Secure Image of Reversible Data Hiding Algorithms for Image Reconstruction

Somya Jain, Prof. Rahul Sahu

• *Somya Jain is currently pursuing master's degree program in Computer science and engineering, LNCT College, India*

• *Prof. Rahul Sahu is currently Assistant Professor in Computer science and engineering dept. in LNCT College, India*

Abstract: - As of now, with the quick advancement of data innovation more information and pictures are accessible on the web. So there is a need to give some sort of verification to such critical information. At the point when the sender communicates the picture/information to the recipient, there might be gatecrashers present in the middle of who may catch the picture/information. In the wake of catching the picture, the interloper may see the significant substance in the picture. It may not be the issue now and again. Be that as it may, in the event that we consider the territories like clinical or military, the entrance of such pictures or information is unsatisfactory. In this paper the concentrated of Data Hiding procedure where the mystery information is installed in to the spread medium with the end goal that lone the sender and beneficiary can get to the shrouded information. The information concealing procedure can be utilized for an expansive scope of uses, as for giving copyright security to the movies, recordings, and so forth The information concealing method is safer and interlopers can't change the substance covered up inside the spread medium, despite the fact that if any adjustment is performed by gatecrasher it will be known by the sender and collector.

Keywords: - Reversible Data, Image Reconstruction, Secure Image

I. INTRODUCTION

Reversible data hiding (RDH) is one of the important and successful applications of Steganography. It is the branch which deals with covert communication. The word steganography is derived from the Greek word stegnos means covered or concealed and graphine means writing [1].

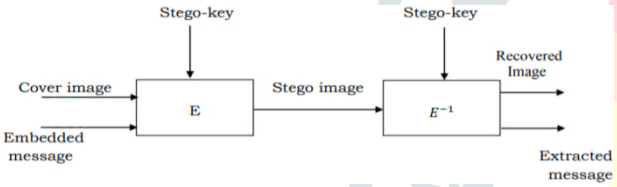

Fig 1: Steganography Model

Not at all like steganography in reversible information concealing mystery messages are inserted into a spread picture by marginally changing its pixel esteems and concentrate the messages at the recipient end with reversibility [2, 3]. The model for steganography is appeared in Fig 1.

The primary standard of information concealing lies in two different ways: one is inserting and the other one is extricating measure. In the principal case i.e., implanting stage secretive data is embedded into spread medium. By doing as such there will be alteration in the spread medium. This embedded secretive data after changed to the spread medium is called as stamped/stego information. In the optional stage i.e., extraction stage the clandestine data is extricated from the checked/stego information and recoups the spread medium. The overall information concealing framework is appeared in Fig 2.

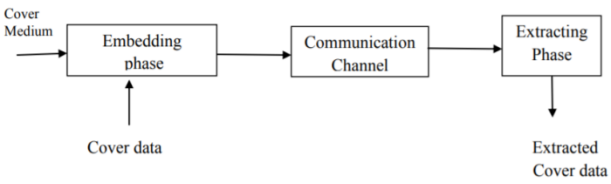

Fig 2: General Data Hiding system

Irreversible Data Hiding:- It is the process of embedding covert data into the cover medium while at the extraction phase only the covert data is extracted but there is a loss in cover medium i.e. from stego medium, input cover medium cannot completely recovered at the receiver end [4].

Reversible Data Hiding:- It is the process of embedding secret data into the cover medium with extraction of the secret data from the cover medium without any loss in the cover medium at the receiver end. As there is loss in cover medium in irreversible data hiding researchers have contributed their work in the field of reversible data hiding and it been challenging area for many researchers to provide solutions [5].

II. LITERATURE REVIEW

In 2002, Chang CC et al. [1] built up an information concealing utilizing ideal LSB replacement and Genetic Algorithm (GA) techniques. The outcomes show that the PSNR for GA is 44.53 dB when contrasted and basic LSB replacement for Lena picture with normal computational season of 0.58 sec which is high contrasted with straightforward LSB replacement strategy.

Wang et al. [2] proposed a strategy for inserting information by encoding the mystery text utilizing Data Encryption Standard (DES) calculation and improved the presentation as far as security and low computational time contrasted with wang et al. strategy.

