ISSN:0975-9646



# Performance Evaluation of an approach for Secret data transfer using interpolation and LSB substitution with Watermarking

Sonia Bajaj, Manshi Shukla

*Computer Science, Punjab Technical University*
*RIMT IET ENGG. College Gobindgarh, India*

***Abstract***: - **In the field of communication, security is the most important issue now days. Most probably of data asecurity and data hiding algorithms have been developed. In the last decade, these algorithms worked as motivation for our research. In this paper, Image Steganography with watermarking using LSB and interpolation Techniques are used. We have designed a system that will allow a user to securely transfer text messages by hiding them in a digital image file using the local characteristics within an image. A combination of image Steganography and interpolation with watermarking provides a strong backbone for its security. In this paper, the proposed system not only hides large volume of data within an image. But it also limits the perceivable distortion that might occur in an image while processing it. This thesis has an advantage over other information security thesis because the hidden text is in the form of image, which is not obvious text information carriers. The performance of hiding method was tested using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and embedding capacity of proposed system.**

***Keywords***: - Steganography, LSB, Interpolation, DWT, Watermarking.

## I. INTRODUCTION

**Steganography** is the art or practice of concealing a file, image, or secret message within another message, image, or file. The word *Steganography* means "covered writing" or "concealed writing". There are three techniques that are mainly used in information security applications and these are: Steganography and watermarking. They are different in some aspects:-

1. Stegnography scrambles the data to be communicated so that unintended receivers cannot perceive the information. The fact that the communication has been carried out is known to everyone.
2. 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.
3. Digital Watermarking mainly prevents illegal copy or claims the ownership of digital media but it is not geared for communication. [1]

### Different Kinds Of Steganography

Almost all digital file formats can be used for Steganography, But these formats are more suitable are those with a high degree of redundancy. An object whose bita are redundant which can be altered without the alteration being detected easily.

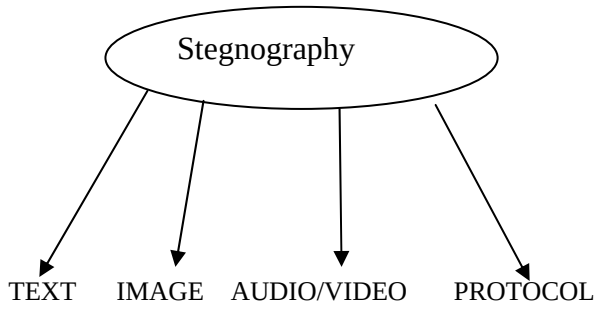



Figure 1: Categories of Steganography

Audio and Image files especially comply with this requirement that can be used for information hiding. The following Fig 1. Shows the process of Steganography.

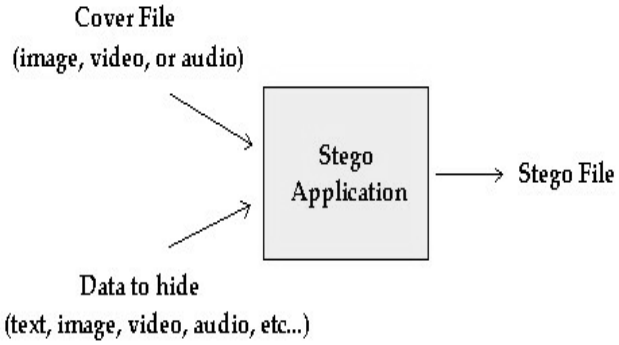



Figure 2: Steganography process

### Watermarking

"Watermarking" is the process of hiding digital information in a carrier signal; the hidden information, but does not need to contain a relation to the carrier signal. The watermarking may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners digital watermarking is a passive protection tool. It is used to marks data, but does not degrade it nor controls the access of data. One of the main application of digital watermarking is *source tracking*. The process of watermark is embedded into a digital signal at each point of distribution. In this process, if a copy of the work is found later. After that the watermark may be retrieved from the copy and the source of the distribution is known. This

technique reportedly has been used to detect the source of illegally copied movies.

1) Copyright identification – provide a proof of ownership.
2) User identification (fingerprinting) – encode identity of legal users to encode sources of illegal copies.
3) Authenticity determination – if the watermark will be destroyed by modification in an image, its presence quarantines authenticity.
4) Automated monitoring – monitor when and where images are used (for royalty collection or the location of illegal uses).
5) Copy protection – they can specify rules of image usage and copying.

