International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 12 Issue 3, May 2024

Enhanced Reversible Data Hiding Scheme for Encrypted Images Using BEHSM for Improved Quality and Security

Aman Khare, Naveen Khare
Babulal Tarabai Institute of Research andTechnology, Sagar (M.P), India
amankhare15@gmail.com, naveenkhare90@gmail.com

Abstract - The rise in digital media transfer has made data modification easier, necessitating secure communication and identity verification methods. Reversible data hiding (RDH), or lossless data hiding, allows for the lossless restoration of the original cover image after the extracted embedded information. Our study introduces a new method, BEHSM, which enhances the quality of encrypted images and allows for the lossless recovery of the secret image. Traditional RDH techniques, such as difference expansion and histogram modification, are common, but previous hierarchical embedding methods (HEM) were found to have low PSNR and high MSE. BEHSM, a reversible image transformation technique, improves upon these shortcomings by embedding secret data into a cover image with minimal distortion and ensuring the correct extraction of secret data while allowing for the recovery of the original cover image. Encryption is utilised before data hiding to address multimedia data transmission and storage security concerns. Our proposed BEHSM method demonstrates improved security, with low MSE and higher PSNR values, making it a robust solution for secure and lossless data hiding in encrypted images.

Keywords: Reversible Data Hiding (RDH), Difference Expansion (DE), histogram modification, Image Encryption, Image Decryption, Image Recovery, PSNR, MSE, BEHSM.

I. INTRODUCTION

Data hiding is considered a promising method to achieve data security for responsible AI. Typically, data hiding involves concealing information in a specific form within another type of media. It can take different forms, such as encoding confidential information into an existing text piece or embedding audio files into a digital image. As digital assets become more diverse and ubiquitous, the importance and scope of data-hiding applications will only grow [1]. As digital communication and multimedia data become increasingly prevalent, data hiding has become crucial in today's digital age. Ensuring responsible AI, such as machine learning as services, as required, necessitates secure communication across all mediums, and the accountability of responsible AI, such as digital intellectual property, necessitates protection against theft and misuse. In its traditional form, the data-hiding process can be categorised into watermarking, steganography, and cryptography [2]. Data hiding is the art and science of communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files.

Digital Steganography and watermarking are the two kinds of data hiding. Reversible data hiding can be defined as an approach in which the data may be hidden in the host media as a cover image. A reversible data-hiding algorithm can recover the original image losslessly after extracting the data. Reversible data embedding, also called lossless data embedding, embeds invisible data (a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation of the image after data embedding should be low. An intriguing feature of reversible data embedding is the reversibility; one can remove the embedded data to restore the original image. Data hiding is a technique for embedding information into covers such as audio, image, and video files. It can be used for copyright protection, media notation, integrity authentication, covert communication, etc. Most data-hiding methods embed messages into the cover media, like images or video, to generate the marked media by only modifying the least significant part of the cover, thus ensuring perceptual transparency. The embedding process usually introduces permanent distortion to the cover; the original cover can never be reconstructed from the marked cover. However, in some applications, such as medical imagery, military, and law forensics, no degradation of the original cover is allowed. We need a special kind of data hiding method for such cases, referred to as reversible data hiding (RDH) or lossless data hiding, by which the original cover can be losslessly restored after the embedded message is extracted. The block diagram of RDH shows that

reversible steganography or watermarking can restore the original carrier without any distortion or ignorable distortion after extracting hidden data. So, reversible data hiding is now becoming popular. Figure 1 shows that hiding reversible data is a basic requirement; the quality degradation of the image after data embedding should be low. An intriguing feature of reversible data embedding is the reversibility; one can remove the embedded data to restore the original image. From the information hiding point of view, reversible data embedding hides some information in a digital image so that an authorised party can decode the hidden information and restore the image to its original, pristine state. An information-hiding system uses four aspects: capacity, security, perceptibility and robustness [3].

