International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 4, July-Aug-2021, ISSN (Online): 2395-566X

A Comprehensive Review on the Various Steganography Methods Based on Encryption and Data Hiding

Research Scholar Savinder Kaur
Dept. of ECE
Universal Institute of Engineering & Technology,
Lalru, Punjab, India
singhjatinder213@gmail.com

Asst. Prof. Shaveta Bala
Dept. of Electrical Engineering,
Universal Institute of Engineering & Technology,
Lalru, Punjab, India
shavetabala@ugichd.edu.in

***Abstract*- As the technology is advancing day by data and with the same pace information and its secure transmission is also crucial in the process of information transmission. Images are usually the simplest digital data which is used in multiple applications. From satellite to whatsapp applications all around and there are billions of images that are transmitted through digital communication channel. To solve the problem of safest delivery of message to the receiver encryption with the steganography method can be used simultaneously. Various researchers had proposed various ways of hiding data into digital images either by using encryption and steganography and some has combined both these methods to make data more secure. In this review paper a deep literature survey is performed on the steganography of digital images where encryption and data hiding are used for making the data safer.**

***Keywords*- Steganography, encryption, data hiding, image, signal to noise ratio, mean square error.**

I. INTRODUCTION

Steganography is the well known way of saving one message into another digital message so that original message becomes more secure. Now this message can be text, audio, image, video or any other data and this data would be stored in some cover message which can be media also like audio, digital image or digital video.

Steganography has various applications in various fields like defense, medical, satellite, forensic and many more. [1-3]

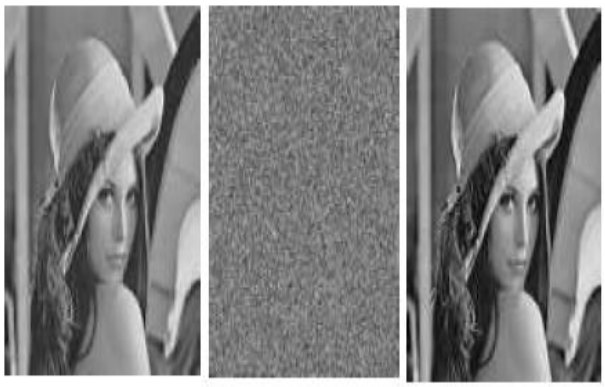

Fig 1. (a, b, c). Input, encrypted and decrypted image of Lena. [7]

Usually data hiding is performed at the sender side. The secret message or data is first encrypted with any of the known encryption algorithms. After that the encrypted message is stored in some digital medium which acts as a cover for that encrypted message.

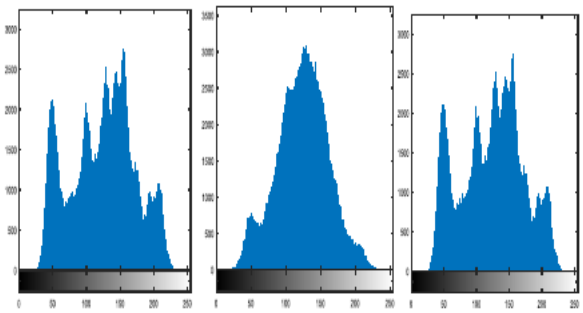

Fig 2. (a, b, c). Histogram of input, encrypted and decrypted image. [7]

Now to recover secret message intruder should know how to decrypt that cover medium which contains actual message. Steganography had a positive edge over cryptography and various researcher are now more concerned towards steganography. [4-8]

II. LITERATURE SURVEY

X. Wu et al. [1] in 2011 proposed a reversible data hiding which was based on the concept of histogram shifting. The proposed method used the core of difference approach of integer wavelet coefficients method. Authors divided the image into various bands and based on these bands a difference integer wavelet was generated amid the two continuous integer wavelet coefficients in each and every sub-band.

There were peak and bottom points in each sub-band and authors used the peak points of each sub-band to save data into integer wavelet coefficients. Authors showed that the

proposed algorithm had high data embedding capacity and also had good peak signal to noise ratio in comparison to other methods.

R. Jose et al. [2] in 2013 proposed a reversible steganography method to hide secret message or data inside the gray scale digital image. There were various phases of the proposed technique. In the first step image was encrypted. In the second step authors performed histogram modification so that data could be stored in the encrypted cover image. Now if the receiver had encrypted key then that could generate image similar to the original image but was not successful to recover the hidden data. Authors used the peak signal to noise ration as an objective parameter for performance evaluation of the proposed method. Author showed that the proposed method had good hiding capacity and good peak signal to noise ratio.

