International Journal of Advanced Computer Technology
ISSN: 2319-7900 www.ijact.org Volume 12, Issue 6, December 2023

An Improved Reversible Data Hiding with Hierarchical Embedding for Encrypted Images and BBET

Ritik Gour, Amar Nayak
CSE Department, TITE, RGPV, MP, Bhopal, India
ritikgour631@gmail.com , amar.n1975@gmail.com

Abstract: This research introduces an enhanced reversible data hiding (RDH) approach incorporating hierarchical embedding for encrypted images and employs a novel technique termed BBET (Binary Bits Embedding Technique). RDH involves concealing information within a host sequence, enabling the restoration of both the host sequence and embedded data without loss from the marked sequence. While RDH has traditionally found applications in media annotation and integrity authentication, its utilisation has expanded into diverse fields. Given the rapid advancements in digital communication, computer technologies, and the Internet, ensuring information security poses a formidable challenge in safeguarding valuable data. Various reversible and stenographic techniques exist for covertly embedding or protecting data, spanning text, images, and protocols, and facilitating secure transmission to intended recipients. An influential approach in data security is reversible data hiding in encrypted images (RDHEI). This paper distinguishes between the conventional RDHEI technique, characterised by lower Peak Signal-to-Noise Ratio (PSNR) and higher Mean Squared Error (MSE), and proposes an improved RDHEI technique. As the prevalence of digital techniques for image transmission and storage rises, preserving image confidentiality, integrity, and authenticity becomes paramount. Text associated with an image, such as authentication or author information, can serve as embedded data. The recipient must adeptly recover both the concealed data and the original image. Reversible data-hiding techniques ensure the exact recovery of the original carrier after extracting the encrypted data. Classification of RDHEI techniques is based on the implemented method employed. This paper delves into a comprehensive exploration of techniques applicable to difference expansion, histogram shifting, and compression embedding for reversible data hiding. Emphasis is placed on the necessity for a reversible data-hiding technique that meticulously restores the host image. Furthermore, the study evaluates performance parameters associated with encryption processes, scrutinising their security aspects. The investigation utilises the MATLAB tool to develop the proposed BBET technique, comparing its efficacy in embedding and achieving enhanced security features. The BBET technique is characterised by reliability, high robustness, and secure data hiding, making it a valuable addition to the evolving landscape of reversible data hiding methodologies.

Keywords: Reversible Data Hiding, Image Encryption, Image Decryption, Histogram Shifting, MSE Measure, PSNR Measure, Security, RDHEI, BBET.

I. Introduction

In contemporary society, digital media has become an integral aspect of daily life, efficiently stored and delivered with exceptional quality. However, the pervasive use of computer systems makes digital content susceptible to manipulation. The ease of data manipulation and the seamless transmission capabilities of data communication networks raise concerns about protecting intellectual property rights, particularly in digital multimedia distributed over the World Wide Web. The rapid and cost-effective transmission of digital data introduces a heightened risk of unauthorised copying, posing a significant threat to intellectual property rights. Encryption emerges as a vital tool in restricting unauthorised data copying; nevertheless, it alone cannot offer comprehensive protection. Encrypted data, once decrypted, becomes vulnerable to unrestricted distribution or manipulation. Integrating ownership data into multimedia content is a viable solution to address this vulnerability. This embedded data, when extracted, serves as proof of ownership, ensuring the authenticity and integrity of the content. Similar to the commonly used method in bank currency, where a watermark is incorporated to verify the note's authenticity, the multimedia domain adopts a parallel concept known as watermarking. In this context, watermarking plays a crucial role in confirming the genuineness of original digital content [1]. By

incorporating ownership information into multimedia data, this technique not only acts as a deterrent to unauthorised copying but also provides a means to substantiate the legitimacy of the content.

Consequently, the adoption of watermarking techniques emerges as a crucial strategy to fortify intellectual property rights and preserve the integrity of digital multimedia content in the ever-evolving digital communication landscape. Securing information within cover images is fundamental to the reversible data-hiding process. This methodology incorporates secret communication to facilitate the extraction of hidden messages while ensuring the complete restoration of the original image and cover content. The primary objective is to embed additional messages within cover media using a reversible approach, allowing the seamless recovery of the original content post-extraction. Image data hiding has conventionally served the purpose of secret communication.

