Current Trends in Technology and Science
www.ctts.in, ISSN: 2279-0535, Volume: X, Number: VI, November 2021

Enhanced Reversible Data Hiding on Encrypted Images Using Selective Pixel Flipping Method and Proposed Pixel Bits Change Method

Sunil Kumar[1], Manish Rai[2]
Computer Science and Engineering Department
Bhabha Engineering Research Institute, Madhya Pradesh, India
sks150691@gmail.com, manishrai2587@gmail.com

Abstract: Enhanced reversible data hiding on encrypted images using selective pixel flipping method and proposed pixel bits change method. Reversible data hiding on encrypted images may be a vigorous area of research within the sector of knowledge security, which involves the technique of carrying knowledge during an appropriate multimedia carrier for secure communication. Image information hiding procedure makes available authentication of data and secret communication other than can reason a loss of the delivery service. RDH uses many procedures are used for patent security, truth validation, image media registration. Applications like medical imagery, military, and forensics degradation don't allow distortion of the original cover, so it needs secure data hiding techniques. In this research, drawback overcome through PM and recovery process without distortion was removed by reversible data hiding methods. RDH techniques recover the primary carrier exactly after the extraction of the encrypted key data. Reversible Data Hiding Techniques are classified supported the strategy of implementation, image data hiding scheme using pixel bits change process confirm data hiding and therefore the exact image recovery at the receiver side, the proposed method uses a bits change histogram process, they also observed that this scheme (selective pixel flipping method) is liable to fail while recovering an image block which contains highly correlated pixel values (very low smooth region). During this study, these schemes (selective pixel flipping method) may help scale back the block size but more error rate. Since equivalent reference pixels are often exploited within the extraction procedure, the embedded secret bits are often extracted from the stego image correctly, and therefore the cover image is often restored losslessly. The experimental study of this scheme is carried on an image dataset, and thus the results show that the improved reversible data hiding on encrypted images using proposed pixel bits change method and improve PSNR, low MSE, original, watermarked image and also to extend Peak signal to noise ratio called best RDH.

Keywords:—Reversible Data Hiding, Image Encryption, Image Decryption, PSNR Measure, Histogram Shifting, MSE Measure, Selective Pixel Flipping Method, PPBCM.

I. Introduction

Digital Steganography and Watermarking are primitive techniques for communicating secrete data in suitable carriers like image, audio, and video files. These techniques may distort the original image after extracting the hidden data. These can be used for copyright protection, media registration, integrity authentication [1]. The embedding process usually distorts the original cover image that carries secret data permanently. But in medical image processing applications, military, and forensics, degradation of original cover cannot be allowed. To overcome this disadvantage, a method to recover the original image without distortion after extracting the secret data emerged. It was known as reversible data hiding (RDH) or lossless data hiding. It embeds invisible data as payload or secret or hidden data into a digital image, reversibly known as a cover image. Fig shows the block diagram of RDH. Data hiding techniques have been widely in practice for the last three decades for secure message transmission. Recent data hiding research focuses more on reversible data hiding on images [2]. The main advantage of reversible data hiding scheme is that the receiver can extract the secret message at the receiver side and recover the original image. Reversible data hiding schemes are useful in medical image transmission where the sender can embed patient details or diagnosis results in the image itself. Besides the medical image transmissions [3], cloud service providers use reversible data hiding schemes to embed necessary metadata on the images uploaded into the cloud storage by the cloud users. Note that cloud service providers cannot permanently modify the images they have received, so conventional data hiding techniques cannot be used in such scenarios [4].