**Least significant bit (LSB)**

Spatial Domain in LSB coding and Frequency Domain. The most-common Steganography techniques are least significant bit (LSB) substitution and pixel-value differencing (PVD). LSB substitution replaces the least significant bit with a secret bit stream. LSB matching is either added or subtracted randomly from the pixel value of the cover data when the embedding bit does not match. The revised LSB matching was proposed to improve by lowering the number of modifications. The PVD offers imperceptibility by calculating the difference of two consecutive non-overlapping pixels. Reversible data hiding methods allow data to be embedded inside a digital media and later retrieved as required, leaving an exact original image. It is mainly used for content authentication of multimedia data, where the original host signal is crucial in order to make the right decision. Reversible data hiding methods can be classified into three types: spatial domain, compressed domain and frequency domain. Image interpolation techniques, such as the nearest neighbor, bilinear, B-spline, cubic, bicubic, Langrange and Gaussian have been used for re-sampling.

Least significant bit (LSB) insertion is a simple approach for embedding information in a cover image. The least significant bit (i.e. the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. In 24-bit image, a bit of each of the green color, red color and blue color components can be used, since they each are represented by a byte. For example, a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

If the number 200, the binary representation is 11001000.Then it is embedded into the least significant bits of this part of the cover image, then the resulting grid is:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

So if the number was embedded into the first 8 bytes of the grid only the three underlined bits needed to be changed according to the embedded message. The average only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. [2]

**Discrete Wavelet Transform (DWT)**

DWT is used for digital images. Many DWTs are available. Depending on the application appropriate one should be used. The simplest transform is hear transform. To hide text message integer wavelet transform can be used. When DWT transform is applied to an image it is decomposed into 4 sub bands are:

a) LL
b) HL
c) LH and
d) HH.

The LL part contains the most significant features. So if the information is hidden in LL part the stego image can withstand compression or other manipulations. Sometimes distortion may be produced in the stego image and then other sub bands can be used. [3]

**Interpolation**

The interpolation is a method of constructing new data points within the range of a discrete set of known data points in the mathematical field of numerical analysis. In the field of engineering and science, a number of data points which is obtained by sampling or experimentation which represents the values of a function for a limited number of values of the independent variable. It is often required to interpolate (i.e. estimate) the value of that function for an intermediate value of the independent variable. It may be achieved by curve fitting. A different problem which is closely related to interpolation is the approximation of a complicated function by a simple function. In the Interpolation, suppose the formula for some given function is known. But it is too complex to evaluate efficiently. There are few known data points from the original function can be used to create an interpolation based on a simpler function. When a simple function is used to estimate data points, interpolation errors are usually present. Hence, the interpolation method is used. The gain in simplicity may be of greater value than the resultant loss in accuracy.

## II. LITERATURE SURVEY

[1] HS Manjunatha Reddy the secure data transmission over internet is achieved using Steganography. In this paper high capacity and security stenography using discrete wavelet transform is purposed The capacity are improved with acceptable PSNR compare to existing algorithm.

[2] S.M Masud Karim (2011) in this paper, hidden information is stored into different position of LSB of image depending on the secret key. As a result, it is difficult to extract the hidden information knowing the retrieval methods. It is a new approach to substitute LSB of RGB true color image.

[3] Mohammad Abdulla (2013) this paper reviewed the latest research work done on digital image watermarking. It presented the basic model of digital image watermarking for embedding and detection. It mentioned the requirements of any digital image watermarking system.

[4] Shailende Gupta (2012): The Least Significant Bit (LSB) Steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure.

[5] Nagham Hamid et. Al (2012): This paper reviewed the main steganographic techniques for both lossy and lossless image formats, such as JPEG and BMP. Techniques include those modifying the image in the spatial domain, in the transform domain, and those modifying the image file formatting.

[6] Navnidhi Chaturvedi et. al (2012). This paper is concerned with image watermarking technique based on a 3-level discrete wavelet transform has been implemented. This technique can embed the invisible watermark into salient features of the image using alpha blending technique. Quality of the watermarked image and the recovered watermark are dependent only on the scaling factors k and q and also indicate that the three level DWT provide better performance than 1-level and 2-level DWT.

[7] L.Rondney Long (2010) proposed in their paper the basics about the Steganography techniques. They suggested the features of an embedding message in the Steganography. Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper we will discuss how digital videos can be used as a carrier to hide messages. This paper also analyses the performance of some of the Steganography tools. Steganography is a useful tool that allows covert transmission of information over and over the communications channel. Combining secret video with the carrier video gives the hidden video. The hidden video is difficult to detect without retrieval. This paper will take an in-depth look at this technology by introducing the reader to various concepts of Steganography, a brief history of Steganography and a look at some of the Steganographic technique.

