ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Image Steganography using Variable Key Technique for Double Tier Security

Khushboo Jain[1], Amrit Kaur[2]

PG Student [ECE], Dept. of ECE, University College of Engineering, Punjabi University, Patiala, India [1]

Assistant Professor, Dept. of ECE, University College of Engineering, Punjabi University, Patiala, India [2]

ABSTRACT: In this Paper, before applying the Steganography technique the secret message change into cipher to ensure the double tier security. In the Proposed technique the encrypted data is hidden in cover image using Modified LSB Technique. The Mean Square Error (MSE) and Peak Signal Noise Ratio (PSNR) measures the Imperceptibility of the proposed technique. Experimental results show that the Stego image is usually indistinguishable from the cover image.

KEYWORDS*:* Cryptography, Image Encryption, MSE, PSNR, LSB.

I.INTRODUCTION

In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communication data. In our daily life, a huge amount of confidential data is being lost every year during transmission by the intruders. Ciphering techniques are widely used to encrypt and decrypt data. But sometimes data encryption does not seem enough and hiding of the data is needed more. The technique used for this idea is called Steganography [1].

Steganography is a Greek word which means concealed writing. The word "stego" means "cover" and "grafia" means "writing". So in other words steganography is the science of concealing secret information into any digital media such as images, audio, video etc. so that no eavesdropper can empathies this secret communication [2].

A steganography system consists of three elements: cover object (which hides the secret message), the secret message and the stego object (which is thecover object with message embedded inside it).

The images are the most popular cover objects for steganography. The pixels have some integer value, based upon the brightness or color. At each pixel information is hidden, depending upon the image size. For example in 1024*1024 image size, 1048576 pixels are available on which data can be hidden.

1. Steganography Techniques

There are several techniques to conceal information inside cover image [3].

1.1 Spatial domain technique

1.2 Frequency domain technique

1.1 Spatial domain technique: These techniques manipulate the cover image bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes.

1.2Frequency domain technique: The transform domain techniques embed the message in the frequency domain of the cover image.

2.Characterization of Steganography

In Steganography techniques a message embed inside a cover image. Various features characterize the strength and weaknesses of a method.

2.1 Capacity

The capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system.

2.2Robustness

Robustness refers to the ability of the embedded data to remain intact if the system undergoes transformation like linear and non-linear filtering, addition of random noise, rotation, scaling and compression.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

2.3Undetectable

The embedded algorithm is undetectable if the image with the embedded message is consistent with a model of the source from which images is drawn. Undetectability is directly affected by the size of the secret message and the format of the content of the cover image.

2.4Invisibility (Perceptual Transparency)

The concept of Invisibility based on the properties of the human visual system. The embedded information is imperceptible if an average human is unable to distinguish between carriers that contain hidden information and others do not. It is important that the embedding occurs without a significant degradation or loss of perceptual quality of the cover.

2.5 Security

The embedded algorithm is to be secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the embedded algorithm and secret key [4].

There are many application of Steganography in the area of featured tagging, secret communication, covert communication, copy right protection, military and intelligence agencies, TV broadcasting, Multimedia content copyrights etc.

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar or different the stego image with the cover image is.

The following metrics are used

1. **Mean Squared Error (MSE)** is computed by performing byte by byte comparisons of the cover image and stego image. The Computation expressed as[3]

$$\text{MSE}=\frac{1}{M*N}\sum_1^M\sum_1^N(Fij-Gij)^2$$

M: number of rows of cover image
N: number of columns of cover Image
Fij: Pixel value from cover image
Gij: Pixel value from Stego Image

Higher value of MSE indicates dissimilarity between Cover image and Stego image.

2. **Peak signal to noise ratio (PSNR)** measures in decibels the quality of the stego image compared with the cover image. The higher the PSNR better the quality. PSNR is computed using the following equation [3].

$$\text{PSNR}=20\log_{10} Peak - 10\log_{10} MSE$$

Peak: Maximum value to represent Pixel value, as in gray scale image the maximum peak value is 255.

II.LITERATURE SURVEY

In the literature, many techniques about data hiding have been proposed.

Walia et al. [5] one of the most common techniques is based on manipulating the least significant bit (LSB) planes by directly replacing the LSBs of the cover image with the message bits.

Islam et al. [1] proposes a technique in which before applying the steganography technique, AES cryptography will change the secret message into cipher text to ensure the two layer security of the message. Large data hide in Bitmap image using filtering based algorithm, which uses MSB bits for filtering purposes. This method uses the concept of status checking for insertion and retrieval of message.

Amirtharajan et al. [6] further proposes one such Symmetric key image encryption algorithm before embedding the message in cover image for security purposes.

In this paper we take motivation from ref. [1, 5, and 6] and proposed a new technique for data hiding. In this technique for double tier security encrypt the data using variable keys then hide data in cover image using modified LSB technique. The modified LSB technique has more data capacity as compared to LSB technique and uses the variable keys for encrypt data give more security as compared to symmetric keys used in ref. [6].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

III. PROPOSED METHODOLOGY

In this proposed model, the RGB color cover image and gray scale image data are read simultaneously. After that variable keys are extracted from cover image. For generation of stego image, encrypted algorithm is applied on cover image to hide encrypted data.