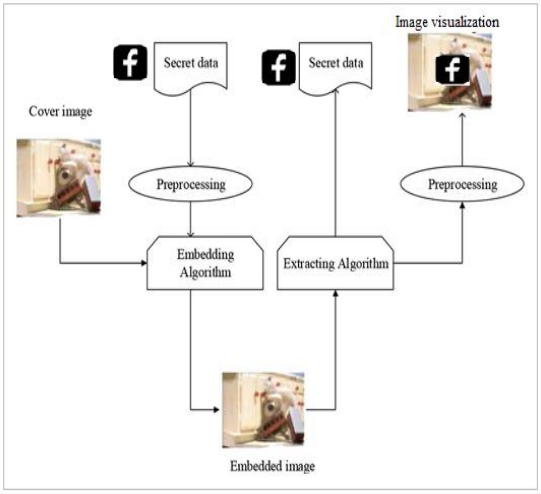


Figure1. reversible data hiding process

Various applications necessitate the encryption of embedded carriers or images to prevent their analysis, thereby safeguarding the covert nature of the embedment. Examples include scenarios where the carrier's owner or image seeks to restrict access to its content, particularly in sensitive contexts like military or secret medical images. Under such circumstances, the content or data owner encrypts the information before handing it over to the data hider for embedment. Several novel reversible data hiding schemes have been proposed, encompassing techniques such as block histogram shifting and data embedding based on 0 and 1 bits. The difference expansion method, utilising histograms and a lossless compression approach, exhibits a lower Peak signal-to-noise ratio (PSNR) and higher Mean Squared Error (MSE) compared to the Block Histogram Shifting (BHS) method [1]. Within the realm of secure data preservation, steganography emerges as a pro-security innovation, embedding confidential information within a cover [2]. This method aligns with reversible data hiding principles, where information bits are inserted into the host signal, allowing for the lossless restoration of the original signal after extracting the embedded information. The ability to precisely recover the original image is important in diverse fields, including legal, medical, and military imaging. An application of reversible data hiding in the realm of document security involves scanning and protecting bank checks using an authentication scheme. These watermarked documents, in most cases, effectively distinguish the document contents. However, the prospect of recovering the original unmarked document adds an intriguing layer to the security paradigm. The block diagram in Figure 1 illustrates the core components of a basic reversible data-hiding system. Notably, existing reversible data hiding schemes often exhibit fragility. Imperceptibility and embedding capacity are two crucial properties evaluated to assess the performance of reversible data-hiding techniques. Imperceptibility measures the similarity between the stego and cover image while embedding capacity gauges the maximum number of information bits seamlessly embedded in the image [3].

1.1 Reversible Data Hiding in Encrypted Images

In the context of RDH-EI (Reversible Data Hiding in Encrypted Images), the process involves implementing reversible data hiding within an encrypted domain. Initially, the content owner encrypts the original image using various encryption methods, forwarding the encrypted image to the data hider. The data hider then employs reversible data-hiding methods to embed additional information into the encrypted image. The receiver can extract the hidden data and decrypt the image upon transmission. Notable methods employed in Reversible Data Hiding include LSB Substitution, Difference Expansion, and Histogram Modification. The encryption phase encompasses two primary types: Symmetric encryption (Private key cryptography) and Asymmetric encryption (Public key cryptography) [4]. Three integral parties are involved in this process: the content owner, the data hider, and the receiver. To delve into specifics, the content owner encrypts the original image using an encryption

key, creating the encrypted image. Subsequently, the data hider embeds additional data into the encrypted image using a designated data hiding key.

Upon receiving the encrypted image with embedded data, the receiver extracts the hidden information and initiates image recovery. The encryption process entails an Exclusive Or operation between original and pseudo-random bits generated using the encryption key. The XOR results from various pixels are then concatenated in an orderly fashion. During data embedding, the data hider segments the encrypted image into non-overlapping blocks of size s*s. Based on a data-hiding key, each block is divided into groups, s0 and s1. Subsequently, the hider flips a small part of the encrypted image to embed additional data. If the data to be embedded is 0, the hider flips the 3 LSB bits of the encrypted pixel in s0.

Conversely, if it is 1, the hider flips the 3 LSB bits of the pixel in s1, with the remaining encrypted data unchanged. For data extraction and image recovery, the receiver, in possession of the encrypted image with embedded data, initiates the decryption process. This involves performing XOR operations between the bits of the encrypted image and pseudo-random bits generated using the encryption key. The 5 MSB bits of each pixel are then received correctly. In the subsequent data extraction step, the decrypted image is divided into different blocks, and the pixels of each block is further divided into two parts, namely s0 and s1 [5].