Zhang J. et al. [3] introduced information concealing utilizing modulus activity. The outcomes show that modulus based information covering up performs well regarding picture quality than straightforward LSB and GA-improved LSB techniques. It is proposed straightforward LSB replacement based information concealing utilizing Optimal Pixel Adjustment Process (OPAP) and improved the picture quality regarding PSNR 51.15 dB for k=1 with low computational unpredictability.

Hong W et al. [4] actualized Inverted Pattern (IP) based information concealing utilizing LSB replacement for various example lengths going from 64 to 2048 pieces with improved picture quality. The proposed steganographic strategies by assessing contrast of the comparing four-pixels and inserting information by changing LSB replacement. The test results exhibit that the normal limit of 8, 25,782 pieces with PSNR 39.11 dB for all the spread pictures.

Sharmila et al. [5] made change to Xin Liao et al. strategy by considering distinction of nine pixel rather than four pixels and partitioned into four gatherings as low level, low-high, high-low and elevated level for installing information with change in 2 LSB bit positions for low level and 3, 4 and 5bits for different levels. The outcomes show that there is an improvement in normal limit of 1,87,069 pieces with normal PSNR of 0.74 dB contrasted with other condition of-workmanship techniques.

Muhammand et al. [6] executed twofold layered implanting plan utilizing wet paper coding component for determination of pixel expansion or deduction with high installing proficiency with low inserting rates. Chan and the introduced a review on data concealing plans for computerized pictures. This review is comprehensively characterized into three classes: Steganography, Image watermarking and verification with their benefits and negative marks.

Tsai YY et al. [7] proposed a novel technique for implanting information into the grayscale spread pictures utilizing base-5 numeral framework by installing 524288 mystery bits into pixel front of 512 X 512 with inserting pace of 2bpp. It executed information installing utilizing pixel division methodology by perpetual the Most Significant Bits (MSB) and modifying Least Significant Bits (LSB) in the spread picture and improved the implanting mystery bits more than 1.7 occasions contrasted with the EMD technique with normal Peak Signal-to-Noise Ratio (PSNR) of 44.3 dB.

Peng et al. [8] proposed a capacity for LSB Matching dependent on Mielikainen by connecting all the pixels in the spread picture as a grouping with the end goal that solitary three pixels are altered to implant mystery bits and expanded the installing proficiency with increment in bit length. It actualized a Generalized LSB Matching (G-LSB-M) in which installing measure is varied by 1 in each spread pixel by diminishing the Expected Number of Modification Per Pixel (ENMPP) from 0.5 to 0.375.

Jung et al. [9] proposed an improved EMD technique utilizing modulus activity which could install information in (2n+1)- ary framework for every pixel in the spread picture and insert information up to 91,129 bytes with normal PSNR of 47.95 dB. The planned a Human Visual Masking Model in spatial space and afterward utilized the model for versatile LSB replacement by installing mystery information in to the clamor non-touchy territories and accomplished PSNR more noteworthy than 39dB with implanting limit up to 7,86,014 pieces for bits position r = 4.

Avci et al. [10] proposed a steganographic conspire utilizing 5-ary framework for inserting information into (2k+1) spread pixels and accomplished a PSNR more prominent than 45 dB with implanting limit of 1.99bpp (bits per pixel). The proposed a novel information concealing technique utilizing modulus work by installing information in both dark scale and shading pictures. The normal PSNR of 51.15dB has been accomplished when the implanting rate is 1 bpp for dark scale pictures.

Q. Wang et al. [11] extended LSB Matching Revisited (LSBMR) and proposed an edge versatile strategy for choosing inserting districts as indicated by the edge of the size of the mystery message and acquired an exactness of 50.21,50.60, 50.45, 50.66,51.12 at 10 , 20, 30, 40 and half installing rates.

