Image Surveillance

P. Subashini[1], Aditya Vashishtha[2], Chitrak Bari[3], Rahul Saha[4]

[1]*Assistant Prof., Computer Science, SRMIST, Tamil Nadu, India.*

[2]*UG Scholar, Computer Science, SRMIST, Tamil Nadu, India.*

[3]*UG Scholar, Computer Science, SRMIST, Tamil Nadu, India.*

[4]*UG Scholar, Computer Science, SRMIST, Tamil Nadu, India.*

ABSTRACT

The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. In order to transfer the data securely to the destination without any modifications, there are many approaches like cryptography and steganography. This paper deals with the image steganography as well as with the different security issues, general overview of cryptography, steganography and digital watermarking approaches and about the different stenographic algorithms like Least Significant Bit (LSB) algorithm, JSteg, F5 algorithms. It also compares those algorithms in means of speed, accuracy and security.This paper gives a brief idea about the new image stenographic approach that make use of Least Significant Bit (LSB) algorithm for embedding the data into the bit map image (.bmp) which is implemented through the Microsoft .NET framework.

Keyword: *Image Surveillance, Image Analysis, LSB, RGB.*

I. INTRODUCTION

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very

simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways.

Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet.

In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography and digital watermarking. The level of visibility is decreased using many hiding techniques in Image Modeling like LSB Manipulation, Masking and filtering. These techniques are performed by different stenographic algorithms like F5, LSB, JSteg etc. and the act of detecting the information hidden through these algorithms is called Steganalysis.

One of the possibilities to close the gap between copyright issues and digital distribution of data is digital watermarking. It is mainly based on Stenographic techniques and enables useful safety mechanisms. It acts as a very

good medium for copyright issues as it embeds a symbol or a logo in the form of a watermark, which cannot be altered manually.

II. LITERATURE SURVEY

Most steganography approaches that embed the data within the pixel space take advantage of the LSB method. When a file is made, usually some of its bytes are not usable[1]. These bytes can be changed without harming the file considerably. This allows us to write some information in these bytes without anybody being aware that the process has taken place. As each video file is merely a binary file that contains colors and light intensity of each pixel according to the binary number [2].

To hide a text in an image. In this case every character, takes up one byte (8 bites). Since these bits should be put into these image pixels, thus are needed to divide these eight bits to a 1-bit packages (or larger packages), and each bit are placed in the least significant bits of one of the main three colors of pixels. This way, words of all languages that are compatible with ASCII or UTF-8 (or any other coding), can be embedded within an image [3].

In digital steganography, the basic technique of data hiding is to replace the LSBs of the input image with the bits of secret data as described in [38] and its basic idea is given as under Binary representation of eight (8) pixels:

10001101, 10000010, 01110110, 01100001, 00101000, 10000100, 01001011, 01110111.

Secret character: A 01000001

After hiding this secret character (A) in these pixels, the pixel values in binary format are obtained as follows: 10001100, 10000011, 01110110, 01100000, 00101000, 10000100, 01001010, and 01110111.

The bold face LSBs indicate the changed pixels during data hiding. It can be seen in the above that only four pixels change which shows approximately half of the pixels change. Therefore, the distortion caused by this approach in stego images is almost undetectable using HVS [4].

A new approach to enhance the robustness of existing LSB substitution method by adding one level security of secret key. In the proposed method, secret key and red channel are used as an indicator while green and blue channels are used as data channels. On the basis of secret key bits and red channel LSBs, the secret data bits are embedded either in green channel or blue channel. An intruder cannot easily extract the secret information without the correct secret key. Moreover, the experimental results also show better image quality and robustness.[5]

The methods discussed so far produce stego images of low quality which are easily detectable using HVS. Furthermore, the data is embedded in cover images without encryption which makes its extraction easy for attackers.

III. EXISTING SYSTEM

A digital watermarking algorithm for copyright protection based on the concept of embedded digital marking and modifying frequency coefficients in discrete wavelet transform(DWT) domain is presented. We embed the watermark into the detail wavelet coefficients of the original image with the use of a key. This key is randomly generated and used to select the exact locations in the wavelet domains in which to embed the data. Original unmarked image is not required for watermark extraction. The performance of existing watermarking algorithm is robust to variety of signal distortion and noises. Doesn't provide security against any modification.

.

IV. PROPOSED METHOD

The proposed method should provide better security when transmitting or transferring the data or messages from one end to another. The main objective of the project is to hide the message or a secret data into an image which further act as a carrier of secret data and to transmit to the destination securely without any modification.

If there are any perceivable changes when inserting or embedding the information into the image or if any distortions occur in the image or on its resolution there may be a chance for an unauthorized person to modify the data. So, the data encryption into an image and decryption and steganography plays a major role in the project.