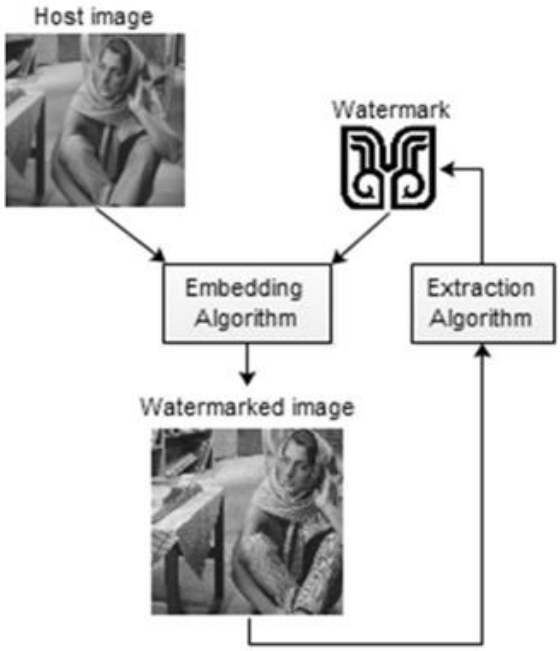

Fig.1 Reversible data hiding in the process

1.1 Reversible Data Hiding Techniques

Reversible data hiding has been an area of research for several years, with various methods proposed over time. The following are different techniques that have been introduced:

Circular Visual Cryptography was introduced in 2005, and this scheme allows a circular shadow image to hide two or more confidential data sets within circular images, displaying them in both the inner and outer regions of the images. However, it can only produce a circular shadow image without the central part, resulting in low resolution in the inner portion, as illustrated in Figure 4. This method encrypts data into two ringed shadow images, simultaneously hiding two confidential data sets [4].

A. LSB Modification-Based Technique: One of the earliest methods is the modification of the LSB (Least Significant Bit). In this well-known method, the LSB of each signal sample is replaced (overwritten) by a secret data bit. These bits are read in the same scanning order during extraction, and the secret data is reconstructed.

B. Difference Expansion (DE) Based Technique: Tian proposed a DE-based technique for reversible data hiding [2]. This technique discovers extra storage space by exploring the redundancy in the image content. The DE technique is noted for its high payload capacity, the visual quality of embedded images, and low computational complexity.

C. Histogram Shift-Based Technique: Histogram-shifting-based reversible data hiding schemes embed data by shifting the histogram in a fixed direction. These schemes focus on two key points: the peak point and the zero point. The peak point corresponds to the grayscale value with the maximum number of pixels in the histogram of the given image, while the zero point is where the histogram count is zero. Pixels between the peak and zero points are modified during the embedding process. The pixel at the peak point carries a bit of the secret message, and others are adjusted to maintain the image's integrity. The hiding capacity of this technique equals the number of pixels at the peak points; thus, a larger number of peak point pixels increases the hiding capacity. More peak and zero-point pairs can increase capacity further, though identifying these pairs can sometimes be challenging [6].

II. RELATED WORK

Reversible data hiding has been done over the past few years. Some important techniques are discussed here. This section will classify the existing RDHEI techniques based on the underlying image-processing mechanisms involved. K. Ma et al. [7] are the first to propose an RRBE method, taking the opposite line to all other state-of-the-art methods developed up to this point. The authors start by splitting the original image into blocks. Within each block, the correlation between the pixels is evaluated by using a fluctuation function. The blocks are further partitioned into two groups, namely, A and B. Specifically, group A is composed of textured blocks, while group B is composed of relatively homogeneous blocks. The blocks in group A are placed at the beginning of the image, and those in group B are placed afterwards. In order to release space for the secret message embedding, the LSB plane of A is embedded

