International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307 (Online), Volume-9 Issue-3, September 2019

Secure Text Hiding Method in Image Processing using Enhanced MSB Technique

Divya Talwar, Dipti Bansal, Mandeep Kaur

Abstract: ***The data hiding is known as a procedure which is used to achieve composite signals by embedding message signals into the host picture. Data hiding approach represents a class of processes which are implemented for embedding data into different formats. In this approach, secret message occurs along with the secret information. The steganography is defined as a process through which information produced from one source can be concealed into other sources. This thesis work presents a novel methodology for image steganography. The tested result demonstrated that the proposed technique shows its supremacy in terms of PSNR and MSE. The PSNR value of proposed approach is increased up to 15 percent in comparison with earlier approach. In comparison with earlier approach, the MSE value of proposed algorithm is decreased up to 10 percent.***

Keywords : MSB, Text Hiding, Steganography, Security

I. INTRODUCTION

This he process which is used to extract valuable information from unprocessed images is called image processing. Several electronic devices are used to collect the images from different locations in daily lives. In image processing, several techniques have been designed. Within the military applications, this kind of application is applied on very large scale and has proven to be very useful. It is feasible to process the optical as well as analog image processing [1]. A common example of this technique is computer graphics that can generate an image very easily. It is possible to enhance and manipulate the images using image processing. Also, computer vision can be used to analyze the images. The collection of sub images particularly known as region-of-interest is known to be one single image. The collection of objects existing in an image is the basic of this region. To operate the image processing in the chosen area, several techniques are designed. In one specific part of the image, improvements are done such that the color rendition can be done or particular part of image can be blurred [2]. The development in computer technology and accessibility of internet services has made the transfer of information from one place to another very easy in the recent times. Though, the preservation of information confidentiality is essential as well. In information protection, the sharing of information across the cover media is a very crucial step. Various techniques have presented for the encoding and decoding of data in order to maintain its secrecy. But, the steganography technique is considered extremely advantageous amid these approaches. This technique in association with the secret information also keeps the secret messages. The image steganography is a process through which data produced from one origin can be concealed in other origins [3]. Edge detection is an essential tool which is used for image segmentation process. The edge detection techniques transform real pictures into edge pictures by modifying grey tones within the image. With the help of image processing, the edge detection procedure deals with localization of imperative differences of a gray level picture. The physical and geometrical features are recognized from the visible objects. The object and edges within the objects are recognized and outlined by this process. Edge detection approach is used widely to detect important variations in intensity values. The local changes are detected within edges in image intensity. The edges are recognized crosswise the edge among two areas. The most important features can be retrieved from the boundaries of a picture. The edge detection is very helpful for picture scrutiny. The least significant bit is converted into a bit of secret message for all bytes occurring within an image. The digital images are found in two different formats i.e. 24 bit images and 8 bit images [4]. The 24 bit images comprise three bits of information in each pixel. One bit is provided for each LSB position of three eight bit values. The modifications in LSB that increases or decreases value cannot alter picture shape. Therefore, the cover picture and the resulted steno picture look alike. The 8 bit images can hide one bit information. This approach provides Encryption and decryption algorithms. The writing data is initiated from last layer due to least significance of this layer. The double importance is given for every upper layer from the layer below [5]. The movement towards higher layer decrease picture quality and transpires picture retouching. The encryption technique conceals information in a picture. Any other user cannot see specifically encrypted file. This module can provide any sort of picture and information. Merely one image file present in the destination is provided here [6]. The universally known Grey Tone Spatial Dependency Matrix is the matrix of an image which comprises identical amount of rows, columns and the number of grey levels.

Revised Manuscript Received on August 25, 2019.
* Correspondence Author
Er. Divya Talwar*, Department of Electronics and Communication Engineering, Punjabi University, Patiala, India. Email: divyatalwar518@yahoo.com
Er. Dipti Bansal, Assistant professor, Department of Electronics and Communication Engineering, Punjabi University, Patiala, India. Email: dipihi@gmail.com
Er. Mandeep Kaur, Assistant Professor, Department of Electronics and Communication Engineering, Punjabi University, Patiala, India. Email:ermandeep0@gmail.com

GLCM is a popular approach which is used to perform image texture analysis. This approach gives knowledge regarding presence of various mixtures of pixel brightness values within the image which is generated in tabular form. This approach extracts statistical surface factors like Inverse Difference Moment, Entropy, Angular Second Moment and Correlation.

