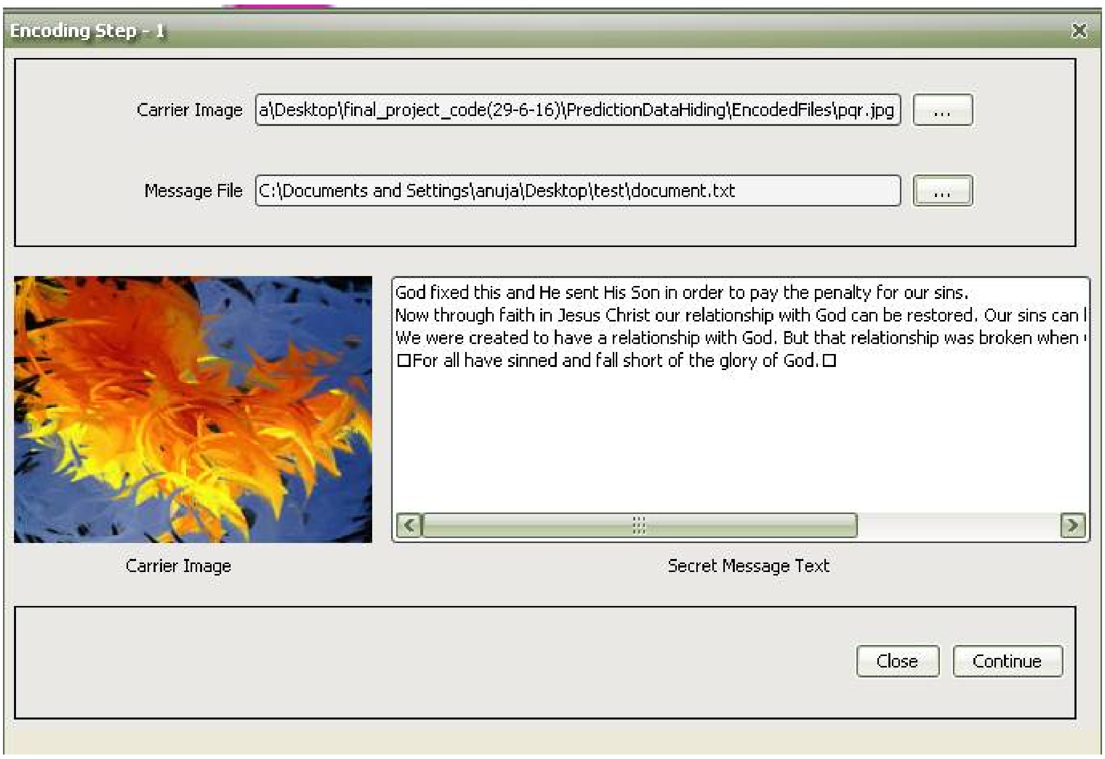
Enter the Key to Encrypt: Anuja12345678910

Key length should be of 16 Size

```
8Ay325T21t2rrRUZdnAfrZcMlRnQ8WCLmzmA1KzCzs84Tn9FlYQ/CPHSWTIP+PchQf1gMJXTPH2X
1FtAGzhIqq/xPB8AhdbHE6n80J5vuIFCUQInbvj7VyRKXrnn0RinIhBFkTaqx06XGBnGG5kcskXZ
RAsE0Nxabvsk3Pd6AlQUv4ErPK8X/f2TNlyrQLJ+zw22Y1h1v7jj7hhO9kqMFWhDPTsLz8YpFqh3
9K07WfknsKPPzYNWNDSQQ4vOIrXM7SqVAuVOTwUq5N8wh9p61bAYk/0R5OPV28A8RXd08R9+Lrz8
jMIgOciG5WmcCISbxsRwxZV2kyzxNWqz3ZllMNj42qNHdl7U+jXa2fe70uovFV0DgxaIcS9pTooQ
tC/+hLVEvmFl3ePh1QzaO56r13sIJAn8OKmyDNIYlwiaVVd/8MlT6Kdx0Rg75iF3uXstqbnC0W3v
2arKLCkAJgazGFiFGNgc158YaER1IkQY23p9fRBVTcmNUBSt7y3K8wF02peRYqMyACD/lTulwoFc
fzAvGUrvM8YOeRsBmH+ZaOsetiW8TrJ7YuEeI2F7VMsvW0cEdwSFy3/qHn+5NBfQ01ZMBLoNC7HJ
mzOUBLlMoVHy7gW0q8G4XfSHyDZ1tHpjTZ81k7Y8EkE0FehzDWMN5hNeuJDPlx+ljimdHO7//PXf
Y6rUHSsoJO/JHPit/ml/OrXttqBw2dOa+2ret8voqwyBXThI5K93If0ljHS4UeDzyUVKP3cv
```

Fig 6: Encryption.

