MSB and PSO Algorithm for the Generation of Stegnography Image

Simran Uppal, Harpreet kaur

ABSTRACT---The image processing is the technique which digital information stored in the form of pixels. The image stegnography is the approach which can secure the text information. In the previous research work, MSB technique is applied for the generation of stegno image. To improve security of the stegno image encryption scheme need to be applied over the stegno image. In this work, PSO algorithm is applied for the key of encryption key which encrypts the stegno image. The proposed algorithm is implemented in MATLAB and results are analyzed in terms of PSNR and MSE

Keywords—MSB, PSO, Stegno image.

INTRODUCTION

Image processing is defined as the process in which useful information is extracted raw images received from cameras placed on satellites, space probes and aircrafts by which normal activity of life is captured to use in different applications [1]. There is development in various techniques so far in image processing. This technique has been widely utilized in the field of military and its applications. The processing of the optical [2] and analog image processing is feasible due to the advantages of this technique [3]. Computer graphics is one of the examples of this technique using which images can be created easily. With the help of image processing, images can be manipulated and enhanced and also images can be analyzed using computer vision [4].A single image is the combination of sub images that specifically, called as regions-of-interest [5]. The main basic of this region is the collection of the objects present in an image. There are various techniques in which operation of the image processing can be done for the selected region [6]. The improvement can be done by processing the one part of an image for the color rendition of an image and to suppress the motion blur other part of an image is used. The process through which composite signals are achieved by embedding the message signals into the host or cover of image is known as data hiding [7]. A class of processes which are applied for embedding the data into different forms is represented by data hiding. The host signal is perceived with least amount of degradation which means that for a human viewer, it might not be possible to visualize or hear the embedded data [8]. For performing encryption, data hiding is different from compression even though they have few similarities. Ensuring that the embedded data remains inviolate and recoverable without any restrictions or regulations accessed to the host signals is the major aim of this approach [9]. The data within a host signal must be embedded along with some important features when data hiding techniques are applied. The degradation of host signal must be done in a non-objectionable manner [10]. Also, the perceptibility on the embedded data should be the least. Keeping the data hidden is the major objective of this approach. To ensure that the data remains intact across the various data file formats, it is important to encode the data directly within the media and not in the header or wrapper directly for embedding it [11]. There are several modifications which range from intentional and intelligent tries performed at the time of removal to the predictable manipulations. The immunity of embedded data should be higher for all such modifications [12]. There are two approaches amongst which different data hiding techniques are classified:

a. **Irreversible data hiding technique:** By ensuring that no loss of data occurs, the recovery of message signal is possible through this technique [13]. However, it is possible to lose the original cover in this process.

b. **Reversible data hiding technique:** It is possible to recover the original cover and message signal with zero loss through this technique [14]. VRAE and RRBE are the two reversible data hiding approaches explained below.

- Vacating Room Before the Encryption: Initially, the cipher is applied with encryption key for the encryption of original image in this method [15]. Further, some auxiliary data is hidden within it by forwarding this data to the data hider who ensures that the room needed for data hiding key is provided with no loss [16]. Further, the data hiding key can be used at the receiver by the authorized perform so that the embedded data can be extracted. For vacating the room to adjust the additional data, the encrypted LSBs of image are compressed by this method. The syndromes of a parity check matrix are identified in this method to do so.

Revised Manuscript Received on May15, 2019.

SimranUppal,Researcher Scholar, Chandigarh University, Mohali, India. (simranuppal0071@gmail.com)

Harpreetkaur, Assistant Professor, Chandigarh University, Mohali, India. (harpreet8307@gmail.com)

