SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I4P104

Volume 11 Issue 4, 34-40, April 2024

Original Article

Advanced Privacy-Preserving RDH Scheme for Encrypting Sensitive Images: A Two-Level LSB Embedding Strategy

Adam Muhudin[1*], Jayanta Mondal[2], Sasmita Dash[2], Osman Diriye Hussein[3], Abdullahi Mohamud Osoble[1]

[1]*Faculty of Computing, SIMAD University, Mogadishu, Somalia.*
[2]*School of Computer Engineering, KIIT University, Odisha, India.*
[3]*Faculty of Engineering, SIMAD University, Mogadishu, Somalia.*

[*]*Corresponding Author : adammuhudin@simad.edu.so*

Received: 05 February 2024 Revised: 04 March 2024 Accepted: 03 April 2024 Published: 30 April 2024

Abstract *- In the digital age, safeguarding the security and privacy of sensitive images presents a paramount challenge. Transmission of confidential images over communication networks demands robust protection mechanisms to preserve their integrity and confidentiality. Encryption emerges as a fundamental practice in this endeavor, ensuring the secure transmission of images amidst the prevalence of multimedia communication. As internet connectivity and cloud storage systems proliferate, the need for enhanced security measures becomes ever more critical. Beyond conventional encryption, the imperatives of preserving image quality, particularly in domains such as forensics and military operations, underscore the importance of Reversible Data Hiding (RDH). RDH offers a promising solution by enabling the embedding of data into images while maintaining their original integrity, facilitating lossless recovery when needed. This thesis delves into efficient RDH schemes within the encrypted domain, proposing a comprehensive two-level security mechanism. By integrating authentication systems, maximizing data hiding capacity, and ensuring complete reversibility, these schemes aim to address the complex security challenges inherent in sensitive image transmission. Through this research, strides are made towards enhancing the security and privacy of sensitive images across various domains.*

Keywords *- Encryption, Image privacy, Lossless data embedding, Reversible Data Hiding, Sensitive images.*

1. Introduction

Traditional security mechanisms have evolved with time, and quite efficient encryption algorithms are available, providing adequate security to normal datasets [1]. However, sensitive datasets are a different story altogether. Sensitive images, for example, forensic images, medical images, astronomical images, etc., have far less redundancy compared to normal images [2]. Similarly, private information falls into the category of sensitive or critical datasets because it holds high-intensity information, like medical diagnosis or forensic analysis [3].

Traditionally, digital images have served as vessels for secret data [4]. Digital watermarking, steganography, and other encryption processes are highly effective in hiding additional data within digital images. The problem arises when a sensitive image is considered as the cover image [5]. Adding additional data to sensitive images has saved a huge amount of space and time and offers privacy [6]. This is where RDH comes into play: when sensitive data needs to be embedded into images [7].

RDH was initially suggested by Barton in the early nineties [1]. Since then, plenty of research has been carried out to improve RDH mechanisms in different sectors. Recent RDH schemes are capable of providing security and preserving the privacy of sensitive datasets [8].

1.1. RDH into Different Image Domains

In this section, different types of RDH methods are discussed based on the image domains. Categorically, RDH methods are categorized into three types: (i) Reversible data hiding into uncompressed images, (ii) Reversible data hiding into encrypted images, and (iii) Reversible data hiding into compressed images. The utilization and methodologies vary depending on the image types [9]. Base-methodologies also vary based on the kind of images [18].

Histogram shift and difference expansion are the two main techniques used as base data embedding methodologies in the case of uncompressed images. DCT, DWT, Haar transform, etc., are used as base data embedding methodologies in the case of compressed images [24]. Least Significant Bit (LSB)

modification is predominantly in the case of encrypted images as the base data embedding methodology.

RDH provides different services based on its implementation, intention and necessity [10]. Basically, four main services are provided by RDH schemes: (i) Authentication, (ii) Confidentiality, (iii) Enhancement of contrast, and (iv) Privacy Preservation.

1.2. RDH Services in Encrypted Domain

X. Zhang proposed an RDH methodology that can be applied to encrypted images [2]. However, it is important to clarify RDH itself is not a form of encryption [4]. Instead, RDH is used alongside encryption, particularly for sensitive images, to exploit the minimal redundancy often found in such data. These reversible methods act as an additional security layer by embedding data during the encryption process. This approach paves the way for using a simple, reversible, and lightweight encryption scheme alongside RDH [5].

