IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Color Image Steganography Approach with Enhancing Security & Data Capacity

Samriti[1], Harshdeep Trehan[2], Dr. Naveen Dhillon[3]

Dept. CSE, RIET, Phagwara[1]

Assistant Professor, Dept. CSE, RIET, Phagwara[2]

Principal, RIET, Phagwara[3]

Abstract: These days, data privacy and secure data communication is one of the main concerns which led to design various techniques to encrypt the data and transmit it in a secure way. Steganography is the mechanism in which the secret message is transferred by hiding it in a covered file such as any media i.e., image, video, audio, etc. Various researches have been made in order to transmit the data in a secure way. Recently, to this end, the 2-1-4 LSB technique was used with RSA and SVD for color image. This approach was proved to be better, but after performing a literature survey, some pitfalls of this technique are observed. Thus, in this paper, a novel technique is proposed to perform secure steganography. In the projected approach, two novel techniques- Huffman Encoding and enhanced fuzzy controlled edge detection are introduced to encrypt the input data and extract hiding location respectively. Simulation is performed using MATLAB tool. Peak-to Signal Ratio, Mean-Square Error and embedding time are three parameters that are used to determine the performance of the proposed system. Comparative analysis of projected and existing techniques is performed which ensured the efficacy of the novel approach.

Keywords: Steganography, Advanced fuzzy edge detection technique, Huffman Encoding, PSNR, MSE, embedding time.

I. INTRODUCTION

Internet services are the mode of communication nowadays. From source to destination, data propagates via several gateways in between. So, data security becomes an important factor in communication. This keeps the data safe and confidential from the illegal hackers or users. If the security measures are not used for data encryption then it becomes easy for the hackers to access the data and make changes in it, which results in the wrong information. Information security has become one of the main areas of research in the up-gradation of the services and enhancing the data transfer speed [1]. With the rapid development in the digital technology of communication, computers have gained more power and various issues like storage, etc. have further increased the challenges in the assurance of the security to individuals' data. The amount of security and suitable privacy facility depends on user to user.

Researchers have evaluated and designed various techniques for the protection of the privacy of the user. Encryption is one of the measures which can be taken in order to ensure privacy and after this other one is steganography. Encryption itself is the reason for the noise and it can be seen easily while steganography can't be detected [2]. Steganography and cryptography are quite appropriate methods of the transmission of online messages using a secured path.

Steganography is the process of transmitting the message secretly by hiding it in any digital media such as text, image, audio or video. In this technique, the message is transmitted in such a way that the intruder does not suspect the presence of the message. Steganography is the word taken from the Greek words named as "Steganos" and "Graphie" in which "Steganos" means hidden and Graphie means "to communicate". Thus, it refers to the hidden or covered data [3]. The basics or the blocks of steganography are shown in figure 1.

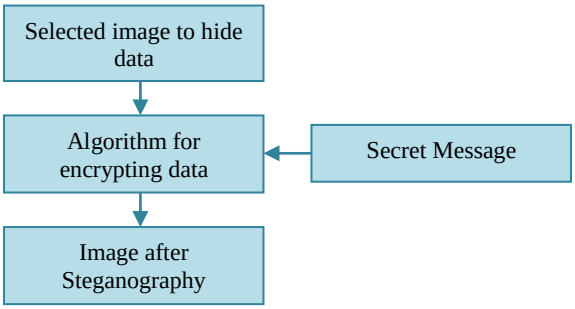

Figure 1: Building block of Steganography

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

Communication among the individuals without any fear of deformation of the message is the main theme in the process of the Steganography. It is used in a few areas of intelligence operations, military and bureaus due to its benefits. There was a great demand for the system which could hide their information and no intruder can evaluate the information meaning. Attacker's concentration avoidance is the major task for the Steganography [4]. Because in case the observer finds that there is some information in the message then he may try to find the data by trying each and every possible concept for reading the messages.
Thus, the security of the data is one of the major concerns.
For this, various Steganography techniques have been proposed earlier such as LSB, Phase Coding, Spread Spectrum, Parity Coding, and Echo Hiding. Some of the proposed approaches are discussed in the next section:

II. LITERATURE REVIEW

Numbers of algorithms have been proposed in the past for making the system that could be used for securing the systems while information exchange.
In the proposed scheme [5], hash capability was used for designing the system in order to hide the information bits into the LSB for the RGB pixel approximation for the image used for covering.
In paper [6], the author introduced the Cyclic Steganographic Technique (CST) depending on the LSB for RGB pictures. The proposed technique hides the secret information in the LSBs of spread image pixels in a randomized cyclic way.
A novel picture steganography strategy dependent on the most noteworthy bits (MSB) of picture pixels was proposed in paper [7]. Bit No. 5 was utilized to store the private bits dependent on the distinction of bit No. 5 and 6 of the big image.
The author in paper [8] had focused on the enhancement of data security with the help of dual steganography in which, firstly the secret message was integrated with the medium of cover. After that, the output stego-object was again embedded in another cover medium.
In the proposed paper [9], the message picture was compacted by utilizing the SPIHT strategy for lossless pressure and afterward it was encoded into the next picture.
The author in the paper [10] has shown the image steganography scheme in which the image was divided into the 2×2 sized pixels which don't overlap. At the initial time, the upper-left pixel of the block was used for embedding the bits of the private bitstream. After that, the changed version of the PVD or pixel-value differencing scheme was taken for integrating the residual pixels from a similar block.
The author of the paper [11] suggested a data hiding algorithm using the DWT and Arnold transform. In this scheme, the private data was twisted with the help of Arnold Transformation in order to make the data secure. DWT was used for getting the wavelet sub-bands for the cover image.
In paper [12], the author evaluated two Steganography calculations - Least Significant Bit and (LSBMR)- based methodology. This paper has taken advanced pictures as spreads and checks a versatile and secure information concealing plan in the spatial space.
The paper [13] suggested a safe image steganography based scheme which was based on the key coordination between the SKA-LSB strategy and staggered cryptography.
The author of the paper [14] suggested a new channel-based payload partition technique depending on the channel amplification changing estimations. This was done for adaptively assigning the capacity in RGB channels parallelly.
Authors designed a novel approach to carry transmission via a safe medium in paper [15]. RSA was utilized for maintaining data security by applying different encryption and decryption mechanisms. In this approach, the author inserted LSB stego image and secret image together with the help of SVD.

III. PRESENT WORK

On the basis of the literature review, it is founded that the technique that was widely used for the purpose of image Steganography was LSB (Least Significant Bit). The main problem in the traditional method is that the canny edge detection approach provides fewer sharp edges due to which we can send less data. So, there is a need to replace the old technique with the new one so that new technique can provide more sharp edges and continuity and more data will be transmitted on more number of sharp edges. Another problem is the size and security of the data. In traditional methods, less data covers large space so data compression technique is needed to compress the data so that more data will be transmitted on low space and security can also be increased by one level with the use of compression technique.
In order to resolve the issues of the existing technique, a new method i.e. fuzzy edge detection technique based on membership decision modeling is combined with the LSB technique. The image steganographic algorithms are presented for embedding secret messages in images. In the proposed technique, the security is the major concern that is why for this, the data is to be embedded. The image will be encoded, for the encoding of the message the huffman

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

approach will be used that will increase the data security in the image processing and also the edge detection approach that is enhanced by using fuzzy logic will give thick edges that will help in embedding more data in the image.
The steps describing the workflow of the proposed work are shown in figure 2.

