**REVERSIBLE DATA HIDING THROUGH BLOCK WISE IMAGE ENCRYPTION**

Project submitted to the

SRM University – AP, Andhra Pradesh

for the partial fulfillment of the requirements to award the degree of

**Bachelor of Technology**

In

**Computer Science and Engineering**

**School of Engineering and Sciences**

Submitted by

**Hema Harshitha Jupalli - AP21110011391**

A picture containing text

Description automatically generated

Under the Guidance of

**Dr.Manikandan V M**

**SRM University–AP**

**Neerukonda, Mangalagiri, Guntur**

**Andhra Pradesh – 522 240**

**November, 2023**

# Certificate

Date: 30-Dec-24

This is to certify that the work present in this Project entitled “**Reversible Data Hiding Through Block Image Encryption**” has been carried out by **Hema Harshitha Jupalli,** the supervision of **Dr.Manikandan V M**. The work is genuine, original, and suitable for submission to the SRM University – AP for the award of Bachelor of Technology in **Computer** **Science and Engineering .**

**Supervisor**

Dr. Manikandan V M,

Assistant Professor,

CSE Department,

SRM University - AP

# Acknowledgements

I would like to convey our sincere appreciation to the people and organizations who supported me throughout the completion of this research project on Reversible Data Hiding Through Block Wise Image Encryption

First and foremost, I extend my sincere thanks to our mentor **Dr. Manikandan V M** for his invaluable guidance and unwavering support. His expertise, patience, and encouragement were instrumental in shaping our understanding of the subject matter and refining our research approach.

I deeply thank SRM University Amaravati for providing the necessary resources, including access to libraries, software, and computational facilities, which were essential for conducting experiments and analyzing data. The conducive research environment provided by the institution significantly contributed to the successful completion of this project.

Finally, I thank all the authors, researchers, and experts whose work laid the foundation for this project. Their innovative ideas and contributions to the field of reversible data hiding and image encryption served as a source of inspiration for our research.

# Table of Contents

[Certificate i](#_Toc152400890)

[Acknowledgements iii](#_Toc152400891)

[Table of Contents v](#_Toc152400892)

[Abstract vii](#_Toc152400893)

[Abbreviations ix](#_Toc152400894)

[List of Figures xi](#_Toc152400895)

[1. Introduction 1](#_Toc152400896)

[2. Methodology 4](#_Toc152400897)

[2.1 Proposed Approach 4](#_Toc152400898)

[2.2 Output Analysis 5](#_Toc152400899)

[3. Discussion 9](#_Toc152400900)

[4. Conclusion 12](#_Toc152400901)

[5. Future Work 14](#_Toc152400902)

[6. References 16](#_Toc152400903)

# Abstract

Digital data security and information hiding are critical concerns in multimedia communication and storage. Reversible data hiding techniques aim to embed additional data within digital content like images, videos while ensuring both security and the ability to perfectly reconstruct the original content after data extraction. In this report we propose an approach to embed message in an image using a key value. The image is divided into k x k blocks, each block is embedded with part of message and encrypted by block based X-OR operation. At last, the decryption is done by performing reverse X-OR operation between image blocks and the key. The results show the image recovery is lossless with PSNR value equal to INF dB and data extraction without any error.

# Abbreviations

RDH Reversible Data Hiding

RDHEI Reversible Data Hiding In Encrypted Images

PSNR Peak Signal-to-Noise Ratio

INF Infinity

dB Decibel

XOR Exclusive OR operation

# List of Figures

Figure 1. Basic idea of RDH…………………........................................................1

Figure 2. Encryption of image……………….........................................................4

Figure 3. Original image, Encrypted image and Decrypted image…………...5

Figure 4. Original image, Encrypted image and Decrypted image…………...5

Figure 5. Original image, Encrypted image and Decrypted image…………...6

Figure 6. Original image, Encrypted image and Decrypted image…………...6

Figure 7. Original image, Encrypted image and Decrypted image…………...6

Figure 8. Original image, Encrypted image and Decrypted image…………...7

Figure 9. Original image, Encrypted image and Decrypted image…………...7

Figure 10. Original image,Encrypted image and Decrypted image…………..7

# Introduction

Reversible data hiding, a technique employed to conceal additional information within digital files like images or audio tracks without altering their appearance. This technique ensures that the hidden data can be extracted without any loss or changes to the original file.