This approach is one of the finest statistical techniques in the extraction of textual feature from an image. The second order statistical information is presented for the neighboring pixels within a picture [7]. The GLCM algorithm is measured within the scaled version of an image. The PCA algorithm minimizes the dimensionality of a data suite which comprises large number of interlinked variables. This algorithm ensures the preservation of maximum possible variation within the data set.

II. LITERATURE REVIEW

Pauline Puteaux, et.al (2018) proposed a novel reversible data hiding method that can be applied on the encoded images. To design a new method, the embedding capacity of MSB prediction needs to be maximum [8]. It is very rare to apply MSB instead of LSB in RDHEI. It is known for a fact that in comparison to LSB prediction, performing MSB prediction is easier in original environment. Thus, maximum numbers of MSB values are replaced in encoded image which helps in hiding a large sized message. Further, in the decoding phase, recovering an original image is possible in lossless manner. The outcomes show that the proposed technique provides a good security level and preserves the confidentiality of the content of genuine image.

Yasutoshi Miura, et.al (2018) proposed a new data hiding mechanism through which it is easy to separate the data [9]. In the image data region it is possible to hide additional data in the images. The proposed technique used the omni-directional JPEG images since large amount of embeddable area is available. The embedded omni-directional image on VR space is viewed. To extract the embedded data and play in VR spaces, the HMDs are applied. It was seen that the performance of proposed technique was highly efficient when applied to embed additional images.

Yi Yao, et.al (2018) proposed a novel data embedding method that was based on the residue number system. The proposed method helped in transforming the image cover and secret information into residues [10]. Since the residues represent the lowest levels of continuous-tone image that is very less sensitive to human eyes, the residues are considered as redundancy. The residues are replaced with embedded residual data without the need to add perceptible distortion. To ensure that additional security is performed, a set of modulus is applied. The proposed technique and existing technique are compared against each other and it is seen that the payload and imperceptibility are increased. The cost of cover was minimized to around 90% and imperceptibility was increased up to 4.87 dB. Further, in the presence of damage, the capability of recovering lossless data was increased based on the application of dynamic range adjustment technique.

Junfeng Qu, et.al (2018) proposed a mechanism in which the stego-image was affected due to certain factors. In the presence of black color, the data can be hidden in the best manner as compared to all the other colors [11]. The data can be hidden since the Delta E value of black color is very less. However, the white color cover-image is not able to handle the data in an appropriate manner. One bit encoding is used by the stego-image to hold the least amount of data. The PSNR value is however higher here as compared to 2-bit encoding. Based on Luminance, the performance of black color is the best as compared to other colors. However, white color results in the worst performance as per the human image model indicators. Even when SSIM provides an analysis of quality of images, it is not good to show the different among original and stego-images. The future research can include the study of effects of image context and the study if steganalysis based on the collected data.

Ioan Catalin Dragoi et.al (2018) proposed a new method which aimed to improve the existing approaches [12]. For embedding the information in an encrypted host image, this method uses a previously chosen bitplane that includes randomly generated pixel group. The adaptive process applies multiple predictors for differentiating among original and improved pixels. There are four different predictors applied as per the four different neighbors. The results are achieved after performing simulations. The proposed technique is shown to achieve a higher embedding bit-rate and minimum distortion.

Ki-Hyun Jung, (2018) proposed a new mechanism that applied the pixel-value difference of dual images [13]. The overlapping of two consecutive pixels is done such that high embedding capacity can be provided. Depending upon the conducted experiments and achieved experimental results the proposed approach was considered to be highly robust. Based on these simulations it was seen that around 845,922 bits were embedded and 38.78 dB were maintained by applying proposed technique. The future work of this research could be based on providing reversibility.