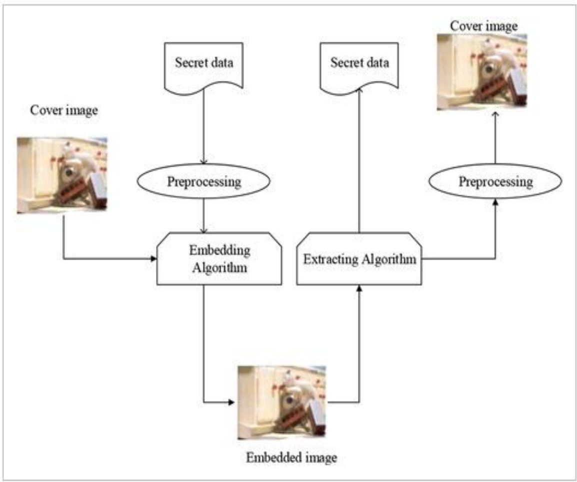

Figure 1 The fundamental structure of RDH

1.1 Properties of data-hiding strategies

The most important properties that arise in the data hiding strategies are given below[5]:

- *Security*: This is available to withstand the targeted attacks, which cannot get the inserted data without knowing secret-key and embedding algorithms.

- *Robustness*: This is the property in which the hidden information can be retrieved using image processing strategies such as linear, a non-linear filter, swapping frames, adding noise, and resembling adjusting scale.
- *Invisibility:* This is the property related to human perceptual transparency.
- *Capacity*: It is the difficulty in detecting the existence of any hidden message in the carrier image.

The way of hiding data in a file such as audio, video, and image is called RDH. This technique makes the receiver could recover both the data and cover files without loss. Barton proposed an RDH algorithm of US patents in 1997. They are applicable in medical image processing, stereo image coding, engineering graphics, image authentication, and vector map retrieval in computer-aided design. This RDH method is used in many fields such as law forensics, military, and medical applications. Displays the basic structure of the RDH method Embedding is an initial stage at which a private message is given to the cover image for hiding personal information. This message can play as an input to the embedding algorithm. After covering the picture, the output will be in the form of the covered image. Then this result is given as an input to the extracting algorithm, which separates the private message from the cover image. The secretive data and cover image must be original and hence named RDH[6].

II. Related Work

The challenge of attacks increases in our daily lives in different formats the developments of algorithms and models by the continuous approach of different authors and research scholars. Here describes the contribution of different authors in the area of reversible data hiding on encrypted images.

Amrutham Abhinav et al. [7] Reversible data hiding on encrypted images is an active area of research in information security. In this paper, we revisit the reversible data hiding scheme proposed by Xinpeng Zhang to ensure the exact image recovery at the receiver side, and the existing scheme uses a block size of pixels, which leads to an embedding rate of bits per pixel. We also observed that the existing scheme fails while recovering an image block that contains highly correlated pixel values (very smooth region). In this manuscript, we propose a new scheme that will help to reduce the block size without compromising the bit error rate. The experimental study of the new scheme is carried on USC-SIPI image dataset managed by the University of Southern California, and the results show that the proposed scheme outperforms the existing scheme

Zhang et al. [8] introduced reversible, lossless, and combined data hiding approaches for ciphertext images. These images were encrypted by the encryption scheme named public-key cryptosystems, using dual properties, namely homomorphic and probabilistic. The pixel division or reorganization was avoided, and encryption or decryption was performed directly on the cover to minimize the computational complexity and encrypted data.

Mintzer et al. [9] Traditionally, reversible watermarks were initiated as visible patterns by Images marked with reversible visible watermarks were posted on the Internet for application in their digital library. The watermarked image was in the form of a puzzle that the users could obtain easily using a program for an extra fee, removing the watermark and thus reconstructing the original image.

Ma et al. [10] proposed a new method by reserving room before the encryption process using the RDH traditional algorithm. Also, this method seems easier for data hider to embed data reversibly in encrypted images. Image recovery and data extraction were free from error. Experimental outcomes showed that the proposed method could embed large payloads and attain outstanding performance without losing secrecy.

Wang et.al.[11] suggested the usage of 2D-vector maps for RDH. They discovered two reversible data-hiding difference expansion schemes. In the first scheme, the coordinates of vertices were the cover data, and altering the differences among the neighboring coordinates was used to hide data. The second scheme calculated the Manhattan distances between the neighboring vertices as the cover data and embedded the hidden data, altering the neighboring distances' differences. Both schemes resulted in high-capacity maps with highly associated coordinates.