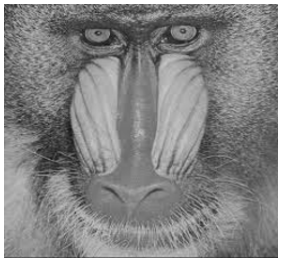
[8] Mr.Vikas Tyagi et.al (2012): In this paper basically discussed a technique based on the L s b and a new encryption algorithm. By matching data to an image there is less chance of an attacker being able to use signalises to recover data before hiding data in an image the application first encrypt it use encryption algorithm to provide more security.

[9] Zunera jalil et. Al (2011): This paper is basically concerned with the problem has become more critical with the increasing using of the internet and digital technologies digital watermarking compare as a solution for copyright protection problem in this paper we propose a novel text watermarking algorithm with embedded the watermark image in the text the algorithm with the blind zero watermark approach gives a robust solution for a text watermarking problem the result show that our algorithm is more robust secure and efficient.

These are four cover images

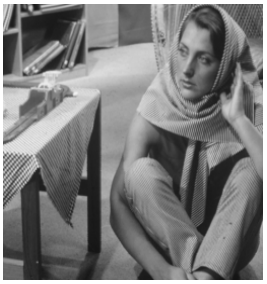
A

B



C

D



## Methodology

The research methodology is divided into 5 phases to achieve our desired goal:

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

**Phase 2:** Then code is developed for secret image and then we apply interpolation for increase or decrease the quality of image.

**FLOW CHART (**SENDER SIDE):-

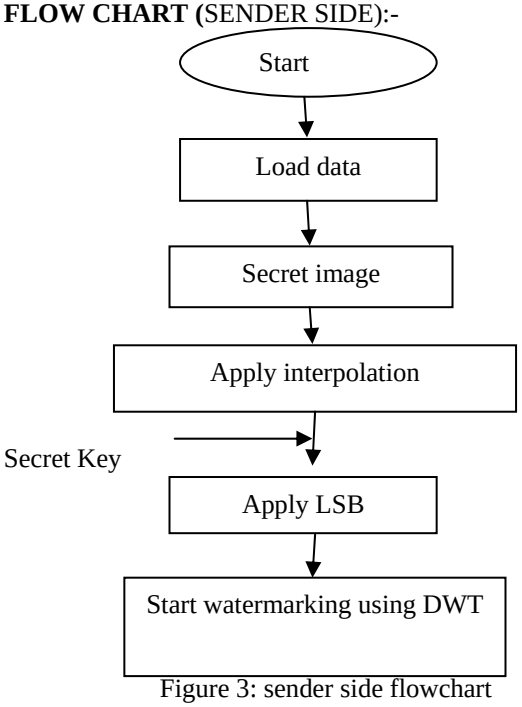



Figure 3: sender side flowchart

**Phase 3:** Code is developed for LSB and watermarking using discrete wavelet transform. Apply both LSB and interpolation with watermarking on image. A code is developed for saving the watermarked file.

**Phase 4:** After that code is developed for the extraction process using LSB and IDWT technique. Within the extraction process we develop code for the stego image extraction from watermarked image and then message extraction from the stego file.

**Phase5:** After that code is developed for the analysis of results obtained using various parameters like MSE, PSNR and embedding capability.