The importance of reversible data hiding lies in its ability to securely embed supplementary information within files while allowing for its seamless retrieval when needed. This method serves as a safeguard for sensitive data and enables covert communication through concealed messages. Reversible data hiding has been an evolving concept, continuously refined to improve its effectiveness. Its applications are diverse, ranging from securing copyright information within multimedia content to ensuring the confidentiality of patient data in medical imaging.

In reversible data hiding, extra information is embedded into the carrier by modifying certain parts of the carrier data without altering it significantly. This is typically achieved by utilizing the redundant or less significant bits within the carrier. The technique employs various methods to achieve its objectives. Some approaches segment files into smaller parts for secure data hiding, while others utilize specific codes or algorithms to embed and extract hidden information, resembling a type of secret language known only to certain individuals.

MESSAGE

ENCRYPTED

IMAGE

IMAGE

RDH

ALGORITHM

DECRYPTION

Fig1: Basic idea RDH

MESSAGE

IMAGE

Reversible Data Hiding (RDH) methods initially created space for extra data within digital images using lossless compression, striving to minimize distortion post-embedding. Over the past two decades, RDH techniques, primarily rooted in histogram shifting and difference expansion, showcased promising rate-distortion performance but were confined to the plain text domain of images. Addressing privacy concerns, reversible data hiding in encrypted images (RDHEI) emerged, encrypting images before embedding data, ensuring error-free extraction, and lossless image restoration.

# Methodology

## 2.1 Proposed Approach

Initially, an original image 'I' is chosen, alongside a randomly generated matrix 'R' of the same size as 'I'. Through a bitwise XOR operation between 'I' and 'R', an encrypted image 'E' is produced. Consider a simplistic example using a 32x32mage matrix 'I' comprising pixel values and a corresponding random matrix 'R'. The XOR operation between 'I' and 'R' results in the creation of 'E', signifying the encryption process.

Following this, the image 'I' is divided into smaller blocks B0, B1, B2, B3 each with 16x16 size to facilitate data embedding. An additional secret image, typically comprising 4 bits , is embedded into these designated blocks. Concurrently, matrices of identical size as 'I' are constructed using keys K0 and K1, aligning them with respective blocks (e.g., K0B0, K0B1, K0B2, K0B3, K1B0, K1B1, K1B2, K1B3).

The message bits, represented as 1s and 0s, are strategically embedded within the corresponding blocks of K1 and K0, essentially integrating the message within the encryption process, culminating in the creation of the final encrypted image 'E'. The

K0BO K0B1

K0B2 K0B3

BO B1

B2 B3

^

K0

Encrypted matrix

Image matrix

Key=1010

K1BO K1B1

K1B2 K1B3

^

K1

BO B1

B2 B3

Fig2. Encryption of image

The decryption and message retrieval process ensue upon the transmission of the encrypted image 'E' to the receiver. The receiver engages in XOR operations between blocks and their corresponding matrices (e.g., B0 XOR K0B0, B0 XOR K1B0, B1 XOR K0B1, B1 XOR K1B1, and so forth) to initiate the decryption process.

Calculate the two versions, v1 and v2 using

V1= B0 ^ K0B0

V2= B0 ^ K2B0

assists in differentiating between potential encrypted versions. By analyzing pixel differences that is the absolute difference between the adjacent values of matrix (|a-b|) derived from these versions, matrices M0 and M1 are generated, facilitating the identification of the correct encrypted image based on the matrix whose summation is smaller (M0 or M1).

Finally, the extraction of the embedded secret message from the identified correct encrypted image involves decoding the message bits embedded in K1 and K0, thereby retrieving the concealed information originally embedded within the image 'I'. This comprehensive process underscores the intricate steps involved in reversible data hiding through encryption, ensuring secure data transmission and retrieval while maintaining the integrity of the original image.