B. Zhao et al. [12] introduced an identification of concealed information in spatial area utilizing Subtractive Pixel Adjacency Matrix (SPAM) for processing highlights for steganalysis and accomplished negligible normal choice mistake of 0.057, 0.055, 0.009 and 0.167 at 0.25bpp for various information bases of CAMERA, BOWS2, JPEG85, NRCS. The introduced an inserting plan dependent on nearby intricacy and Human Vision Sensitivity (HVS) by taking two diverse limit esteems and got a PSNR of 40.78 dB with installing limit of 7,83,889 pieces for a square of 4x4 size for Baboon picture with th1=0 and th2=3.1. Ordinary Singular (RS) steganalysis has been performed for all the stego pictures and neglected to recognize the concealed messages inside the stego pictures.

Subramanyam et al. [13] introduced an overview on picture steganography and steganalysis. In steganography the primary center was in LSB, Bit-Plane Complexity Segmentation (BPCS), commotion including based, expectation mistake, modulo activity, quantization based. In this survey two elements were examined: first how to adaptively choose the implanting areas and later diminishing the twisting and expanding productivity.

T. bianchi et al. [14] proposed a concealing plan by misusing adjustment in eight ways and accomplished a subtlety of 52.39, 46.75, 40.83, 34.83, and 31.70 dB for implanting paces of 1, 2, 3, 4 and 4.5bpp.

III. REVERSIBLE DATA HIDING METHOD

Data can be embedded into images in two ways: one is Creating Vacant Space After Encryption (CVSAE) and other is Creating Vacant Space Before Encryption (CVSBE). In the primary case there are few limitations: 1) embedded data can be completely recovered from the cover medium but there is distortion in cover medium i.e. cover medium cannot be completely recovered. 2) As embedding capacity keeps on increasing there will be increasing distortion at the receiver end. To overcome these limitations we create vacant space before encryption by taking

Threshold value T such that the original cover image can be recovered at the receiver without any errors and also maintains high embedding capacity with improved peak signal-to-noise ratio (PSNR) compared to previous methods. From Fig 3, the vacant space is created by dividing the image into two regions as X and Y using the threshold values. Let T1 and T2 are two different thresholds. In general T1 and T2 are selected as 0.25(max 0.35bpp) and 0.2bpp (max 0.3bpp) respectively so that there will not be much degradation of the quality of the image [9]. The threshold T1 is for choosing the least significant bit plane for the subimage X and the threshold T2 is for replacing pixels in image Y with the pixels of X image whose threshold values are less than 0.35bpp. The pixels whose threshold values are less than 0.35bpp in image X are replaced by embedded data that is to be sent from source to destination.

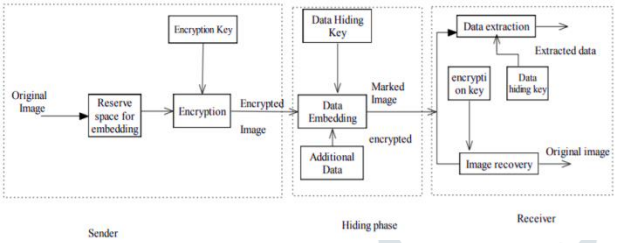

Fig 3: Schematic representation of Reversible Data Hiding

Generating Encrypted Images:- To generate the encrypted images, first the original cover image is divided into two portions as X and Y so as the LSB's of X are reversible embedded into Y using RDH algorithm as shown in Fig 4. The LSB planes of X are used to store information bits.

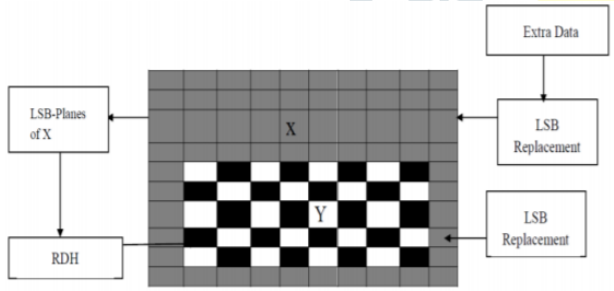

Fig 4: Representation of Image partitioning

Let us consider P as original cover gray scale image of 8-bit with M x N dimensions and pixels ranging from 0 to 255 and let the size of the secret data as Q. Now based on Q the sender extracts overlapping blocks.