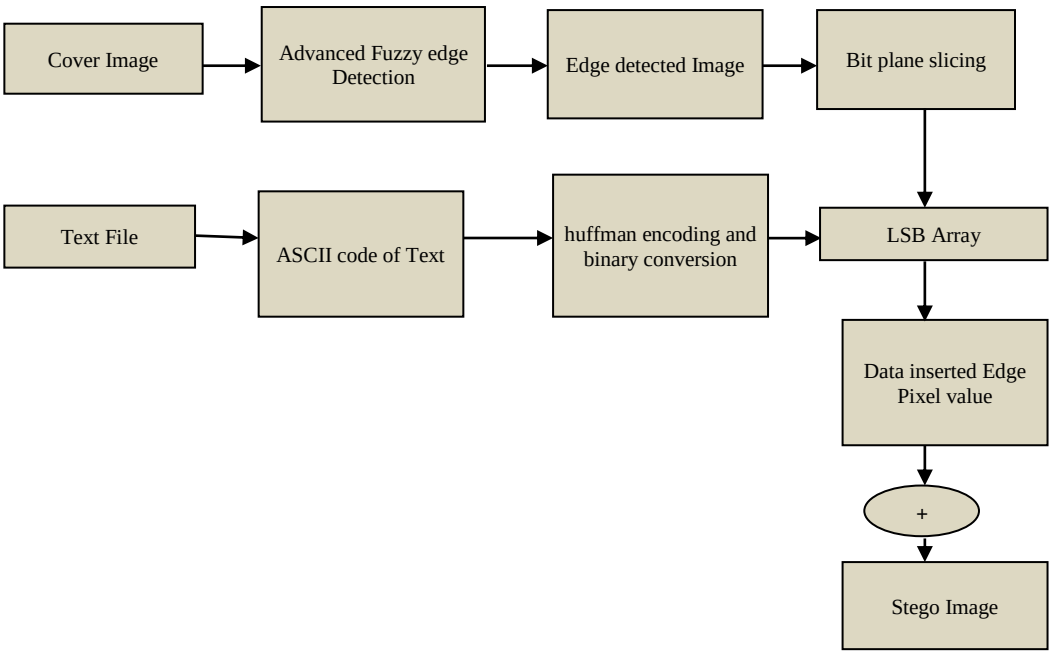

Figure 2: Block Diagram of proposed work

IV. RESULTS AND DISCUSSIONS

The proposed technique has been implemented and in this section, the results are discussed along with the comparative analysis. The novel technique of steganography is introduced in which different parameters are taken for its evaluation which includes PSNR, MSE, and Embedding Time.

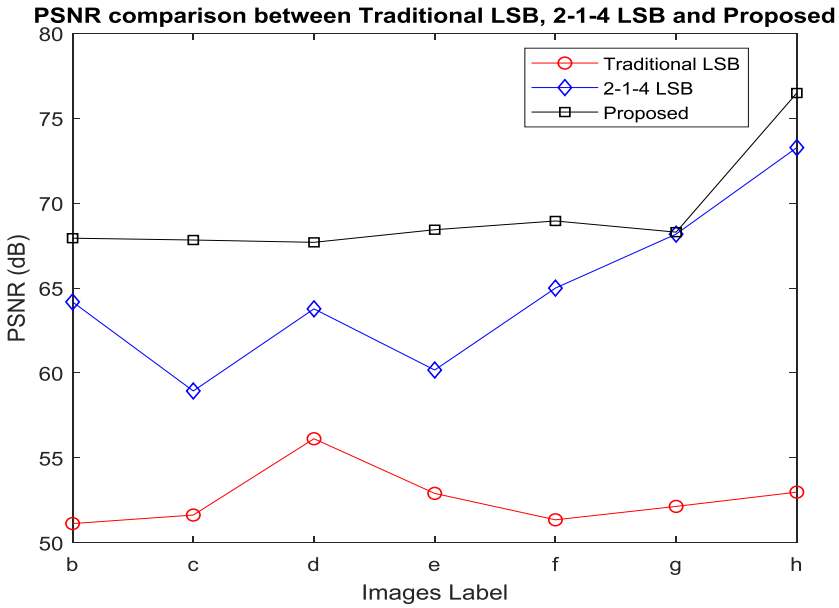

Figure 3: Comparative analysis of PSNR

The graph shown in figure 3 compares the performance of the proposed, traditional LSB and 2-1-4 LSB with respect to PSNR value. It is inferred that the line graph representing the PSNR of the proposed work is higher than both the traditional techniques. High PSNR ensures better efficiency of the system. The corresponding values of the peak-to-signal noise ratio for different image labels are recorded in table 1.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Table 1: Comparative analysis of PSNR with traditional and proposed techniques