**FLOW CHART** (RECEIVER SIDE):-

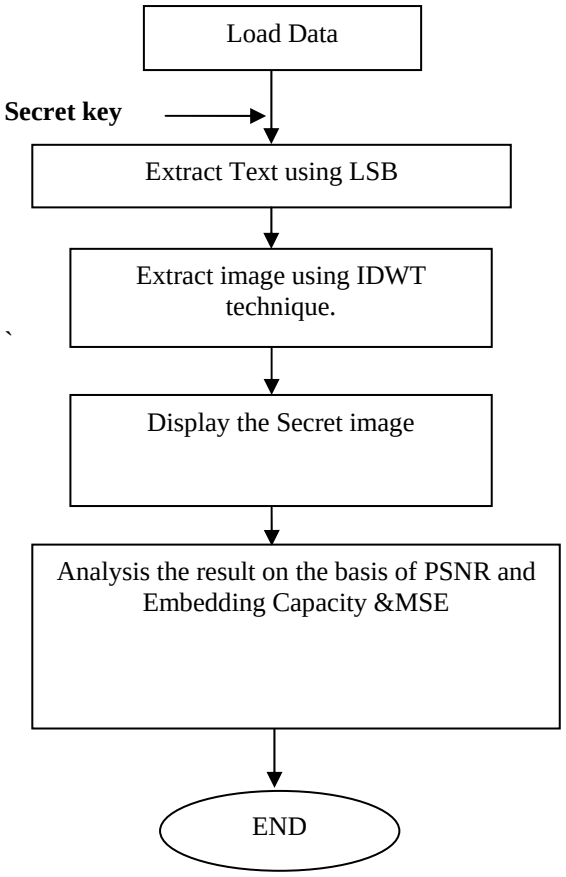



Figure 4: Receiver side flowchart

## III.RESULTS

Comparison between previous and proposed work on the basis of PSNR and MSE and Embedding Capacity. The following figures show the implementation of secret data transfer using LSB substitution and interpolation with watermarking:-

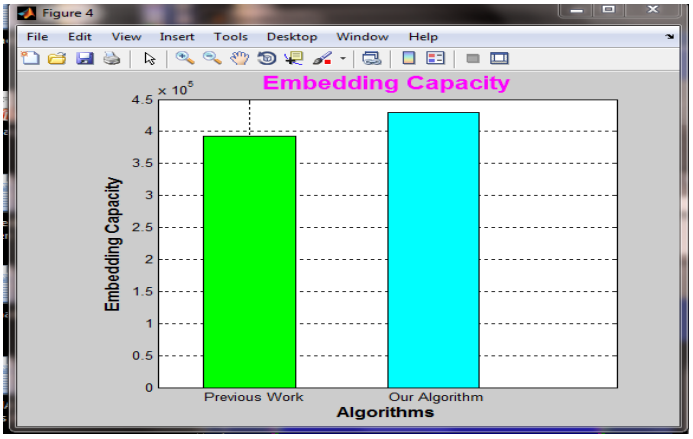



Figure 5: Increase and embedding capacity

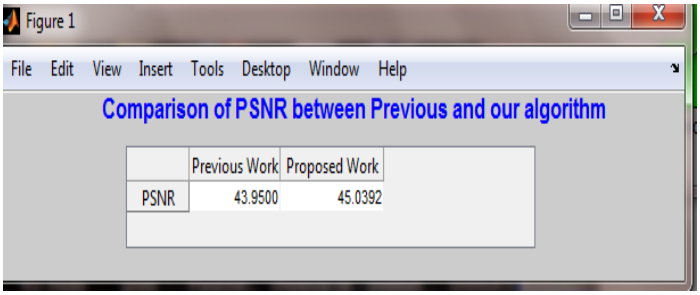



Figure 6: Comparison between previous and proposed work

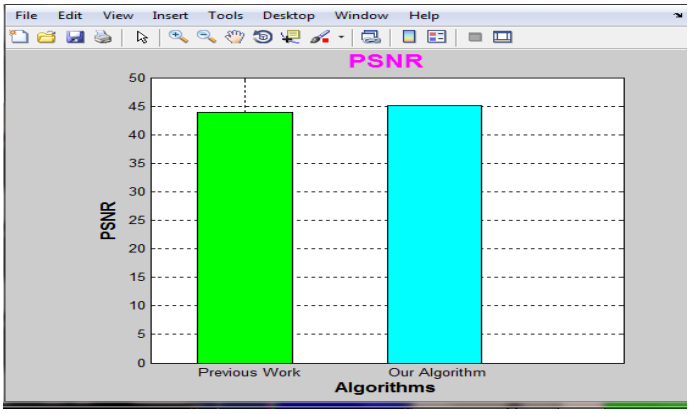



Figure 7: PSNR values of previous and proposed work

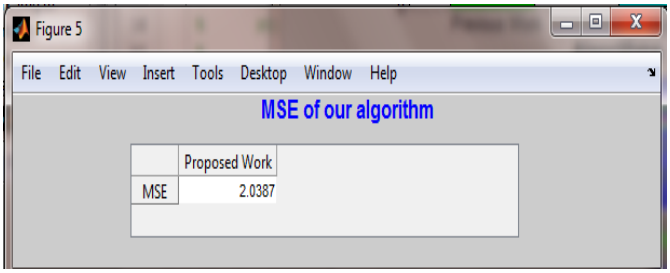



Figure 8: MSE values of proposed work

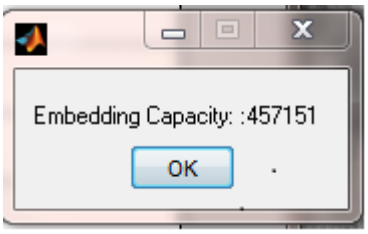
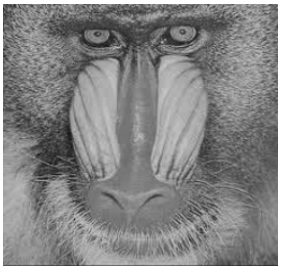