Fig 6, shows encryption screen, in this I have entered “Anuja12345678910” as a key and then I have encrypted data using that key. So this is one way of protecting data. In this receiver also contain same key to decrypt the data. For this encryption and decryption, I have used AES algorithm.



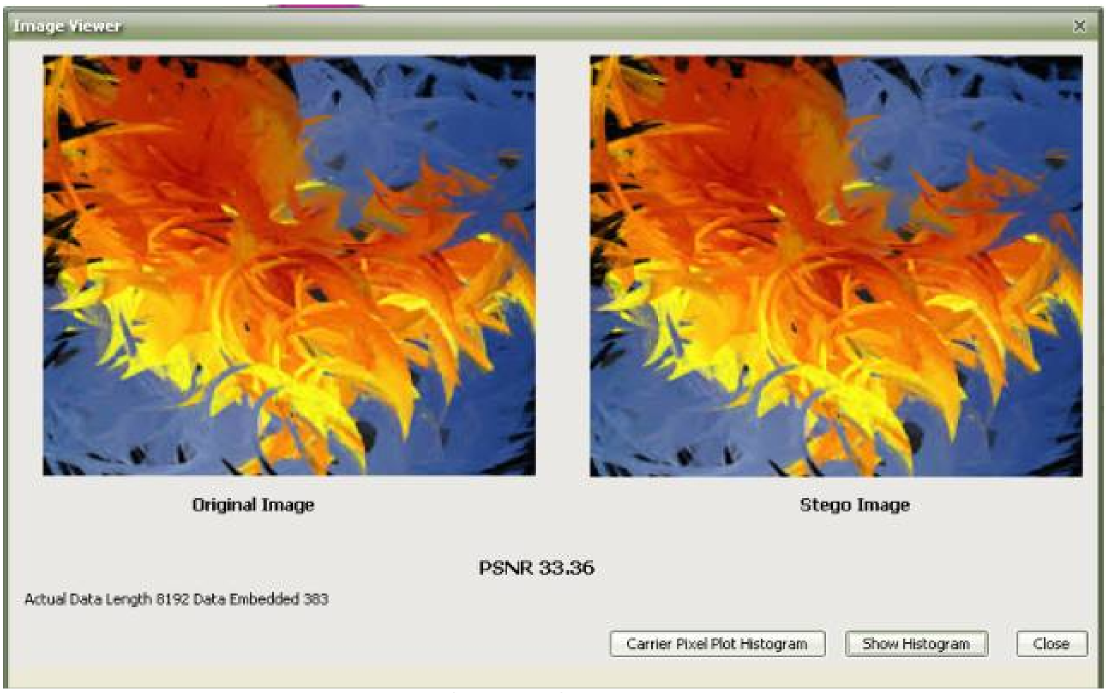
Carrier Image: a\Desktop\final_project_code(29-6-16)\PredictionDataHiding\EncodedFiles\pqr.jpg

Message File: C:\Documents and Settings\anuja\Desktop\test\document.txt

God fixed this and He sent His Son in order to pay the penalty for our sins.
Now through faith in Jesus Christ our relationship with God can be restored. Our sins can b
We were created to have a relationship with God. But that relationship was broken when
□For all have sinned and fall short of the glory of God.□

Fig7: Embedding of message into image.

Fig 7, shows that embedding of text document into image, in the first line I have selected the carrier image/cover image in which data is going to be embed, second line contains message file, in this we can select the text file in which we can specify the data for hiding, same data will display in the following block. So that we can ensure the text. After continuing “Stego image” will be created.