1.2 Characterised of RDHEI

Reversible Data Hiding (RDH) is a technique that aims to restore the original image with minimal distortions and satisfactory quality following the extraction of concealed data, rendering it increasingly popular. RDH in Encrypted Images (RDHEI) techniques have garnered attention for their effectiveness. From a secure communication system perspective, RDHEI involves embedding digitised information within an image so that only an authenticated party can extract the concealed data, restoring the original image. An information hiding system can be assessed and characterised based on four fundamental aspects [6]:

1. Capacity pertains to the quantity of hidden information the cover media can accommodate. In the context of RDHEI, the system's capacity determines the volume of concealed data that can be seamlessly integrated into the image without compromising its integrity.

2. Security: Security features are incorporated to safeguard the extraction of hidden information from potential threats posed by unauthorised access or hacking attempts. The robustness of security measures ensures that only authenticated parties can successfully extract the concealed data.

3. Perceptibility: This aspect refers to the system's ability to conceal information discreetly, minimising any noticeable impact on the image's visual quality. An effective RDHEI system should invisibly embed information in the human eye, maintaining the natural appearance of the cover media.

4. Robustness: The system's robustness measures its resilience against modifications applied to the stego medium. In the context of RDHEI, the hidden information must remain intact even when the stego medium undergoes alterations, ensuring the integrity of the concealed data despite external modifications.

II. Related Work

Reversible Data Hiding (RDH) has been a longstanding concept, with researchers exploring various methods to enhance its characteristics, particularly in the context of encrypted images. This section provides an overview of different RDH methods applied to encrypted images, showcasing the evolution and advancements in this field over the years. In the study conducted by Yu, Chunqiang et al. [7], Reversible Data Hiding in Encrypted Images (RDHEI) is recognised as an effective data security technique. Despite the effectiveness of RDHEI, many contemporary methods in this domain fall short of achieving a desirable payload. In response to this limitation, the researchers propose a novel RDHEI method with hierarchical embedding, making two key contributions. Firstly, the paper introduces a novel technique for hierarchical label map generation tailored to the bit-planes of the plaintext image. This hierarchical label map is computed using prediction techniques, subsequently compressed, and embedded into the encrypted image. Secondly, the proposed hierarchical embedding is designed to maximise the embedding payload. This technique categorises prediction errors into three magnitudes: small, medium, and large. Each magnitude is assigned different labels. Notably, this approach

differs from conventional techniques, as pixels with small and large magnitude prediction errors are utilised to accommodate secret bits in the hierarchical embedding process. Collectively, these innovations enhance the overall effectiveness and payload capacity of the RDHEI method. In the work by W. Puech et al. [8], the authors propose an analysis based on the local standard deviation of marked encrypted images. This analysis removes embedded data during the decryption step, contributing to the protection of multimedia content. The approach is rooted in Encryption and watermarking algorithms that adhere to Kirchhoff's principle. According to this principle, all algorithm details are known, with only the encryption and decryption keys being kept confidential. The paper addresses three primary challenges. The first challenge arises in homogeneous zones, where all blocks within these zones are encrypted uniformly. The second challenge is the lack of robustness in block encryption methods against noise. Due to the substantial size of the blocks, encryption algorithms (both symmetric and asymmetric) per block struggle to maintain resilience in noisy conditions. The third challenge relates to data integrity. The authors argue that amalgamating encryption and data-hiding techniques can effectively address these problems. Consequently, the proposed reversible data hiding method enables data embedding in encrypted images. During the decryption process, the embedded data is removed, facilitating the reconstruction of the original image. However, the authors acknowledge a limitation – this approach may not be suitable for high-capacity reversible data-hiding methods in encrypted images. In the study by Q. Ying et al. [9], the traditional focus of Reversible Data Hiding (RDH) on enlarging embedding payloads while minimising distortion, typically measured by the mean square error (MSE) criterion, is revisited. Recognising that imperceptibility can also be attained through image processing, the authors propose a novel RDH method with contrast enhancement (RDH-CE) using histogram shifting. The proposed RDH-CE method is structured in two key parts: baseline embedding and extensive embedding. In the baseline phase, the authors initially merge the least significant bins to create spare bins, followed by embedding additional data using a histogram-shifting approach employing arithmetic encoding. During histogram shifting, a transfer matrix is constructed by maximising the entropy of the histogram. The outcome of this process is a marked image containing additional data with higher contrast than the original image. The extensive embedding part involves concatenating the baseline embedding with an MSE-based embedding. On the recipient side, the proposed method allows for the exact extraction of additional data, enabling the lossless recovery of the original image. Comparative analysis with existing RDH-CE approaches demonstrates that the proposed method achieves a superior embedding payload, providing advancements in reversible data hiding with contrast enhancement. In the work by Jun Tian et al. [10], the authors propose a method for reversible data embedding, also known as lossless data embedding. This technique involves embedding invisible data into a digital image in a reversible manner, ensuring minimal quality degradation on the image after data embedding. The hallmark of reversible data embedding is its unique property of reversibility, enabling the extraction and removal of embedded data, ultimately restoring the original image. This distinguishing feature sets reversible data embedding apart, emphasising its capacity to recover the initial content seamlessly without permanent alteration. A common strategy in high-capacity reversible data embedding is to select an embedding area, such as the least significant bits of certain pixels in an image, and embed both the payload and the original values into this area. This ensures the exact recovery of the original image from the embedded data. The authors introduce the Difference Expansion (DE) technique as part of this method, which explores the redundancy in image content to discover extra storage space. DE is employed to embed a payload into digital images reversibly. The primary significance of this method lies in its payload capacity limit and the visual quality of the embedded images. However, the authors acknowledge a potential fragility in the technique. In cases where the embedded image undergoes manipulation or lossy compression, the decoder can detect that it is not authentic, leading to the inability to restore the original content. This underscores reversible data embedding limitations in scenarios where authenticity preservation is critical, especially under external modifications. In the study by C. Yu et al. [11], reversible data hiding is a significant aspect of data concealment. The paper introduces a novel approach to separable and error-free reversible data hiding within an encrypted image, focusing on two-layer pixel errors. The proposed scheme begins by dividing the original image into non-overlapping blocks, followed by the permutation of these blocks. Subsequently, a closed Hilbert curve scans each block, generating a

