



Reversible Data Hiding using Multi-MSB Technique

Priyanka V. Deshmukh^{1*}, Avinash S. Kapse², V. M. Thakare³, Arvind S. Kapse⁴

Abstract

Data-hiding technology performs an important role in fields of image such as copyright identification and annotation. Methods of data hiding that have been used in the previous article result in persistent visual distortion. Each pixel of an image is critical in the legal, medical, and military domains, and image distortion is intolerable. Reversible Data-Hiding (RDH) approach has sparked attention as a result. Data may be hidden using RDH algorithms, and the original images may be retrieved without instigating any damage. Early RDH approaches were unable to deliver satisfactory results. Consequently, for secure data image transfer, the article suggested the High-Capacity Reversible Data Hiding in Encrypted Images (RDH-EI) approach. The main idea underlying RDH-EI is that a cover image is converted into unreadable format and then concealed information is hidden in the encrypted image using a data hider. The inserted data from the hidden image may be recovered using the information hiding key, and the encryption key may be used to rebuild the original image. The original image was pre-processed by the content owner to free up hiding space in the RRBE scheme, following which the image will be encrypted and transferred to the data hider. Initially, to offer authenticity and integrity, Elliptic Curve Cryptography (ECC) is proposed to encrypt, decrypt, and authenticate the cipher image. The encrypted images are then sent on to the data hiding step. A considerable amount of data is employed to embed in the image encryption domain in data hiding. Subsequently, a Multi-MSB (Most Significant Bit) data hiding scheme was developed to increase capacity. With encryption quality, the suggested approach achieves an embedding capacity of more than 1 bpp (bits per pixel). The additional data may be taken from the indicated encrypted image after the decoding process, finally restoring the original image. The experiment was carried out in MATLAB software using a built-in function. The efficacy of the stego image may be tested using typical Peak Signal to Noise Ratio (PSNR) methods to gauge image quality. The suggested approach can achieve huge embedding capacity, excellent security, and image quality, according to the experimental findings. The findings reveal that the suggested method outperforms conventional RDH strategies in terms of embedding performance. This demonstrates that the suggested scheme's embedding rate is 3.6 bpp respectively, which ensures the security of the hidden data.

5004

KeyWords: Reversible Data Hiding, Image Encryption, Elliptic Curve Cryptography, Multi MSB Prediction, Image Security, Hiding Capacity, Location Map

DOI Number: 10.14704/nq.2022.20.8.NQ44526

NeuroQuantology2022; 20(8):5004-5012

Introduction

Digital data transfer through the Internet is becoming a critical component of modern civilization. With the rise of digital data transmission, researchers are faced with a difficult task: ensuring the security of digital information transmitted via the network [1]. The security systems for digital information are determined by the needs of the users, such as the protection of

original digital information, authentication-based security, and security in a non-obtrusive manner. The security system's fundamental goal is to create a safe digital data connection between sender and recipient over the Internet [2]. The technique of transforming plaintext messages into ciphertext messages is known as cryptography.

Corresponding author: Priyanka V. Deshmukh

Address: ^{1*}Assistant Professor, Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Maharashtra 444203, ²Associate Professor & Head, Dept. of IT, Anuradha College of Engineering, Chikhali, Maharashtra 443201, ³Professor & Head, Dept. of CSE, Sant Gadge Baba Amravati University, Amravati, Maharashtra 444602, ⁴Professor, New Horizon College of Engineering, Bengaluru, Karnataka 560103

E-mail:

priyanka8deshmukh@gmail.com



To keep them safe and immune to assaults, and only authorized users may access the message using a key, intruders can cryptanalysis the ciphertext. On the other hand, data hiding techniques improve the security of secret information by converting it into unreadable format in a digital medium known as the "host" or "cover" media and without creating perceptual changes, its contents can be modified [3].

Reversible Data Hiding

Encryption, mathematics, computer vision, and computer application technology are all used in data hiding, which is a multidisciplinary topic of information security. Its major purpose is to safeguard communication, copyright maintenance, and other services by using carrier data redundancy to transmit or conceal secret information [4]. It is a necessary piece of research in the information security field. Traditional data concealing techniques like Reversible Data Hiding (RDH), steganography, and watermarking have certain unique features [5]. Steganography is a type of covert Internet communication in which hidden digital information is silently placed in covering media consequently that the opponent is unaware of its presence. Digital watermarking, on the other hand, focuses on how to reliably retrieve inserted data from potentially damaged manifest media. RDH focuses on recovering both embedded information and input images from marked media in a lossless way [6]. This was utilized widely in various sectors such as military imagery, law, medical images, and forensics it plays a crucial part in some delicate settings. Traditional information hiding is primarily associated with irreversible data hiding [7]. This will produce irreversible changes to the image and other carriers during the process of embedding and extracting new information, and its application situations are restricted. RDH was initially proposed by Barton [8].

