International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Authentic Data Transmission in Image with Different LSB Methods

Alaknanda Patil, G. Sundari

Abstract: ***A technique to hide undisclosed information from third party as well, the method of investigation to conceal secret data into the cover frame like text, audio, image and video without any change in substantial results to the carrier image is nothing but Steganography. The contemporary safe and taut steganography of image represents an exigent form of transformation of the inserted secrecy for the receiver with getting undetected [1-5]. In Image steganography, image is the carrier and any secret message (audio or text or image) can be transmitted. This algorithm of LSB can be executed in embedding territory where the secret audio data is inserted into the LSB of envelope image for creating the stego image. This paper gives the hiding of audio data as secret data in an image file using LSB with secret key and an improved inverted LSB image Steganography with improved mean square error and peak signal to noise ratio.***

Keyword: LSB, secret key, steganography, stego image, image steganography audio steganography, & video steganography,.

I. INTRODUCTION

Now a day, online transformation of data is increased tremendously with the internet revolution in human life. The certainty and sturdiness of transformation is totally dependent on the channel of wireless exchange methodology. Encryption, watermarking or cryptography are the options to maintain the secrecy of data during transformation, but important data is not fully protected with one step encoding [1]. Because of open channel communication, it is vulnerable to the threats during the transformation of data. Steganography is one of the genuine way-out for the digital fraud [1-5]. Steganography is the proficiency to conceal important data in same or other type of data, which will increase the security. The data to be concealed is called as secret information and it might be of text, image, audio or video. Envelop data used to embed secret data is called as cover or carrier and it might be again text, image, video or audio. The resultant of secret data embedded in a cover file is called as stego-data. Steganography is the more prudent method uptill today to send the secret data over open source network. Steganography is a dominant area of investigation in current scenario. It plays a key role in hiding data [1-5, 14].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Alaknanda Patil*, Sathyabama Institute of Science and Technology, Chennai, Tamilnadu - India
G. Sundari, Sathyabama Institute of Science and Technology, Chennai, Tamilnadu - India

II. STEGANOGRAPHY SYSTEM

In steganography system steps can be involved as follows. There is one cover and message file in which message file can be covered inside of cover file, by using steganography tool one single stego file obtained which can be used for hiding messages. While extracting message the same stego file can be used as output to extract message by using steganography tool, finally message file obtained [1-5,15].

III. STEGANALYSIS

It is the technique to retrieve the secret data from stego message/cover message, exactly opposite to the steganography. It has to detect the cover media by either the pixel color change or change in transform coefficients values [12, 19].

IV. IMAGE ENCODING TECHNIQUES AND METHODS

Masking, filtering & LSB embedding can be used to conceal the information in an image. These types are applied to variety of images, with different degrees of accomplishment. These get suffers to change degrees from functions applied on images such as resolution decrementing or cropping or decrease in the color saturation.

Similarly, image steganography methods are of mainly two types as spatial domain steganography & Frequency domain steganography [1,3,12,16,19].

➢ **LSB encoding -**

LSB is the simple to understand but can be arranged in a complicated method by arranging different combinations in spatial domain technology [10, 17]. The simple LSB method for the image steganography is elaborated here.

- Take 11100110 as a character T. It will require 8 pixels to reserve these eight bits of T.
- Each bit of secret data is then restored to LSB of each Image byte as cover file.
- Example : Embed a secret word DEAD

  Lets assume, D = 01100010, E = 01101111, A = 01101101, D = 01100010
- Bits of cover image before embedding secrecy is,

```
01011010 00101011 10101011 10101010 11101011 11010100 01000111 11111001
01011010 10101101 10010111 10101111 10101011 10100111 01010110 01011011
10110111 11111011 00101011 10010101 10101000 01010100 10101010 11010101
10100100 01011000 11011010 01010101 01001001 10110000 01000010 01010100
```