Hu et al. [12] proposed an embedding scheme that helped the authors to create a payload-dependent overflow location map. This map aimed to minimize unnecessary image alteration because this map has the capacity for good compressibility. The algorithm of this work represents a larger embedding capacity under similar image quality. This method performs better in different images types than other algorithms, whereas the existing approaches face issues in acquiring high image quality and better embedding capacity.

In [13], RDH was accomplished based on two-dimensional difference histogram modification using difference-pair-mapping (DPM), an injective mapping defined on difference-pairs. First, a sequence consisting of pixel differences is computed by taking each pixel pair and its context into consideration. Then, taking the frequency count of the resulting difference pairs generates a 2D histogram. Thus, reversible data is embedded according to the specifically designed DPM. Better image redundancy and improved performance was the result when compared with the previous one-dimensional histogram-based methods

Chang and Wu [14] presented the data hiding reversible approach for digitally compressed images based on side match vector quantization (SMVQ). The receiver performed a two-step process with the presented concept. In the first step, the secret data was extracted, and in the next step, the original SMVQ compression codes were reconstructed. Experimental outcomes showed that for vector quantization and SMVQ-based compressed images, the proposed approach is better than the other information hiding schemes. The performance was measured and analyzed in terms of visual quality, compression rate, and secret data size.

Bin et al. [15] designed a code division-multiplexing algorithm for RDH. The covert data was represented by different orthogonal spreading sequences using the Walsh Hadamard matrix and embedded into the cover image. The original image could be completely retrieved exactly after the data was extracted. Multilevel data embedding enriched embedding capacity

Hong et al. [16] introduced a data hiding reversible scheme based on modifying prediction error (MPE). The histogram of prediction errors (PEs) was modified using the proposed method to formulate vacant positions of data embedding. The peak signal-to-noise ratio (PSNR) of stego-image produced using MPE was obtained 48 dB. The embedding capacity is higher than the methods with similar PSNR. Moreover, MPE can also be applied to images with 5665 a flat histogram, whereas fewer data bits needless error modification.

Zhang et al.[17] proposed a Reversible Data Hiding technique for encrypted images. It includes encryption of the image, embedding data extraction for image recovery phases. The data of the original image is encrypted entirely by a stream cipher. This method offers a low computational complexity. The following steps describe the entire scheme. A data hider can embed additional data into the encrypted image by modifying a part of encrypted data. This data hider need not necessarily know the original content of the encryption image using the encrypted image containing embedded data, a receiver first decrypts it using the encryption key, and the decrypted version is similar to the original image. The embedded data can be correctly extracted, while the original image can be perfectly restored using the data hiding key with spatial correlation in the natural image.

III. Problem Formulation

This method performs better in dissimilar images types than other algorithms, whereas the existing approaches face issues. As one of the ways to solve the security problem is data hiding technology that embeds the secret data imperceptibly into the cover media, the main problem block effect in the existing approach (selective pixel flipping method) low PSNR and high MSE reversible data hiding on encrypted images. Due to the rapid development of the internet and computer techniques, more and more multimedia files are stored and transmitted. As a result, multimedia files' copyright, authentication, and integrity protection problems raise much attention. Data hiding is considered to be an effective technique to solve these problems.

IV. Implementation Tool

MATLAB (short for "matrix lab") can be a proprietary multi-paradigm programming language and digital computing environment developed by MathWorks. MATLAB enables the manipulation of matrices, the drawing of functions and data, the applications of algorithms, the creation of user interfaces and interfaces with programs written in other languages. Although MATLAB is primarily synonymous with numerical computation, an optional toolkit uses the MuPAD symbolic engine allows symbolic access to computer skills. Another package, Simulink, adds multi-domain simulation graphics and design-based models for dynamic and integrated systems. During this thesis, all of the improved results of efficient data retrieval were achieved in MATLAB, the high-level language with an interactive background used by many universal engineers and scientists

V. Result Analysis

(a) Experimentation1:

1. first experimentation on the cover image using Serum institute building image,93KB,1200x900, jpeg as a cover image large size image (MxN) and next image using data image using who_messgae_logo images,5.74KB, 225x150, jpeg as a data image small size image (PxQ).