into pixels in group B in the clear by using histogram shifting. The resulting image is then encrypted using a stream encryption algorithm, and the number of pixels that can be marked is stored in the LSBs of the first A pixels. With this information, the secret message can be embedded simply by substituting the LSBs of the remaining pixels in A. We note that the first three LSBs of each pixel can be used. F. Huang et al. [8] discovered that the previously proposed algorithms for embedding secret data in the clear domain cannot be applied in the encrypted domain [37]. Indeed, classical encryption methods do not allow the correlation between neighbouring pixels to be maintained without introducing security flaws. The authors introduce a new strategy to encrypt an image in their work. The objective is for the conventional data-hiding algorithms designed in the clear domain to be deployed directly to embed data in the encrypted image. Specifically, the original image is split into non-overlapping blocks. All pixels are encrypted within each block by applying the XOR operation using the same pseudo-randomly generated byte. The encrypted blocks are then pseudo-randomly permuted. Note that pixels within the same block are not scrambled, but only the order of the blocks is changed. With this encryption method, the statistical properties of the clear image, especially the histogram of pixel differences or prediction errors, are preserved. Therefore, the conventional data-hiding algorithms in the clear domain can be applied in the encrypted domain. Still, the embedding capacity is limited by the handling of the under/overflow problem. Ge et al. [9] proposed a novel reversible data hiding in encrypted images (RDH-EI) method. We first provide an RDH-EI approach using single-level embedding, in which three parties are involved, including an image owner, a data hider, and a recipient. The image owner encrypts an original image into a ciphertext image. After dividing the original image into blocks, the owner pseudo-randomly permutes all blocks by a permutation key. With an encryption key, the image owner further encrypts the contents of all blocks using a stream cypher algorithm, during which pixels inside each block share the same stream bytes. Once the encrypted image is uploaded onto the server, a data hider embeds additional messages into the ciphertext. The data hider divides the encrypted image into blocks and selects peak pixels from each block using an embedding key. With the peak pixels, the data hider embeds an additional message using histogram shifting inside each block. On the receiver side, a recipient extracts the hidden message using the embedding key and recovers the original image losslessly with the permutation and encryption keys. Based on the single-level algorithm, we further construct a multi-level approach. The embedding process is iteratively used to generate the marked encrypted images. Compared with state-of-the-art works, the proposed method achieves a better embedding efficiency and an error-free recovery.

Xiao et al. [10] propose a separable reversible data hiding scheme in encrypted images based on pixel value ordering (PVO). After the original image is encrypted using homomorphism encryption by the content owner, the data hider embeds the secret data in the encrypted domain. The PVO strategy realises hiding data in each block. Additive homomorphism guarantees the performance of PVO in the encrypted domain is close to that in the plain domain. Besides, the homomorphism encryption does not cause data expansion, and the payload can be further improved. With the watermarked encrypted image, if the receiver has only the data hiding key, he can extract the additional data. If the receiver has only the encryption key, he can obtain a decrypted image similar to the original one. If the receiver has the data hiding and encryption keys, he can extract the additional data without any error and recover the original image losslessly. Xu et al. [11], Digital images sometimes need to be stored and processed in an encrypted format to maintain security and privacy, e.g., cloud storage and cloud computing. The cloud servers must embed additional information directly in these encrypted images for content notation and tampering detection. As an emerging technology, reversible data hiding in the encrypted domain will be useful in cloud computing due to its ability to preserve confidentiality. This paper proposes a novel, separable, error-free, reversible data hiding scheme in encrypted images. After analysing the property of interpolation technology, a stream cypher is utilised to encrypt sample pixels and a specific encryption mode is designed to encrypt interpolation-error of non-sample pixels. Then, the data-hider, who does not know the original image content, may reversibly embed secret data into interpolation error using a modified histogram shifting and difference expansion technique. In order to adapt to different application scenarios, data extraction can be done in encrypted or decrypted domains. In addition, real reversibility is realised; data extraction and image recovery are error-free.

Experimental results demonstrate the feasibility and efficiency of the proposed scheme. Lin et al. [12] designed a bit-plane block embedding (BPBE) algorithm to hide secret messages in binary images.

Meanwhile, we apply BPBE to hide reversible data in encrypted images. It embeds the part of least-significant-bit (LSB) planes into higher most-significant-bit (MSB) planes using BPBE for reserving room before encryption so that additional data can be embedded into the LSB planes of encrypted images. If the receiver only has the data hiding key, they can extract the additional data but don't know the exact information of the original image. The receiver can reconstruct the original image if they are provided with only the encryption key. Data extraction and image recovery can be completed correctly when both keys are acquired.