The RDH approach that operates through an encrypted domain has the following principal implications: (i) privacy preservation by way of additional data hiding, (ii) confidentiality by way of encryption, (iii) additional data security through the data hiding and (iv) authentication along with data hiding [11].

1.3. Problem Statement

Security mechanisms for sensitive images, e.g. medical, forensic, military, astronomical, geospatial, etc., have been a big challenge [9]. Several areas are there concerning sensitive images that need much improvement before online service implementation of any kind, such as security of cover image [19], proper authentication measures [20], efficient data hiding techniques for privacy preservation [21], and most importantly lossless recovery of both cover image and additional embedded bits [12]. RDH offers some solutions to the above-mentioned problem [13].

Among several RDH techniques proposed in the past two decades, some are very efficient in marking the image [22], some are quite efficient in data embedding [23], and some are focused on recovered image quality [25]. Several different mechanisms, e.g. LSB modification [16], difference expansion [14], histogram shift [24], etc., are better than each other in different aspects. Proposing a novel and improved method based on any single RDH mechanism that can outperform preexisting schemes in all categories is surely tough and research-worthy. Further research is needed to improve these techniques and to address the specific concerns of various industries that rely on sensitive image data.

2. Literature Review

This work focuses primarily on the additional data-hiding process into encrypted images [17]. The additional data hiding serves not only as a privacy-preserving technique but also helps provide an additional level of security to the sensitive cover image [3]. In this section, some RDH schemes are reviewed and later compared with the proposed method.

In 2011, Zhang [2] suggested an RDH method for image encryption. This method uses two-stage encryption. First, the image owner encipher the initial uncompressed image with a key before transferring it to the data concealer. The system enables the addition of extra data into an enciphered image, even if the person hiding the data (the data hider) does not have the encryption key. To accomplish this, the data hider first breaks the enciphered image into equally sized blocks that do not overlap; then, the modification of the least significant bits (usually the last three) within each block will be carried out to embed the additional data. This data-hiding process uses a separate key, distinct from the encryption key. At the receiving end, both the initial image and the hidden data can only be recovered if both the encryption key and the data hiding key are available.

In 2012, Hong [3] improved Zhang's proposal [2] by introducing the concept of side-matching. While the image encryption and data hiding processes remain unchanged, Hong's method enhances data extraction and image recovery. This improvement is achieved by increasing the smoothness factor, which considers the correlation of border pixels within each block. Side-matching is then employed to reduce errors in the recovered image data further.

In 2015, Liao [4] further improved Zhang's [2] and Hong's [3] work by calculating the absolute mean variance of the bordering pixels, which further decreased the bit error rate of the recovered image. In his proposal, he considered the border pixels, which were ignored by Zhang [2] in his work and also, all the adjacent pixels based on the pixel location are considered, unlike only two neighboring pixels as used by Hong [3]. The consideration of all the adjacent pixels and calculating their average value outcomes in the improvement of the extracted image quality, thus reducing the bit error percentage of the extracted image.

In 2016, Qian [5] proposed an enhanced approach using a joint RDH algorithm for encrypted images. Similar to Zhang's method, this technique utilizes a stream cipher for encryption. Data hiding occurs on a cloud server, where the data is transformed (encapsulated) during the process. Here, the encrypted image is first divided into four blocks. Each block undergoes a different type of reversible data-hiding technique, thus enhancing the overall security level. Data removal and image recovery are achieved at the decryption stage by reversing the processes applied during encryption.

3. Proposed Method

With the rise of access to the internet and digital data, the security of digital data has recently taken on more significance, especially when it comes to the security of

sensitive Images. The development of various image encryption algorithms to protect sensitive images is a result of the desire for privacy and secrecy. Image encryption and data hiding have emerged as crucial ways of protecting digital images from unwanted access among these strategies.

The proposed method tries to optimize the additional capacity for data covering while encrypting. The proposed method primarily focuses on maximizing the additional data-hiding capacity. Privacy preservation is the primary focus here. The proposed structure can be categorized into three parts-first, the cover image encryption. Bits are being inserted into the encrypted image following the data-hiding algorithm.