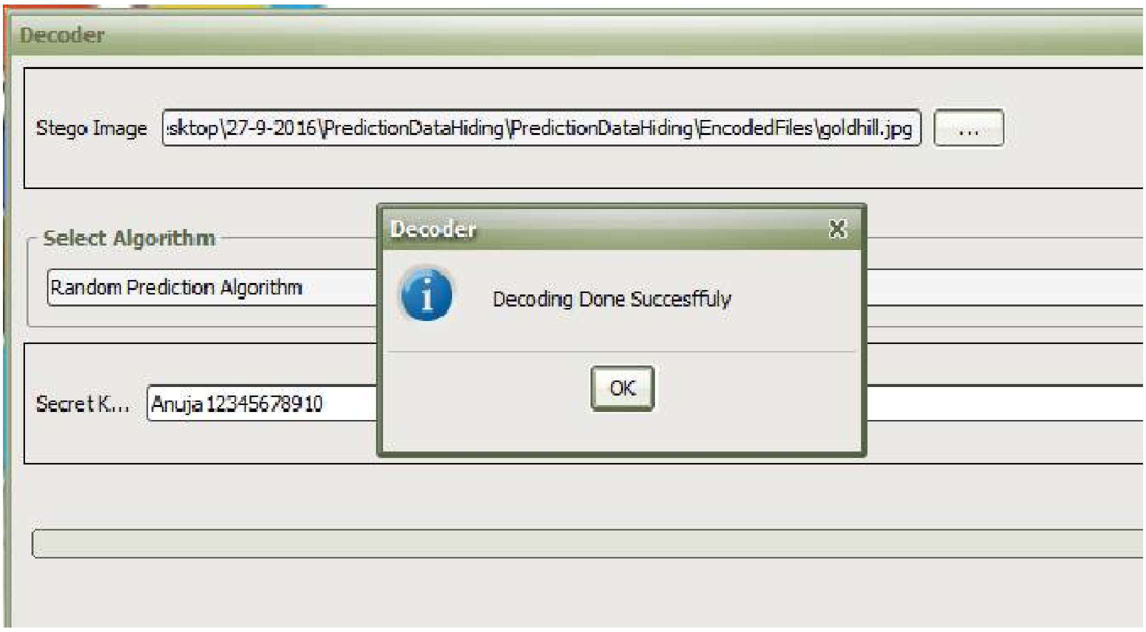


PSNR 33.36

Actual Data Length 8192 Data Embedded 383

Fig8: Image before and after message embedding.

Fig 8, illustrate that cover image before and after message embedding.it also contains value of PSNR. If the value is between 28DB to 52DB it will give assured that image is having good quality, below to that Actual data length and data embedded is specified.



Stego Image sktop\27-9-2016\PredictionDataHiding\PredictionDataHiding\EncodedFiles\goldhill.jpg

Select Algorithm: Random Prediction Algorithm

Secret K... Anuja 12345678910

Decoding Done Succesffuly

Fig 9: Decoding.

Fig 9, illustrate that decoding status at receiver end. For the decoding the receiver should contain same algorithm as well as the same key which is used for the encryption.