III. RESEARCH METHODOLOGY

The objective behind designing the EPE-HCRDH mechanism is to reconstruct the original image in an appropriate manner. It is possible to minimize the amount of payload that is caused due to the storage of error location information. To highlight the prediction errors the to-be-inserted information is used that is based on the error location binary map that is designed when detecting the phase of prediction error. In an encrypted image, the error location information is embedded after encrypting the original image. When performing the data hiding step, only the bits including secret bits are hidden in the available pixels. The location error data is used in the last step to reconstruct an original image by ensuring that no visible alteration occurs.

i. Used predictor: In this method, for every individual pixel, there are two possible predictors achieved which are left pixel and top pixel and they are denoted as $p(i;j-1)$ and $p(i-1;j)$ respectively. Further, this method calculates the absolute difference in relevance to the latest pixel $p(i;j)$. To identify which of the values can be considered as predictor, the nearest value is chosen.

ii. Embed the error location information: To detect the prediction error, the location of prediction error is saved in the error location binary map. Further, the original image *I* is encrypted in the next step.

Before performing embedding step, the encrypted image I_e is responsible to prevent prediction errors. The encrypted image is then divided to generate eight pixels of blocks. Then, in an organized manner, these blocks are scanned. In case when at least one prediction error is found in a block based on the error location binary map, the current block is surrounded by two flags. For every pixel available in the just previous and next blocks, the MSB substitution is performed.

iii. Extracting Data extraction and Recovering Image: The steps performed in the decoding method are:

a For I_{ew} which is a marked-encrypted image, the pixels are scanned initially. Following this, the retrieval and storage of MSB value for each pixel is done. Before the initial sequence of eight MSB is equal to 1, the extracted values are assumed to be bits of embedded message.

b When encountering such sequence, the initiation of error sequence is shown. Until the presence of subsequent sequence, the pixels are not scanned. The subsequent sequence includes eight MSB which are equal to one. Depending upon the condition, the end of error sequence is presented.

c This method is executed in an iterative manner until the image is covered.

Since this method is completely reversible, it is possible to reconstruct the original image I. By decoding the marked encoded image I_{ew}, it is possible to regain the seven LSB of each pixel initially. It is possible to predict the MSB values of pixels.

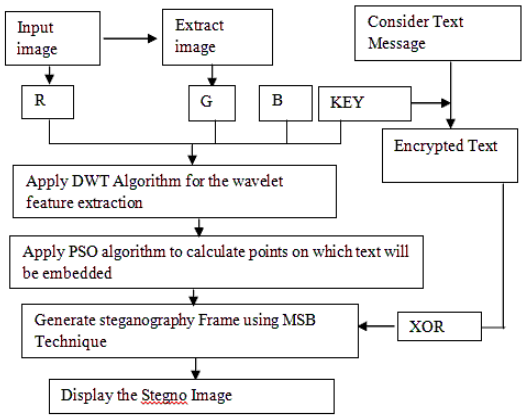

Fig 1: Flowchart for Proposed Research Methodology

IV. EXPERIMENTAL RESULTS

The proposed method is implemented in MATLAB and the results are evaluated by comparing the proposed and existing techniques in terms of performance parameters.

The comparative analysis of proposed and existing techniques in terms of PSNR value is depicted by figure 2. On the stegno image, sharpened image, salt & pepper image and contrast image, the performance of both algorithms is tested. The performance of proposed technique is analyzed in all these scenarios. The results show that with the involvement of GLCM and PCA algorithms, the proposed method performs better in terms of PSNR.

Figure 3 shows the comparative analysis of proposed and existing techniques in terms of MSE value. The stegno image, contrast image, salt & pepper image and sharpened image are utilized for testing the performance of both algorithms. The proposed approach outperforms the existing techniques as per the results.