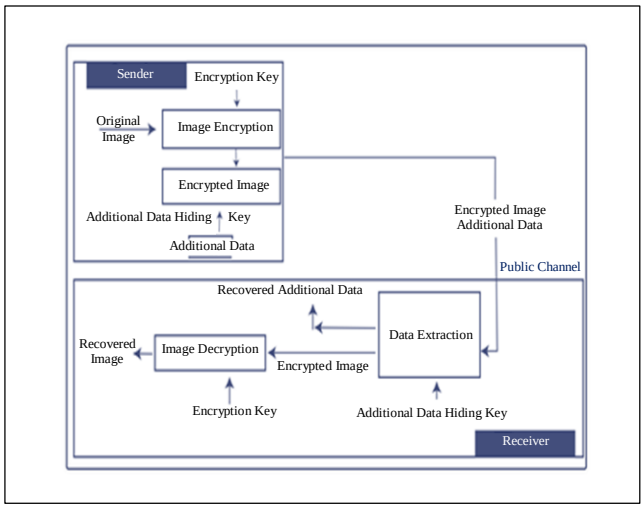

Fig. 1 Proposed RDH schema

3.1. Cover Image Encryption

There are three main stages in the proposed technique. It starts by encrypting the original image. This encryption acts as a protective layer, encrypting the image content and making it unreadable for anyone who does not have the key. This ensures the privacy of the image's information. Once the image is encrypted and secured, the next stage involves embedding the additional secret data within this encrypted image. Essentially, the encrypted image becomes a container that holds the hidden information.

3.2. Data Security

In the second phase, the secret data is hidden inside the encrypted image using a technique called "Least Significant Bit (LSB) modification." This method essentially alters the least important part (the last bit) of the data that represents each pixel in the image. A key advantage of LSB modification is that it introduces minimal changes to the image's visual quality. Even though the image is altered, it appears almost identical to the original to the naked eye.

3.3. Image and Data Recovery

The final stage involves retrieving the hidden data and the initial image. The receiver can recover the image to its original form with the help decryption key. With the initial image recovered, the receiver can then employ the key used for data hiding (which might be different from the decryption key) to extract the secret information that was cleverly concealed within the encrypted image. This two-key approach ensures that only authorized individuals who possess the two keys can access the hidden data and the initial image, maintaining confidentiality.

3.4. Roles of Sender and Receiver

The proposed approach involves two parties: the sender and the receiver. The sender enciphers the initial image and inserts hidden data into it. The receiver then extracts the additional bits hidden in the enciphered image and decrypts it to retrieve the initial image. Additional information about the roles of both the sender and receiver can be found below.

3.4.1. Sender

The cover image needs to be encrypted by its sender using a secure encryption method. The sender then selects the hidden data to be concealed using the LSB modifications technique to encrypt the image while hiding its contents. The key required for the encryption of the image and retrieval of the secret data has to be given by the sender to the receiver. The encrypted image and hidden information must be safely sent to the receiver in the manner indicated by the sender.

3.4.2. Receiver

The receiver has to remove the encrypted image in order to decrypt and recover it to its initial state. The receiver has to acquire the hidden data from the deciphered image. The deciphered image and hidden data must be kept private and away from the hands of unauthorized individuals, as instructed to the receiver.

3.5. Encryption Method

In the enciphering part of the initial image, a 512×512 bit private key, which is randomly generated in Matlab, is used for encryption.

During the encryption process, a unique 512×512 bit private key is generated randomly within the Matlab environment. This key will be utilized to encrypt the image.

3.6. Encryption Algorithm

Phase 1: The original color image, which is M pixels by N pixels, is converted to grayscale. To do this, we take each pixel's original value (represented by I(i, j)) and multiply it by the sum of a and b. The resulting value, Igrey(i, j), represents the pixel's strength in the grayscale image. (1).

The width (M) of the original image is related to the constant a by the equation M = 2a. This means the width is always twice the value of a. Similarly, the height (N) of the image is related to the constant b by the equation N = 2b. The height is always twice the value of b.

$I_{grey(i,j)}$ denotes the grayscale value calculated for each pixel at the point (i,j) in the image. This value is derived from the original RGB color information of that pixel.

In which, M = 2a while N = 2b and $I_{grey(i,j)}$ = the greyscale weight that is produced from RGB measure.

