Implementation of Steganographic Method based on Interpolation and LSB Substitution of Digital Images with Watermarking and Visual Cryptography

Manjinder Kaur
M.Tech CSE, Department of Computer Science
Guru Nanak Dev University, Regional Campus
Jalandhar, Punjab, India

Varinder Kaur Attri
Asst. Professor, Department of Computer Science
Guru Nanak Dev University, Regional Campus
Jalandhar, Punjab, India

ABSTRACT

Today's data is transferred in public network is not secure because of interception by eavesdropper. Steganography, is a better technique for writing the hidden messages in another file format like text, image, videos. In this paper, we proposed a technique of data hiding using interpolation, least significant bit, digital watermarking and cryptography. Performance is tested through the measures mean squared error(MSE) & peak signal to noise ratio and data embedding capacity. Result shows with these parameter are shows better results from the previous results. Results are also shows in bar charts form. The experimental results showed that the average PSNR was 45.05 dB and 429888 bit data embedding capacity was respectively which is better results from the previous algorithm

Keywords

LSB, Interpolation, watermarking, PSNR, MSE, capacity, cryptography.

1. INTRODUCTION

Steganography is the art of hiding a file, image, or secret message within another message, image, or file[2]. The word steganographic combination of the Ancient Greek words steganos , meaning "covered, concealed", and graphein meaning "writing"[2]. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Steganography technique is that which is basically used for information security. Steganography transmits data by actually hiding the existence of the message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it[2]. Steganography is not to alter the structure of the secret message, but hides it inside a cover object. After hiding process cover object & stego object are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Detecting procedure of steganography known as Steganalysis[3].

Some of the applications of Steganography include ownership protection, proof for authentication, air traffic monitoring, medical applications etc. Steganography is the practice of hiding secret messages within cover image to produce a stego image. The recipient of a stego image can use his knowledge of the particular method of steganography employed to recover the hidden text from the stego image[11]. Information hiding is a recently rapidly developed technique in the field of information security and has received significant attention from both industry and academic. It contains two main branches: digital watermarking and steganography with cryptography. The carrier for steganography can be image, text, audio and video. Multimedia data is easy to destroy by the unauthorized persons through Internet. So, it becomes important to be able to transmit the data secretly.

In steganography does not alter the structure of the secret message, but hides it inside a cover image so that it cannot be seen. A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganography methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. Steganography software is becoming effective in hiding information in image, video, audio or text files. Most used steganography technique in least significant bit.

The main objective of Steganography is to communicate securely in such a way that the true message is not visible to the observer. That is unwanted parties should not be able to distinguish any sense between cover-image (image not containing any secret message) and stego image (modified cover-image that containing secret message). Thus the stego image should not deviate much from original cover image[10]. Steganography transmits data by actually hiding the existence of the message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it[9]. Steganography is a technique used to transmit a secret message from a sender to a receiver in a way such that a potential intruder does not suspect the existence of the message. Generally this is done by embedding the secret message within another digital medium such as text, image, audio or video[14].

1.1. LSB

The most important image Steganographic technique is Least Significant Bit embedding technique. In this data can be hidden in least significant bits of the cover image and human eye would be unable to see the hidden image in the cover file. This technique can be used to hiding images in 24-bit, 8-bit or gray scale format. In this technique, least significant bit of each pixel is replaced with the secret message bit until message end. When using a 24 bit image one can be store 3 bit in each pixel by changing a bit of each if the green, red and blue color components. An 800 x 600 pixel image can be store 1,4400,00 bits or 180,000 bytes of the embedded data. For example, a 24 bit can be as follows:

(10110101 01101100 10101101)

(10110110 11001101 00111110)

(10110101 01100011 10001110)

The number 150 that binary representation is 10010110 is embedded into least significant bits of this part of image, the resulting grid as follows:

(10110101 01101100 10101100)

(10110111 11001100 00111111)

(10110101 01100010 10001110)

Although the number is embedded into first 8 bytes of grid, only 3 underlined bits need to be changed according to embedded message. On an average, only the half of bits in an image will need to be modified to hide secret message using maximum cover size. There are 256 possible intensities of the each primary color. Therefore, changing LSB of a pixel results in small changes in intensity of colors. These changes cannot be perceived by the human eye, thus message is successfully hidden. If the message is hidden even in second to least significant as well as in least significant bit then too no difference is seen in image. In LSB, consecutive bytes of the image data from first byte to the end of message are used to embed the information. More secure system can be in which sender and receiver share a secret key which specifies only certain pixels to be changed. Even if the intruder suspects that LSB steganography has been used, there is no way of knowing that pixels to target without the secret key. Thus it is very important techniques[8].