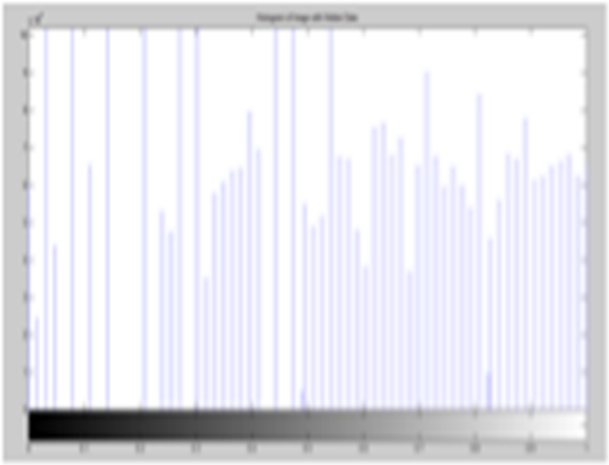
one-dimensional pixel sequence. The pixels within this sequence are encrypted with key transmission. During the data hiding process, each non-overlapping block of the encrypted image is scanned in the closed Hilbert order to create a one-dimensional encrypted pixel sequence. The scheme then leverages the histogram of two-layer adjacent encrypted pixel errors for embedding secret data through histogram shifting, generating a marked encrypted image. The effectiveness of the proposed scheme is validated through numerous experiments, demonstrating its ability to achieve a high payload. Furthermore, the results indicate that the proposed scheme outperforms some existing reversible data-hiding schemes specifically designed for encrypted images. In Zhang *et al.* [12] presented an RDHEI that instead of directly embedding data in encrypted images, some pixels are predicted before encryption so that the secret data can be embedded in the prediction errors. Thus, some of these prediction errors will not be encrypted. In the research by Shuang Yi et al. [13], the original methodology involves randomly selecting pixels from an original image to obtain estimation errors for secret data embedding. However, their proposed approach aims to enhance the maximum embedding rate while maintaining a high image quality of the marked decrypted image. In this new method, half of the pixels in the original image are estimated to obtain the necessary estimation errors. The encryption process involves encrypting both the estimation errors and the remaining pixels. The data hider subsequently embeds the secret data into the encrypted estimation errors and scrambles the image using a shared key. On the recipient side, the secret data and the original image can be extracted and recovered separately, facilitated by using different security keys. In the work by Xu Wang et al. [14], a Reversible Data Hiding in Encrypted Images (RDHEI) scheme is reported, leveraging the correlation between sample pixels and non-sample pixels. Sample pixels, acting as reference points, are used to calculate prediction errors for non-sample pixels. A stream cypher is applied to encrypt sample pixels, while a specific encryption procedure is devised for encrypting prediction errors of non-sample pixels. Notably, some prediction errors that occur more frequently are intentionally left unencrypted. This strategic approach involves a modified version of histogram shifting and the difference expansion technique. The scheme ensures that a part of the prediction errors remains unencrypted, contributing to the overall effectiveness of the RDHEI method. In the work by Zhaoxia Yin et al. [15], a new detachable RDHEI framework is proposed and evaluated. This framework allows additional data to be embedded into a cypher image that was previously encrypted using Josephus traversal and a stream cypher. A Block Histogram Shifting (BHS) approach, utilising self-hidden peak pixels, is adopted for reversible data embedding. Depending on the keys held, legal receivers can either extract only the embedded data with the data-hiding key or decrypt an image closely resembling the original image with the decryption key. If both keys are available, they can extract the embedded data and recover the original image error-free. The results demonstrate a higher data embedding capacity, superior decrypted-marked-image quality, error-free data extraction, and accurate image reconstruction. In the work by Yin et al. [16], an RDHEI method is devised based on Multiple Most Significant Bit Predictions and Huffman Coding (MMPHC). This method compares the original and predicted pixel's most significant bit (MSB). The bits of the same sequence are then utilised as a label, and the pixel is marked with a pre-defined Huffman code. However, experimental results indicate that pre-defined Huffman encodings do not perform well in marking. Further refinements and optimisations are explored to leverage the correlation of adjacent pixels.