❖ Bits of cover image after embedding secrecy is,

```
01011010 00101011 10101011 10101010 11101010 11010100 01000111 11111000
01011010 10101101 10010111 10101110 10101011 10100111 01010111 01011011
10110110 11111011 00101011 10010100 10101001 01010101 10101010 11010101
10100100 01011001 11011011 01010100 01001000 10110000 01000011 01010100
```

Original Image

Stego Image

Fig.1 : LSB Implementation

V. AUDIO FILE EMBEDDING AND AUDIO FILE EXTRACTING

In this method color image has been used as a carrier and hidden message is audio data. Audio file used is wave files. Wave files store samples, which will not requier processing. First 44 bytes describes the header. The initial 40-43 bytes gives information about the length of audio data and actual samples of audio occupies the remainder of the file starting from byte 44. Digital image corresponds to either 8 bit or 24 bit. For 8-bit image, each color is represented by a value of 8 bit where as each pixel is denoted by 3 bytes in the 24 bits image. Each byte in cover image represents the magnitude of the primary colors. Those are red, green and blue respectively. The size of secret information to embed is relatively depends upon on the size of carrier image. It will decide the embedding capacity of the system. The cover image size must be larger than secret message size [6-8].

VI. PROPOSED METHODS

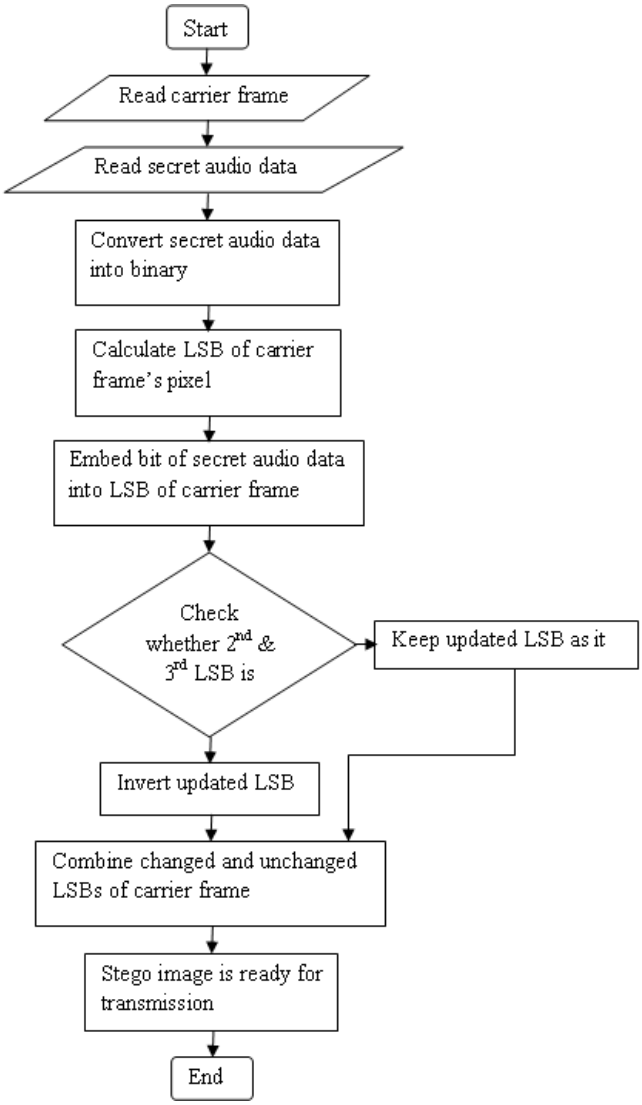
The varieties of methods are available for the image steganography, but the methods are implemented here for the comparative study as – Bit inversion method & Steganography with secret key.