Y. C. Chou et al. [3] in 2014 proposed a reversible data hiding scheme which was based on the two hybrid methodologies ripple strategy and histogram shifting. Authors used the concept of distribution of pixel differencing in the local region of the natural digital image. Prime function of ripple strategy was to subtract the pixels present in the outermost ripple and the pixels present in the adjacent inner ripple. Authors found that at three different locations -1, 0 and at 1the pixel differences were maximum. Authors used three objective parameters namely peak signal to noise ratio, mean square error and embedding capacity. From the experiments it was cleared that the proposed algorithm showed good results in embedding capacity as an objective parameter in comparison to the Huang's and as well as Chang's method.

Y. Yang et al. [4] in 2015 proposed contrast enhancement of medical images which had hidden data inside it. The proposed method could hide the data into smooth region of images with improvement in the visual quality of the stego image. The prime step of the proposed method was the use of histogram shifting method for hiding information into the texture area of image and use of contrast enhancement method for improving the visual quality of image. Authors compared the proposed method with the other reversible data hiding method that also used histogram shifting. Authors used the peak signal to noise ratio as an objective parameter. From the results it was cleared that proposed method performed better in comparison to the other methods.

R. Punidha et al. [5] in 2017 used the concept of integer wavelet transform for sending audio speech signal through steganography technique. Authors used the well known Haar wavelet method with the integer wavelet transform for hiding secret messages. Authors used various objective parameters signal to noise ratio, mean square error, peak signal to noise ratio and structural similarity index metric for performance evaluation of the proposed steganography approach. Authors used the LL band of wavelet to store the data inside the image. Authors also used the Daubechies method along with the Haar for comparison purposes. Algorithm with the Daubechies method performed better in comparison to Haar wavelet method.

M. V. Vardhan et al. [6] in 2017 proposed a reversible steganography technique which was based on the wavelet transform. Authors used the integer wavelet transform method on the encrypted digital images. Authors had performed mapping of integers with the cumulative density functions. Further authors had used on sub-band of the encrypted image to store the secret message inside the cover image. Authors used the concept of histogram shifting for performing the steganography. Authors compared the proposed method with the other known steganography methods like logistic mapping and least significant methods. From the results it was cleared that proposed method outperformed the other methods.

B. Yin et al. [7] in 2017 performed steganography using reversible data hiding. Authors performed steganography in encrypted digital images with the classification permutation. The permutation method used the XOR encryption and then data was embedded into the most significant bit of the encrypted image. With this approach the visual quality of the recovered original image was very good. Authors compared the proposed algorithm with the other known methods of reversible data hiding like Zhang method and as well as with the Wu method. With the results it was showed that the proposed method showed lossless recovery of the original image even when the embedding rate was higher.

V. M. Manikandan et al. [8] in 2019 used the concept of encryption for obtaining the image and message from the stego image using reversible data hiding technique. Authors performed the research on the medical digital images. Authors saved the data of patients into the concerned medical images of same patient and benefit of it was that there was no need of sending patient data into another file. The main aim of proposed method was to get good data embedding capacity and method should have low bit error rate in comparison to other methods. In the encryption mechanism authors used three keys to share data between sender and receiver. From the results it was showed that proposed method had good embedding capacity and took less time of execution.

K. Dhande et al. [9] in 2019 proposed a reversible stegeanography method which was based on encryption mechanism. Main utilization of the proposed algorithm was for the gray scale digital images which could hide the images in the cover image with the help of suitable encryption mechanism. Authors used two keys for performing steganography. One key was used for hiding

the data and another for encrypting the data. Authors used the advance encryption standard method for performing the encryption in the digital images. Authors used least significant method of steganography to get the accuracy and efficiency in the proposed approach.

P. Marella et al. [10] in 2019 utilized the well known least significant method for secring data in the human faces. Authors tried to store the message into the various texture features of the human face lik eye, nose, and mouth. First of all authors tried to find the maximum region available out of various texture features of face. Then authors tried to save secret message in those free space. Authors first used encryption to encrypt the message which had to be hidden in the image. From the results it was showed that the proposed algorithm could store the data in the facial features of human face and it was not easy to detect the presence of some hidden data inside the digitally encrypted image.

A. G. Benedict et al. [11] in 2019 enhanced the file security with the help of multiple image steganography. In this paper authors proposed a way to store various images inside a single cover digital image. Authors used the image sequential hashing concept in which it was difficult for intruder to judge that whether the given pixel belongs to given image or other image. Authors used ZIP file format to compress the file. Authors used file size of image before and after steganography and execution time of algorithm as objective parameters. Authors showed that after performing steganography the size of final stego image was comparable to the original image.