Table 1 Description of all RDHEI Related Work

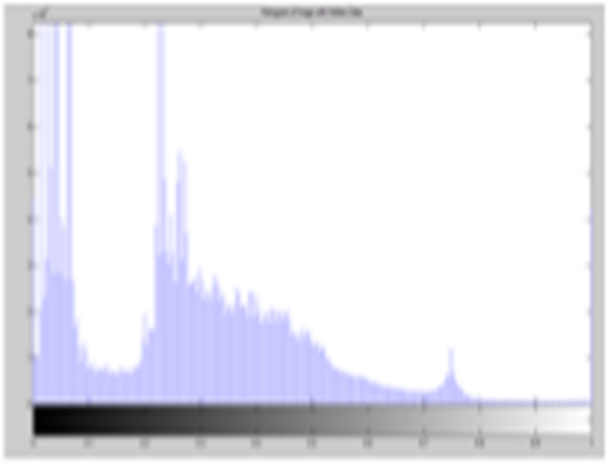
Ref.	Year	Title	Description
[7]	2021	Reversible data hiding with hierarchical embedding for encrypted images	Low PSNR And high error rate (MSE)
[8]	2020	A Reversible Data Hiding Method for Encrypted Images	high error rate (MSE), block effect and low robustness
[9]	2019.	Reversible Data Hiding with Image Enhancement Using Histogram Shifting	block effect based on block shifting Low PSNR And high error rate (MSE)
[10]	2003	Reversible data embedding using a difference expansion	high error rate (MSE), block effect and low robustness

[11]	2018	Separable and Error-Free Reversible Data Hiding in Encrypted Image Based on Two-Layer Pixel Errors	Low PSNR And high error rate (MSE)
[12]	2014	Reversibility improved data hiding in encrypted images	block effect based on block shifting Low PSNR And high error rate (MSE)
[13]	2015	An Improved Reversible Data Hiding in Encrypted Images	Low PSNR And high error rate (MSE)
[14]	2016	Separable and error-free reversible data hiding in encrypted images	Not error-free also has Low PSNR And high error rate (MSE)
[15]	2016	Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting	block effect based on block shifting Low PSNR And high error rate (MSE)
[16]	2020	Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding	Low PSNR And high error rate (MSE)
[17]	2016	Reversible data hiding in encrypted images by reversible image transformation	Not properly encrypted image, low robustness quality image and more error
[18]	2018	An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images	Not efficient MSB, low robustness quality image and more error
[19]	2007	Digital Watermarking and Steganography	Low PSNR And high error rate (MSE)
[20]	2014	Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme	Lossless Data Hiding, low robustness quality image and more error
[21]	2014	A Survey on Separable Reversible Data Hiding in Encrypted Images	block effect based on block shifting Low PSNR And high error rate (MSE)
[22]	2006	Reversible data hiding	low robustness quality image and more error
[23]	2014	Histogram Shifting based reversible data hiding	block effect based on block shifting Low PSNR And high error rate (MSE)
[24]	2013	Study on Separable Reversible Data Hiding in Encrypted Images"	Low PSNR And high error rate (MSE)
[25]	2008	DWT-DCT-SVD based watermarking	low robustness quality image and more error
[26]	2016	Digital Image Watermarking Techniques and Applications: A Survey	block effect based on block shifting Low PSNR And high error rate (MSE)
[27]	2015	Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation	Low PSNR And high error rate (MSE)
[28]	2014	Secure Data Transmission Using Reversible Data Hiding	block effect based on block shifting Low PSNR And high error rate (MSE)