1.2. Discrete Wavelet Transform

Discrete Wavelet Transform is a technique frequently used in compression, watermarking, digital image processing. The transforms in discrete wavelet transform is based on small waves, called wavelet, of varying frequency and also limited duration. A wavelet series is a representation of a square integrable function by a certain orthonormal series generated which is by a wavelet. Further, the properties of wavelet could decompose original signal into wavelet transform coefficients that contains the position information. The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients. Watermarking in the wavelet transform domain is generally a problem of embedding watermark in the sub bands of the cover image. There are four subbands created at the end of each level of image wavelet transformation: they are High-Low (horizontal) subband (HL), Low-Low pass subband (LL), High-High (diagonal) pass subband (HH) and Low-High (vertical) subband (LH). So, subsequent level of wavelet transformation is applied to LL subband of previous one.

1.3. Image Interpolation methods

Interpolation techniques are used for improve the capacity, maintain a good image quality and recover cover image. Image interpolation methods, such as nearest neighbor, B-spline, bilinear, cubic, Langrange, Gaussian and bicubic have been used for the re-sampling. The nearest neighbor method can find the closest corresponding pixels of cover image for each block and set them for a new pixel value for destination image using neighboring pixels. The bilinear interpolation method determines new value from the weighted average of four closest pixels. So, these methods are used to change the size of the images to estimate unknown values of the pixels[7].

1.3.1 Nearest Neighbor technique for Interpolation

INP is that pixels at near the neighboring locations tend to have the similar intensity values. It means that we can be improve image quality with the less distortion. Suppose that a the cover image has four pixels. We can calculate new pixels for up-scaling image 2 times as follows[7].

X'_{10} = (140+(140+120)/2)/2=135

X'_{01} = (140+(140+195)/2)/2=153

X'_{11}= (135+153)/2=144

X'_{21}= (120+(120+188)/2)/2=137

X'_{12}= (195+(195+188)/2)/2=193

For the cover image of the four pixels (140, 120, 195, 188), new pixels (x'_{00}, x'_{20}, x'_{02}, x'_{23}) are retained. But new intermediate pixels (x'_{10}, x'_{01}, x'_{11}, $x'_{21,}x'_{12}$) are calculated[7].

1.4. Cryptography

RSA Algorithm was given by three MIT's Rivest, Shamir & Adleman and has been published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and after that the product of these numbers is used to create a private and a public key, that is further used in encryption and decryption. By using the RSA algorithm we are increasing the security. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure. RSA algorithm procedure can be illustrated in brief as follows [1]:

- Select two large strong prime numbers, p and q. Let n = p q.
- Compute Euler's totient value for n: f (n) = (p - 1) (q - 1).
- Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (n)) = 1.
- Calculate a number d such that d = e-1 mod f (n).
- Encryption: Given a plain text m satisfying m < n, then the Cipher text c = m e mod n.
- Decryption: The cipher text is decrypted by m = c d mod n[5].

2. RELATED WORK

Ki-Hyun Jung et al. [7] in 2014, they have proposed semi-reversible data hiding method based on interpolation and LSB substitution. The interpolation method has been preprocessed before hiding the secret data for the purpose of good quality and higher capacity. Then, the LSB substitution method was applied for the embedding secret data. The cover image with the scaled down size and secret data could be extracted from the stego-image without the need of any extra information.

G. Raj Kumar et al. [14] in 2014, have been improved least significant bit steganalyzers by analyzing and manipulating features of the some existing least significant bit matching steganalysis techniques. This paper explains the LSB Embedding technique with lifting based DWT schemes by using Micro blaze Processor implemented in a FPGA using System C coding. Future work can be extended to RGB or color image processing and can be extended for video processing level also.