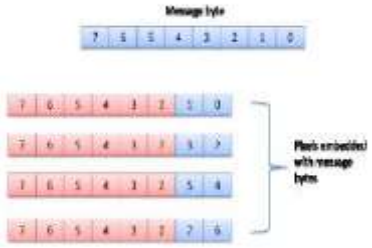

Fig 4.1 Proposed Algorithm

V. ADVANTAGES

In this section for encryption, LSB (Least Significant bit) algorithm is used which helped to build a stenographic application to provide better security. The LSB algorithm provides better security compared to JSteg algorithm with improved data compression and data hiding capacities. The image is used as carrier for transmission of data and by using the Least Significant bit Algorithm the message bits are to be inserted in to the least significant pixels of an image. The decryption process is similar but opposite to the encryption process. When the receiver wants to decrypt the data from the image, it uses same least significant bit algorithm for extracting the data from the image by taking password or key as reference.

VI. LSB ALGORITHM

LSB substitution is the process of adjusting the least significant bit pixels of the carrier image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) are changed. There are many approaches available for hiding the data within an image: one of the simple least significant bit submission approaches is
Optimum Pixel Adjustment Procedure.

The simple algorithm for OPA explains the procedure of hiding the sample text in an image.

(a) A few least significant bits (LSB) are substituted with in data to be hidden.

(b)The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.

(c)Let n LSBs be substituted in each pixel.

(d)Let d= decimal value of the pixel after the substitution.d1 = decimal value of last n bits of the pixel.d2 = decimal value of n bits hidden in that pixel.

(e)If (d1~d2)<=(2^n)/2then no adjustment is made in that pixel.Else

(f)If(d1<d2)d = d
–

2^n.If(d1>d2)d = d + 2^n.

This "d" is converted to binary and written back to pixel.

VII. MODULE IMPLEMENTATION

VII. A ENCRYPTION

The encryption module of steganography is the primary stage. In this stage, the sender sends the data as well as the image file which act as a carrier image to transfer the data to destination. Bit map (.bmp) image is used as carriers because bmp images are highly resistant for Steganalysis compared to jpeg images. In the encryption module, the text message will be embedded into the image file. The embedding will be done based on the principle of Least Significant Bit(LSB) algorithm.

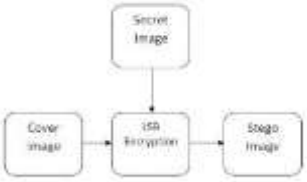

Fig 7.1 Encryption Algorithm

The LSB algorithm uses the least significant bits of each pixel and replace with the significant bits of the text document, such that the message will be encrypted into the image.This process makes the picture not to lose its resolution.

VII. B DATA TRANSMISSION

The encrypted data is send to the receiver or authorized person with the help of transmission media for example through web or Email. The image in which the data is embedded acts as a carrier file such that the data can be transmitted easily with high security. Using the Least Significant Bit (LSB) algorithm the message bits can be embedded properly in the place of least significant bits of image, such that the image doesn't lose its resolution. The encrypted image is protected with password such that we can avoid the damages caused due to hackers or unauthorized persons.

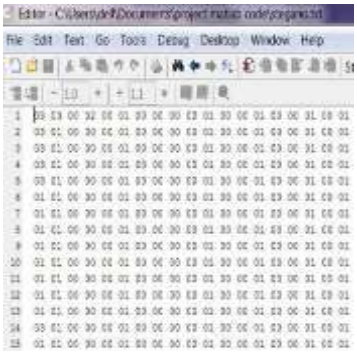

Fig 7.2 Intensity values of

Stegano-image

VII C. DECRYPTION

The receiver receives the carrier image from sender through the transmission medium. The receiver then sends the carrier image to the decryption phase. In the decryption phase, the same Least Significant Algorithm is implemented for decrypting the least significant bits from the image and merge in an order to frame the original message bits. After successful arrangement, the file is decrypted from the carrier file and accessed as an original text document.The data extraction from the image i.e., dec ryption is implemented using Microsoft Visual C#.

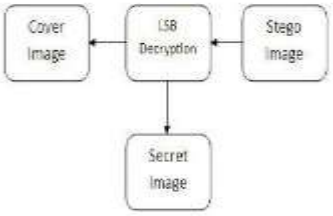

Fig 7.3 Decryption Algorithm

VIII. CONCLUSION

The proposed algorithm thus ensures the transmission of hidden data in the image without the risk of it being attacked by hackers, etc. LSB algorithm provides better security compared to JSteg algorithm with improved data compression and data hiding capacities. The existing method is robust to noise and variety of signal distortion. The watermark embedded into the detail wavelet coefficients of the original image with the use of a key. Doesn't provide security against any modification.

IX. REFERENCES

[1] P.Wayner,Disaapearing Cryptography, 2nd Ed., Elsevier Science: US, 2002

[2] R.J.Anderson and F.A.P.Petitcolas, "On the limits of steganography," IEEE J. of Selected Areas in Communication, vol. 16, no. 4, May 1998.

[3] Al-Shatnawi A.M., "A New Method in Image Steganography with Improved sequential bits", Applied Mathematical Sciences, vol. 6

[4] Muhammad K, Sajjad M, Mehmood I, Rho S, Baik S. A Novel Magic LSB Substitution Method (M-LSB-SM) Using Multi-Level Encryption and Achromatic Component of an Image. Multi Tool App 2015

[5] Karim M. A New Approach for LSB Based Image Steganography Using Secret Key. In: 14t h International Conference on Computer and Information Technology (ICCIT 2011). Dhaka, Bangladesh: 2011.