Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Adaptive Edge-Aware Reversible Data Hiding in Encrypted Images Using Hybrid Prediction and Dynamic MSB Selection

Rameswara Reddy Boddu
Assistant Professor, Department of MCA, Rajeev Gandhi Memorial College of Engineering & Technology, Nandyal

Madaboina Dhanush
Department of MCA Scholar, Rajeev Gandhi Memorial College of Engineering & Technology, Nandyal

Abstraction: ***Reversible Data Hiding in Encrypted Images (RDH-EI) has attracted a lot of interest in the transmission of secure images and securing privacy in the cloud world. Nevertheless, most current RDH-EI approaches have a low embedding capacity and inaccuracy in predicting complex image areas that could impact embedding efficiency and image reconstruction accuracy. In order to overcome these difficulties, this paper suggests a high capacity RDH-EI algorithm that combines edge directed prediction (EDP) with a multi-MSB self-prediction approach to enhance the prediction accuracy and data embedding effectiveness. The data owner encrypts the grayscale image first of all in the proposed framework and then adds more data to the encrypted domain by use of adaptive prediction and MSB-based embedding methods. The system also has a secure access control whereby users with authorization access encrypted images by a measure of OTP based authorization. The proposed method is capable of significantly improving the embedding capacity and high visual quality and lossless recovery of the image by embedding using prediction and dynamic selection of the MSB. In the course of the experiment, it is proven that the proposed technique has better embedding rates and reconstruction performance than existing RDH-EI methods and maintains a high degree of data confidentiality and integrity. The suggested scheme offers a secure and efficient reversible data hiding scheme in encrypted images, and thus, it can be used in privacy-preservation image storage and transmission in cloud-based systems.***

Keywords- Reversible Data Hiding in Encrypted Images (RDH-EI), Edge-Directed Prediction, Multi-MSB Prediction, Prediction Error Embedding, Image Encryption, Data Embedding Capacity, Lossless Image Recovery and Secure Image Processing.

I. INTRODUCTION

With the fast evolving cloud computing as well as the multimedia communication technologies, the need to have images that are safely transmitted and stored has been a significant concern. Images with sensitive contents should be secured against unauthorized access but should still be accessible to be expanded with additional information in a sensitive image in various real life processes such as medical imaging, military communications and cloud-based data storage. One way to conceal secret data in a cover image is Reversible Data Hiding (RDH), which allows the secret data to be hidden into a cover image in such a way that the secret data and original image may be recovered perfectly. However, since there is a possibility of coding pictures to protect the information within them before the pictures are transmitted across or stored, the traditional RDH techniques cannot be implemented directly. In order to overcome this issue, Reversible Data Hiding in Encrypted Images (RDH-EI) has emerged as a hot research subject which is an integration of image encryption as well as reversible data hiding. RDH-EI also enables the owners of the data to encrypt pictures and outsource them on cloud servers without revealing the nature of the images and more data can be added to it.

A. Objective

The primary purpose of the research is to ensure a successful and secure reversible method of data hiding within encrypted pictures that enhances the data embedding ability and simultaneously retains the original image quality. It will be suggested to implement edge-directed prediction with the multi-MSB self-prediction scheme that should improve the accuracy of prediction and effective data hiding in the encrypted grayscale images. By adaptive prediction and dynamic selection of MSBs, the system will target at maximizing the performance of embedding and at the same time being able to restore the hidden data and the original image without information being lost. The study will also promote the level of data confidentiality and make sure that images could be accessed through encryption and user authentication with the assistance of OTP. Lastly, the objective of the study is to create a reliable RDH-EI system that will allow the delivery of images safely, the confidentiality of personal data, and the reversibility of data in the cloud-based environment.

B. Scope

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

In this research paper, the scope is reduced to the design and implementation of a reversible data hiding of encrypted grayscale images, to facilitate the safety of data and to obtain a more effective way of embedding in the cloud-based environment. The proposed system is a hybrid of edge directed prediction and multi-MSB self-prediction algorithm to increase the accuracy of prediction and capacity of embedding data and to preserve the image quality. The major interest of the research will be on how to add additional information into coded images in such a way that the hidden information and the original image can be entirely recreated with no information loss. In addition, the proposed scheme also encompasses the encryption algorithms as well as the application of the OTP-based authentication to achieve the security of the access to the embedded pictures. Embedding capacity, prediction accuracy, security of encryptions, and image recovery are the areas that this research will cover. However, it can only attain grayscale images and considerable focus is given to prediction-based reversible data hiding methods in storing and transmitting of images among cloud computing environments to safeguard images.