Image recovery after Data retrieval: - From the stego images data can be extracted in two ways:

- Extraction from encrypted images.
- Extraction from decrypted images.

In the first case, using data hiding key, the three least significant bits embedded into the encrypted image will be extracted and then the receiver checks the server for updating by LSB replacement. It is secured than other methods as data is extracted from the encryption images. In the second case the sender decrypts the image first and then extracts data from the decrypted images. When compared to Second case all the changes are done in encrypted stage for embedding and extracting data in the first case.

IV. CONCLUSION

The usage of digital data in modern communication has been rapidly growing. In order to provide security for digital data the steganography is used. Steganography is popularly used for data hiding. The process of embedding data in to the cover medium is known as steganography. The key parameters namely imperceptibility, capacity, and security are used for data hiding. Imperceptibility is measured by using PSNR, capacity can be determined by using embedding rate and security is addressed by means of encryption.

REFERENCES

[1] Chang CC, Lin MH, Hu YC. "A fast and secure image hiding scheme based on LSB substitution". International Journal of Pattern Recognition and Artificial Intelligence. Vol 16 No 4, Jun 2002, PP.399-416.

[2] Wang ZH, Kieu TD, Chang CC, Li MC. "A novel information concealing method based on exploiting modification direction". Journal of Information Hiding and Multimedia Signal Processing. Vol 1 No 1, Jan 2010, PP.1-9.

[3] Zhang J, Zhang D. "Detection of LSB matching steganography in decompressed images". IEEE Signal Processing Letters. Vol 17 No 2, Feb 2010, PP.141-144.

[4] Hong W, Chen TS. "A novel data embedding method using adaptive pixel pair matching". IEEE transactions on information forensics and security. Vol 7 No 1, Feb 2012, PP.176-84.

[5] Sharmila B, Shanthakumari R. Efficient Adaptive Steganography for color images based on LSBMR algorithm. ICTACT Journal on image and video processing. Vol 2 No 3, Feb 2012, PP.387-392.

[6] Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW. "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image". Multimedia Tools and Applications. Vol 75 No 22, Nov 2016, PP.14867-93.

[7] Tsai YY, Tsai DS, Liu CL. "Reversible data hiding scheme based on neighboring pixel differences". Digital Signal Processing. Vol 23 No 3, May 2013, PP.919-927.

[8] Peng F, Li X, Yang B. "Improved PVO-based reversible data hiding". Digital Signal Processing. Vol 25, Feb 2014, PP.255-265.

[9] Jung KH, Yoo KY. "Data hiding method using image interpolation". Computer Standards & Interfaces. Vol 31 No 2, Feb 2009, PP.465-470.

[10] Avci E, Tuncer T, Avci D. "A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain". Arabian Journal for Science and Engineering. Vol 41 No 8, Aug 2016, PP.3153-3161.

[11] Q. Wang, W. Zeng, and J. Tian, "A compressive sensing based secure watermark detection and privacy preserving storage framework," IEEE Transactions on Image Processing, vol. 23, no. 3, pp. 1317–1328, 2014.

[12] B. Zhao, W. D. Kou, H. Li, L. Dang, and J. Zhang, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," Information Sciences, vol. 180, no. 23, pp. 4672–4684, 2010.

[13] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," IEEE Transactions on Multimedia, vol. 14, no. 3, pp. 703–716, 2012.

[14] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: a review of its benefits and open issues," IEEE Signal ProcessingMagazine, vol. 30, no. 2, pp. 87–96, 2013.

[15] J. Guo, P. Zheng, and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain," Journal of Visual Communication and Image Representation, vol. 30, pp. 125–135, 2015.

[16] H. Liu, D. Xiao, R. Zhang, Y. Zhang, and S. Bai, "Robust and hierarchical watermarking of encrypted images based on Compressive Sensing," Signal Processing: Image Communication, vol. 45, pp. 41–51, 2016.

[17] D. Xu, R. Wang, and Y. Q. Shi, "Data hiding in encrypted H.264/AVC video streams by codeword substitution," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 596–606, 2014.