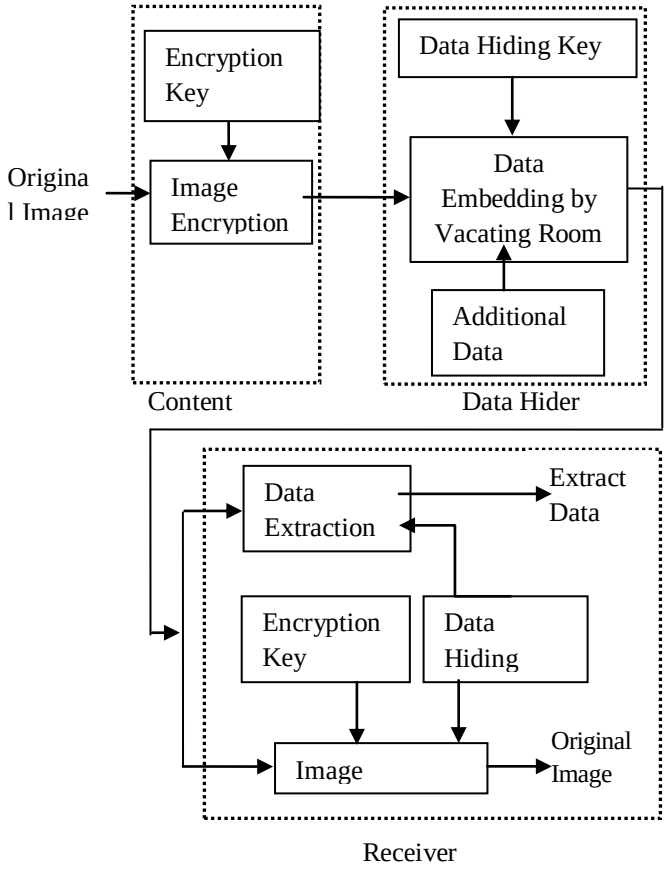

Fig 1: Vacating Room after Encryption (VRAE)

- Reserving room before the encryption:

Before performing encryption on the original process, enough space is provided through this method. Encryption and data hiding are performed consecutively after that [17]. The important steps are explained in the figure below.

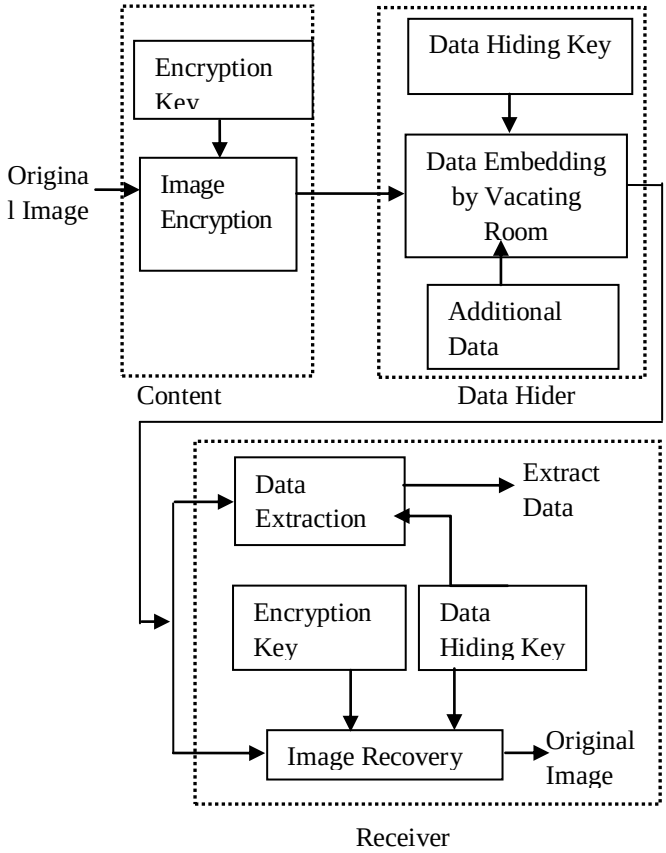

Fig 2: Reserving Room before Encryption (RRBE)

Literature Review

Pauline Puteaux, et.al (2018) proposed a novel reversible data hiding mechanism for encrypted images. The embedding capacity of MSB prediction is the highest due to which it is used to develop this novel mechanism [18]. Here, within RDHEI, MSB is applied instead of LSB which is very rare. Therefore, it is possible to hide a large message by substituting most of the MSB values within the encrypted image. Also, it is possible to recover an original image losslessly within the decoding phase. It is this seen that, a good security level is achieved and the original image content's confidentiality can be preserved by implementing proposed technique.

Yasutoshi Miura, et.al (2018) proposed a novel data hiding approach [19]. To ensure that the data cannot be separated easily, the additional data of images is hidden within the image data region. Due to the presence of huge amount of embeddable area available, omni-directional JPEG images are utilized as cover data by the proposed technique. It is also possible to view the embedded omni-directional image on VR space. The HMDs are utilized for extracting the embedded data and playing within the VR spaces. It is seen that with respect to payload, overhead and PSNR, the performance of proposed technique for embedding additional image into other images is highly efficient.