II. LITERATURESURVEY

RDH has become a significant instrument of information analysis and processing of multimedia. RDH enables the addition of hidden information into an electronic photograph and in tandem, it was possible to restore the original glory of the photograph once any data was deleted and replaced in any manner. It is what makes RDH particularly applicable to the applications that are sensitive to the information like medical imaging, military communications and cloud-based data storage where integrity and confidentiality of the information has been the major issue [1]. The major traditional ways of RDH data manner were to place it directly in unencrypted images by approaches like histogram shifting and difference expansion. Such methods despite the good embedding capacity that it offered could not offer adequate security provisions to the image contents as they pass across insecure networks [2].

Scholars came up with an idea of Reversible Data Hiding in Encrypted Images (RDH-EI), in an effort to reduce the issue of image privacy. This technique involves the owner of the image encrypting the original image first before it is outsourced to a third-party server or a cloud computing system [3]. Addition of more data can then be added to the encrypted image without revealing the initial message. According to Zhang (2011), one of the earliest approaches to RDH-EI however, the suggested approach was, the encrypted images were divided into blocks and the embedded data were flipped by reversing some bits. Although the method offered reversible data hiding to encrypted images, it was inadequate in terms of capacity to embed and was associated with a rather high distortion in a retrievable image [4].

After that, Hong et al. (2012) perfected Zhang by proposing a side-match algorithm, which utilized spatial correlation between matching pixels to reduce the errors of prediction [5]. The process of recovering the image was improved significantly by the technique and a reduced distortion was caused when extracting the data. The embedding ability, however, was extremely bad and the algorithm still required additional peripheral knowledge in order to re-construct the original image [6]. After this, Wu and Sun (2013) suggested a prediction error expansion (PEE) based RDH algorithm that enhanced the efficiency of embedding by taking advantage of prediction errors between adjacent pixels. Their method was superior in embedding capacity and reduced distortion over the previous RDH methods [7].

With the introduction of the prediction based methods, researchers began to think about edge directed prediction algorithms to enhance the accuracy of prediction [8]. The idea behind edge-directed prediction (EDP) is based on the characteristics of edges of an image and it is a better predictor of the pixel value based on the analysis of the surrounding pixel arrangement. One method of RDH that was suggested by Li et al. (2016) was based on edge-based prediction to reduce the prediction error and improve the embedding capacity [9]. Results of the experiment showed improved peak signal-noise ratio (PSNR) and embedding results. However, the prediction accuracy can be still affected in the complicated image regions having disordered textures [10].

Multi-bit embedding techniques are the other significant advancement in the research of RDH-EI. The conventional RDH techniques usually store data based on the least significant bit (LSB) of a pixel, limiting its total capacity [11]. To address this shortcoming, various researchers suggested multi-MSB embedding plans in which a number of most important bits are used to enhance the data embedding capacity [12]. These methods greatly enhanced the embedding capacity and needed special methods of predicting to ensure the image quality and avoid over-distortion [13].

More recent research has been done on integrating prediction-based methods with the adaptive embedding strategies to enhance the performance of the RDH-EI systems. Adaptive prediction schemes examine the local image properties and respectively modify the embedding strategy that enables the quality of image to be high and the embedding capacity augmented [14]. Moreover, RDH frameworks have been coined with encryption methods to make images transmission and storage in cloud environments secure. There are also systems that have provisions of authentication to prevent unauthorized access to encrypted images like OTP based verification [15].

III. PROPOSED SYSTEM

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The suggested system presents a high level of data concealment reversible algorithm on the encrypted pictures that incorporates image encryption, edge-directed prediction (EDP), and multi-MSB self-prediction algorithm to enhance image covering capacity and maintain image reconstruction quality. In this case the original grayscale image is encrypted by the owner of the data to protect the information that is contained in the image and then any other information is inserted. To ensure the transmission and storage of the visual content of the picture, which is confidential information, one can encrypt the image with the help of image encryption, particularly when working with clouds. Once the image is encrypted, it then uses the reversible data hiding techniques in order to infuse secret information without exposing the information that the original picture carries.

