ISSN:0975-9646

A Novel Approach for Secret Data Transfer using Interpolation and LSB Substitution with Watermarking: A Survey

Sonia Bajaj [1],Manshi Shukla[2]

[1] *Research scholar computer science and engineering RIMT IET, Mandi Gobindgarh, punjab, india*
[2] *Assistant professor computer science and engineering department of RIMT IET, Mandi Gobindgarh, punjab, india*

***Abstract* :- Today's large demand of internet applications requires data to be transmitted in a better manner. Data is transferred in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the better solution for this issue is Steganography, which is the technique of writing hidden messages in such a way that no one, apart from the sender and main receiver recipient, detects the existence of the message, a type of security through obscurity. In this thesis, the Steganographic method used is based on steganography which is concerned with embedding secret data in a file. In this thesis a semi-reversible data hiding method that utilizes interpolation and the least significant substitution technique is proposed with watermarking technique. The least significant-bit (LSB) based technique are very popular for steganography in spatial domain. The easiest LSB technique simply replaces the LSB in the cover image with the bits from secret information. Further latest techniques use some criteria to identify the pixels in which LSB(s) can be replaced with the bits of secret information. The performance of hiding method was tested using the fidelity measures Mean Square Error (MSE), and Peak Signal to Noise Ratio (PSNR) to describe the overall error rate.**

***Keywords*—steganography.LSB substitution. interpolation. image security**

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: cryptography, steganography and watermarking. They are different in some aspects 1. Cryptography 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.

Different Kinds Of Steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Audio and Image files especially comply with this requirement that can be used for information hiding. Fig 1. Shows the four main categories of file formats that can be used for steganography.

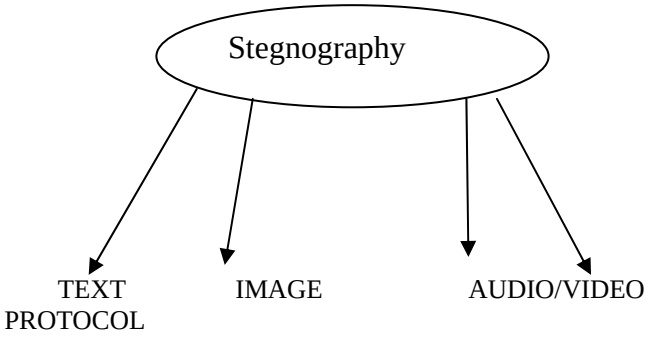

Fig 1 .Categories of steganography

Hiding information in text is historically the most important method of steganography. A method was to hide a secret message in every nth letter of every word of a text message.

II. 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 due to the emerging demand for it in various fields, 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, red 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, 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.

III 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 haar 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: LL, HL, LH and HH. 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. But sometimes distortion may be produced in the stego image and then other sub bands can be used.

IV.REVIEW OF LITERATURE

[1] HS Manjunatha Reddy The secure data transmission over internet is achieved using Steganography. In this paper high capacity and security stegnography using discrete wavlet 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 .

V. PROPOSED WORK

- Interpolation with LSB and Watermarking has demonstrated its capability for solving complex data hiding problems.
- The relative performance evaluation of this algorithm has been carried out.
- We use Watermarking with Interpolation and Stegnography thus providing three tier security.
- Even if Stego image is tampered or noise is added in Stego image secret message is recognized and thus our purpose is fulfilled.
- Better PSNR results of Interpolation with LSB and Watermarking

VI. CONCLUSIONS

This paper analysed the different techniques for embedding and security. After analysing we concluded 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 further we use Watermarking using DWT technique which is best.

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]Katzenbeisser and Petitcolas,”Information Hiding Techniques for Stenography and Digital watermarking” Artech House, Norwood, MA. 2000.