International Journal of Computational and Electronic Aspects in Engineering
Vol. 5, Issue 3, Nov 2024, pp 73-79
https://doi.org/10.26706/ijceae.5.3.20240801

Embedded Reversibility Data in an Encrypted Photograph: A Case Study

Habeeb Noori Jumaah

Department of the Security Permits, University of Telafer, Tal Afar, Iraq

Correspondence: habeebnoori32@gmail.com

Abstract: Multimedia data protection has grown in importance over the past few years. Data concealing methods or encryption can be used to accomplish this. Data compression is required to minimize transmission time; however, combining data compression, encryption, and data concealing in one step presents a new difficulty. Few methods for combining picture compression and encryption have been put forth. Currently, data embedding in encrypted pictures is a hurdle. Standard data hiding strategies are inapplicable for encrypted images as their entropy is maximum since the embedding stage is regarded as noise. This research provides a new approach to reversible data embedding in encrypted photos that preserves picture quality while guaranteeing data security. Three primary stages make up the proposed scheme: data embedding, picture recovery/extraction, and image encryption. The suggested method achieves good picture quality and low computing complexity while retaining strong security characteristics, as shown by the experimental findings. This method works especially well for applications like digital forensics, medical imaging, and secure communications that need to hide data securely and reversibly.

Keywords: Image encryption; Recovery of Photograph; Reversible data hiding**.**

Article – Peer Reviewed
Received: 25 July 2024
Accepted: 29 August 2024
Published: 30 Sept 2024

Cite this article: Habeeb Noori Jumaah, "Embedded Reversibility Data in an Encrypted Photograph: A Case Study", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 5, issue 3, pp. 73-79, 2024.
https://doi.org/10.26706/ijceae.5.3.20240801

1. Introduction

Recently, protecting the privacy of image data has attracted great attention due to the appearance of internet image sharing, social networks, and cloud computing. In these cases, the original picture is first encrypted using a symmetric secret key by the content owner. After that, the secured picture is delivered to the outside service provider so that image processing may be done. Reversible data hiding, in which extra data may be inserted into an encrypted image, has gained popularity as a means of safeguarding the privacy of the image content. Sending the encrypted picture with concealed data to the recipient allows them to get the original image by extracting the embedded data **[1]–[3]**.

The Internet has seen a sharp rise in the quantity of digital photos. For many applications, including military, medical, video surveillance, and sensitive transmission, image security is becoming more and more crucial.

For instance, in the medical field, quick and secure diagnosis is essential. These days, sending pictures via networks is a regular occurrence, therefore it's important to figure out how to do it effectively. Data compression is required to shorten the transmission time. Data hiding methods or encoding can be rummage-sale to secure this hypermedia data. Attempting to integrate data concealing, encryption, and compression in one step has been a challenge for a few years **[15]-[19]**. Researchers have proposed integrating picture compression and encryption in some investigations. To do this, there are primarily two methods. The first strategy is centered on using encryption to secure content. Binary or grayscale pictures can be encrypted using a variety of techniques that guarantee correct decryption needs a key. The second strategy, known as data hiding or digital watermarking, tries to include a hidden message into the picture. These are two approaches that work well together and may be combined.

By appending a digital signature of the original picture to the encoded version, Sinha and Singh devised a way to encrypt images for safe transmission. Once the picture has been received and decrypted, its validity may be confirmed using the digital signature. Kerckhoff's principle, which asserts that only the encryption key needs to be kept secret and that all method specifics are available, is the foundation for both encryption and watermarking **[4]–[6]**.

With three stages—image encryption, data entrenching, and data extraction/image recovery— This paper offers a brand-new, reversible method for hiding data in encrypted images. A piece of the encrypted data is changed to include additional messages, while the original cover image is kept completely encrypted. By utilizing the spatial correlation present in actual pictures, the contained data is successfully recovered at the receiving end and the original image is flawlessly reconstructed.