There have been a lot of RDH algorithms for plaintext images proposed so far. The following strategies are often used in classic RDH algorithms includes Pixel Value Ordering (PVO), Different Expansion (DE), modification of prediction errors, and Histogram Shifting (HS) [9]. To hide a hidden message, all of these approaches rely on information redundancy and spatial correlation between the cover image pixel values. RDH is divided into four domains: compressed, spatial, frequency, and encrypted. Due to correlations, these algorithms are unable to function directly on

encrypted images, and redundancy cannot be retained after encryption [10].

Reversible Data Hiding in Encrypted Images (RDH-EI)

Due to the increasing popularity of cloud-based services in recent years, users rely on a cloud server to store their multimedia files. The cloud server allows access to the uploaded multimedia files at any time and from any location [11]. Apart from that, consumers want cloud servers to protect their original multimedia assets. In this context, RDH-EI has increased popularity. Using this method, the content owner inserts extra information into the cover media (image, music, video), after which the receiver may retrieve lossless embedding of new information and original media from the given media [12]. This not only ensures protection from third parties but also allows the data hider/cloud service provider to add new data to it without knowing the original media content [13]. The receiver may also recover the original media as well as any new data that was inserted. Two important metrics for proving the performance of RDH-EI systems are the visual quality and the Embedding Rate (ER) of the instantly decrypted image [14]. Nonetheless, the quality of the image is evaluated in decibels (dB) as the Peak Signal to Noise Ratio (PSNR), while the Embedding Rate is measured in bits per pixel (bpp). Process distortion is created during embedding, causing the PSNR of the immediately decrypted image to be impacted by the embedding rate. For a successful RDH-EI approach, researchers must maintain an ideal balance between PSNR and ER of directly decrypted images [15].

Therefore, the suggested approach presents a unique RDH-EI technique for increasing image capacity while preserving good image quality when recovered (PSNR). The rest of the article is organized as follows: a literature survey of related studies, are presented in section 2. The proposed strategy is detailed in Section 3. Section 4 shows the experimental findings and performance comparisons on Embedding Rate and PSNRs with several state-of-the-art systems. Section 5 ends with a conclusion.

Literature Survey

This section provides an overview of past RDH strategies. RDH is a technique for retrieving the original cover material without loss after extracting the embedded data. It's commonly used in



industries where the original cover image has no manipulation is acceptable, such as images in the field of medical, military, and legal forensics.

The RDH-EI approach, which uses the Median Edge Detector (MED) was proposed by Rui Wang et al [16]. For the original pixels, create the predicted values and quantify prediction errors, the Median Edge Detector prediction technique is employed. Most prediction errors are encoded using the adaptive-length two's complement. The two's complement is labelled in the pixels to reserve a room. A labelled map is created and inserted into the image to capture the unlabeled pixels. The image can then be incorporated with the data after it has been encrypted. On the three datasets, the suggested technique can achieve an average embedding rate according to the result findings.

To accomplish high level data embedding capacity in encrypted images, Shaowei Weng et al [17] presented the RDH-EI approach, which combines GCC (Group Classification Encoding) with SIBRW. There are sixteen image-based rearrangement algorithms in this technique. Each SIBRW approach aims to bring strongly correlated bits from each higher bit plane. By exploiting a strong correlation between neighbouring groups, GCC may compress not just a huge number of groups whose bits have a value of one (or 0), however, still contain a big quantity of embedding space. The security is improved by the encryption mechanism, which includes scrambling operations and bit-level XOR encryption. The results of the experiments reveal that the suggested system is capable of huge embedding capacity and good security.

In encrypted images, Sisheng Chen et al [18] addressed an RDH technique in which the information hiding key is not necessary at any point in time. Reserve embedding room relies on the pixel values congruence relations inside image blocks prior to image encryption. The original image is further converted into unreadable format using a multi-secret image encryption approach based on additive homomorphism-satisfying. Without utilizing a data concealing key, insert the confidential information straight into the unreadable format images in the given embedding room. By examining the congruence connection between pixel values in an unreadable format image block, the secret information might be extracted by the recipient.