Phase 2: To encrypt the photo and make it unreadable, it is mixed with a secret code using a special XOR operation. $I_{E(i,j)}$ is the result of performing a bitwise XOR operation between the original image data $I_{(i, j)}$ and the secret key $K_{(i, j)}$. (2)

This refers to a specific element (identified by i and j) within a structure that has M rows and N columns. The element itself is called a key.

3.7. Data Hiding Algorithm

- Phase 1: We are taking an element (represented by "I_E") and dividing it into n equal pieces. Each piece is a square block with dimensions S by S. There are a total of n such blocks, numbered from 1 to n.

- 1st Level- For each of the odd-numbered blocks (from 1 to n-1), a replacement operation is performed. This means the original content of that block is taken and substituted with something else.

- Phase 2: the first row of pixels stays the same.
- Phase 3. XOR every 3 LSB bits located in the second, third, and fourth places of the 1st and 2nd rows.
- Phase 4: If the outcome is zero, no alteration is made. Otherwise, add an extra bit to the 1st LSB.
- Phase 5: Repeat the XOR technique with all remaining pixels and the initial unaltered pixel.
- Phase 6: Repeat Steps 4 and 5 for each of the odd blocks.

- Second Level: For the even blocks with options starting with block numbers 2 to n.

- Phase 7: Replace the following extra bit with the most recent LSB of the very last pixel.
- Phase 8: Repeat Step 7 until those blocks with even numbers are concealed.
- Phase 9: Lastly, we combine all the even and odd numbered blocks to create the final embedded-encrypted image, called I_M.

3.8. Recovery Algorithm

- Phase 1: we take the Encrypted Image (I_E) and divide it into n equal-sized pieces. These pieces are square-shaped blocks, each with a width and height of S units (S x S). It's important to note that these blocks don't overlap (they are non-coinciding).
- Phase 2: Repeat the data hiding process to extract the additional bits and created I_E.
- Phase 3: The secret key is applied to produce the initial image.

The image (I) is obtained by XORing the enciphered image (I_E) and the encipherment key (K).

4. Analysis of Experimental Results

The proposed technique's reliability was shown using four 512x512 sized images. Specifically, two ordinary test photos and two medical images. Figures 3-6 illustrate the procedures involved: (a) Initial image, (b) enciphered image for privacy, (c) enciphered image which has the additional hidden data, and (d) embedded-decrypted image and (e) final image when both stages (encrypting and data hiding) have been appropriately removed.