To utilize the given method, an edge-directed prediction (EDP) algorithm is employed to improve prediction accuracy and embedding capacity. In edge-directed prediction, the values of the adjacent pixels are compared and edge data are detected in the image to make more accurate predictions on the pixel. The EDP algorithm enables to minimize the error of the predictions and provides the high quality of the image during the embedding process by considering spatial correlation of neighbouring pixels. This prediction scheme is particularly effective in preserving meaningful image content particularly in edges and textured regions where predictive performance is extremely important.

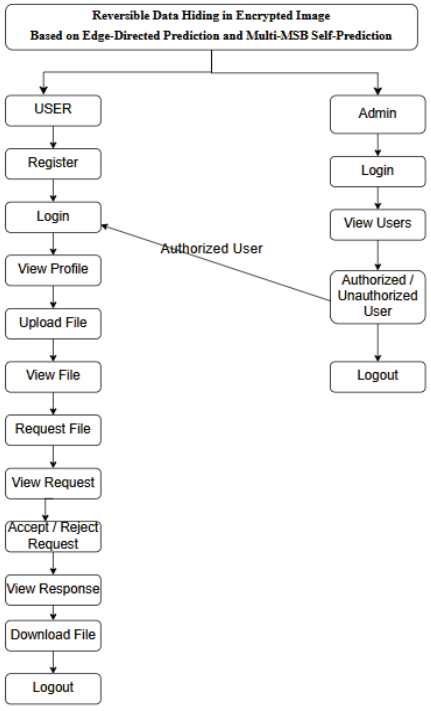

Fig. 1. Block diagram for proposed system

IV. METHODOLOGY

The design of a secure and efficient reversible data hiding approach in encrypted images by image encryption, edge-directed prediction, and multi-MSB self-prediction mechanism will be used as the study methodology. The system will also guarantee that it safely implants additional information in the encrypted grayscale pictures and the concealed information along with the original picture can be restored completely and not a single information was lost. The algorithm has a series of steps like image encryption, edge-directed prediction, multi-MSB prediction, data embedding and data extraction along with image recovery.

1. Image Encryption

The encryption of the images is the most crucial in the proposed protocol of Reversible Data Hiding in Encrypted Images (RDH-EI) whereby the encryption forms a good background in which the confidentiality of the original image information can be preserved. Here the grayscale image is encrypted using an encrypted encryption algorithm by the owner of the data and then data embedding would ensue. The encrypting algorithm alters the initial values of the pixels to become incoherent and actually eliminates the attacks of the unauthorized access, visual interpretation and statistical analysis. This will do much in disconnecting the natural pixel affiliation of the initial picture and will be required where the transmission of delicate pictures to the cloud or the cloud storage will be required. The image will then be coded and the coded image will be the input to the next data hiding process by making sure that only the auxiliary data will be incorporated in encrypt domain. The given system will offer the high degree of deterrence to the security because the encryption and embedding of the data will be divided to ensure the safety of not only images but also the concealment of information.

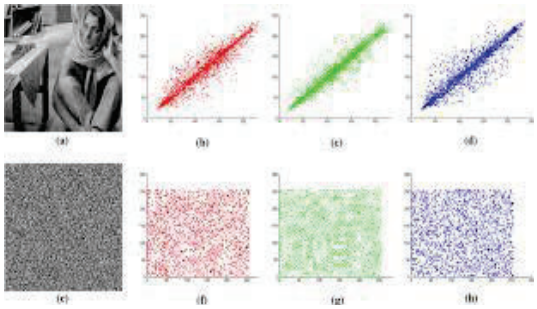

Fig. 2. Encryption image

It is actually a pixel correlation analysis and as such it is easy to determine the efficiency of image encryption as

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

part of the Reversible Data Hiding in Encrypted Images (RDH-EI) scheme.