The remainder of the document is arranged as follows. The related work is explained in Section 2. The concept of picture encryption in cryptography algorithm is explained in Section 2, along with specifics on the suggested adjustable data concealing procedure for encoded photos. In Section 3, we present and discuss the outcomes of using the suggested approach on actual photos. In Section 4, a final conclusion and future work is formed.

2. Related work

Through minor cover medium modifications, data hiding allows data to be embedded into multimedia, including images, music, and video, and to be extracted error-free **[7], [8]**. Currently, data masking technology is effectively used in a number of industries, including legal evidence, medical diagnostics, and military communication. A reversible data hiding (RDH) technique is a special data hiding method that can lossless reconstruct the cover medium before embedding the data (or secret message). Because it can reproduce the original image lossless, it is widely used in applications that require the strictest preservation of the unique image satisfied. Apart from the noise-free recovery of the original content, the image before the data embedding must fulfill other conditions as well, such as the image not being tampered with, not having been substituted, and not having had the data embedded before. As a result, a number of RDH algorithms have been proposed based on various types of images, including grayscale, color, and JPEG compressed images. With the rapid growth of online image storage and transmission, many online cloud applications have emerged in recent years, including cloud image hosting, cloud medical image sharing, and cloud authentication service. In such applications, users usually delegate essential tasks, including backup, sharing, processing, and analyzing images, to cloud service providers. However, for some privacy and security reasons, sensitive images can’t be uploaded to the cloud in the clear. Instead, they must be encrypted before being uploaded to the cloud. To this end, a class of RDH in encrypted images (RDHEI) methods has been studied and proposed **[9]**.

A portion of the refuge data is utilized to transport the extra note in certain current systems that combine data concealing with encryption, with the remaining portion of the data being encrypted. For instance, in one way, the signs, motion vector difference, and intra-prediction mode of the DCT parameters are encrypted and a watermark is added to their amplitudes. Another method uses encryption and watermarks to cover data in the top and lower bit-planes of the transform domain, respectively. Alternatively, the host DCT component signatures are encrypted by the content owner, and each user uses a different key to decode a portion of the coefficients, creating several copies with distinct user fingerprints. Nevertheless, these combined techniques only encrypt a portion of the data, which may cause some of the cover data to leak. They also don't take into account the fact that the entrenched data and original cover are separate from a watermarked version. Using the homomorphic feature of encryption on each sample of a cover signal encrypted with a public-key procedure, additional data is inserted into the encrypted signal in various approaches. However, this method significantly increases the encrypted signal size and processing complexity, and the data embedding is irreversible.

Reversible data hiding in encrypted images (RDH-EI) is an area of intense study that aims to safely hide data into encrypted photos while preserving the recoverability of the original picture. A technique that divides the encryption and data embedding stages was presented by Zhang et al. **[10]**. This enables the recipient to get the embedded data first and then the original picture. Although this method guarantees picture accuracy and data secrecy, its two-step procedure may result in higher computing complexity. Ma et al. **[11]** anticipated a scheme that utilizes the spatial association of pixels in natural images to improve the efficiency of data extraction and image recovery. By preserving the statistical properties of the image, this technique enhances the superiority of the improved image while allowing for robust data embedding. However, its reliance on spatial correlation might limit its effectiveness in images with low spatial redundancy. Another approach by Hong et al. **[12]** focuses on joint encryption and data embedding using a single-step process that simplifies the overall procedure. This method employs a stream cipher to encrypt the image while embedding additional data using a reversible watermarking technique. Although this technique offers efficiency and simplicity, the embedded data capacity is relatively limited compared to other methods. In the field of selective encryption and watermarking, efforts have been made to balance encryption strength and data embedding capacity. For example, Liu et al. **[13]** explored using compressive sensing to encrypt image data, which allows for simultaneous encryption and compression. This approach effectively combines encryption with data hiding, but the complexity of compressive sensing algorithms can be a challenge for real-time applications. Finally, some researchers have focused on the security aspects of RDH-EI systems. Zhang et al. **[14]** highlighted the importance of using secure key management and encryption techniques to protect against unauthorized access and data leakage. They proposed a framework that integrates key management with data hiding to enhance the overall security of the system. Despite these advancements, challenges remain in achieving a balance between data embedding capacity, image quality, computational efficiency, and security. The proposed work, "Embedded Reversibility Data in an Encrypted Photograph," aims to address these challenges by introducing a novel framework that improves data capacity and image quality while maintaining robust security features and efficient processing.