1. BIT INVERSION ALGORITHM

The complexity level can be improved by changing some characteristics in the routine LSB insertion. To understand the method consider four bit data 1100 are to be hidden into 10101000, 10101101, 10001001 and 10101000 pixels of cover image. When LSB-1 repalcement steganography is applied then pixels becomes 1010100**1**, 1010110**1**, 1000100**0** and 1010100**0**. Only one pixel of first place LSB of carrier image is changed. Here we will consider the combination of two bits at the place of second and third LSB of carrier image as 00. The possible combinations are 00, 01, 10 and 11. Examine the stego image for the considered combination and find changed and unchanged LSB. In above example, for combination 00, two pixels are changed. The inversion of those bits has been done for 00 combination at second and third place of LSB. Hence cover image pixels are 1010100**0**,1010110**1**,1000100**1** and 1010100**1.** Only one pixel of stego frame is different from cover frame, so PSNR ratio is improved.

For decryption it is necessary to store pattern for which corresponding LSB bits are inverted. To recover audio data from stego image, analyse first, second and third LSB pattern of stego image. In that second and third are same but first LSB are changed. So for correct decryption, receiver must have original frame of carrier.

❖ **Flow chart of bit inversion method –**



Carrier image prior to steganography

Carrier image subsequent to Bit-Inversion steganography

Fig 2: Carrier image prior and subsequent to Bit Inversion steganography

2. STEGANOGRAPHY WITH SECRET PASSWORD:

The novel image steganography extend a demanding task of sending the concealed information to the receiver with undetectable form. So to provide security secret password is used. First fifty pixels are used to store the size of secret audio message, next fifty pixels are used to store the secret password and next onwards secret message is embedded. While on receiving side secret message size and secret key is extracted. If password matches then only next embedded secret data is extracted [11, 14, 18].

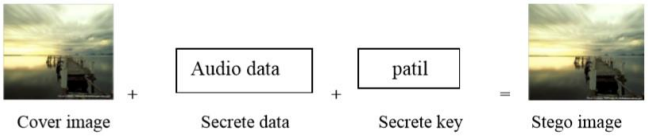


Fig. 3: Stego image with secrete key

VII. RESULTS

Comparative analysis of LSB with secret key and a bit inverted LSB image Steganography has been done on various images and the results are analyzed. If ratio of PSNR is high then better quality images can be retrieved. The audio embedded in the carrier image is by the algorithm "LSB with secret key" and "bit inversion technology with LSB". Two images are taken on which steganography is implemented. Results are as shown in fig 4 & 5. The use of secret key in an image steganography gives better security. In bit inversion techniques, LSB's of some pixels of cover image are inverted for particular pattern of some bits. Due to this minimum quantity of pixels are refined as compare to LSB method, PSNR is increased.

Carrier frame prior to steganography

Carrier frame posterior to bit Inversion steganography

Fig 4: Bit Inversion steganography

Carrier frame prior to steganography

Carrier frame posterior to bit Inversion steganography

Fig 5: LSB with secret key steganography

The LSB of cover image file is embedded with bits of audio file. The recovered secret data is similar. Only the thing is LSB with key is more vigorous and giving high PSNR rate than LSB with bit inversion. The image used to cover the secret audio can be JPEG, BMP and PNG.

VIII. CONCLUSION

Comparative analysis of LSB with secret key and bit inverted LSB image Steganography has been done on foundation of parameters as MSE and PSNR on variety of images. Images are of best quality, if PSNR ratio is high. LSB using secret key steganography provides good security. In bit inversion techniques, LSB's of some pixels of carrier frame are inverted for particular pattern of some bits. As minimum quantity pixels are modified, the increased PSNR is achieved.

FUTUR WORK

The future work is to conceal the secret audio into the video file using LSB with secret key and bit inverted LSB with real time implementation can be attempted.