Zhaoxia Yin et al [19] introduced the RDH-EI technique of multi-MSB (most significant bit) planes. The projected value is first calculated using

the predictor as median edge detector (MED). Next, unlike earlier techniques, the suggested method uses a one-bit plane to indicate signs of Prediction Errors (PEs), while other bit planes are used to represent absolute values of PEs. Thereafter, rearrange bit planes by dividing them into non-uniform and uniform blocks. Finally, varying numbers of extra data are adaptively integrated according to different pixel prediction techniques. By taking consideration existing approaches, the experimental findings show whether the method has a greater embedding capacity.

For encrypted images with separability, Dawen Xu et al [20] presented the high-capacity RDH approach. The image is initially separated into non-overlapping parts, with each block using the same random value to encrypt it. The benefit is that the relationship between neighbouring pixels may be maintained. The data-hider may insert extra data into unreadable format images without having access to the information of the original image by using difference expansion and histogram shifting. At the receiving end, the original image and the embedded supplemental data may be retrieved in an error-free and inseparable manner. The suggested scheme's viability and efficiency are demonstrated through experimental findings.

The RDH-EI approach proposed by Xu Wan et al [21] is based on Prediction Error and Block Categorization (PB-RDHEI). By combining a prediction error matrix with a bit planes block classification strategy, which is distinct from standard techniques, to build a newly extent for an unreadable format picture. To optimise the available reserved area, several MSB bit planes can be used to hide more data in each block. Receivers can individually take out the complete new data or get the original picture. The experimental results demonstrate that the suggested method considerably improves the embedding rate and can retrieve the image without loss.

Proposed Research Methodology

Most suitable approaches to guarantee appropriate security in the sphere of data transfer are cryptography and steganography methodologies. Combining steganography with cryptography is a great idea, and images are the most typical steganography cover images. The current research focuses on Reversible Data Hiding (RDH) addressed to achieve major qualities such as improved data security, very high embedding capacity, and good stego image quality. High-Capacity Reversible Data



Hiding in Encrypted Images (RDH-EI) is a method for embedding extra data into an unreadable format image while protecting the image content from disclosure, in response to the advent of cloud

computing and the requirement for content owner privacy. The flow diagram for the proposed work is shown in Figure 1.

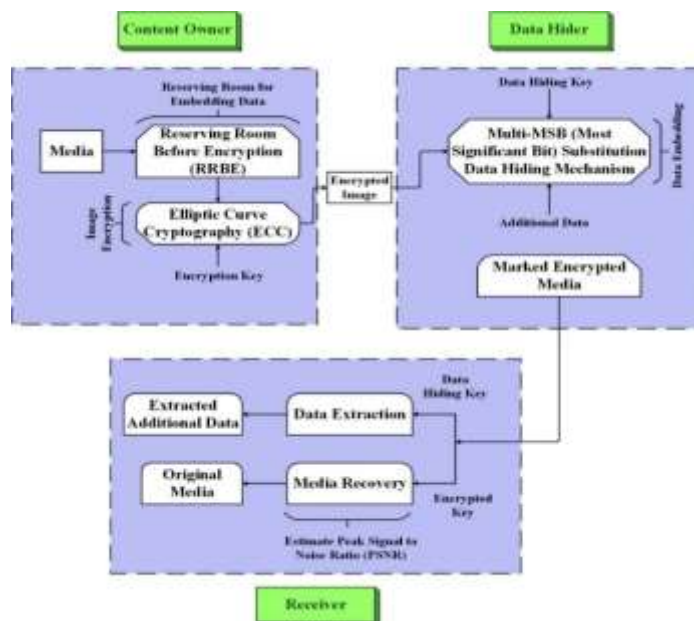


Figure 1: Flow Diagram of the Proposed Work

This section proposed an RDH-EI approach, which may be separated into three sections, as indicated in Figure 1. The embedded room and encryption are the responsibility of the content owner; data embedding is the responsibility of the data hider, and data extraction and image recovery are the responsibility of the receiver. (1) Encrypted image production, (2) data concealment, and (3) data extraction/image recovery are three processes. The content owner first converts the image into unreadable format using an encryption key and then leaves the room to hide it. The confidential data is then hidden in the empty room using a concealing key. At the receiver's end, depending on whatever key(s) they have, they can get different images, such as a directly decrypted image if they only have the encryption key, or concealed secret data if they only have the concealing key. The suggested approach provides for the hiding of a huge quantity of data, as well as a high embedding rate (payload) and good reconstructed image quality (PSNR).