3. Proposed Method

Figure 1 shows an outline of the suggested plan. An encryption key is used by the content owner to encrypt the original, uncompressed image before creating an encrypted picture. Next, a data hider inserts extra data into this encrypted image using a data-hiding key without needing to access the original data. An image that resembles the original can be obtained by the recipient by first using the encryption key to decode an image that is encrypted with embedded data. By extracting the embedded data with the data-hiding key, the recipient may entirely restore the original image from the encrypted version. The particular stages are as follows.

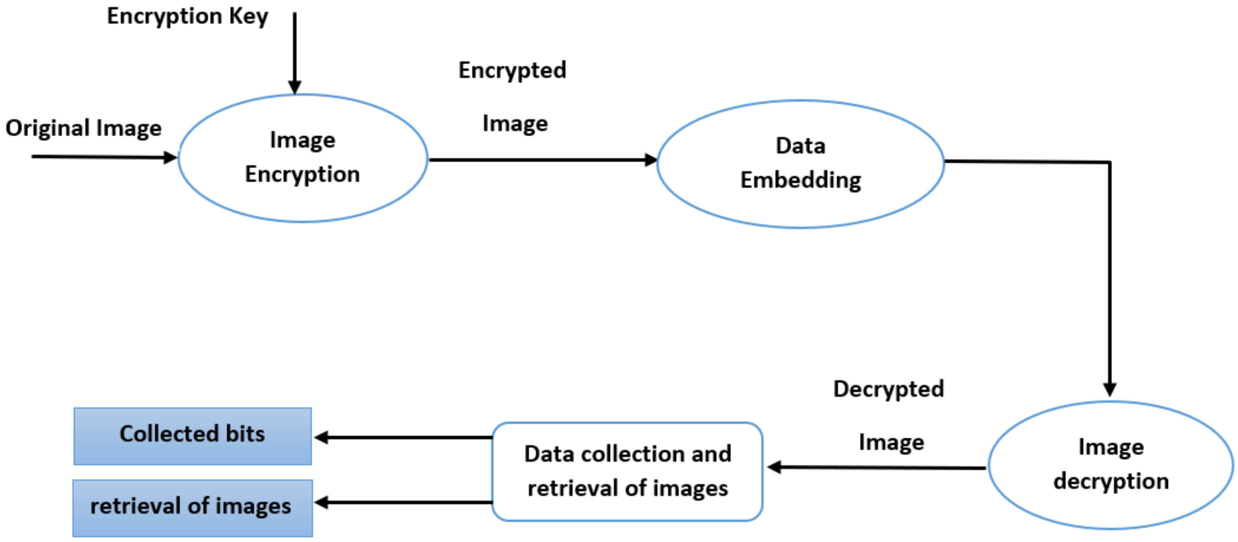


Fig 1. Show the proposed method

A. Picture Cryptography

Suppose that the source picture is in unstructured version and that there are eight bits per grayscale pixel (ranging from 0 to 255). Indicate a pixel's bits as $a_{i,j,0}, a_{i,j,1}, \dots, a_{i,j,7}$ where *(i, j)* the picture element situation is indicated and the amount of gray as $m_{i,j}$. Consequently

$$a_{i,j,k} = \frac{p_{i,j}}{2^k} \bmod 2 \qquad k = 0,1, \dots, 7 \qquad (1)$$

$$m_{i,j} = \sum_{v=0}^{7} a_{i,j,k} \cdot 2^k \qquad (2)$$

Pseudo-random bits and the actual bits' exclusive-or outcomes are calculated during the encryption phase.