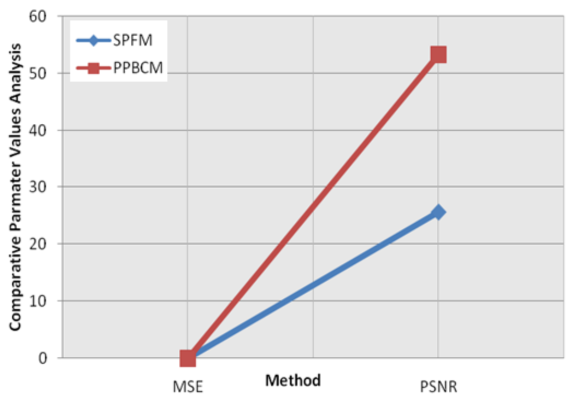

Figure 2 Comparison between SPFM and PPBCM on experimentation 1

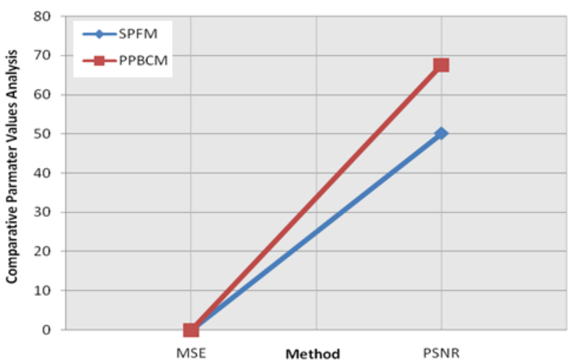

Figure 3 Comparison between SPFM and PPBCM on experimentation 2

b). Experimentation 2:

1. second experimentation on the cover image using Mackenzie_Garden_Finsbury_Park image,391Mb, in jpg,3872x2592 as a cover image large size image (MxN)

and next image using Data image using cisco-logo images,15.8KB,640x403, jpeg as a data image small size image (PxQ).

VI. Conclusion

Enhanced reversible data hiding on encrypted images using selective pixel flipping method and proposed pixel bits change method. Reversible data hiding techniques recover the primary carrier exactly after the extraction of the encrypted key data. Applications like medical imagery, military, and forensics use these techniques for copyright protection, media registration, integrity authentication, an honest spread survey of object detection and tracking methods are presented. Merits and demerits of accessible methods of object detection, classification, and tracking are discussed all right. The background subtraction method is the only method that provides the complete details about the thing compared to frame difference and optical flow detecting methods. Point tracking involves detection in every frame. Learning on different previous reversible image data hiding procedures is performed, and all images are secure data. Reversible data hiding schemes for encrypted images with low computation complexity are analyzed, including image encryption, data hiding, and data extraction/ image recovery phases. An encryption strategy encrypts the initial images. So, learning regarding an encryption approach is executed; although a knowledge hider doesn't know the primary content, he can embed the key data into the encrypted image by modifying a region of encrypted data. So, methods for data embedding are also noticed of those techniques aim at reproducing the initial image within which the data was hidden with low PSNR, and this type of problem is overcome through the proposed method. Proposed Pixel Bits Change Method (PPBCM) in encrypted images may be a new topic drawing attention due to the confidentiality of image data hiding requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, against which Proposed Pixel Bits Change Method (PPBCM) by reserving room before encryption. Therefore, the information hider can have the extra space blank call at the previous stage to make the data hiding process effortless. The Proposed Pixel Bits Change Method (PPBCM) can benefit from all traditional RDH techniques for plain images and achieve excellent performance (high PSNR and low MSE) without loss of perfect secrecy.

References

[1] Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography. Morgan Kaufmann, 2007.

[2] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, and S. Pogreb, "Applications for data hiding," IBM systems journal, vol. 39, no. 3.4, pp. 547–568, 2000.

[3] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," in Proceedings. International Conference on Image Processing, vol. 2. IEEE, 2002, pp. II-II.