Yi Yao, et.al (2018) proposed a data embedding approach which is based on residue number system. The image cover and secret information are transformed into residues with the help of this proposed approach [20]. A set of modulus is also applied to provide additional security. It is seen through the comparative analysis that higher imperceptibility and payload are achieved by applying the proposed technique. There is around 90% of reduction in the cost of cover and 4.87 dB of increment in imperceptibility as per the comparative analysis performed against proposed and LSB embedding techniques are compared. Further, depending upon the dynamic range adjustment technique, the capability of recovering lossless data is higher in case of proposed technique when the damage occurs.

JunfengQu, et.al (2018) presented a study related to the manner in which certain factors affect the stego-image. It is seen that in comparison to all the colors, the capability of hiding the data is the best in case of black color [21]. The Delta E value of black color is very less due to which it can hide the data. Black color outperforms all the rest of the colors with respect to Luminance. However, in terms of human visual system indicators, the performance of white is the worst. Showing the different amongst stego-image and original image cannot be represented as good indicator even though the quality of images can be analyzed using SSIM. With respect to the data gathered, the effects of image context and the study of steganalysis can be studied in future.

IoanCatalinDragoi et.al (2018) proposed a novel vacating room for enhancing the previous approaches [22]. A preselected bitplane of randomly generated pixel group is

used to embed the hidden data within the encrypted host image. In order to distinguish amongst original and improved pixels, the multiple predictors are applied within an adaptive procedure. A higher embedding bit-rate is achieved along with less distortion by implementing the proposed technique as per the comparisons made amongst proposed and existing approaches.

Ki-Hyun Jung, (2018) proposed a novel data hiding approach in which the pixel-value difference of dual images is utilized [23]. For availing high embedding capacity, two consecutive pixels are overlapped. The robustness of proposed approach to histogram was shown as per the experimental results achieved by implementing proposed technique. Around 845,922 bits were embedded and 38.78 dB were maintained as per these simulation results. Reversibility could be provided in future to extend this proposed technique.

Research Methodology

Re-constructing the original image in the exact manner is the major objective of EPE-HCRDH approach. Due to the storage of error location information, a small reduction of payload is a possibility in this case. Depending upon the error location binary map which was generated at the phase of prediction error detection, the to-be-inserted information is adapted so that the prediction errors can be highlighted. The encryption of original image is done which is followed by embedding the error location information within the encrypted image. Only the bits that contain secret bits can be hidden in the available pixels during the data hiding step. Without causing any visible alteration it is possible to reconstruct an original image at the end of decoding step using the location error information. Figure 3.1 showed the global scheme used in this approach.

i. Used predictor: The left pixel denoted by $p(i;j-1)$ and top pixel denoted by $p(i-1;j)$ are the two possible predictors for each pixel of this mechanism. The absolute different related to the current pixel $p(i;j)$ is computed and selection of the closest value is done for determining which of these values is known to be the predictor.

ii. Embed the error location information: Within the error location binary map the location of prediction errors is saved at the time of detecting prediction error. Further, the encryption of original image *I*is done. The prediction errors are avoided by the encrypted image I_e before performing the embedding step. Eight pixels of blocks are generated then, by dividing the encrypted image I_e and then they are scanned individually in the arranged manner. Two flags surround the current block by replacing the MSB of each pixel that is present within the just previous and next blocks in case when minimum one prediction error is recognized within a block as per the error location binary map.

iii. Data extraction and image recovery: Following are the steps to be performed at the time of decoding step:

a. In the scan line order, the pixels of marked-encrypted image I_{ew} are scanned and the MSB value for each pixel is extracted and stored. The extracted values are assumed to be the bits of embedded message before the initial sequence of eight MSB equals to 1.
b. A beginning of error sequence is indicated when such a sequence is encountered. The scanning of pixels is not done until the next sequence in which eight MSB are equal to one as there is no marking of next pixels at the time of data hiding. The end of error sequence is indicated as per this condition.
c. Till the image ends, this process continues in an iterative manner.

It is possible to reconstruct the original image I since this method is fully reversible. Initially, the seven LSB of every pixel are recovered by decrypting the marked encrypted image I_{ew}. Further, the prediction of MSB values of the pixels is done.