$$A_{i,j,k} = a_{i,j,k} \oplus r_{i,j,k} \tag{3}$$

where $r_{i,j,k}$ are ascertained by means of a conventional stream cipher and an encryption key. $A_{i,j,k}$are then orderly concatenated with the secret information. Here, a variety of secure stream cipher techniques may be applied to guarantee that the encrypted data cannot reveal any secrets regarding its original form to anybody lacking the encoding key, such as a prospective invader or the data hider.

B. Data Incorporation

Even if a data-hider is unaware of the innovative image satisfied, he can incorporate extra note using the encrypted data. $s \times s$ by the alteration of a tiny percentage of encrypted data, into the picture. First, the encrypted picture is divided into many nonoverlapping blocks of varying sizes by the data-hider. In the other forms, the encrypted bits $A_{i,j,k}$ satisfying $(m-1).\ s+1 \leq\ i \leq\ m.s,\ (n-1).s\ +1 \leq\ j \leq\ n.s\ and\ \ 0 \leq k \leq\ 7,$ there are two positive integers (m and n) in the same block. Next, one more bit will be carried by each block. S^2 split each block's values into two groups using pseudo-randomness S_0 and S_1based on a data-hiding key. In this case, the likelihood that a pixel is S_0 or $S_1$is 1/2. Flip each encrypted pixel's three least significant bits (LSB) in if the extra bit to be embedded is 0.

$$A'_{i,j,k} =\ A_{i,j,k},\ for\ (i,j) \in s_0\ and\ k = 0, 1, 2. \tag{4}$$

Flip the three scrambled LSB of pixels in S_1 if the extra bit is 1, leaving the other scrambled facts unchanged.

C. Data Restoration and Image Retrieval

A receiver first creates $r_{i,j,k}$ computes the exclusive–or of the information obtained based on the secret key, and $r_{i,j,k}$ then decrypts the encrypted picture containing embedded data. The decrypted bits are designated as $a'_{i,j,k}$ It is evident that the initial five most important bits (MSB) have been accurately recovered. When a pixel is embedded in a block and its embedded bit is either zero or one, meaning that the pixel belongs to that block, then no encrypted bits of that pixel are affected by data-hiding. Given that the three decrypted LSB must coincide with the original LSB, this implies that the decoded gray value of the pixel is correct. Conversely, if the pixel's block contains an embedded bit of 0 and it belongs to S_0, or if the pixel has an embedded bit of 1 and it belongs to S_1, the decoded LSB

$$a'_{i,j,k} =\ a_{i,j,k}, \qquad k = 0, 1, 2. \tag{5}$$

This implies that the three encoded LSB cannot possibly be the same as the original LSB. Here:

$$a'_{i,j,k} +\ a_{i,j,k}=1 \qquad k = 0, 1, 2. \tag{6}$$

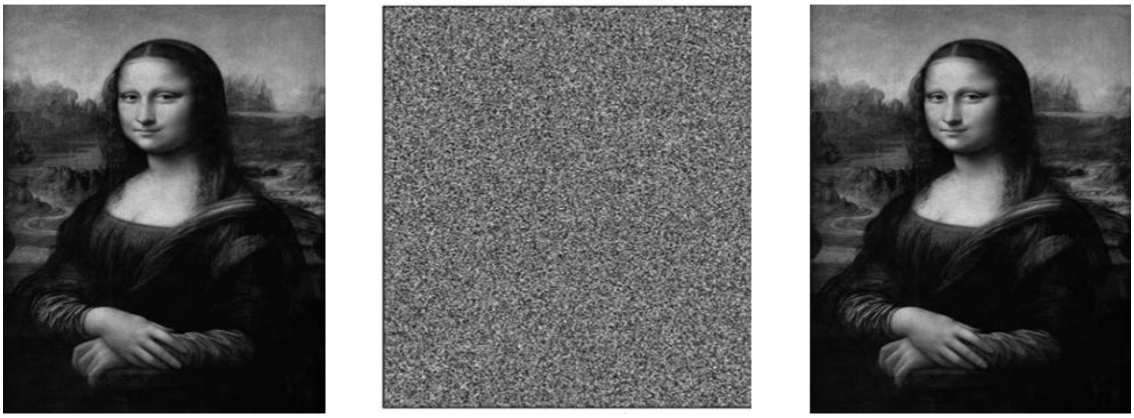
Consequently, three encoded LSB and three original LSB's decimal values added together must equal seven. Between the original value set and the decrypted principles, the average energy of mistakes is

$$E_Y = \frac{1}{8}\ .\sum_{v=0}^{7}[v-(7-v)]^2=21. \tag{7}$$

When reconstructing a picture using the encoded data, the PSNR value in the encrypted version of the image is about because the likelihood of improper LSB-decryption is 1/2.

$$\text{PNSR}=10.\ \log_{10}\frac{255^2}{\frac{E_Y}{2}} = 37.88\ dB \tag{8}$$

The recipient will then be able to extract the embedded bits and retrieve the original content of the encrypted image. With the data-hiding key, he may divide the pixels in each block of the decrypted picture into two groups. For every block that is decoded, the receiver flips the three LSBs of pixels in to create a new block, which it then flips again to create a new block. The two new blocks are referred to as H_0 and H_1. Either H_0 or H_1 must be the initial block, and the LSB flip operation has more significantly disrupted another one. Define a function to gauge the volatility in the two blocks sized by $s{\times}s$ and represent, respectively, the values of the fluctuation functions for H_0 and H_1. Because of spatial correlation in natural pictures, the changing caused by the original block is frequently less than that of a highly disturbed version. Thus, by comparing f_0 and f_1, the receiver may carry out data extraction and picture recovery. Consider H_0 to represent the block's initial content if f_0 < f_1, and set the extracted bit to 0. If not, consider H_1 to be this block's original content and remove a small portion of 1. Concatenate the retrieved portions to obtain the extra message at the end, then gather the recovered blocks to create the original picture.



(a) (b) (c)

Fig 2. shows the original image, an encrypted form, and a decrypted form with embedded data.

$$\mathrm{f}{=}\sum_{v=2}^{s-1}\sum_{z=2}^{s-1} \mid p_{v,z}-\frac{p_{v-1,z}+p_{v,z-1}+pv+1,z+pv,z=1}{4} \mid \tag{9}$$

4. Experimental Results

As seen in Figure 2(a), the test picture "test picture" which had a resolution of 512x512 pixels, was utilized as the first cover image in the experiment. The encrypted picture, seen in Figure 2(b), was created by converting each pixel's eight encrypted bits into a grayscale value after the image had been encrypted. Then, we used each block's side length to insert 256 bits into the encrypted picture. The resultant decrypted image is shown in Figure 2(c). Data embedding produced an unnoticeable PSNR value of 37.88 dB, which supports the theoretical analysis in equation (8). In the end, the embedded information was efficaciously retrieved, and the encrypted image flawlessly restored the original image. A lower block size in the suggested method enables the embedding of more extra data. Nevertheless, there is a greater chance of failed bit extraction and image recovery. The blocks where bit extraction failed when utilizing the original cover picture " test picture 1" are displayed in Figure 3. Weak spatial connection causes the majority of these blocks to be located in textured regions. Four test photos, "test picture," "Example-1," " Example-2," and " Example-3," all 512x512 in size, are used as the original covers in Figure 4 to show the extracted-bit error rate regarding block sizes. These covers are common test pictures that may be found in many image databases. In this instance, the extracted-bit error rate equals the block recovery failure rate. It is evident that smoother cover images provide superior outcomes for image recovery and data extraction. For most cover images, when the block side length is 32 or greater, all embedded bits can be exactly recovered and the original image may be properly recovered.