[29]	2012	Separable reversible data hiding in the encrypted image,	Not properly encrypted image, low robustness quality image and more error
[30]	2013	A reversible data hiding method by histogram shifting in high-quality medical images	low robustness quality image and more error



Output Based on RDHEIT



Output Based on BBET

Figure 2 Histogram output based on RDHEIT and BBET in the First Experimentation.

III. Result Analysis

In the concluding phase of our dual analyses, we meticulously assessed the outcomes based on two pivotal parameters: PSNR (Peak Signal-to-Noise Ratio) and MSE (Mean Squared Error). The first experimentation revolved around a cover image utilising Chandrayaan-3 Rover imagery, featuring a JPG format, a size of 104 KB, and dimensions of 1500 x 1000. The corresponding data image incorporated ISROLOG images, characterised by a JPG format, a size of 12.7 KB, and dimensions of 228 x 221. The Chandrayaan-3 cover and ISROLOG data images were integral to the experiment. The comprehensive analysis culminated in the presentation of Figure 2 and Figure 3, depicting the output in terms of PSNR and MSE. Significantly, the new technique demonstrated a higher PSNR than the old one, indicating superior image quality preservation. Conversely, the MSE was lower in the new technique but higher in the old technique, underscoring the former's efficacy in minimising errors. This thorough examination highlights the advantageous performance of the new technique over its predecessor.

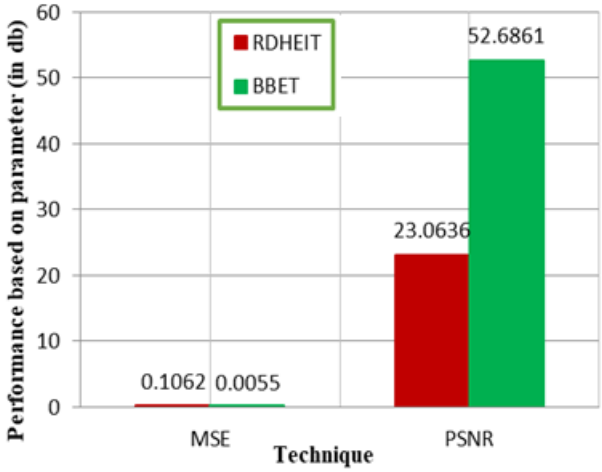


Figure 3 output analysis based on two-parameter MSE and PSNR in Experimentation1

In the subsequent phase of our analysis, we directed our attention to another experiment focused on a cover image incorporating COVID-19 vaccine imagery. The cover image was characterised by a JPG format, a size of 414 KB, and dimensions of 1050 x 600. The associated data image utilised vaccine logo images featuring a JPG format, size 7.95 KB, and dimensions 225 x 225. The COVID-19 vaccine cover image and the vaccine logo data image played crucial roles in this experiment. The conclusive results were visually presented in Figure 4 and Figure 5, illustrating the output concerning PSNR and MSE. Remarkably, the new technique exhibited a higher PSNR than the old technique, indicative of enhanced preservation of image quality. Conversely, the MSE was lower in the new technique but higher in the old technique, underscoring the former's proficiency in minimising errors. This comprehensive analysis firmly establishes the advantageous performance of the new technique compared to its predecessor,

specifically in the context of the COVID-19 vaccine cover image.