2. Reversible Data Hiding in Encrypted Images:

Reversible Data Hiding in Encrypted Images (RDH-EI), is a technique of data security that is utilized to add secret information to an encrypted image without loss to the original image that can again be restored to its perfection once the secret information is removed. The technique is an integration of two important processes, which are image encryption and reversible data hiding (RDH). The RDH-EI data owner encrypts the original image keeping the visual content of the image intact and sends the encrypted image to the external server or cloud data. After encrypting the image, additional information, such as authentication data, metadata or secret messages can be overlaid on the encrypted image and it does not show any indication of the contents of the original image. The main advantage of RDH-EI is that it would allow storing data safely, and to retrieve the hidden data but the initial image at the recovery phase. The method finds extensive use in the practice of secure cloud storage, protection of medical images, military communication and transmission of multimedia that are privacy-related.

RDH-EI Mathematically represented.
Where the original grayscale image may be modeled as:

$$I = \{I(i,j)\}$$

Where,
$I(i,j)$ represents the pixel value at position (i,j).

1. Image Encryption:
The original image is encrypted using an encryption key Ke.

$$E(i,j) = I(i,j) \oplus Ke$$

Where,

$E(i,j)$ = encrypted image pixel
Ke = encryption key
$\oplus$ = XOR operation

The encrypted image is:

$$E = \{E(i,j)\}$$

2. Prediction Error Calculation:

The prediction error is calculated as:

$$e(i,j) = E(i,j) - P(i,j)$$

Where,

$e(i,j)$ = prediction error

3. ata Embedding

Let the secret data bit be b.

The modified prediction error becomes:

$$e'(i,j) = 2 \times e(i,j) + b$$

Then the embedded pixel becomes:

$$E'(i,j) = P(i,j) + e'(i,j)$$

Where,

$E'(i,j)$ = encrypted image with embedded data.

4. age Recovery

The original pixel value is reconstructed as:

$$I(i,j) = P(i,j) + e(i,j)$$

After decryption:

$$I = E'(i,j) \oplus Ke$$

Thus, the original image is perfectly recovered.

3. Multi-MSB Self-Prediction:

Multi-MSB Self-Prediction is a reversible data hiding scheme, which is used to improve the capacity of embedded data on encrypted pictures. In the traditional methods of data hiding, a covert data is usually encoded on the Least Significant Bit (LSB) of pixel values as a modification of LSB results in the least amount of distortion on an image. However, LSB-based methods possess low embedding capacity due to the fact that only one bit per pixel can be the highest possible data embedding capacity that is most commonly followed. In order to overcome this disadvantage, Multi-MSB Self-Prediction method uses multiple Most Significant Bits (MSB) of pixels values to encode secret information.

Multi-MSB Self-Prediction Mathematically Representation:

Encryption of the image can be represented as:

$$E = \{E(i,j)\}$$

Where,

$E(i,j)$ Represents the pixel value at position (i,j).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

3. *1. Pixel Prediction*

The predicted pixel value is calculated using neighbouring pixels.

$$P(i,j) = (E(i-1,j) + E(i,j-1) + E(i+1,j) + E(i,j+1))/4$$

Where,

$P(i,j)$ is the predicted pixel value.

2. MSB Prediction:

The predicted MSB bits are obtained from the predicted pixel value.

$$MSB\_k(P(i,j)) = (p7, p6, \ldots, p(8-k))$$

In the event that the predicted MSB bits are similar to the original MSB bits, these bits can be taken as predictable and embedded.

3. Data Embedding:

Let the secret data bit sequence be

$$D = \{d1, d2, \ldots, dk\}$$

The MSB bits of the pixel are modified to embed the secret data:

$$E'(i,j) = (d1\ d2 \ldots dk\ b(7-k) \ldots b0)$$

Where,

$E'(i,j)$ is the pixel value after embedding.

V. DISCUSSION AND RESULTS

Performance Graph:

According to the graph it is observed that both embedding performance and recovery performance increase as the size of the batch is increased between 4KB to 256KB which implies that RDH-EI algorithm is more effective with the larger size of data. The embedding performance gains rapidly with the peak being 4MB which shows that the algorithm can embed data better with a larger size of the input. Similarly, the recovery performance also increases slowly with an increase in the size of the batch and hence the ability of the system in restoring the original image and also recovering the hidden information.