Shilpa Thakar et al.[15] in 2013, this paper describe the review of Steganography. Image Steganography alongwith the LSB insertion method used in Image Steganography. The paper suggested a few for future research like integrity and data capacity of cover image. Some steganographic methods need to improve security by using cryptography against attacks.[35]

Gurpreet Kaur et al. [16] in 2013, they compare digital watermarking with other techniques of data hiding.

Steganography, Fingerprinting, cryptography and Digital signature techniques are compared with watermarking. It provides ownership assertion, authentication and integrity verification, usage control and content labeling. All techniques of data hiding secure data with their methods, but watermarking is more capable because of its efficiency. In Watermarking they mark the information which is to be hiding. Security of data is essential today because of cybercrime, which is highly increased day by day. Watermarking provide us easy and efficient security solutions of digital data. Watermarking provide security of not only images, but also audio video and text.

Shamim Ahmed Laskar et al. [11] in 2012, proposed method has been employed for applications that require high-volume embedding with robustness against certain statistical attacks. The present method is an attempt to identify the requirements of a good data hiding algorithm. Steganography is not a good solution to secrecy, but neither is encryption. But if these methods are combined, we will have two layers of protection. If a message is encrypted and hidden with a LSB steganographic method the embedding capacity increases and thus we can hide large volume of data. And the method satisfies the requirements such as capacity, security and robustness which are intended for data hiding. The proposed algorithm is analyzed in the light of the statistical framework in order to prove its efficiency and also to show its level of security. The main focus of the paper is to develop a system with extra security features where a meaningful piece of text message can be hidden by combining two basic data hiding techniques.

Shilpa Gupta et al.[12] in 2012, In this paper existing Least Significant Bit Algorithm has been analyzed and found to have a more amount of distortion, so a new method has been proposed "Enhanced Least Significant Bit (ELSB). It improves the performance of the LSB method because information is hidden in only one of the three colors that is BLUE color of the carrier image. This minimizes the distortion level which is negligent to human eye.

Chunlin Song et al. [17] in 2009, have presented description and analysis of the recent advances in the watermarking in digital images. These techniques are classified into the several categories depending upon domain in which hidden data is inserted, size of hidden data and the requirement of which hidden data is to be extracted. The experiment shows the different effective algorithms of watermark. The result indicates frequency domain is more robustness than spatial domain. Several challenges that are often unaddressed in the literature have also been identified. Meeting these challenges is essential in advancing the current state of the art of watermarking in digital images.

3. PROPOSED METHODOLOGY

In this section we explain the methodology for the proposed technique and also draw the flow chart of proposed technique. we divide the methodology in three phase and further explain the all steps.

Phase 1:
Code is developed for opening GUI for his implementation. After that we develop a code for loading the image file and message file in the MATLAB database.

Phase 2:
Code is developed for LSB & watermarking using discrete wavelet transform. Apply both LSB and interpolation with watermarking and visual cryptography on watermarked image. A code is developed for saving the stegano and crypto file.

Phase 3:
After this code is developed for the extraction process. Within the extraction process we develop code for the message extraction from the watermarked image after cryptography.

Phase 4:
After that code is developed for the analysis of results obtained using various parameters like MSE, PSNR and Capacity.