Experimental results illustrate that the proposed scheme can achieve a higher embedding rate (ER) compared to some state-of-the-art methods and maintain an acceptable image quality. Lai et al. [13] propose an image transformation technique which selects a target image similar to the secret image, then replaces each block of the target image with a similar block of the secret image and embeds the map between the secret blocks and the target blocks; it forms an Encrypted image of the secret image. A greedy search method is used to find the most similar block. Although this method is reversible, it is only suitable for a target image similar to the secret image, and the visual quality of the encrypted image is not so good. Lee et al. [14] improve the work of [13]'s method by transforming the secret image to a randomly selected target image without using a database. In Lee et al.'s method, each block of the secret image is transformed into a block of the target image with a reversible colour transformation. Then, the required information for restoring the secret image, such as parameters and indexes of the block, is added to the transformed blocks, giving an Encrypted image. Lee et al.'s method can transform a secret image into a randomly selected target image, increasing the quality of the encrypted image. However, the transformation is not reversible in Lee et al.'s method. So that secret image cannot be losslessly reconstructed. Yu et al. [15] proposed reversible data hiding in encrypted images (RDHEI) is an effective data security technique. Most state-of-the-art RDHEI methods have not yet achieved a desirable payload. To address this problem, we propose a new RDHEI method with hierarchical embedding. Our contributions are twofold. (1) A novel hierarchical label map generation technique is proposed for the bit-planes of plaintext images. The hierarchical label map is calculated using a prediction technique and compressed and embedded into the encrypted image. (2) Hierarchical embedding is designed to achieve a high embedding payload. This embedding technique hierarchically divides prediction errors into three kinds: small-magnitude, medium-magnitude, and large-magnitude, which are marked by different labels. Different from the conventional techniques, pixels with small-magnitude/large-magnitude prediction errors are used to accommodate secret bits in the hierarchical embedding technique and, therefore, contribute a high embedding payload. Experiments on two standard datasets are discussed to validate the proposed RDHEI method.

III. IMPLEMENTATION TOOL EXPLANATION

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, and 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. It allows symbolic access to computer skills, and another package, Simulink, adds multi-domain simulation graphics and design-based models for dynamic and integrated systems. During this thesis, all 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. It makes exploring and visualising ideas possible, working together in different disciplines and signals, and processing images, messages and results calculations.

IV. RESULT ANALYSIS

Research focusing on theory, framework, methodology, and applications must be further investigated and thoroughly developed in reversible data hiding. Achieving the best possible trade-off between payload, reconstructed image quality, and security level remains a significant challenge. Additionally, specific methods must be designed for new formats and containers, particularly JPEG images, to address low PSNR (Peak Signal-to-Noise Ratio) and high error rates found in base papers using BHS (Block Histogram Shifting). The proposed method aims to improve performance by reducing error rates and increasing PSNR.

(a) Result analysis compares the new method (BEHSM) with the old method (HEM), focusing on parameters

such as PSNR and MSE (Mean Squared Error). Different images include grayscale, colour, black-and-white, and various formats (JPG/JPEG, PNG, BMP, GIF). A data image (Di-Kanha-Tiger-Reserve, 74.1 KB, dimensions 755x366) and a cover image (ci-wolf image, 185 KB, dimensions 512x512) are trialled for experimentation. The process involves generating a histogram, embedding the image, calculating MSE, and determining PSNR values.