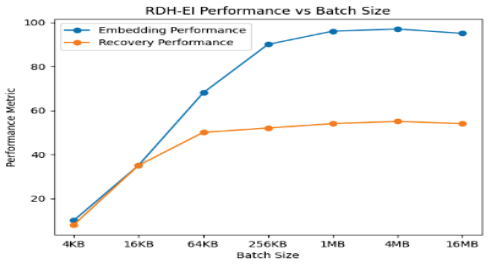

Fig. 3. RDH-EI Working Performance

Encryption and Decryption Timing:

The graph that is called the Encryption and Decryption Timing vs Image Size shows the correlation between the image size and the time required to perform the encryption and decryption of the messages in the proposed system. The horizontal axis is different image sizes (4KB to 16MB) and the vertical one is time in which the processing has occurred (milliseconds (MS)). There are two curves in the graph, which are Encryption Time and Decryption Time (blue and orange line, respectively).

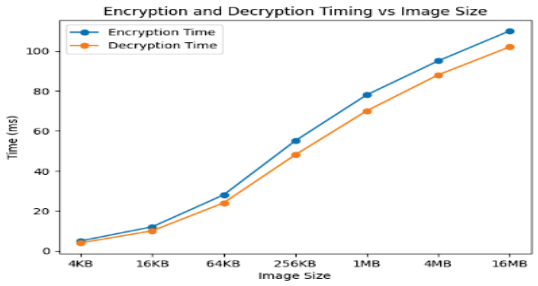

Fig. 4. Encryption and Decryption

Storage capacity of Encryption Image:

Contrary to what the graph shows the smaller images such as 4KB and 16KB do not have a lot of room to hold any hidden information. The storage capacities begin to rise gradually when the image sizes are increased to 64KB and 256KB image size. When the size of the image is 1MB and above, a steep increase would be registered since at this stage the encrypted image has the capacity to store a lot of concealed information.

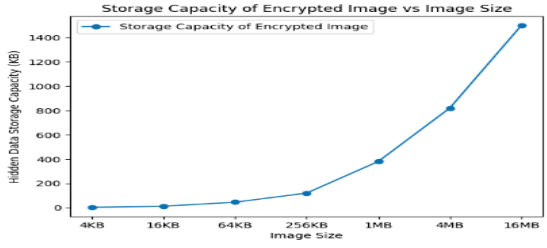

Fig. 5. Storage capacity of encryption image

VI. CONCLUSION

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The paper has proposed high capacity Reversible Data Hiding in Encrypted Images (RDH-EI) scheme to enhance the procedure of attaching safe data and securing images in the cloud computing system. The solution proposed is a combination of edge-directed prediction (EDP) and multi-MSB self-prediction algorithm, which will guarantee the accuracy of prediction and the capacity of the data embedding at the same time maintain the high image quality. The system encrypts the original grayscale image to ensure the content in the visual is safe and adds hidden messages to the encrypted image with the help of plans of adaptive embedding through prediction. Using experimental analysis, it is established that the method suggested has achieved an efficient performance in embedding, recovery of the data and lossless reconstruction of the original image. Further, the results show that embedded capacity increases with the size of images simultaneously as the encryption and decryption speed are balanced. The confidentiality and integrity of the transmitting data is also enhanced by the integration of the security access mechanism. Overall, the suggested RDH-EI is an effective and scalable technique of secure transmission of pictures, privacy, and reversible data extraction, and it could be implemented in secure cloud storage, medical image security, and confidential multimedia transmission.

VII. FUTURE ENHANCEMENTS

Although the proposed Reversible Data Hiding in Encrypted Images (RDH-EI) algorithm is recording promising performance levels with regards to embedding capacity and prediction and recovery of the image with security, several limited aspects can be enhanced in the future research. The proposed method can be extended to the color images and high-resolution multimedia data to make it more pertinent to the multimedia systems in real-life settings, which can be studied further. In addition, one can make it more advanced through the introduction of advanced machine learning or deep learning prediction models to improve prediction accuracy in the more complex parts of images, as well as make embedding more efficient. There is, however, the possibility that the integration of more enabling encryption algorithms and blockchain-based protection systems may provide a more effective protection to the sensitive image data in the cloud-based settings. Further, another method of adapting the system to suit the real-time applications such as the secure video transmission system and the large-scale image storage systems is to simplify the algorithm to reduce the computational complexity and processing time. The adaptive embedding and hybrid data embedding methods also might be explored in the future to acquire even more embedding capacity and be able to preserve the high image quality and complete reversibility. Typically, such enhancements can produce a far-greater scalability, security, and performance of RDH-EI systems in upper-level multimedia security applications.