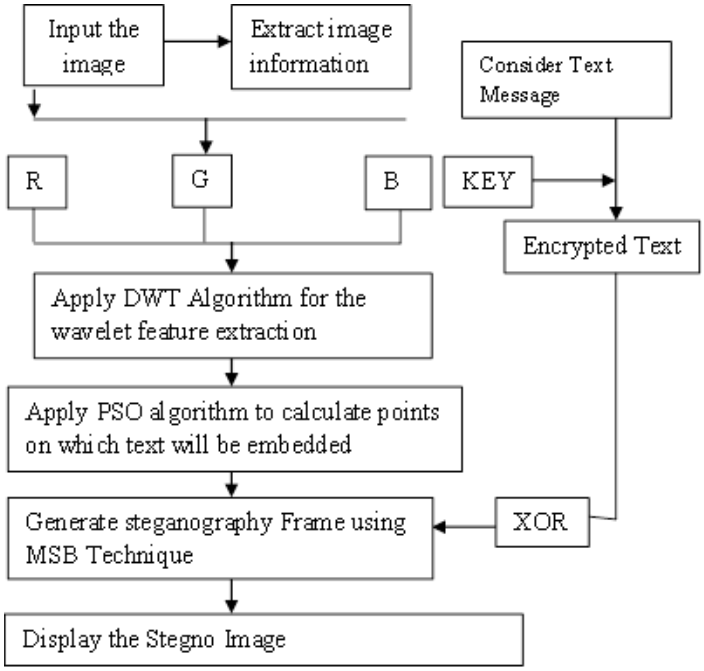

Fig 3: Proposed Flowchart

Result and Discussion

The proposed model is based on the secure stegno image generation to hide sensitive text information. The proposed model use the DWT algorithm for the feature extraction and PSO algorithm to simplify the features. The simplified features are applied for the key generation which can encrypt the stegno image which is generated with the MSB technique. The performance of proposed algorithm is analyzed in terms of PSNR and MSE

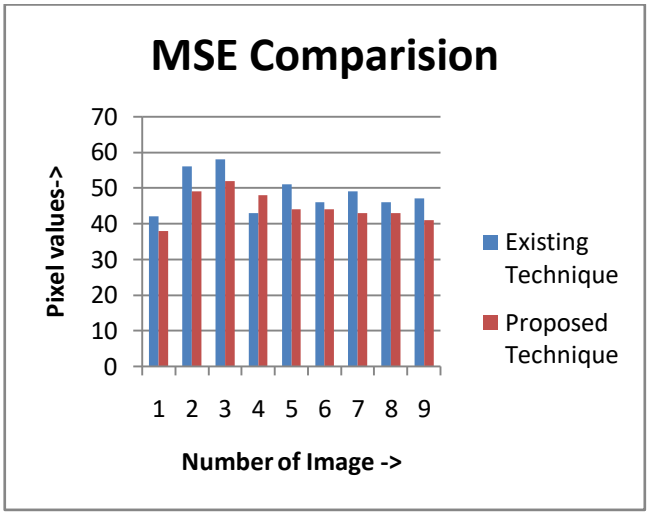

Fig 4: MSE Comparison

As shown in figure 4,the MSE value of the proposed and existing algorithm is compared for the performance analysis. Due to increase in security of the proposed algorithm MSE value is reduced as compared existing algorithm

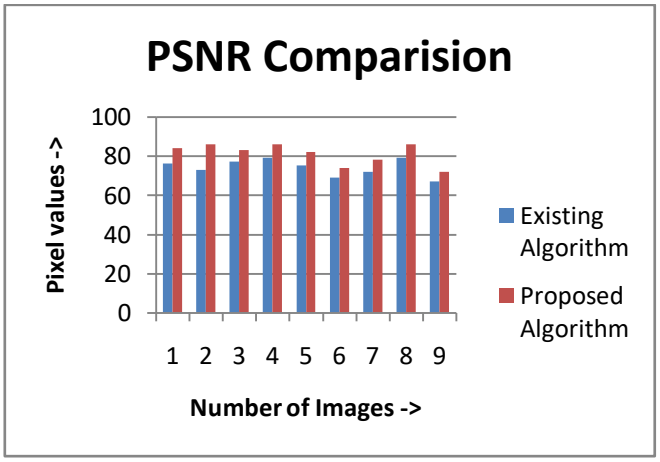

Fig 5: PSNR Comparison

As shown in figure 5, the PSNR value of the proposed and existing algorithm is compared for the performance analysis. The proposed algorithm has high PSNR value as compared to existing algorithm

CONCLUSION

In this work, it is concluded that image stegnography is the technique which can increase security of the sensitive text information. The MSB is the improved version of LSB technique which generate secure stegno image. The technique of PSO algorithm is applied in the key generation which can encrypt the stegno image. The proposed algorithm is implemented in MATLAB and results are analyzed in PSNR, MSE. The proposed algorithm has high PSNR value and low MSE value as compared to existing algorithm.