Reserving Room before Encryption (RRBE)

RRBE (Reserving Room before Encryption) approaches were utilized depending on whether the additional data embedding space was created before or after the encryption of the image. Before

employing the RRBE approach to encrypt the original image, the content owner will preprocess it to free up hiding space. RRBE approaches offer the benefit of using the image's redundant space to reserve as the concealing region before encryption, resulting in a much larger hiding space than the previous algorithm.

Encryption Using Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is used to encrypt, decode, and digitally sign the cipher image to assure its validity and integrity. The algebraic structure of elliptic curves over finite fields provides the basis for this public-key cryptography. ECC uses fewer keys to provide equivalent security as non-EC cryptography (such as RSA) and is thus employed when more efficiency or security (through larger keys) is needed.

Multi-MSB (Most Significant Bit) Substitution Data Hiding Mechanism

Multi-MSB substitution depending on the pixel can be used to insert multi-bit data in each encrypted pixel during the embedding phase. The content owner conducts pixel prediction first for the original image size $m \times n$. A data hiding mechanism in the proposed method is meant to forecast

5007



numerous meaningful bit-planes to increase compression performance.

Data Extraction and Reconstruction of Image

The additional message may be derived from indicated unreadable format and the original input image with the encrypted key, which can be recovered without any mistakes, on the recipient's side. Huffman coding rule are extracted by the receiver and the label map from the tagged

encrypted image E_m first. In addition to the label map, the reference pixels and encrypted extra information may be retrieved in the coupled way. Return the reference pixels to the first row and column at the end. The operation mentioned can be performing without the key; however, the next step will provide different results depending on which key the recipient possessed. The inserted information can be accessed by immediately decrypting the extracted unreadable format additional information if the receiver just possesses

the data hiding key D_h . However, the original input image cannot be recreated if there is no use of encryption key. The original input image may be retrieved without loss if the recipient simply possesses the encryption key E_k .

Experimentation And Result Discussion

Several experiments are carried out in this section to assess the suggested system and compare it to existing system. To test the applicability of the suggested approach, the well-known picture dataset UCID is used. Evaluate the simulation results of the suggested technique in Section (a). Previously, Section b contained the proposed scheme's performance and security analyses. In Section c, compare the proposed approach to existing methods techniques in terms of embedding rates.

Simulation Output of the Data hiding Process

The content owner values the privacy of the original input image by using the RDHEI approach. The image below is used as an example to evaluate the method's security, and the argument is $\alpha = 8$. Because of the encryption, this approach is more secure than the previous one. The suggested approach is reversible; in testing findings, the owner converts the image into readable format first, and then extracts the contained information from the decrypted image without error.