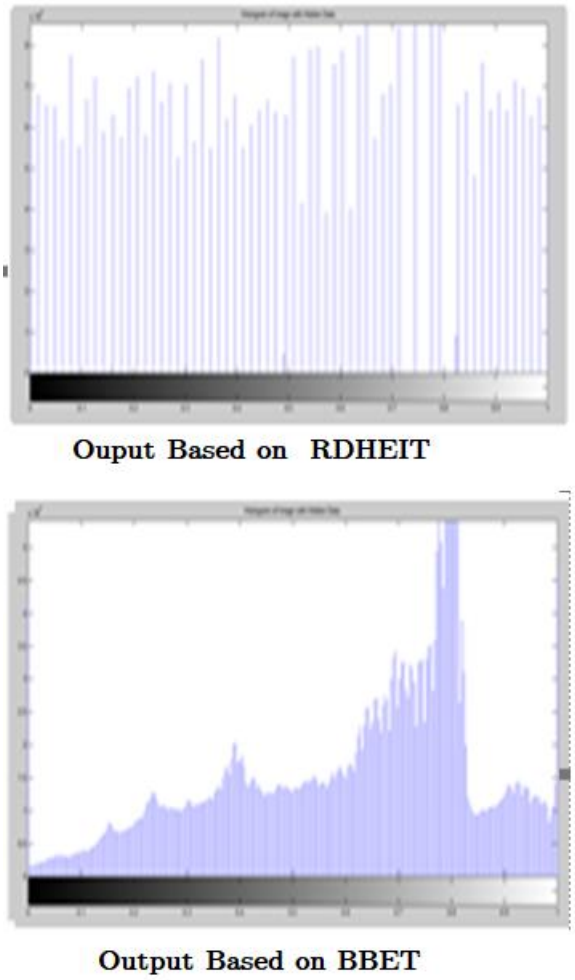


Figure 4 Histogram output based on RDHEIT and BBET in the Second Experimentation.

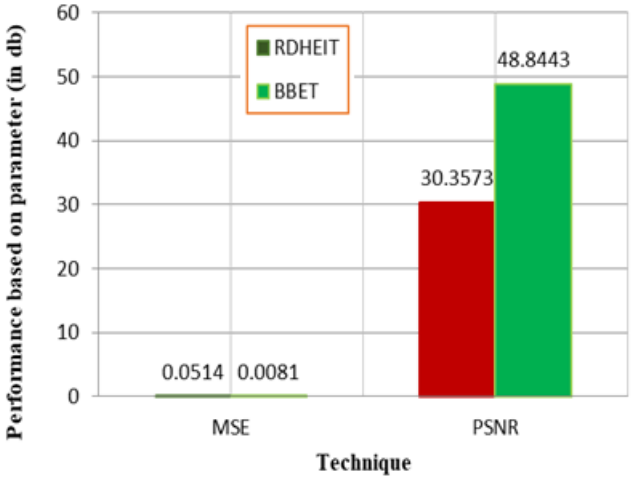


Figure 5 output analysis based on two-parameter MSE and PSNR in Experimentation2

V. Conclusion

In conclusion, this study presents an enhanced reversible data-hiding method employing hierarchical embedding for encrypted images, focusing on the Binary Bit Embedding Technique (BBET). The increasing popularity of reversible data-hiding methods stems from the inherent reversibility of the carrier medium, facilitating the retrieval of secret data at the receiving end. Performance assessment factors include the image's visual quality and the algorithmic complexity. Within the realm of reversible data hiding techniques, this research investigates various approaches, specifically focusing on schemes tailored for encrypted images that require minimal Peak Signal-to-Noise Ratio (PSNR) computation. The analytical framework encompasses image cryptography, data activity, and data extraction/image recovery phases. The encryption of initial images is executed through a cryptography strategy, allowing the data hider to embed additional information without knowledge of the original image content. Importantly, data extraction and image recovery processes can be conducted independently. This study delves into the analysis of reversible data hiding errors, identifying image blocks that necessitate evacuation before encryption, albeit with a trade-off between low PSNR and high Mean Squared Error (MSE). These block features are pivotal in hierarchically embedding and extracting data, encompassing themselves and the concealed information.

As explored in this paper, reversible data hiding techniques serve the dual purpose of concealing secret information within cover images and facilitating the recovery of the cover image post-extraction of the secret message. Applying Reversible Data Hiding (RHD) on encrypted images adds a layer of security by concealing the original content from unauthorised access. In particular, the study scrutinises various methods to comprehend how information is embedded in graphical representations. The proposed Binary Bit Embedding Technique (BBET) stands out, showcasing the content owner's perfect reconstruction of the original image, eliminating the need for a data hider key. Furthermore, BBET demonstrates increased PSNR and reduced MSE, indicating superior performance compared to older techniques. The BBET technique is a reliable, highly robust, and secure data-hiding. Noteworthy improvements in PSNR and MSE metrics underscore its efficacy, positioning it as a promising advancement in reversible data hiding for encrypted images.

References

[1] Zhang, X., Reversible data hiding in encrypted image. IEEE Signal Processing Letters, 18(4), 255-258, 2011.

[2] Puech, William, Marc Chaumont, and Olivier Strauss. "A reversible data hiding method for encrypted images." In security, forensics, steganography, and watermarking of multimedia contents X, vol. 6819, pp. 534-542. SPIE, 2008.