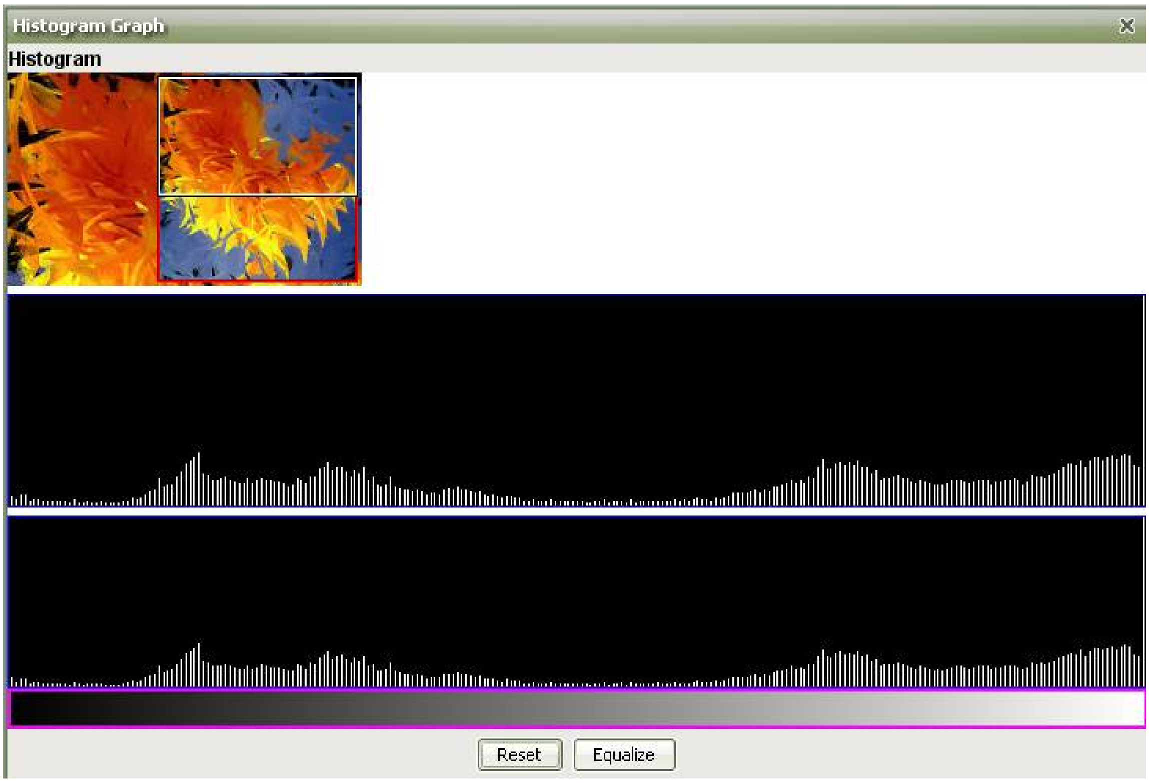


Fig 10: Result analysis using histogram.

In above simulation result analysis, system ensures security in two way, one way is to encrypt the data before embedding. And another is through embedding information in an image. Fig 2 and 5, showing encoding and decoding respectively. So at both end, sender and receiver need the same key for encryption and decryption process. Another way of security is achieved through, embedding of message, in fig 3, left hand shows image and right hand shows encrypted information which we need to embed. The quality of image is ensured by histogram and PSNR which is shown fig 4 and fig 6. Result set also outputted in PSNR that proves the quality, which must be between 28dB to 52dB.

VI. Conclusion and Future Work

This work deal with secure transmission of data. This system deals with implementation of security using stenography i.e. Hiding large amount of info in an image without disturbing the image clarity and quality. Our results indicates that the LSB insertion using random pixel prediction are best in case of lossless compression.The outcome of paper is to create a method that can effectively hide a message inside a digital image file.The paper focuses on the approach like increasing the security of the message, increase embedding capacity and reducing the distortion rate.

References

1. Xiaocheng Hu, Weiming Zhang, Xiaolong Li, and Nenghai Yu Minimum Rate Prediction and Optimized Histograms Modification for ReversibleData Hiding IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015.
2. Wei-Liang Tai, Chia-Ming Yeh and Chin-Chen Chang,(2009), Reversible Data Hiding Based on Histogram Modification of Pixel Differences,IEEE Transaction on circuits and systems for video technology, Vol. 19, No. 6, pp. 906-910
3. Yongjian Hu, Heung-Kyu Lee and Jianwei Li,(2009), DE- BasedReversible Data Hiding With Improved Overflow Location Map, IEEE Transaction on Circuits and systems for video technology, Vol. 19, No.2, pp. 250-260.

4. ShaoweiWeng, Yao Zhao, Jeng-Shyang Pan and Rongrong Ni,(2008),Reversible Watermarking Based on Invariability and Adjustment onPixel Pairs, IEEE signal processing letters, Vol. 15, pp. 721-724.
5. B. Macq, Lossless multiresolution transform for image authenticatingwatermarking, in Proc. EUSIPCO, Sept. 2000, pp. 533536.
6. ZhenfeiZhaoa, HaoLuoc,, JengShyangPand, Reversible data hidingbased on multilevel histogram modification and sequential recovery International Journal of Electronics and Communications, 2010.
7. J. Tian, Reversible data embedding using a difference expansion, IEEETrans. Vol. 13, No. 8, pp. 890896, Aug.2003.
8. Sunil Lee, Chang D. Yoo, Reversible Image Watermarking Based onInteger to integer wavelet transform 2007.
9.]R. Caldelli, F. Filippini, and R. Becarelli, Reversible watermarkingtechniques: An overview and a classification, EURASIP J. Inf. Security,vol. 2010, Jan. 2010.
10. Miss AnujaBhondve, Prof. Swapnaja Suryawanshi " Minimum rate prediction and optimized histograms modification for efficient data hiding." International Journal of Innovative Research in Computer and Communication Engineering(IJIRCCE) ISSN: 2320-9801 Vol. 3, Issue 11, November 2015
11. ShaoweiWeng, Yao Zhao, Jeng-Shyang Pan and Rongrong Ni,(2008), "Reversible Watermarking Based on Invariability and Adjustment on Pixel Pairs", IEEE signal processing letters, Vol. 15, pp. 721-724.
12. M. Wu, H. Yu, and B. Liu, "Data hiding in image and video .II. designs and applications," IEEE Trans. Image Process., vol. 12, no. 6, pp. 696–705, Jun. 2003.
13. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking Steganography, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2007.