[4] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: advances in the past two decades," IEEE Access, vol. 4, pp.3210–3237, 2016.

[5] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: a new high capacity and reversible data hiding technique," Journal of biomedical informatics, vol. 66, pp. 214–230, 2017.

[6] W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," IEEE Transactions on Multimedia, vol. 18, no. 8, pp. 1469–1479, 2016

[7] Abhinav, Amrutham, V. M. Manikandan, and A. A. Bini. "An improved reversible data hiding on encrypted images by selective pixel flipping technique." In 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), PP. 294-298. IEEE, 2020.

[8] Zhang X., Long J., Wang Z., et al.: ' Lossless and reversible data hiding in encrypted images with public-key cryptography, IEEE Trans. Circuits Syst. Video Technol., 2016, 26, (9), pp. 1622– 1631.

[9] F. Mintzer, J. Lotspeich, and N. Morimoto, "Safeguarding digital library contents and users: Digital watermarking," D-Lib Mag., Dec. 1997.

[10] Ma K., Zhang W., Zhao X., et al.: ' Reversible data hiding in encrypted images by reserving room before encryption,' IEEE Trans. Inf. Forensics Sec., 2013, 8, (3), pp. 553– 562.

[11] XiaoTong Wang, ChengYong Shao, XiaoGangXu, and XiaMu Niu," Reversible Data Hiding Scheme for 2D Vector Maps Based on Difference Expansion," IEEE Transactions on Information Forensics and Security,vol:2,pp:311-320,2007.

[12] Hu Y., Lee H-K., Li J.: ' DE-based reversible data hiding with improved overflow location map,' IEEE Trans. Circuits Syst. Video Technol., 2009, 19, (2), pp. 250– 260.

[13] Xiaolong Li, Weiming Zhang, Xinlu Gui, and Bin Yang, "A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification," IEEE Transactions on Information Forensics and Security, vol:8, pp:1091-1100, 2013.

[14] Chang C.-C., Wu W.-C.: ' A steganographic method for hiding secret data using side match vector quantization, IEICE Trans. Inf. Syst., 2005, 88, (9), pp. 2159– 2167.

[15] Bin Ma and Yun Q. Shi, "A Reversible Data Hiding Scheme Based on Code Division Multiplexing," IEEE Transactions on Information Forensics and Security vol:11, pp:1914-1927, 2016.

[16] Hong W., Chen T.-S., Shiu C.-W.: ' Reversible data hiding for high-quality images using a modification of prediction errors,' J. Syst. Softw., 2009, 82, (11), pp. 1833– 1842.

[17] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, IEEE Trans. Image Process., vol. 20, no. 12, pp.3524–3533, 2011.
[18] Celik, Mehmet Utku, Gaurav Sharma, A. Murat Tekalp, and Eli Saber. "Reversible data hiding." In Proceedings. International Conference on Image Processing, vol. 2, pp. II-II. IEEE, 2002.
[19] Mishra, Minati, Priyadarsini Mishra, and M. C. Adhikary. "Digital image data hiding techniques: A comparative study." arXiv preprint arXiv:1408.3564,2014.
[20] Joshi, Saurabh V., Ajinkya A. Bokil, Nikhil A. Jain, and Dipali Koshti. "Image steganography combination of spatial and frequency domain." International Journal of Computer Applications 53, no. 5,2012.
[21] Valandar, Milad Yousefi, Peyman Ayubi, and Milad Jafari Barani. "A new transform domain steganography based on the modified logistic chaotic map for color images." Journal of Information Security and Applications 34: 142-151, 2017.
[22] Lin, Chia-Chen, and Pei-Feng Shiu. "DCT-based reversible data hiding scheme." In Proceedings of the 3rd international conference on ubiquitous information management and communication, pp. 327-335. 2009.
[23] Yang, Wen-Chao, and Ling-Hwei Chen. "Reversible DCT-based data hiding in stereo images." Multimedia Tools and Applications 74, no. 17: 7181-7193, 2015.