Flow Chart: Sender Side

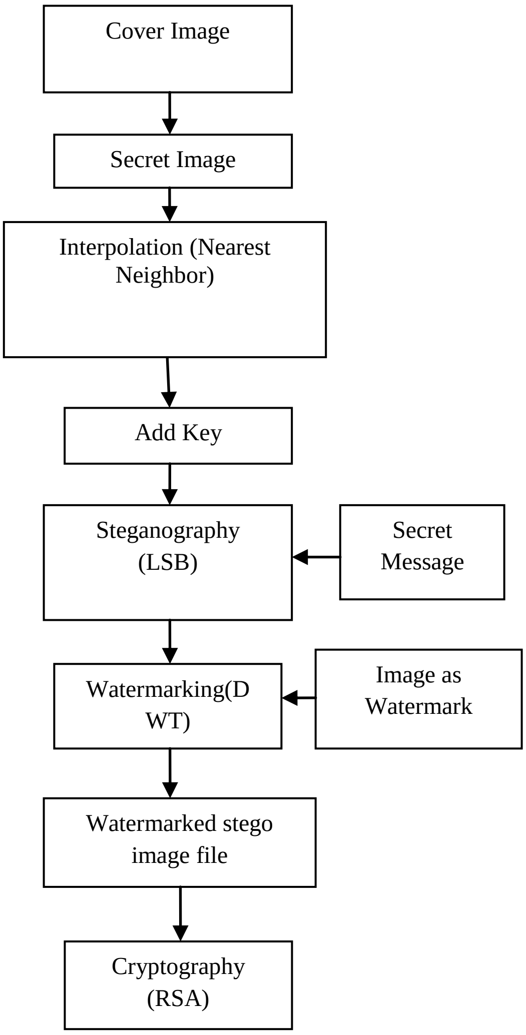


Figure: 3.1 Sender Side flow chart

Flow Chart: Receiver Side

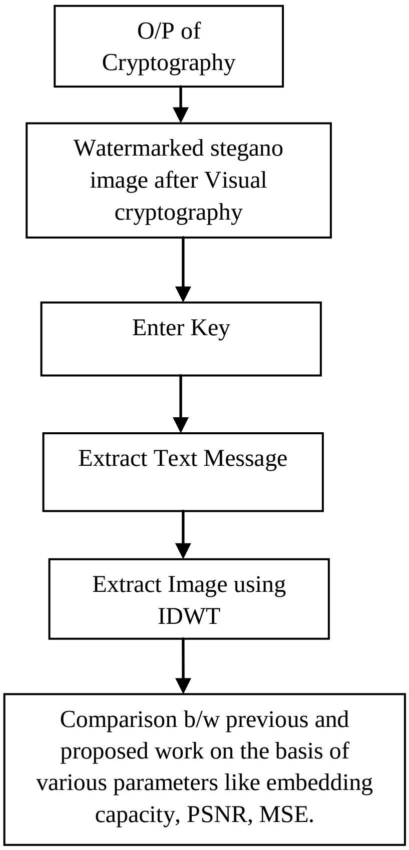

O/P of Cryptography
Watermarked stegano image after Visual cryptography
Enter Key
Extract Text Message
Extract Image using IDWT
Comparison b/w previous and proposed work on the basis of various parameters like embedding capacity, PSNR, MSE.

Figure: 3.2 Receiver Side Flow Chart

4. EXPERIMENTAL RESULTS & DISCUSSION

In this section we present and discuss the implementation of the proposed technique, data parameter used, experimental results of the proposed method and also shows the results in the bar charts form and table form also.

4.1. Implementation process of proposed technique

Implementation of proposed algorithm in matlab with inbuilt toolbox image processing using GUI functions.

4.4.1 Embedded Process

1.) load the cover image
2.) Load Secret image
3.) Apply Interpolation using (Nearest Neighbor)
4.) Add Key
5.) Hide secret data using LSB
6.) Apply watermarking using DWT on secret image
7.) Apply RSA algorithm on watermarked image

4.4.2 Extraction Process

1.) Load watermarked and crypto image
2.) Load watermarked image after cryptography
3.) Enter Key
4.) Extract text message using ILSB
5.) Extract secret image using IDWT
6.) Find MSE, PSNR, Embedding Capacity

4.2. Parameters

Following are the parameters which are used implementation:

4.2.1 PSNR

The Peak Signal to Noise Ratio (PSNR) is the ratio between maximum possible power and corrupting noise that affect representation of image. PSNR is usually expressed as decibel scale. The PSNR is commonly used as measure of quality reconstruction of image. The signal in this case is original data and the noise is the error introduced. High value of PSNR indicates the high quality of image[13].

PSNR1 =10*log10((255)^2/MSE)

Here MSE is a mean square error

4.2.2 MSE

Mean Square Error can be estimated in one of many ways to quantify the difference between values implied by an estimate and the true quality being certificated. MSE is a risk function corresponding to the expected value of squared error. The MSE is the second moment of error and thus incorporates both the variance of the estimate and its bias. The MSE of an estimate and is defined as[13]