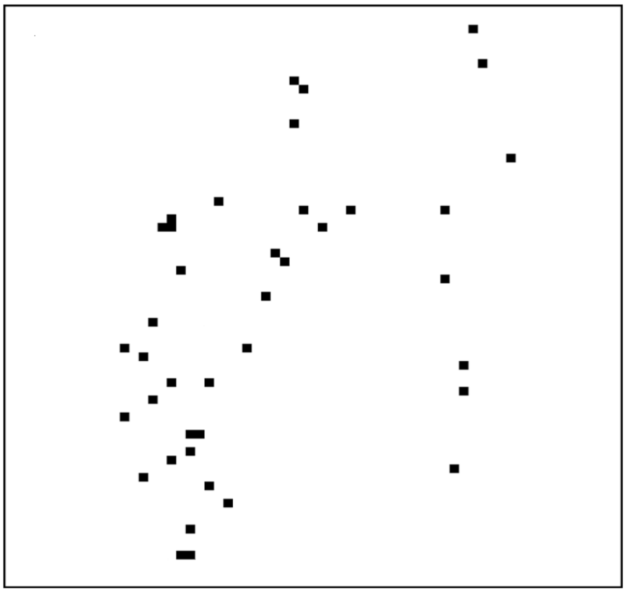


Fig 3. Inaccurate bit-extraction blocks assuming the cover test picture and s=8

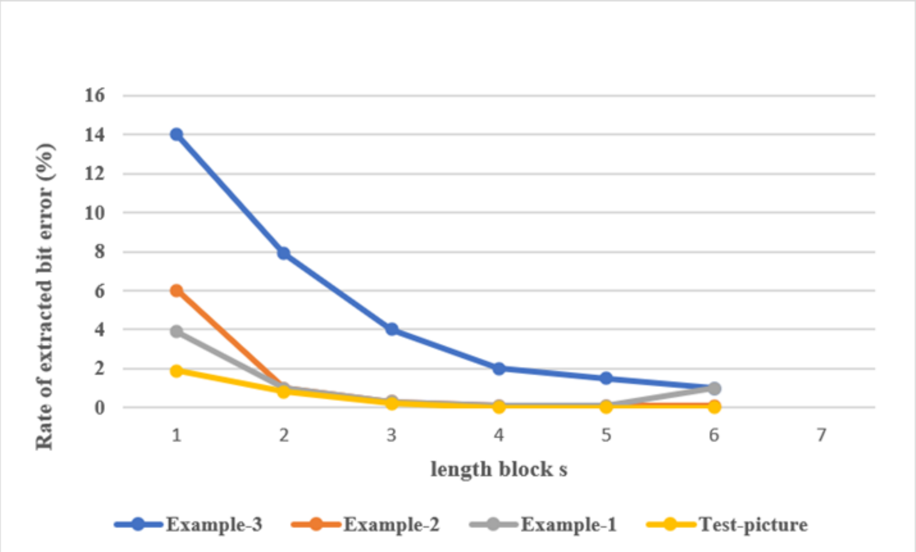


Fig 4. Error rate of obtained bits in relation to block sizes.

5. Conclusion and Future work

In this study, a revolutionary low-complexity embedded reversibility data concealing strategy for encrypted pictures is proposed. Three stages make up the scheme: data embedding, picture recovery/extraction, and image encryption. The original image data is fully encrypted using a stream cipher. A data hider can add more data to an encrypted image without knowing the original by changing a portion of the encrypted data. The recipient can use the encryption key to decode the private picture with embedded data and create an image that looks similar to the original. The data-hiding key and spatial correlation observed in natural pictures may be used to reliably extract the enclosed data and restore the original image. Even while someone can use the encryption key to decode the image and apply LSB steg analysis techniques to locate hidden data, they cannot extract the extra data or restore the original picture without the data-hiding key. A large number, like 32, can be used as the block size to ensure precise data extraction and faultless image recovery. Alternatively, an error correcting mechanism can be added before data hiding to safeguard the extra data, albeit doing so would lower its overall capability. To ensure that the encrypted data is secure, we may use a range of secure stream cipher approaches in future work.