## 2.2 Output Analysis

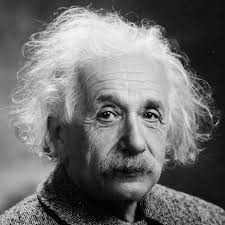
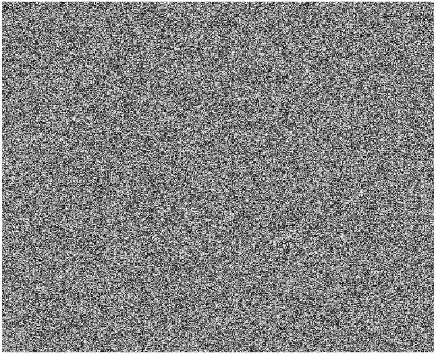
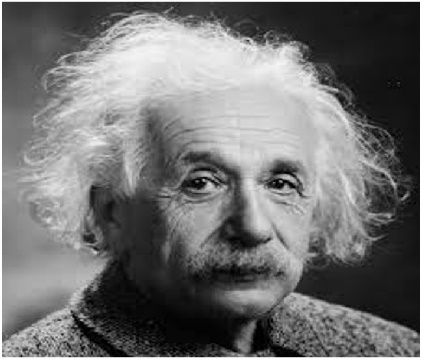
  