5008

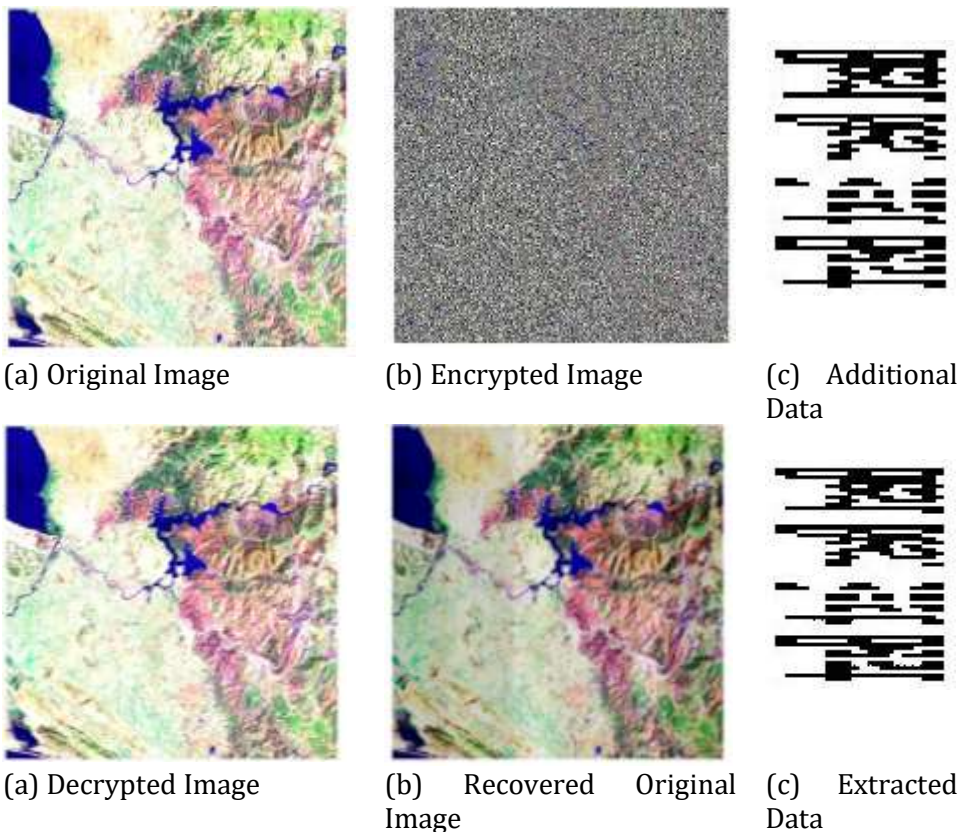
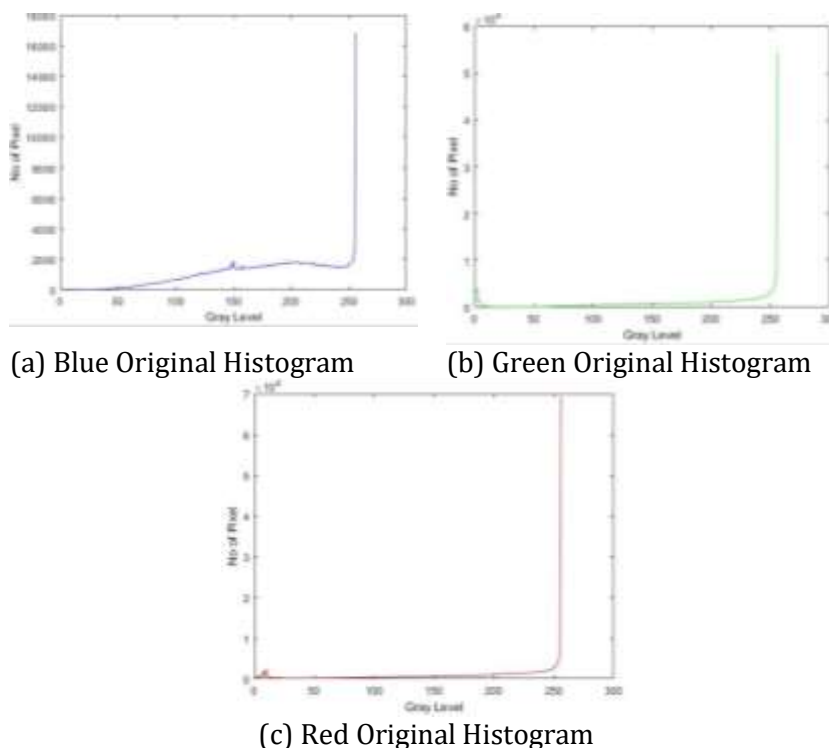


Figure 5: Proposed Method Experimental Results at Different Stages

Figure 5 depicts the experiment's outcomes at various phases. Figure 5a shows the original input image, whereas Figure 5b shows the unreadable format image. Furthermore, the encrypted secret data may be easily recovered from multi-MSB planes according to the embedding capacity, the receiver can restore original data using the data concealing

key. Furthermore, statistical properties of the encrypted image after data embedding remain considerably different from the original, and the distribution of all pixels before and after secret data embedding is almost identical. As a result, obtaining the content of the original image is challenging, demonstrating that the technology is safe.



(a) Blue Original Histogram

(b) Green Original Histogram

(c) Red Original Histogram

Figure 6: Analysis of Histogram in Original (Text) Image

The analysis of the histogram with the frequency of each pixel of the image is shown in Figure 6. The value of each pixel is a perfect cypher image that has a frequency distribution. The pixel distribution in the plain image differs from the histogram of the cypher image, which is distributed identically and gave the cypher image the upper hand.