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[(i,j) - K(i,j)]^2$$

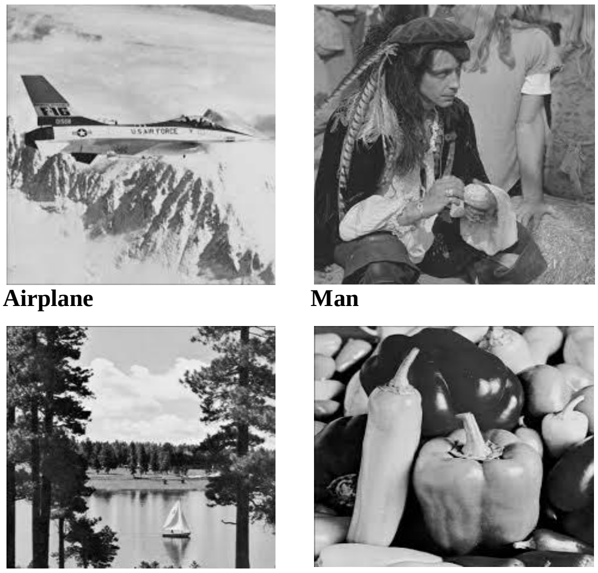
4.2.3 Capacity

The maximum amount of information that can be carried in the media, steganography algorithm can be implanted without being carried in the media to apply tangible change. High capacity steganography algorithms is to evaluate the main parameters However, high capacity, reduced image quality due to use of the algorithm can establish a compromise between quality and capacity of the application or the preference of one over the other.

4.3. Experimental results, bar charts and tables

Experimental results, bar charts and tables of results shows as following:

For the testing of results we used four images 512*512 which shows different results for different image. Airplane, man, boat and pepper images are used for testing as following.

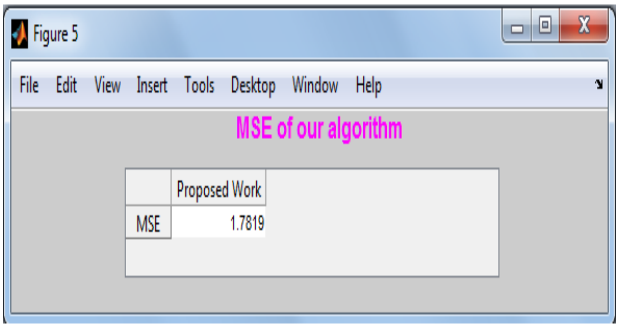


Airplane **Man**

Boat **Pepper**

Figure 3.3 Four original cover image

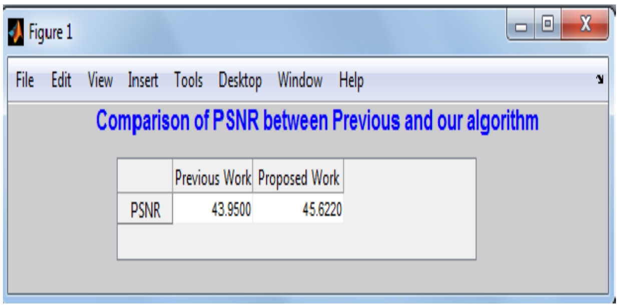
Results are shown in the bar charts form as following:



MSE of our algorithm

	Proposed Work
MSE	1.7819

Figure: 3.4 MSE of Our algorithm of Airplane



Comparison of PSNR between Previous and our algorithm

	Previous Work	Proposed Work
PSNR	43.9500	45.6220

Figure 3.5 Comparison of PSNR b/w previous & our algorithm of Airplane

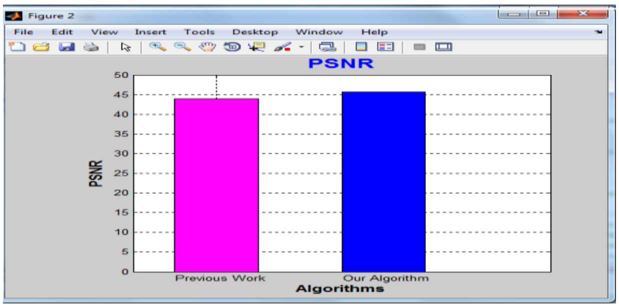
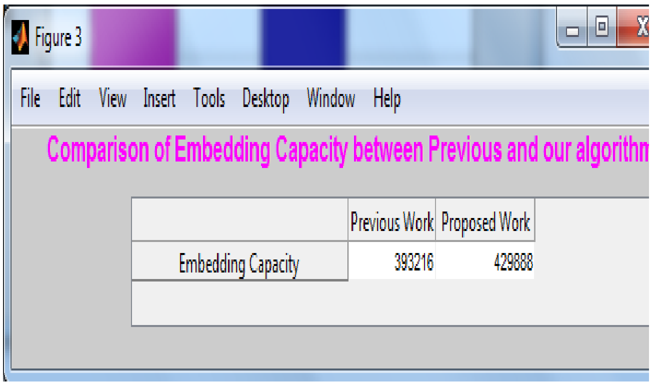