References

[1] C.-Y. Weng and C.-H. Yang, "Reversible data hiding in encrypted image using multiple data-hiders sharing algorithm," *Entropy*, vol. 25, no. 2, p. 209, 2023.

[2] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Processing*, vol. 94, pp. 118–127, 2014.

[3] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," in *Security, forensics, steganography, and watermarking of multimedia contents X*, 2008, vol. 6819, pp. 534–542.

[4] Y. Qiu, Q. Ying, X. Lin, Y. Zhang, and Z. Qian, "Reversible data hiding in encrypted images with dual data embedding," *IEEE Access*, vol. 8, pp. 23209–23220, 2020.

[5] Z. Fu, X. Chai, Z. Tang, X. He, Z. Gan, and G. Cao, "Adaptive embedding combining LBE and IBBE for high-capacity reversible data hiding in encrypted images," *Signal Processing*, vol. 216, p. 109299, 2024.

[6] Q. Feng, L. Leng, C.-C. Chang, J.-H. Horng, and M. Wu, "Reversible data hiding in encrypted images with extended parametric binary tree labeling," *Applied Sciences*, vol. 13, no. 4, p. 2458, 2023.

[7] C. Yu, X. Zhang, X. Zhang, G. Li, and Z. Tang, "Reversible data hiding with hierarchical embedding for encrypted images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 2, pp. 451–466, 2021.

[8] P. Puteaux and W. Puech, "A recursive reversible data hiding in encrypted images method with a very high payload," *IEEE Transactions on Multimedia*, vol. 23, pp. 636–650, 2020.

[9] Q.-H. Le, N.-H. Nguyen, and V.-A. Pham, "High-performance RDH in encrypted images using optimal linear predictor and bit-plane compression of sub-images," *Multimedia Tools and Applications*, pp. 1–36, 2024.

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

[11] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "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.

[12] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE signal processing letters*, vol. 19, no. 4, pp. 199–202, 2012.

[13] M. Li, D. Xiao, A. Kulsoom, and Y. Zhang, "Improved reversible data hiding for encrypted images using full embedding strategy," *Electronics Letters*, vol. 51, no. 9, pp. 690–691, 2015.

[14] Z. Qian and X. Zhang, "Reversible Data Hiding in Encrypted Images With Distributed Source Encoding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 4, pp. 636–646, 2016.

[15] Davis S Cherian "Image Caption Generator Using CNN and LSTM", *International Journal of Computational and Electronic Aspects in Engineering,* RAME Publishers, vol. 3, Issue 2, pp. 26-31, 2022.

[16] Arya Ravindran, Anand Lokapure, Dr. Aisha Fernandes "A Survey on Underwater Image Processing Techniques", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 3, Issue 2, pp. 18-25, 2022.

[17] Shital B. Tiwaskar and Gajendra Singh Chandel, "Enhancing Reversible Data Hiding Technique in Encrypted Images", *International Journal of Computational and Electronics Aspects in Engineering*, RAME Publishers, vol. 1, issue 1, pp. 5-10, 2014, Revised in 2020.

[18] Faris Sattar Hadi "Image Compression Process Using Fractional Fourier Transform and Wavelets Techniques", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 5, Issue 1, pp. 25-29, 2024.

[19] Mohammed Fareed Mahdi "The Role of IT in Transforming Traditional Education to Digital Learning", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 4, Issue 4, pp. 134-147, 2023.