Figure 9: Embedding capacity

A B

PSNR=45.9518 db PSNR=45.0375db

C D


PSNR=45.9486 PSNR=45.6715 db

Four watermarked images

## IV. CONCLUSION

This paper analysed the different techniques for embedding and security. After analysing these techniques, interpolation, the least significant bits (LSB); technique is the best technique for hiding a secret message or image into cover media. For protecting the secret message, transform domain techniques DWT is best .The main advantage of this system is to provide high security for key information exchanging.

## V. FUTURE SCOPE

The proposed method can be developed to work on the different scanned images simultaneously .Also in future more parameters like by enhancing the number of pixels quality can be considered. As the work can be extend for the infinite number of users.

## REFERENCES

[1] Shilpa Gupta, ''Enhanced least significant bit algo for image stegnography,'' IJCEM International Journal of Computational Engineering & M anagement, Vol. 15, 4, July 2012.

[2] Shailender Gupta,''information hiding using least significant bit stegnography and cryptography,''IJMECS I.J modern Education and computer science,june 2012,

[3] HS Manjunatha Reddy "High Capacity and security "Stegnography using DWT,"IJCSS international journal of computer science and security,vol.(3)

[4] S. M. Masud Karim, Md. Saifur Rahman "*A New Approach for LSB Based Image Steganography using Secret Key*" International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 2011 IEEE

[5] N. Provos and P. Honeyman, "Hide and Seek: An introduction to Steganography," IEEE Security & Privacy Journal 2003.

[6] Navnidhi Chaturvedi, Dr.S.J.Basha "Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR" International Journal of Innovative Research in Science, Engineering and Technology Vol. 1, Issue 2, December 2012.

[7] Pallavi Patil, "*DWT Based Invisible Watermarking Technique for Digital Images*" International Journal of Engineering and Advanced Technology (IJEAT) Volume-2, Issue-4, April 2013

[8] Blossom Kaur, Amandeep Kaur, Jasdeep Singh "*Steganographic approach for hiding image in dct domain*" International Journal of Advances in Engineering & Technology, July 2011. ©IJAET ISSN: 2231-19

[9] Steven W. Smith, the Scientist and Engineer's Guide to Digital Signal Processing.

[10] Mr vikas tyagi and Mr Atul kumar,"Image stegnography [using Least Significant Bit with Cryptography " JGRCS Journel of global Research in computer Science,vol.3,no.3,March 2012

[11]. Weiqi Luo, Fangjun Huang "Edge Adaptive Image Steganography Based on LSB Matching Revisited" IEEE transactions on information forensics and security, vol. 5, no. 2, June 2010.

[12]. L. Reyzen and S. Russell, "More efficient provably secure Steganography" 2007.

[13]. Jarno Mielikainen, "LSB Matching Revisited" IEEE SIGNAL PROCESSING LETTERS, VOL. 13, NO. 5, MAY 2006

[14]. Mitsugu Iwanmoto and Hirosuke Yamamoto, "The Optimal n-out-of-n Visual Secret Sharing Scheme for GrayScale Videos", IEICE Trans. Fundamentals, vol.E85- A, No.10, October 2002, pp. 2238-2247.

[15]. Z.Zhou, G.R.Arce, and G.Di Crescenzo, "Halftone Visual Cryptography", IEEE Tans. On Video Processing,vol.15, No.8, August 2006, pp. 2441-2453.

[16]. Shen Wang, Bian Yang and Xiamu Niu "A Secure Steganography Method based on Genetic Algorithm" Journal of Information Hiding and Multimedia Signal Processing c 2010 ISSN 2073-4212 Ubiquitous International Volume 1, Number 1, January 2010

[17]. Anuj Kumar, Prateek Bansal "Analysis and Implementation of Algorithm to Hide Secret Message" International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X Volume 3, Issue 2, February 2013.

[18]. Muhammad Abdul Qadir, Ishtiaq Ahmad "Digital Text Watermarking: Secure Content Delivery And Data Hiding In Digital Documents" 2005 IEEE.