Performance Metrics of the Proposed Technique

The suggested method's efficiency is calculated through experimental analysis. To demonstrate steganography and study its behavior, a few example images are given as cover images. For performance evaluation, the traditional dataset is employed. This formula is used to find the comparison between the quality of the original and repaired images. The greater the PSNR number, the higher the quality of the restored or reconstructed

image that comes through. To assess performance, the article used two key metrics: PSNR (dB) and embedding rate (bpp). PSNR quantifies the visual quality difference between readable format image and original images, which may be determined using equations ten and eleven. Use the error metrics PSNR and the MSE to compare the image quality. Calculate the mean-squared error first, and then the following equation is used to compute the PSNR value:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (O_{i,j} - D_{i,j})^2 \tag{10}$$

The values M and N represent the number of rows and columns in the input photos, respectively. The PSNR is then calculated using the equation below.



$$PSNR = 10 \log_{10} \frac{(255)^2}{MSE} (dB) \tag{11}$$

The highest fluctuation in the input image is represented by R. Because the image is an 8-bit unsigned integer data format, the value of R is 255.

$$\gamma = \frac{|A|}{M \times N} (bpp) \tag{12}$$

The embedding rate that is nothing but payload is the average number of bits that may be inserted per pixel, and it can be calculated using equation (12), where |A| stands for the length of A.

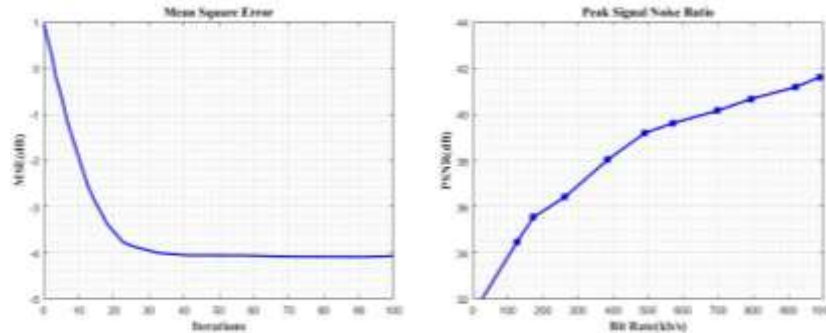


Figure 7: Performance Analysis of MSE and PSNR

Figure 7 illustrates the MSE and PSNR estimated graph. The embedding rate, mean square error, and PSNR have an inverse relationship. The mean square error increases as the embedding rate increases, while the picture quality in terms of PSNR decreases. This shows that for text images, MSE is closer to one at embedding rates of 3.6 bpp, and image quality is greater. Moreover, when compared to other embedding rates PSNR is higher.

over some existing schemes. Simulate the appropriate settings for each comparing scheme to get the best embedding rate. Prediction direction is chosen adaptively for the given picture in the suggested scheme. For the test image, the embedding rates of the scheme are comparing with three comparable schemes [26, 27, 28]. Further, comparing the PSNR values with the existing techniques of [27, 28, 29], the PSNR value was relatively high, compared to the conventional reversible data hiding techniques.

5010

Comparison Analysis of Proposed Technique

Conduct embedding rate comparisons in this part to illustrate the benefits of the proposed procedure

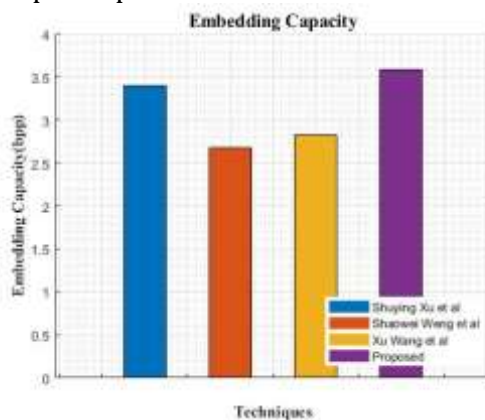


Figure 8: Embedding Capacity Comparison Graph

The highest ERs on the test image of the proposed approach are compared to those of these four methods in Figure 8. The ER of each image acquired by the suggested technique is larger than other

methods, with the ERs of the proposed method reaching 3.6 bpp correspondingly. The suggested approach may greatly enhance the ER, demonstrating that it performs well on any picture.