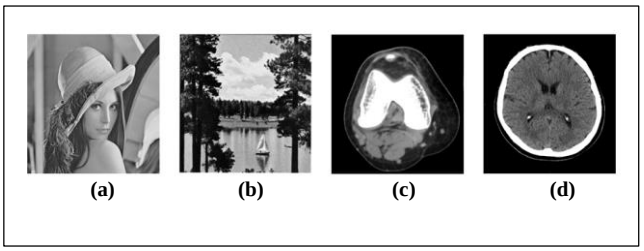

Fig. 2 Test images: (a) Image 1, (b) Image 2, (c) CT, and (d) MRI

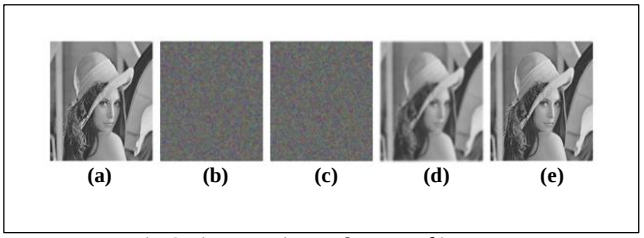

Fig. 3 Five experimental stages of image 1

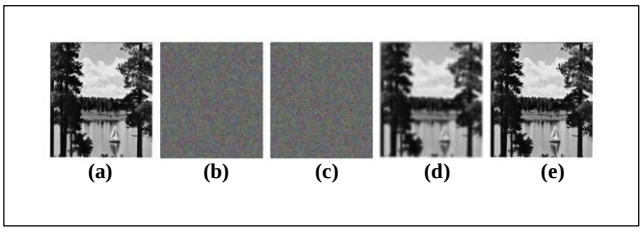

Fig. 4 Five experimental stages of image 2

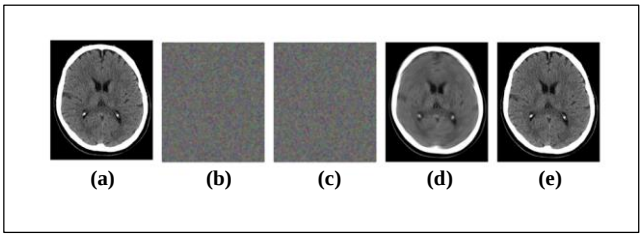

Fig. 5 Five experimental stages of CT image

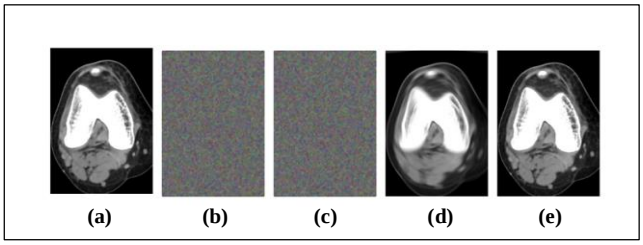

Fig. 6 Five experimental stages of MR image

4.1. Evaluation Matrices

In this section, three primary evaluation metrics used for image quality evaluation in RDH-based methods are presented with mathematical formulae.

4.1.1. Mean Squared Error

Calculates the average squares variance among equivalent pixels in the initial image and the image that has been encrypted. A higher MSE indicates better image protection.

$$MSE = \frac{1}{s \times s} \sum \sum (X_{ij} - Y_{ij})^2$$

4.1.2. Peak Signal-to-Noise Ratio (PSNR)

Calculates the proportion among the highest conceivable pixel value (usually 255 for 8-bit images) and the noise introduced by encryption. Higher PSNR indicates better image quality (less noise).

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{MAX}_I^2}{\mathrm{MSE}}\right) = 20.\log_{10}\left(\frac{\mathrm{MAX}_I}{\sqrt{\mathrm{MSE}}}\right)$$

$$= 20.\log_{10}(\mathrm{MAX}_I) - 10.\log_{10}(\mathrm{MSE})$$

4.1.3. Structural Similarity Index (SSIM)

Compares the structural similarities of the actual and enciphered images. It examines the brightness, contrast, and structure. Higher SSIM suggests better quality of perception (images appear more similar).

$$\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

In terms of additional data hiding capacity, the proposed method is set side by side with the above-reviewed RDH schemes and the result is shown in Table 1. Each image is divided into 4 X 4 blocks. So the total number of blocks turns to (512 X 512) / (4 X 4).

Since, in the proposed method, three LSBs from each block have been used for embedding, it will definitely increase the data embedding capacity by at least 10% of the previous best. Hence, it will definitely be more than 8192 (at least nearly equal to 11000). In future work, we will consider every image for calculating data embedding capacity using our proposed method.

Table 1. Comparison table on additional data hiding capacity

Test Images	[2]	[3]	[4]	[5]	Proposed Method
Image 1	1156	3894	1296	1296	>8192
Image 2	1024	1024	1296	1296	>8192
CT	9	8439	9	9	>8192
MRI	9	8439	9	9	>8192

Table 2. Compares the PSNR (quality) of the image after decryption and after removing the hidden data

Images	Directly Decrypted Image	Recovered Image
Image 1	39.98	69.38
CT	37.83	69.22

Table 3. Demonstrates the evaluation of SSIM values among the recovered image and the decrypted image after removing the additional bits

Images	Directly Decrypted Image	Recovered Image
Image 2	0.9788	0.9993
MRI	0.9699	0.9989

5. Conclusion

This paper gives an overview of the RDH methods for encrypted images that have been developed so far. Over the past decades, significant advancements have been made from the conventional RDH procedures. RDH accomplishes all the fundamental objectives of cryptography in the domain of encryption: first, encryption guarantees confidentiality, data hiding techniques offer integrity through authentication, and minimal overhead through simple, reversible procedures.

The proposed method enhances the privacy preservation mechanism of RDH schemes through improving the additional data hiding capacity. Two-level data hiding mechanisms are proposed using LSB modification. The experimental results show huge improvement. The data hiding capacity is increased by more than 10 percent. The additional secret data process does not depend on the type of images. The recovered image quality is also better than the preexisting RDH schemes.