O. Elharrouss et al. [12] in 2020 utilized k-least significant bit of cover image to perform steganography. Authors stored one image inside the other cover image. First of all at sending side the most significant bit was selected which could be stored in the cover image and in this way complete secret image was hidden in the cover image. At the decoding side authors used the concept of region detection. Here algorithm searched the various regions where the data of the secret image was hidden. Peak signal to noise ratio was used as an objective parameter. The proposed algorithm outcomes were not up to mark.

A. Y. Rafiqi et al. [13] in 2021 proposed a image steganography technique which was based on used Grey Scale Co-occurrence Matrix. Authors used the well known principal component analysis to detect edges so that information can be stored into it. Authors performed encryption on text data before hiding it into the cover image. Various objective parameters like peak signal to noise ratio, mean square error and entropy were used for performance evaluation of proposed algorithm. From the experiments it was cleared that the value of peak signal to noise ratio and mean square error were better in comparison to other methods.

III. CONCLUSIONS

In this paper a review on the various image steganography methods has been done. Various research papers in which encryption of the data and the data hiding methodologies are used have been elaborated in detail. In the future more research papers can be used to evaluate the performance of various steganography methods so that maximum information can be taken from the review of literature.

ACKNOWLEDGMENT

I am very thankful to my supervisor Mrs. Shaveta Bala, Assistant professor at the department of electrical engineering at Universal Institute of Engineering & Technology Lalru, Mohali to help me in this review work.

REFERENCES

[1] Y. Rafiqi and A. Singh, “Features Analysis and Extraction Techniques for the Image Steganography”, Turkish Journal of Computer and Mathematics Education, Vol. 12, No.8, pp. 2103-2109, 2021.
[2] X. Wu and X. Zheng, “Reversible Data Hiding Based on Histogram Shifting Using Difference Integer Wavelet Coefficients,” International Conference on Business Computing and Global Informatization, pp. 383-386, 2011.
[3] R. Jose and G. Abraham, “A separable reversible data hiding in encrypted image with improved performance,” International Conference on Microelectronics, Communications and Renewable Energy, pp. 1-5, 2013.
[4] Y. C. Chou, H. C. Lee and Y. J. Yu, “A Novel Reversible Data Hiding Scheme Using Ripple Strategy and Histogram Shifting,” Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 138-141, 2014.
[5] Y. Yang, W. Zhang and N. Yu, “Improving Visual Quality of Reversible Data Hiding in Medical Image with Texture Area Contrast Enhancement,” International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 81-84, 2015.
[6] R. Punidha, and M. Sivaram, “Integer Wavelet Transform Based Approach for High Robustness of Audio Signal Transmission,” International Journal of Pure and Applied Mathematics, Volume 116 No. 23, 295-304, 2017.
[7] M. Vishnu Vardhan, B. Rama Krishna and V. Thanikaiselvan, “IWT Based Data Hiding in Encrypted Images,” Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 614-618, 2018.
[8] Yin, F. Chen, H. He and S. Yan, “Separable Reversible Data Hiding in Encrypted Image with Classification Permutation,” IEEE Third International

Conference on Multimedia Big Data (BigMM), pp. 201-204, 2017.
[9] V. M. Manikandan and V. Masilamani, "An Improved Reversible Data Hiding Scheme Through Novel Encryption," Conference on Next Generation Computing Applications (NextComp), pp. 1-5, 2019.
[10] K. Dhande and R. Channe, "A Brief Review on Reversible Data Hiding in Encrypted Image," International Conference on Communication and Signal Processing (ICCSP), pp. 0135-0138, 2019.
[11] P. Marella, J. Straub, B. Bernard, "Development of a Facial Feature Based Image Steganography Technology", IEEE International Conference on Computational Science and Computational Intelligence, pp. 675-678, 2019.
[12] A. G. Benedict, "Improved File Security System Using Multiple Image Steganography", IEEE International Conference on Data Science and Communication, pp. 1-5, 2019.
[13] O. Elharrouss, N. Almaadeed, S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)", IEEE, pp. 131-135, 2020.
[14] A. Y. Rafiqi and A. Singh, "Features Analysis and Extraction Techniques for the Image Steganography", Turkish Journal of Computer and Mathematics Education, Vol. 12, No.8, pp. 2103-2109, 2021.