PSNR		
Traditional LSB	**2-1-4 LSB**	**Proposed**
51.129	64.182	67.93605631
51.631	58.938	67.82913963
56.125	63.774	67.69238925
52.906	60.172	68.43499337
51.35	64.996	68.95093842
52.14	68.176	68.29148732
52.98	73.271	76.48673566

MSE of the novel approach is compared with the MSE obtained for the conventional technique- 2-1-4 LSB and the obtained results are depicted in figure 4. The graph clearly shows that the proposed technique has minimum MSE which gradually decreased in the entire process. However, for traditional LSB, MSE has very high value. At the beginning of the process, MSE experiences a steep decrease in the value but it dramatically increased.

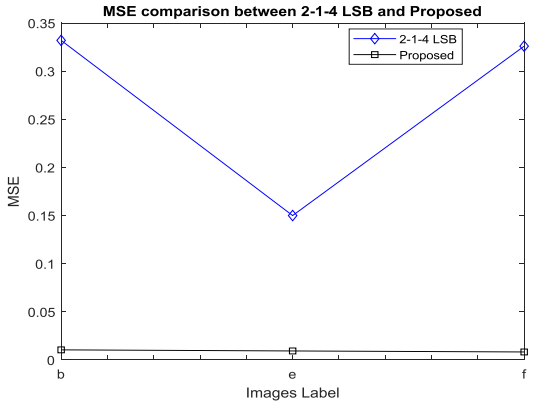

Figure 4: Comparative analysis of MSE

The highest values accounted for proposed and traditional technique is 0.00827916 and 0.326 respectively. Thus, it is proved that the proposed method is better than the existing techniques. Table 2 shows the respective values of both techniques.

Table 2: Comparative analysis of MSE with traditional and proposed techniques

MSE	
2-1-4 LSB	**Proposed**
0.332	0.01045863
0.15	0.00932354
0.326	0.00827916

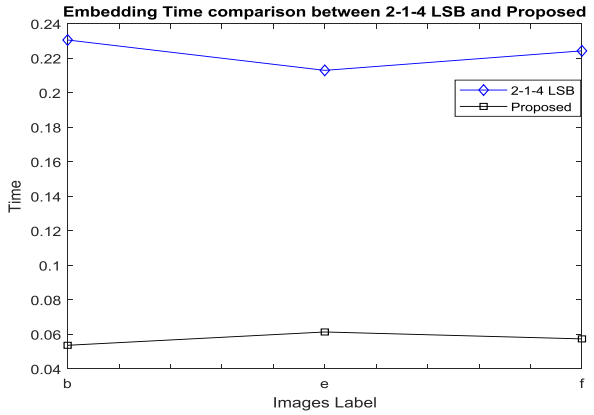

Figure 5: Comparative analysis of Embedding Time

The performance analysis of the proposed work in terms of embedding time is represented in the graph shown in figure 5. There is a huge difference between the embedding time taken by both approaches. Traditional approach takes more embedding time than proposed which ensured that the proposed technique is more effective in terms of embedding time. Table 3 records the different values of time obtained at different image labels.