REFERENCES

1. K. E. Prager and P. F. Singer, ―Image enhancement and filtering using wavelet‖, Conf. Rec. Asilomar Conf. on Sig., Sys. & Computers, vol. 1, pp. 169–174, November 1991
2. Sachin D Ruikar and Dharmpal D Doye, ―Wavelet Based Image Denoising Technique‖, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.
3. F. Admiraal-Behloul, D. M. J. Van Den Heuvel, H. Olofsen, M. J. P. Van Osch, J. Van Der Grond, M. A. Van Buchem, and J. H. C. Reiber, "Fully automatic segmentation of white matter hyperintensities in MR images of the elderly," Neuroimage, vol. 28, no. 3, pp. 607–617, 2005.
4. Kede Ma. Weiming Zhang, Xianfeng Zhao, NenghaiYu,Fenghua Li, "Reversible Data Hiding in Images by Reserving Room Before Encryption", IEEE Trans on Information Forensics and security, Vol. 8, No. 3, March 2013
5. Jun Tian, "Reversible Data Embedding Using a difference Expansion", IEEE Transaction , Vol.13, No. 8, Aug 2003
6. Jose, R.; Abraham, G, "A separable reversible data hiding in encrypted im age with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy(AICERA/ICMiCR), 2013 Annual International Conference l'IEEE 2013.
7. MoniNaor, Adi Shamir," Visual Cryptography", in Proc. EUROCRYPT'94, Berlin, Germany, 1995, vol. 950, pp. 1-12,Springer-Verlag, LNCS [8] Siddharth Malik, Anjali Sardana, Jaya, "A Keyless Approach to Image Encryption", 2012 international conference on Communication systems and Network Technologies l'2012 IEEE
8. Yan Chen, Delu Huang, Guangyao Ma, Jianjun Wang, "Gradient-based Directional Predictor for Reversible Data Hiding", 2018, IEEE
9. Vishnu Vardhan M, Rama Krishna B, Thanikaiselvan V, "IWT Based Data Hiding in Encrypted Images", Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018)
10. Yi-Chun Weng, Wen-Chung Kuo, Chun-Cheng Wang, Yu-Chih Huang, "Novel New Idea of Data Hiding Using GEMD Technique", Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE
11. Yuqing Li, Zebiao Guan, Chi Xu, "Digital Image Self Restoration Based on Information Hiding", Proceedings of the 37th Chinese Control Conference, 2018
12. Ahmed A. Abd El-Latif, BassemAbd-El-Atty, M. ShamimHossain, Md. AbdurRahman, AtifAlamri, B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing", 2018, IEEE
13. Suah Kim, Rolf Lussi, XiaochaoQu, Fangjun Huang, HyoungJoong Kim, "Reversible Data Hiding with Automatic Brightness Preserving Contrast Enhancement", 2018, IEEE
14. Shih-ChiehShie, Ji-Han Jiang, Yi-Jen Su, Wei-Yan Chang, "An Improved Steganographic Scheme Implemented on the Compression Domain of Image Using BTC and Histogram Modification", 2018 32nd International Conference on Advanced Information Networking and Applications Workshops
15. Yanxiao Liu, Chingnung Yang, and Qindong Sun, "Enhance Embedding Capacity of Generalized Exploiting Modification Directions in Data Hiding", 2017, IEEE
16. DongdongHou, Weiming Zhang, Yang Yang and Nenghai Yu, "Reversible Data Hiding under Inconsistent Distortion Metrics", 2018, IEEE
17. ZhenxingQian, HaishengXu, XiangyangLuo, Xinpeng Zhang, "New Framework of Reversible Data Hiding in Encrypted JPEG Bitstreams", 2018, IEEE
18. Pauline Puteaux, and William Puech, "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images", 2018, IEEE

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

19. Yasutoshi Miura, Xuefei LI, Seok Kang, Yuji Sakamoto, "Data hiding technique for omni-directional JPEG images displayed on VR spaces", 2018, IEEE
20. 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
21. JunfengQu, Yinglei Song, Yong Wei, Jia Song, "Analysis of Data Hiding with Multi-bit Image Steganography", 2018, IEEE
22. IoanCatalinDragoi and DinuColtuc, "REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BASED ON RESERVING ROOM AFTER ENCRYPTION AND MULTIPLE PREDICTORS", 2018, IEEE
23. Ki-Hyun Jung, "Data Hiding Scheme Based on Pixel-Value Differencing in Dual Images", 2018 International Conference on Electronics, Information, and Communication (ICEIC)