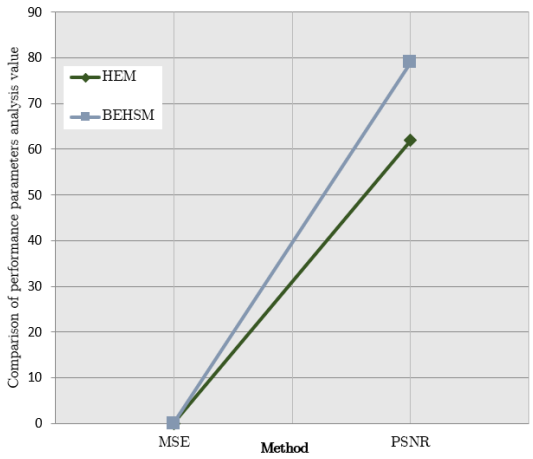

Fig. 2 Comparison between new method (BEHSM) and old method (HEM) in case1

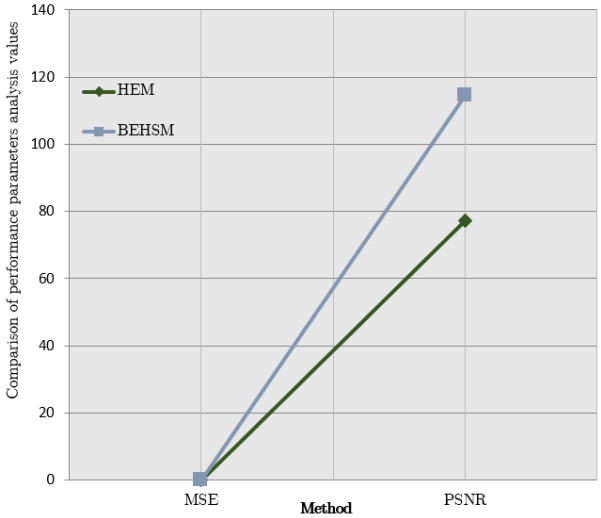

Fig. 3 Comparison between the the new method (BEHSM) and old method (HEM) in the case 2

Generate result graph-based analysis between new method (BEHSM) and old method (HEM), main calculate parameter PSNR and MSE, in show Figure 2, new method (BEHSM) calculates PSNR high but low MSE and old method (HEM) PSNR low but high MSE.

(b) Result analysis between new method (BEHSM) and old method (HEM), main calculate parameter PSNR and MSE. Different images use grayscale, cooler images, black-white and different image formats such as JPG/JPEG, PNG, BMP, GIF, etc. Experimentation2 on data image (Di-logo_maruti_suzuki,19.3KB, dimensions 64x480) and cover image (ci-Maruti Suzuki-swift,230KB, dimensions 1600x1200) both are trialling data then generate a histogram, generate an embedding image, calculate MSE and finally calculate PSNR values. Generate result graph-based analysis between new method (BEHSM) and old method (HEM), main calculate parameter PSNR and MSE, in show Figure 3, new method (BEHSM) calculates PSNR high but low MSE and old method (HEM) PSNR low but high MSE.

IV. CONCLUSION

Reversible Data Hiding in Encrypted Images (RDHEI) through enhanced methods like BEHSM offers a significant advancement. This technique can transform a secret image into a randomly selected target image, achieving encryption with high visual quality. The secret image can be restored without any loss. The BEHSM method combines various techniques to create a more efficient data-hiding scheme. The new BEHSM method is expected to enhance embedding capacity and image quality while maintaining security. This paper presents the evolution and motivations behind RDHEI methods, highlighting their growing popularity due to the reversibility of the carrier medium after secret data extraction. Traditional reversible data-hiding techniques in encrypted images have limitations, including the inability to protect image content and data privacy, low hiding capacity, complex computations, and poor image clarity. Implementing RDH in encrypted images (RDH-EI) addresses these issues, offering improved security and image quality. This field holds great potential for significantly impacting digital security. The proposed BEHSM method demonstrates improved security (low MSE) and higher PSNR values than the old HEM method. Our results show that BEHSM achieves a higher PSNR with lower MSE, whereas the HEM method results in lower PSNR and higher MSE.

REFERENCES

[1]. Li, Xiaolong, Bin Li, Bin Yang, and Tieyong Zeng. "General framework to histogram-shifting-based reversible data hiding." IEEE Transactions on Image Processing 22, no. 6: 2181-2191, 2013.