VIII. REFERENCES

[1] Y. Qiu, “Reversible Data Hiding in Encrypted Images Based on Edge-Directed Prediction and Multi-MSB Self-Prediction,” *IEEE Access*, vol. 13, pp. 63000–63012, 2025, doi: 10.1109/ACCESS.2025.3558369.

[2] Y. Wang, G. Xiong, and W. He, “High-capacity reversible data hiding in encrypted images based on pixel-value-ordering and histogram shifting,” *Expert Syst. Appl.*, vol. 211, Jan. 2023, doi: 10.1016/j.eswa.2022.118600.

[3] H. ZOU and G. CHEN, “Reversible data hiding in encrypted image with local-correlation-based classification and adaptive encoding strategy,” *Signal Processing*, vol. 205, Apr. 2023, doi: 10.1016/j.sigpro.2022.108847.

[4] 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, doi: 10.1109/TIFS.2013.2248725.

[5] S. Xu, C. C. Chang, and J. H. Horng, “A Steganography Based on Optimal Multi-Threshold Block Labeling,” *Computer Systems Science and Engineering*, vol. 44, no. 1, pp. 721–739, 2022, doi: 10.32604/csse.2023.026046.

[6] C. Qin, X. Qian, W. Hong, and X. Zhang, “An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer,” *Inf. Sci. (N Y).*, vol. 487, pp. 176–192, Jun. 2019, doi: 10.1016/j.ins.2019.03.008.

[7] Y. Fu, P. Kong, H. Yao, Z. Tang, and C. Qin, “Effective reversible data hiding in encrypted image with adaptive encoding strategy,” *Inf. Sci. (N Y).*, vol. 494, pp. 21–36, Aug. 2019, doi: 10.1016/j.ins.2019.04.043.

[8] Z. L. Liu and C. M. Pun, “Reversible data-hiding in encrypted images by redundant space transfer,” *Inf. Sci. (N Y).*, vol. 433–434, pp. 188–203, Apr. 2018, doi: 10.1016/j.ins.2017.12.044.

[9] S. Yi and Y. Zhou, “Separable and Reversible Data Hiding in Encrypted Images Using Parametric Binary Tree Labeling,” *IEEE Trans. Multimedia*, vol. 21, no. 1, pp. 51–64, Jan. 2019, doi: 10.1109/TMM.2018.2844679.

[10] X. Wang, C. C. Chang, and C. C. Lin, “Reversible data hiding in encrypted images with block-based adaptive MSB encoding,” *Inf. Sci. (N Y).*, vol. 567, pp. 375–394, Aug. 2021, doi: 10.1016/j.ins.2021.02.079.

[11] X. Zhang, “Separable reversible data hiding in encrypted image,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012, doi: 10.1109/TIFS.2011.2176120.

[12] X. Zhang, “Reversible data hiding in encrypted image,” *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, 2011, doi: 10.1109/LSP.2011.2114651.

[13] W. Hong, T. S. Chen, and H. Y. Wu, “An improved reversible data hiding in encrypted images using side match,” *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, 2012, doi: 10.1109/LSP.2012.2187334.

[14] M. Li, H. Ren, Y. Xiang, and Y. Zhang, “Reversible data hiding in encrypted color images using cross-channel correlations,” *J. Vis. Commun. Image Represent.*, vol. 78, Jul. 2021, doi: 10.1016/j.jvcir.2021.103166.

[15] X. Li, J. Li, B. Li, and B. Yang, “High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion,” *Signal Processing*, vol. 93, no. 1, pp. 198–205, Jan. 2013, doi: 10.1016/j.sigpro.2012.07.025.