Except for the MSB plane, the smooth sections in accuracy. the multi-MSB planes match the bigger blocks, implying that the projected multi-MSBs has higher

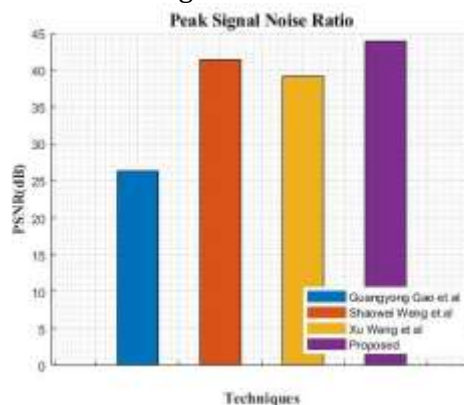


Figure 9: Peak Signal to Noise Ratio Comparison Graph

The proposed method Peak Signal-To-Noise Rate (PSNR) of the restored image comparison is shown in Figure 9. This implies that as long as the encryption keys are known, the original input image may be recovered without loss. The PSNR values of the images obtained using the former algorithm are not as high as those for the images obtained using the proposed method. Compared with other techniques, the proposed methodology has a high PSNR value of 40.895 dB.

Research Conclusion

Authentication, watermarking, encryption, copyright protection, safe data transfer, and other applications all fall under the category of data concealing. Even while steganography cannot be used to replace encryption, it is utilized to increase an individual's privacy by offering secret communication. These techniques are unable to combine a high embedding rate with the excellent reconstructed quality of the image. Subsequently, the article proposed High-Capacity Reversible Data Hiding in Encrypted Images (RDHEI) procedure for secure data image transmission. The main idea underlying RDHEI is that a cover image is converted into unreadable format image, and then concealed information is embedded in the unreadable format image using a data hider. The information hiding key can be used to recover the inserted information from the disguised image, and the key which is used to convert into unreadable format may be used to reconstruct the original image. Preprocessing on the original image is by using content owner to free up the hiding space in the RRBE scheme, after which the image will be encrypted and transmitted to the data hider.

To offer authenticity and integrity, Elliptic Curve Cryptography (ECC) is proposed to encrypt, decode, and digitally sign the cypher image. Further, the encrypted images are sent to the data hiding phase. In data hiding, a large amount of data is used to embed in the image encryption domain. Consequently, proposed a Multi-MSB (Most Significant Bit) substitution data hiding mechanism for enhancing capacity. Following the decoding phase, from the marked unreadable format image, the additional message may be retrieved, and the original input image can be regained without any mistakes. The efficacy of the stego image may be tested by using typical Peak Signal to Noise Ratio methods to gauge image quality (PSNR). The suggested approach may achieve a huge embedding capacity of 3.6 bpp, as well as strong security and picture quality, according to the experimental findings. Furthermore, comparisons of experimental findings show that the suggested approach is capable of achieving a higher ER than existing methods. Future efforts with large amounts of data will need to be hidden by balancing the quality of the recovered image, the resilience of the hidden data, and qualities like separability and commutative.

References

- Wang, J., Chen, X., Ni, J., Mao, N. and Shi, Y., 2019. Multiple histograms-based reversible data hiding: Framework and realization. *IEEE Transactions on Circuits and Systems for Video Technology*, 30(8), pp.2313-2328.
- Fu, Y., Kong, P., Yao, H., Tang, Z. and Qin, C., 2019. Effective reversible data hiding in encrypted image with adaptive encoding strategy. *Information Sciences*, 494, pp.21-36.
- Aziz, F., Ahmad, T., Malik, A.H., Uddin, M.I., Ahmad, S. and Sharaf, M., 2020. Reversible data hiding techniques with