[2]. Li, Xiaolong, Weiming Zhang, Xinlu Gui, and Bin Yang. "Efficient reversible data hiding based on

multiple histogram modification." IEEE Transactions on Information Forensics and Security 10, no. 9: 2016-2027, 2015.

[3]. Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi. "New framework for reversible data hiding in the encrypted domain." IEEE Transactions on Information Forensics and Security 11, no. 12: 2777-2789, 2016.

[4]. Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB-based image steganography techniques." In Proceedings 2001 international conference on image processing (Cat. No. 01CH37205), vol. 3, pp. 1019-1022. IEEE, 2001.

[5]. Hu, Yongjian, Heung-Kyu Lee, Kaiying Chen, and Jianwei Li. "Difference expansion based reversible data hiding using two embedding directions." IEEE Transactions on Multimedia 10, no. 8: 1500-1512,2008.

[6]. Tai, Wei-Liang, Chia-Ming Yeh, and Chin-Chen Chang. "Reversible data hiding based on histogram modification of pixel differences." IEEE Transactions on Circuits and Systems for Video Technology 19, no. 6: 906-910,2009.

[7]. K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Transactions on Information Forensics and Security 8, 553–562, 2013.

[8]. F. Huang, J. Huang, Y.-Q. Shi, New framework for reversible data hiding in the encrypted domain, IEEE Transactions on Information Forensics and Security 11,2777–2789, 2016.

[9]. Ge, Haoli, Yan Chen, Zhenxing Qian, and Jianjun Wang. "A high-capacity multi-level approach for reversible data hiding in encrypted images." IEEE Transactions on Circuits and Systems for Video Technology 29, no. 8: 2285-2295, 2018.

[10]. Xiao, Di, Yanping Xiang, Hongying Zheng, and Yong Wang. "Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism." Journal of Visual Communication and Image Representation 45: 1-10, 2017.

[11]. Xu, Dawen, and Rangding Wang. "Separable and error-free reversible data hiding in encrypted images." Signal Processing 123: 9-21, 2016.

[12]. Lin, Jiang-Yi, Yu Chen, Chin-Chen Chang, and Yu-Chen Hu. "Reversible Data Hiding in Encrypted Images Based on Bit-plane Block Embedding." J. Inf. Hiding Multim. Signal Process. 10, no. 2: 408-421, 2019.

[13]. I.-J. Lai and W.-H. Tsai, "Secret-fragment-visible mosaic image–a new computer art and its application to information hiding," IEEE Trans. Information Forensics and Security, vol. 6, no. 3, pp. 936–945, 2011.

[14]. Y. L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible colour transformations," IEEE Trans. Circuits Syst. & Video Technol., vol. 24, no. 4, pp. 695–703, 2014.

[15]. Yu, Chunqiang, Xianquan, Xinpeng, Guoxiang Li, and Zhenjun Tang. "Reversible data hiding with hierarchical embedding for encrypted images." IEEE Transactions on Circuits and Systems for Video Technology 32, no. 2: 451-466, 2021.

[16]. D. Wang, X. Zhang, C. Yu, and Z. Tang, "Reversible data hiding by using adaptive pixel value prediction and adaptive embedding bin selection," IEEE Signal Process. Lett., vol. 26, no. 11, pp. 1713–1717, Nov. 2019.

[17]. J. Qin and F. Huang, "Reversible data hiding based on multiple two-dimensional histograms modification," IEEE Signal Process. Lett.,vol. 26, no. 6, pp. 843–847, Jun. 2019.

[18]. B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise prediction error expansion for efficient reversible data hiding," IEEE Trans. ImageProcess., vol. 22, no. 12, pp. 5010–5021, Dec. 2013.

[19]. W. Qi, X. Li, T. Zhang, and Z. Guo, "Optimal reversible data hiding scheme based on multiple histograms modification," IEEE Trans. Circuits Syst. Video Technol., vol. 30, no. 8, pp. 2300–2312, Aug. 2020.

[20]. J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, ''Secure reversible image data hiding over encrypted domain via key modulation,'' IEEE Trans. Circuits Syst. Video Technol., vol. 26, no. 3, pp. 441–452, Mar. 2016.