Figure 3.5 Comparison of PSNR b/w previous and our algorithms in bar charts



Comparison of Embedding Capacity between Previous and our algorithm

	Previous Work	Proposed Work
Embedding Capacity	393216	429888

Figure: 3.6 Comparison of embedding capacity between previous and our algorithm of Airplane

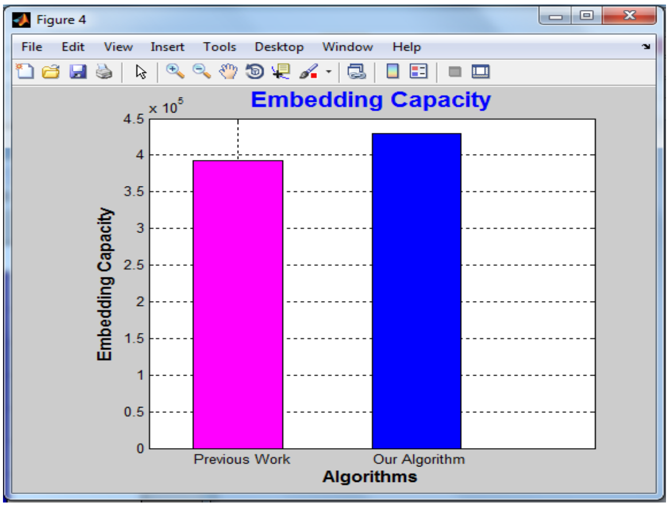
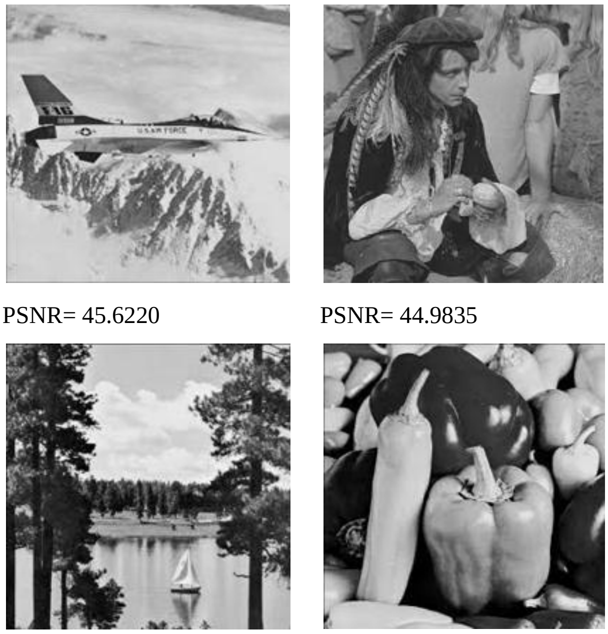


Figure: 3.7 Comparison of embedding capacity between previous and our algorithm in bar charts of Airplane



PSNR= 45.6220 PSNR= 44.9835

PSNR= 44.4977 PSNR= 45.1199

Figure: 3.8 Four watermarked image after visual cryptography with PSNR result

Experimental results shows in the form of tables as following:

Table: 1. MSE, Capacity and PSNR values of our algorithms with different images

Cover Image	**MSE**	**Capacity(bit)**	**PSNR(dB)**
Airplane	1.7819	429888	45.6220
Man	2.0641	429888	44.9835
Boat	2.3084	429888	44.4977
Peppers	2.0003	429888	45.1199

Table: 2. Comparison of data embedding capacity of our algorithms with previous work

Cover Image	**Capacity of Previous Work**	**Capacity Our Algorithm**
Airplane	393216	429888
Man	393216	429888
Boat	393216	429888
Pepper	393216	429888