[3] Ma, Kede, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li. "Reversible data hiding in encrypted images by reserving room before encryption." IEEE Transactions on Information Forensics and Security 8, no. 3: 553-562, 2013.

[4] 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.

[5] Awrangjeb, Mohammad. "An overview of reversible data hiding." In Proceedings of the Sixth International Conference on Computer and Information Technology, pp. 75-79,2003.

[6] Wang, Junxiang, Jiangqun Ni, Xing Zhang, and Yun-Qing Shi. "Rate and distortion optimisation for reversible data hiding using multiple histograms shifting." IEEE Transactions on Cybernetics 47, no. 2: 315-326, 2016.

[7] 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.

[8] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Images", SPIE, IS & T'08: SPIE Electronic Imaging, Security, Forensics, Steganography and Watermarking of Multimedia Contents, San Jose, CA, USA.

[9] Q. Ying, Z. Qian, X. Zhang and D. Ye, "Reversible Data Hiding with Image Enhancement Using Histogram Shifting," in IEEE Access, vol. 7, pp. 46506-46521, 2019.

[10] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transaction on Circuits and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 - 896.

[11] C. Yu, X. Zhang, Z. Tang and X. Xie, "Separable and Error-Free Reversible Data Hiding in Encrypted Image Based on Two-Layer Pixel Errors," in IEEE Access, vol. 6, pp. 76956-76969, 2018.

[12] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Processing, vol. 94, no. 1, pp. 118-127, Jan. 2014.

[13] Shuang Yi, Yicong Zhou" An Improved Reversible Data Hiding in Encrypted Images" Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on, Pages:9, 2015.

[14] D. Xu, and R. Wang, "Separable and error-free reversible data hiding in encrypted images," Signal Processing, vol. 123, pp. 9-21, Jun. 2016.

[15] Zhaoxia Yin, Andrew Abel, Xinpeng Zhan, Bin Luo "Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting "Acoustics, Speech and Signal Processing (ICASSP), IEEE International Conference on,2129-2133, 2016.

[16] Z. Yin, Y. Xiang and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," IEEE Transactions on Multimedia, vol. 22, no. 4, pp. 874–884, 2020.

[17] Zhang, Weiming, Hui Wang, Dongdong Hou, and Nenghai Yu. "Reversible data hiding in encrypted images by reversible image transformation." IEEE Transactions on Multimedia 18, no. 8: 1469-1479, 2016.

[18] Puteaux, Pauline, and William Puech. "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images." IEEE Transactions on Information Forensics and Security 13, no. 7 1670-1681, 2018.

[19] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking and Steganography, Morgan Kaufmann, 2nd edition, 2007.

[20]] Nutan Palshikar, Prof. Sanjay Jadhav, "Lossless Data Hiding using Histogram Modification and Hash Encryption Scheme", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 4, Issue 1, 2014.

[21] Mithu Varghese, Teenu S Jhon, " A Survey on Separable Reversible Data Hiding in Encrypted Images", International Journal of Computer Applications Advanced Computing and Communication Techniques for High-Performance Applications,0975 – 8887,2014.

[22] Z. Ni, Y. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on

Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

[23] L. R. Mathew, A. C. Haran V., "Histogram Shifting based reversible data hiding", IJETT, pp. 482-485, 2014.

[24] Rini. J, 4th Semester M.Tech, Dept. of Computer Science and Information Systems FISATAngamaly, Kerala, India "Study on Separable Reversible Data Hiding in Encrypted Images" International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013 Copyright © 2013 SciResPub. IJOART.

[25] K. A. Navas, M. C. Ajay, M. Lakshmi, T. S. Archana, and M. Sasikumar, "DWT-DCT-SVD based watermarking," in Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on, 2008, pp. 271–274.

[26] Chauhan Usha, Singh Rajeev Kumar, "Digital Image Watermarking Techniques and Applications: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016.

[27] Jiantao Zhou, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang, "Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation", IEEE transactions on circuits and systems for video technology,2015.

[28] Ashwind S, Ganesh K, Gokul R and Ranjeeth Kumar C, "Secure Data Transmission Using Reversible Data Hiding", International Journal of Computer Science and Information Technologies, Vol. 5 Issue 2 pp. 861-1863, 2014.

[29] X. Zhang, "Separable reversible data hiding in the encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[30] M.S Hwanga, L.Y. Tsengb, LC Huang, "A reversible data hiding method by histogram shifting in high-quality medical images", Journal of Systems and Software, Vol. 86, (3), pp. 716–727, 2013.