- high message embedding capacity in images. *PLoS One*, 15(5), p.e 0231602.
- Hassan, F.S. and Gutub, A., 2020. Efficient reversible data hiding multimedia technique based on smart image interpolation. *Multimedia Tools and Applications*, 79(39), pp.30087-30109.
- Kumar, R. and Jung, K.H., 2020. Robust reversible data hiding scheme based on two-layer embedding strategy. *Information Sciences*, 512, pp.96-107.
- Wang, J., Mao, N., Chen, X., Ni, J., Wang, C. and Shi, Y., 2019. Multiple histograms based reversible data hiding by using FCM clustering. *Signal Processing*, 159, pp.193-203.
- Kumar, R. and Jung, K.H., 2020. Enhanced pairwise IPVO-based reversible data hiding scheme using rhombus context. *Information Sciences*, 536, pp.101-119.
- Sahu, A.K. and Swain, G., 2019. Dual stego-imaging based reversible data hiding using improved LSB matching. *International Journal of Intelligent Engineering and Systems*, 12(5), pp.63-73.
- Yamac, M., Ahishali, M., Passalis, N., Raitoharju, J., Sankur, B. and Gabbouj, M., 2020. Multi-Level Reversible Data Anonymization via Compressive Sensing and Data Hiding. *IEEE Transactions on Information Forensics and Security*, 16, pp.1014-1028.
- Sahu, A.K. and Swain, G., 2019. High fidelity based reversible data hiding using modified LSB matching and pixel difference. *Journal of King Saud University-Computer and Information Sciences*.
- Malik, A., He, P., Wang, H., Khan, A.N., Pirasteh, S. and Abdullahi, S.M., 2020. High-capacity reversible data hiding in encrypted images using multi-layer embedding. *IEEE Access*, 8, pp.148997-149010.
- Qiu, Y., Qian, Z., Zeng, H., Lin, X. and Zhang, X., 2020. Reversible data hiding in encrypted images using adaptive reversible integer transformation. *Signal Processing*, 167, p.107288.
- Tang, Z., Xu, S., Ye, D., Wang, J., Zhang, X. and Yu, C., 2019. Real-time reversible data hiding with shifting block histogram of pixel differences in encrypted image. *Journal of Real-Time Image Processing*, 16(3), pp.709-724.
- Xu, D. and Su, S., 2019. Separable reversible data hiding in encrypted images based on difference histogram modification. *Security and Communication Networks*, 2019.
- Wu, X., Yang, C.N. and Liu, Y.W., 2020. High capacity partial reversible data hiding by hamming code. *Multimedia Tools and Applications*, 79, pp.23425-23444.
- Fatima, E. and Islam, S., 2019, December. A New High Capacity and Reversible Data Hiding Technique for Images. In *International Conference on Information Systems Security* (pp. 290-304). Springer, Cham.
- Wang, R., Wu, G., Wang, Q., Yuan, L., Zhang, Z. and Miao, G., 2021. Reversible Data Hiding in Encrypted Images Using Median Edge Detector and Two's Complement. *Symmetry*, 13(6), p.921.
- Weng, S., Zhang, C., Zhang, T. and Chen, K., 2021. High capacity reversible data hiding in encrypted images using SIBRW and GCC. *Journal of Visual Communication and Image Representation*, 75, p.102932.
- Chen, S., Chang, C.C. and Lin, C.C., 2021. Reversible data hiding in encrypted images based on homomorphism and block-based congruence transformation. *Multimedia Tools and Applications*, pp.1-24.
- Yin, Z., She, X., Tang, J. and Luo, B., 2021. Reversible data hiding in encrypted images based on pixel prediction and multi-MSB planes rearrangement. *Signal Processing*, 187, p.108146.
- Xu, D. and Su, S., 2021. Reversible data hiding in encrypted images with separability and high embedding capacity. *Signal Processing: Image Communication*, 95, p.116274.
- Wang, X., Chang, C.C. and Lin, C.C., 2021. High capacity reversible data hiding in encrypted images based on prediction error and block classification. *Multimedia Tools and Applications*, pp.1-23.
- Xu, S., Horng, J.H. and Chang, C.C., 2021. Reversible Data Hiding Scheme Based on VQ Prediction and Adaptive Parametric Binary Tree Labeling for Encrypted Images. *IEEE Access*, 9, pp.55191-55204.
- Weng, S., Zhang, C., Zhang, T. and Chen, K., 2021. High-capacity reversible data hiding in encrypted images using SIBRW and GCC. *Journal of Visual Communication and Image Representation*, 75, p.102932.
- Wang, X., Li, L.Y., Chang, C.C. and Chen, C.C., 2021. High-Capacity Reversible Data Hiding in Encrypted Images Based on Prediction Error Compression and Block Selection. *Security and Communication Networks*, 2021.
- Gao, G., Tong, S., Xia, Z., Wu, B., Xu, L. and Zhao, Z., 2021. Reversible data hiding with automatic contrast enhancement for medical images. *Signal Processing*, 178, p.107817.