Table: 3. Comparison of PSNR of our algorithms with previous work

Cover Image	**PSNR of Previous Work**	**PSNR Our Algorithm**
Airplane	43.95	45.6220
Man	43.93	44.9835
Boat	43.92	44.4977
Pepper	43.93	45.1199

5. CONCLUSION & FUTURE SCOPE

We have proposed Steganographic method based on Interpolation and LSB substitution of digital images with Watermarking and Cryptography. The interpolation method has been applied before hiding secret data for the purpose of higher capacity and good quality. Then, the LSB substitution method was applied for embedding secret data. Then applied DWT on the image. After this cryptography RSA algorithm used security purpose. The experimental results showed that the average PSNR was 45.05 dB and 429888 bit data embedding capacity was respectively which is better results from the previous algorithm. In future work the work possible with histogram and also improve the PSNR using different techniques and also work done based on other file format.

6. REFERENCES

[1] Kalaivanan.S, Ananth.V and Manikandan.T, “A Survey on Digital Image Steganography”, International Journal of Emerging Trends and Technology in Computer Science, ISSN 2278-6856, Volume 4, Issue 1, January-February 2015.

[2] Steganography. en.wikipedia.org/wiki/Steganography.

[3] Aruna Varanasi, M. Lakshmi Anjana and Pravallika Pasupulate, “Image Steganography with Cryptography using Multiple Key Patterns”, International Journal of Computer Applications (0975 – 8887), Volume 90 – No 15, March 2014.

[4] G. Raj Kumar, M. Maruthi Prasada Reddy and T. Lalith Kumar, “An Implementation of LSB Steganography Using DWT Technique”, International Journal of Engineering Research and General Science, ISSN 2091-2730, Volume 2, Issue 6, October-November, 2014.

[5] Fundamentals of Cryptography. http://www.iimahd.ernet.in/~jajoo/ec/cryptography.htm

[6] Monika Birara and Subhash chander, “Steganography based on interpolation and LSB substitution with visual cryptography on digital images”, International Journal of Computer Application and Technology , ISSN: 2349-1841, May - 2014, pp. 68-70.

[7] Ki-Hyun Jung & Kee-Young Yoo, “Steganographic method based on interpolation and LSB substitution of digital images” Springer Science+Business Media New York, 5 jan., 2014

[8] Mukesh Garg and A.P. Gurudev Jangra, “An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques”, International Journal of Advanced Research in Computer Science & Software Engineering, ISSN: 2277 128X , Volume 4, Issue 1, January 2014.

[9] Sonia Bajaj, Manshi Shukla, “Review on: secret data transfer using interpolation and lsb substitution with water marking”, Global Journal of Advanced Engineering Technologies, ISSN: 2277-6370, Vol3, Issue3 2014.

[10] Mehdi Hussain & Mureed Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Volume 54, May, 2013.

[11] Shamim Ahmed Laskar and Kattamanchi Hemachandran, “High Capacity data hiding using LSB Steganography and Encryption”, International Journal of Database Management Systems, Vol.4, No.6, December 2012.

[12] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, “ Enhanced Least Significant Bit algorithm For Image Steganography”, International Journal of Computational Engineering & Management, ISSN (Online): 2230-7893, Vol. 15 Issue 4, July 2012.

[13] Pooja Kaushik and Yuvraj Sharma, “Comparison Of Different Image Enhancement Techniques Based Upon Psnr & Mse”, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11, 2012.

[14] Ankit Chaudhary, J. Vasavada, J.L. Raheja and Sandeep Kumar, Manmohan Sharma, “A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images”, The 22nd International Conference on Computer Graphics and Vision, Russia, Moscow, October 01, 05, 2012.

[15] Sidham Abhilash and S M Shamseerdaula,” A Novel Lossless Robust Reversible Watermarking Method for Copyright Protection of Images,” Journal of Engineering Research and Applications, Vol. 3, Issue 6, Nov-Dec 2013.

[16] Gurpreet Kaur and Kamaljeet Kaur, “Digital Watermarking and Other Data Hiding Techniques”, International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, Volume-2, Issue-5, April 2013.

[17] Chunlin Song, Sud Sudirman, Madjid Merabti, “Recent Advances and Classification of Watermarking Techniques in Digital Images”, ISBN: 978-1-902560-22-9,2009PGNet.