To measure the imperceptibility of stego image, MSE and PSNR are calculated and compared with the existing algorithms.

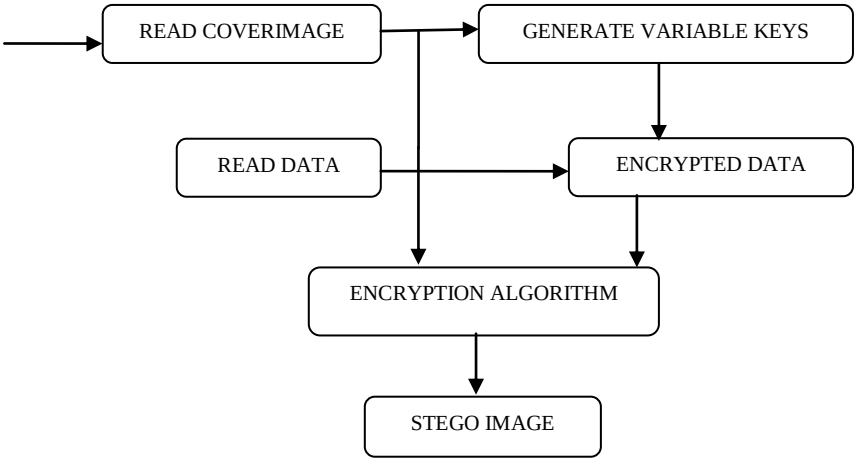

Fig.1. BLOCK DIAGRAM OF PROPOSED ALGORITHM

PROPOSED ALGORITHM

1. Read Cover Image, Data Image.
2. Generate variable keys from Cover Image.
3. If (Data_pixel_value<246)
   3.1 Data_pixel_value=Data_pixel_value+variable key
   Else
   Data_pixel_value=Data_pixel_value
4. Apply Modified LSB Steganography algorithm on Encrypted Data to hide in Cover Image.
5. Calculate Mean Square Error (MSE), Peak Signal Noise Ratio (PSNR) and Compare with Existing Algorithms.

IV. SIMULATION RESULTS

For the purpose of illustration, we have taken cover as Lena image of 512*512 dimensions and data of 128*128 dimensions as shown in Fig. 2 and Fig. 6. From the cover image we generated variables keys. After that the variable keys are added to the data pixels as shown in example.

Example:

1. Cover Image Pixel values

246	199	285
99	186	240
100	138	155

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

2. Generated variable keys from Cover Image

6	9	5
9	6	0
0	8	5

3. Data Pixel Values

250	230	180
135	100	140
167	248	195

4. Encrypted Data

250	239	185
144	106	140
167	248	200

The stego image is generated after hiding the encrypted data in cover image using Modified LSB technique, as represented in Fig. 7

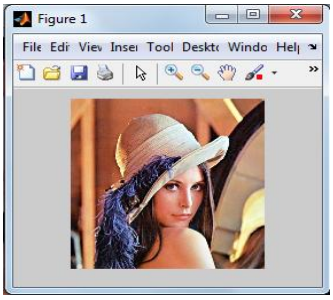

Fig.2. Cover image (512*512)

Fig.3. Plane1

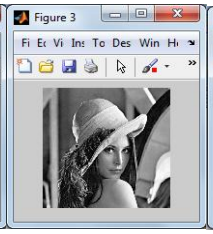

Fig.4.Plane2

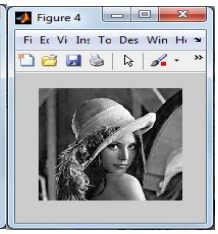

Fig.5. Plane3

Plane 1, plane 2, plane 3 represents the R (Red), G (Green), B (Blue) colours of the image. RGB is an additive colour space and each of the numbers represents the amount of red, green and blue components in a colour.
In this paper extraction of the different planes of RGB image is done after that algorithm is applied on that.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

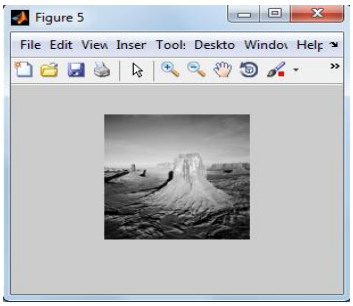

Fig.6. (128*128) Data image

Fig.7. Stego image (512*512)

To measure the performance of this method, the MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) is calculated and compared with the existing algorithms in Table I and Table II