REFERENCES

1. A H M Kamal, "Steganography: Securing Message in wireless network", International Journal of Computers & Technology (IJC&T), Volume 4, No. 3, March-April 2013, ISSN 2277-3061, pp. 797-801.
2. Urmila Kumari and Saroj Hiranwal, "Data Hiding in Gray-Scale Images by LSB Method using IWT with Lifting Scheme", International Journal on Recent and Innovation Trends in Computing and Communication (IJR&ITCC), Volume 1, Issue 10, ISSN: 2321-8169, pp. 782 – 792.
3. Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, January 2012, Vol. 62. No. 1, pp. 11-18.
4. C. Vanmathi, S. Prabhu, "A Survey of State of the Art Techniques of Steganography", International Journal of Engineering and Technology (IJET), Feb-Mar 2013, Vol. 5, No. 1.
5. Tara Bansal and Ruchika Lamba, "Steganography Using Various Quantization Techniques: A Review", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCS&SE), Vol. 3, Issue 7, July 2013.
6. M. I. Khalil, "Image Steganography : Hiding short audio message within digital image", JCS&T, October 2011, Vol. 11, No. 2.
7. Jasril, Ismail Marzuki, Faisal Rahmat, "Capacity Enhancement of Messages Concealment in Image and Audio Steganography", International Journal on Smart Sensing and Intelligent System (IJSS&IS), Vol. 6, No. 5, December 2013.
8. Pawar Ashwini, Pawar Bhagyashree, Rajguru Ashwini, Y. R. Nagargoje, M. A. Khan, "Image and Audio Based Secure Encryption and Decryption", International Journal of Advanced Research in Computer and Communication Engineering (IJARC&CE), Vol. 3, Issue 3, March 2014.
9. A. M. F. ElGamal, A. E. Mustafa, M. E. ElAlmi, Ahmed.BD, "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit", Research Journal Specific Education, Mansoura University, April 2011, Issue No. 21.
10. Dr. Emad S. Othman, "Hide and Seek: Embedding Audio into RGB 24-bit Color Image Sporadically Using Linked List Concepts", IOSR Journal of Computer Engineering (IOSRJCE), ISSN: 2278-0661 Volume 4, Issue 1, Sep-Oct. 2012, PP 37-44
11. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Proceeding of 14th International Conference on Computer and Information Technology, 22-24 December 2011, Dhaka, Bangladesh, IEEE.
12. Bin li, Ming Wang, Shunquan Tan, Jiwu Huang, Xiaolong Li, " A Strategy of Clustering Modification Directions In Spatial Image Steganography", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 9, Sep. 2015.
13. Ramandeep Kaur Toor and Ramanjot Kaur, "A steganographic Method Based Upon JPEG and Quantization Table Modification", International Journal of Information Technology and Knowledge Management (IJIT&KM), December 2012, Vol. 6, No. 1, pp.19-21.
14. Kuo-Chen, Chung-Ming Wang and Wu, "Steganography Using Reversible Texture Synthesis", IEEE Transactions on Image Processing, January 2015, Vol. 24, No. 1.
15. Hong Cao, Alex C. Kot, "On Establishing Edge Adaptive Grid for Bilevel Image Data Hiding", IEEE Transactions on Information Forensics and Security, September 2013, Vol. 8, No. 9.
16. Bin Li, Shunquan Tan, Jiwu Huang and Ming Wang, "Investigation On Cost Assignment in Spatial Image Steganography", IEEE Transactions on Information Forensics and Security, August 2014, Vol. 9, No. 8.
17. Weixuan Tang, Haodong Li, Jiwu Huang and Weiqi Luo, "Adaptive Steganalysis Based on Embedding Probabilities of Pixels", IEEE Transactions on Information Forensics and Security, April 2016, Vol. 11, No. 4.
18. Wei-Jen Wang, Cheng-Ta Huang, and Shiuh-Jeng Wang, "VQ [/.. Applications in Steganographic Data Hiding Upon Multimedia Images", IEEE Systems Journal, December 2011, Vol. 5, No. 4.
19. Vojtech Holub and Jessica Fridrich, "Random Projections of Residuals for Digital Image Steganalysis", IEEE Transactions on Information Forensics and Security, Dec. 2013, Vol. 8, No. 12.