References

[1] J.M. Barton, "Method and Apparatus for Embedding Authentication Information within Digital Data" *US Patent 5,646,997*, 1997. [Google Scholar] [Publisher Link]

[2] Xinpeng Zhang et al., "Reversible Data Hiding in Encrypted Image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255-258, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[3] Wien Hong, Tung-Shou Chen, and Han-Yan Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199-202, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[4] Xin Liao, and Changwen Shu, "Reversible Data Hiding in Encrypted Images Based on Absolute Mean Difference of Multiple Neighboring Pixels," *Journal of Visual Communication and Image Representation*, vol. 28, pp. 21-27, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[5] Zhenxing Qian et al., "Improved Joint Reversible Data Hiding in Encrypted Images," *Journal of Visual Communication and Image Representation*, vol. 40, pp. 732-738, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[6] M. Fallahpour, D. Megias, and M. Ghanbari, "Reversible and High-Capacity Data Hiding in Medical Images," *IET Image Processing*, vol. 5, no. 2, pp. 190-197, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[7] Chia-Chen Lin, Wei-Liang Tai, and Chin-Chen Chang, "Multilevel Reversible Data Hiding Based on Histogram Modification of Difference Images," *Pattern Recognition*, vol. 41, no. 12, pp. 3582-3591, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[8] Piyu Tsai, Yu-Chen Hu, and Hsiu-Lien Yeh, "Reversible Image Hiding Scheme Using Predictive Coding and Histogram Shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129-1143, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] Zhiguo Chang, and Jian Xu, "Reversible Run Length Data Embedding for Medical Images," *2011 IEEE 3rd International Conference on Communication Software and Networks*, Xi'an, China, pp. 260-263, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[10] Jun Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[11] Dinu Coltuc, and Jean-Marc Chassery, "Very Fast Watermarking by Reversible Contrast Mapping," *IEEE Signal Processing Letters*, vol. 14, no. 4, pp. 255-258, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[12] L. Kamstra, and H.J.A.M. Heijmans, "Reversible Data Embedding into Images Using Wavelet Techniques and Sorting," *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2082-2090, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[13] Diljith M. Thodi, and Jeffrey J. Rodriguez, "Expansion Embedding Techniques for Reversible Watermarking," *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721-730, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[14] A.M. Alattar, "Reversible Watermark Using Difference Expansion of Quads," *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Montreal, Canada, pp. iii–377, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[15] Tohari Ahmad et al., "An Improved Quad and RDE-Based Medical Data Hiding Method," *2013 IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM)*, Yogyakarta, Indonesia, pp. 141-145, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[16] Shang-Kuan Chen, "A Module-Based LSB Substitution Method with Lossless Secret Data Compression," *Computer Standards Interfaces*, vol. 33, no. 4, pp. 367-371, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[17] Yuling Liu, Xinxin Qu, and Guojiang Xin, "A ROI-Based Reversible Data Hiding Scheme in Encrypted Medical Images," *Journal of Visual Communication and Image Representation*, vol. 39, pp. 51-57, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[18] Xinpeng Zhang et al., "Separable Reversible Data Hiding in Encrypted Image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826-832, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[19] Kede Ma et al., "Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553-562, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[20] A. Lavanya, and V. Natarajan, "Watermarking Patient Data in Encrypted Medical Images," *Sadhana*, vol. 37, no. 6, pp. 723-729, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[21] Vasiliy Sachnev et al., "Reversible Watermarking Algorithm Using Sorting and Prediction," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 7, pp. 989-999, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[22] Hao-Tian Wu, Jean-Luc Dugelay, and Yun-Qing Shi, "Reversible Image Data Hiding with Contrast Enhancement," *IEEE Signal Processing Letters*, vol. 22, no. 1, pp. 81-85, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[23] Guangyong Gao, and Yun-Qing Shi, "Reversible Data Hiding Using Controlled Contrast Enhancement and Integer Wavelet Transform," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 2078-2082, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[24] Vanmathi Chandrasekaran, and Prabu Sevugan, "Applying Reversible Data Hiding for Medical Images in Hybrid Domain Using Haar and Modified Histogram," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 4, pp. 126-134, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[25] Chuan Qin, and Xinpeng Zhang, "Effective Reversible Data Hiding in Encrypted Image with Privacy Protection for Image Content," *Journal of Visual Communication and Image Representation*, vol. 31, pp. 154-164, 2015. [CrossRef] [Google Scholar] [Publisher Link]