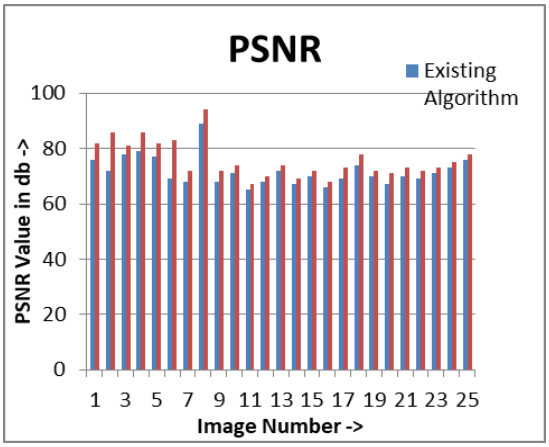

Fig 2: PSNR Comparison

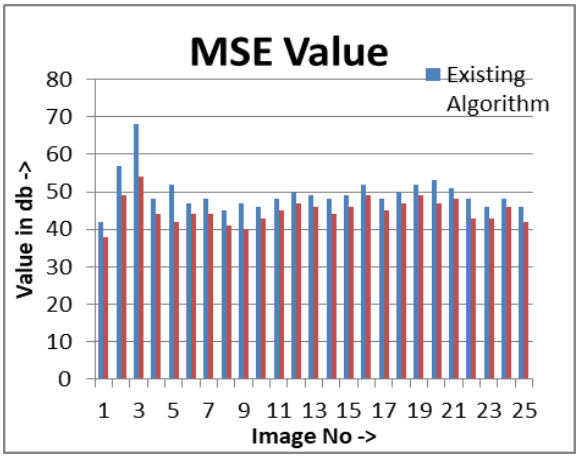

Fig 3: MSE Comparison

V. CONCLUSION

Generating an efficient stegno image through which the security of sensitive data can be improved is the aim of this research. This proposed method is based PCA and GLCM algorithms. The chaos encryption algorithm is applied here to increase the security of stegno image. The MATLAB simulator is used to implement the proposed method and the reliability of proposed approach is examined through its comparison with earlier method. The MSE and PSNR values are calculated to test the performance of proposed algorithm. The outcomes achieved exhibit that in comparison to existing technique the quality encrypted image is better. There is around 10% of increment in the PSNR value when applying proposed algorithm and 15% of reduction in MSE value when applying proposed algorithm.

REFERENCES

1. A. Setyono, D. R. I. M. Setiadi and Muljono, "StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery," in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2017.
2. A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali and M. Naeem, "An Improved Image Steganography Technique based on MSB using Bit Differencing," in International Conference on Innovative Computing Technology (INTECH), Dublin, 2016.
3. E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi and C. A. Sari, "A Performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size," in International Seminar on Application for Technology of Information and Communication (ISemantic), Semarang, 2017.
4. E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto and D. R. I. M. Setiadi, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in International Conference on Innovative and Creative (ICITech), Salatiga, 2017.
5. K. Joshi, P. Dhankhar and R. Yadav, "A New Image Steganography Method in Spatial Domain Using XOR," in Annual IEEE India Conference (INDICON), New Delhi, 2015.
6. P. S. Sapra and H. Mittal, "Secured LSB Modification using Dual Randomness," in International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, 2016.
7. C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption," in International Conference on Informatics and Computational Sciences (ICICoS), Semarang, 2017
8. Pauline Puteaux, and William Puech, “An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images”, 2018, IEEE
9. Yasutoshi Miura, Xuefei LI, Seok Kang, Yuji Sakamoto, “Data hiding technique for omni-directional JPEG images displayed on VR spaces”, 2018, IEEE
10. Yi Yao, Jun Zhou, Bo Yan, Yuqian Li, “RNS-based embedding scheme for data hiding in digital images”, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering
11. Junfeng Qu, Yinglei Song, Yong Wei, Jia Song, “Analysis of Data Hiding with Multi-bit Image Steganography”, 2018, IEEE
12. Ioan Catalin Dragoi and Dinu Coltuc, “Reversible data hiding in encrypted images based on reserving room after encryption and multiple predictors”, 2018, IEEE

AUTHORS PROFILE

Divya Talwar, Done B.tech in Electronics and Communication Engineering, Punjabi University, Patiala. Currently, persuing M.Tech in Electronics and Communication Engineering, Punjabi University, Patiala. Area of interests include Digital Image Processing and Digital Signal Processing.

Dipti Bansal, Done B.tech in “Electronics and Instrumentation”from Punjab Technical University. Done ME in “Electronics product Design and Technology” from PEC, Chandigarh.Currently, working as “Assistant Professor”, Punjabi University, Patiala.

Mandeep kaur, Done B.tech in “Electronics and Communication Engineering” from Punjabi University, Patiala. Done M.tech in “VLSI Design” from Punjabi University, Patiala. Currently, working as “Assistant Professor” in “Electronics and Communication Engineering Department”, Punjabi University, Patiala.