Table 3: Comparative analysis of Embedding Time with traditional and proposed techniques

Embedding Time	
2-1-4 LSB	**Proposed**
0.2306	0.05369079
0.213	0.0614
0.2243	0.0574

V. CONCLUSION AND FUTURE SCOPE

This paper presents a novel approach of steganography in which two techniques are introduced in the existing technique. The data which is to be transmitted is encoded by applying Huffman encoding technique. Enhanced fuzzy controlled edge detection is applied in order to extract the hidden location in the media. By implementing both the techniques, the novel technique is then evaluated for its performance by considering three parameters i.e. PSNR, MSE and embedding Time. A comparison of traditional and novel techniques is carried out and from the results obtained the efficacy of the novel approach is ensured in terms of considered parameters. MSE for proposed technique is decreased to a great extent which constitutes to 2.5% of MSE of traditional 2-1-4 LSB. Moreover, PSNR is increased by 3.2157 dB and the embedding time is reduced to 74.4 % from the traditional technique.
In the future, more work can be performed to make enhancements in the system. Fuzzy based edge detection can be replaced by novel techniques to obtain sharp edges to extract the locations. Secondly, attacks on the communication could be considered in order to maintain the security of the system and to transmit secret data more efficiently.

REFERENCES

[1] K. Mandal and Debashis Das, “Color Image Steganography Based on Pixel Value Differencing in Spatial Domain” International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, Pp 83-93, 2012
[2] Y. J. Chanu, T. Tuithung and K. Manglem Singh, "A short survey on image steganography and steganalysis techniques," 2012 3rd National Conference on Emerging Trends and Applications in Computer Science, Shillong, 2012, pp. 52-55, IEEE
[3] Mamta juneja, Parvinder Singh Sandhu, “Improve information security using Steganography & Image Segmentation during transmission”, 2010
[4] C.P.Sumathi, T.Santanam and G.Umamaheswari, “A Study of Various Steganographic Techniques Used for Information Hiding”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013
[5] Anil Kumar (2013), “A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, Pp 363-372
[6] Khan Muhammad, Jamil Ahmad, Naeem Ur Rehman, Zahoor Jan, Rashid Jalal Qureshi, A Secure Cyclic Steganographic Technique for Color Images using Randomization, vol. 19, pp. 57-64, 2014.
[7] Ammad Ul Islam et al., “An Improved Image Steganography Technique based on MSB using Bit Differencing”, Proceedings of IEEE 6th International Conference on Innovative Computing Technology, pp. 1478-1485, 2016.
[8] Jigar Makwana and S.G Chudasama, “Dual Steganography: A New Hiding Technique for Digital Communication”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, No. 4, pp. 1346-1354, 2016
[9] M.J. Thenmozhi and T. Menakadevi, “A New Secure Image Steganography Using LSB and SPIHT Based Compression Method”, Proceedings of National Conference on Information Communication, VLSI and Embedded Systems, pp. 843-850, 2016
[10] Mohamed M. Fouad, “Enhancing the imperceptibility of image steganography for information hiding”, Computer Science and Information Systems (FedCSIS), 2017 Federated Conference on, September 2017
[11] Geeta Kasana, Kulbir Singh, and Satvinder Singh Bhatia, “Data Hiding Algorithm for Images Using Discrete Wavelet Transform and Arnold Transform.” Journal of Information Processing Systems, Volume 13, Issue 5, pp. 1331-1344, 2017
[12] Smitha, G. L., and E. Baburaj. “A Survey on Image Steganography Based on Least Significant Bit Matched Revisited (LSBMR) Algorithm.” In 2016 International Conf on Emerging Technological Trends, pp. 1–6. Kollam, India, Publisher IEEE, DOI:10.1109/ICETT.2016.7873746
[13] Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M. (2016). CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimedia Tools and Applications, 76(6), 8597–8626
[14] X. Liao, Y. Yu, B. Li, Z. Li and Z. Qin, "A New Payload Partition Strategy in Color Image Steganography," in IEEE Transactions on Circuits and Systems for Video Technology
[15] S. Yadav, P. Yadav and A. K. Tripathi, "Image steganography on color image using SVD and RSA with 2-1-4-LSB technique," 2017 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), Melmaruvathur, 2017, pp. 164-169.