TABLE I

COVER IMAGE SIZE	DATA SIZE	MSE FOR EXISTING ALGORITHM[3]	MSE FOR PROPOSED ALGORITHM
512*512	128*128	2.5	0.6228

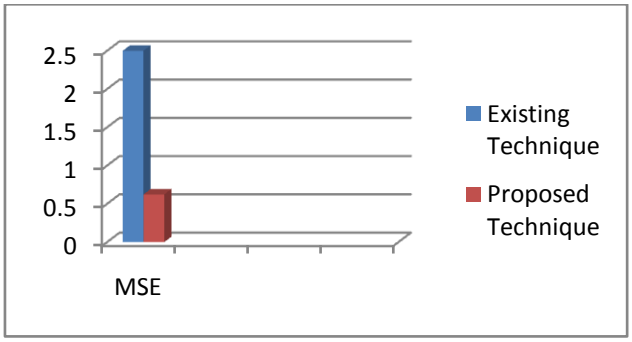

Fig.8. Histogram for MSE

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

TABLE II

COVER IMAGE SIZE	DATA SIZE	PSNR FOR EXISTING ALGORITHM[3]	PSNR FOR PROPOSED ALGORITHM
512*512	128*128	44dB	50dB

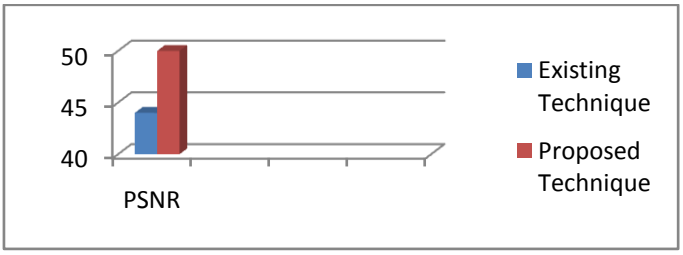

Fig.9. Histogram for PSNR

The lower the value of MSE, higher the value of PSNR (Peak Signal to Noise Ratio); it indicates that the image is fairly of high quality and also is devoid of visual artifacts during retrieval.

V. CONCLUSION

In this paper for double tier security, the variable keys are generated and encrypted data is hidden in cover image using Modified LSB Algorithm. The proposed algorithm has improved MSE and PSNR values as compared to existing Modified LSB technique. Thus the algorithm built in this combination of steganography and cryptography is personalized that it clues none but privacy and robustness.

VI. FUTURE SCOPE

As future work, other image Steganography algorithm are to be investigated such as varying the contrast or the gamma level of the carries image, giving the communicating parties more options to parameterize their secret communication. Also to increase hiding data capacity, video can be taken as a cover media and apply these all techniques to video. Also, work can be carried on masking and region of interest on videos for more security.

REFERENCES

[1] Md. Rashedul Islam, AyashaSiddiqa, Md. PalashUddin, Ashis Kumar Mandal and Md. DelowerHossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", 3rd International Conference on Informatics, Electronics and Vision, 2014.
[2] Juned Ahmed Mazumder, KattamanchiHemachandran, "Color Image Steganography Using Discrete Wavelet Transformation and Optimized Message Distributed Method", International Journal of Computer Sciences and Engineering, Vol. 2, 2014.
[3] BassamJamilMohd, Saed Abed and Thaier Al-Hayajneh and Sahel Alouneh, "FPGA hardware of the LSB Steganography", International Conference on Computer, Information and Telecommunication Systems (CITS), Pages 1-4, 2012.
[4] ZaidoonKh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi "Overview-Main Fundamental for Steganography" Journal of Computing, vol 2, March 2010.
[5] E. Walia, P. Jain, Navdeep, "An Analysis of LSB and DCT based Steganography", Global journal of Computer Science and Technology, Vol. 10, pp.4-8, April 2010.
[6] Rengaranjan Amirtharajan, P. ShanmugaPriya, G. Revathi, A. Kingsly Infant and RayappanJ.B.B , "Random hide to hide Random-A stego Affair Encryption for We(e/a)k Secret", IEEE Conference on Information and Communication Technologies, 2013.
[7] M.M Amin, M. Salleh, S. Lbrahim,M.R.KAtmin,and M.Z.I Shamsuddin,"Information hiding using steganography", IEEE 4th National Conference on Telecommunication Technology Proceeding, Shah Alam.Malaysia,pp.21-25,January 2003.
[8] Deshpande Neeta, KamalapurSnehal and Daisy Jacobs, "Implementation of LSB steganography and its evaluation for various bits" IEEE 1st International Conference on Digital Information Management, India, pp. 173-178, December 2006.
[9] J. Madison, S.D. Dickman, "An Overview of Steganography", 2007.
[10] A. Gupta and R.Garg, "Detecting LSB Steganography In Images", 2012.
[11] Liu, S., Sun, J. &Xu, "An improved image encryption algorithm based on chaotic system", Journal of Computers, vol.4, no. 11, pp.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

1091-1100, 2009.

[12] C.C. Thien, J.C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function"Pattern Recognition, pp. 2875-2881, 2003.

BIOGRAPHY

Khushboo Jainis pursuing M.TECH final year in department of Electronics and Communication Engineering at University College of Engineering, Punjabi University, Patiala. She has done her B.TECH in trade Electronics and Communication Engineering from RIMT-MAEC, MandiGobindgarh. Her research interest includes Image Processing, Security Systems.

AmritKaur is Assistant Professor at University College of Engineering, Punjabi University, Patiala. She has received her M.TECH degree from Punjab University, Chandigarh in 2005.She has eight years of teaching experience. Her areas of interest are control engineering, fuzzy logic, neuro fuzzy, MATLAB. She has to her credit many papers in international journals and national and international conferences.