Fig3.Original image, Encrypted image and Decrypted image

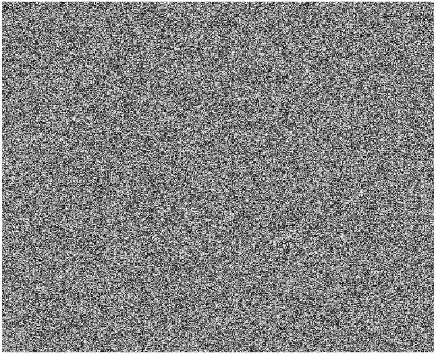
  

Fig4.Original image, Encrypted image and Decrypted image

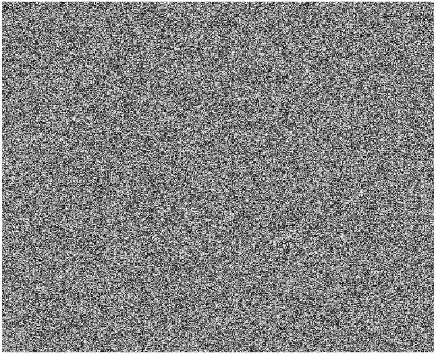


Fig5.Original image, Encrypted image and Decrypted image

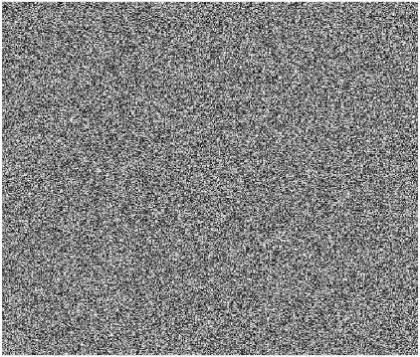
  

Fig6.Original image, Encrypted image and Decrypted image

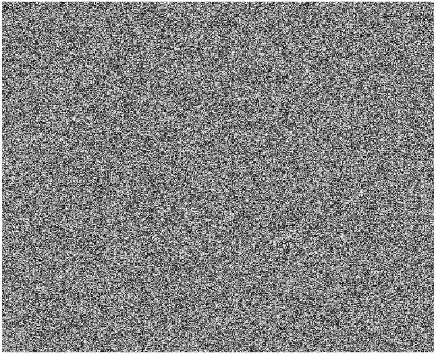
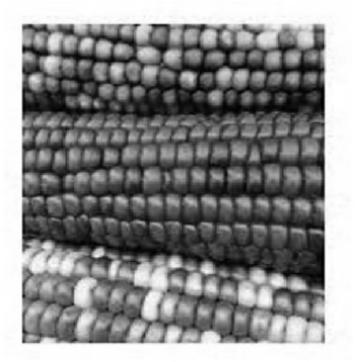
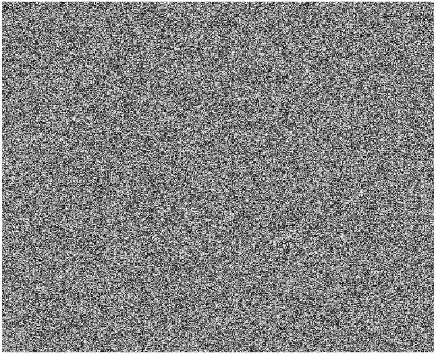
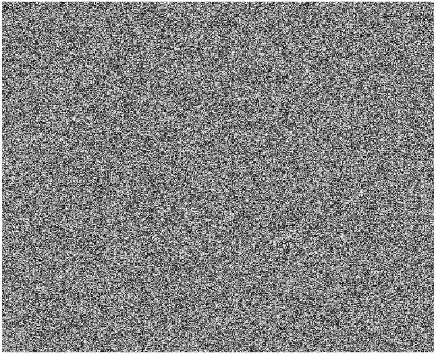
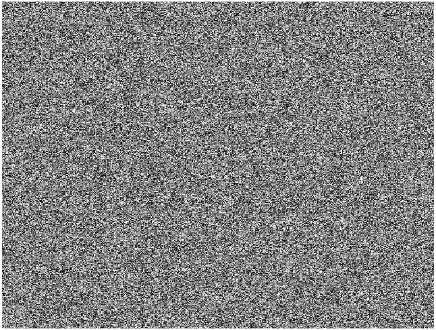
  

Fig7.Original image, Encrypted image and Decrypted image

Fig8.Original image, Encrypted image and Decrypted image

Fig9.Original image, Encrypted image and Decrypted image

Fig10. Original image, Encrypted image and Decrypted image

# Discussion

Through the process of encryption, embedding, and subsequent decryption, the original image 'I' is preserved, and the embedded message is successfully retrieved. The output of the algorithm showcases the ability to encode sensitive information within the image while maintaining the image's visual quality. The decryption process allows the receiver to accurately extract the embedded message from the encrypted image 'E'. However, the algorithm exhibits limitations in terms of the size of the message that can be embedded, typically constrained by the number of bits available within the image blocks. This restricts the capacity for larger or more complex messages to be hidden within the image, thus need of improvements for enhanced data embedding capabilities.

The obtained output metrics, PSNR (Peak Signal-to-Noise Ratio) reflecting infinity and Hamming Distance at 0, are indicative of exceptional image fidelity and perfect message retrieval. A PSNR value of infinity signifies that the original image and the retrieved image are identical, indicating no loss in image quality throughout the encryption, embedding, and decryption process. Similarly, a Hamming Distance of 0 signifies an exact match between the embedded message and the extracted message, highlighting error-free data retrieval.

The algorithm demonstrates an exceptional ability to embed and recover the hidden message without introducing any distortions or discrepancies in the original image. This signifies the robustness of the algorithm in maintaining the integrity and visual quality of the image while securely concealing and accurately retrieving the embedded information. Such high PSNR and a Hamming Distance of 0 validate the effectiveness and reliability of the reversible data hiding process through encryption.

**Ways to Further Enhance the Algorithm:**

Increased Embedding Capacity: While achieving perfect fidelity and accurate message retrieval is commendable, enhancing the algorithm to accommodate larger messages within the image without compromising quality would be beneficial. Exploring methods to increase embedding capacity without impacting image integrity is essential.

Advanced Security Measures: Despite achieving flawless retrieval, implementing more sophisticated encryption techniques or integrating additional security layers could fortify the algorithm against potential attacks or unauthorized access, enhancing its robustness.

Efficiency and Speed Optimization: Although the algorithm demonstrates high performance, optimizing its efficiency and processing speed would enhance its practical applicability. Streamlining processes for faster data embedding and extraction could improve overall usability.

Error Resilience Mechanisms: Introducing error correction or recovery mechanisms within the algorithm would bolster its resilience against potential data corruption or transmission errors, ensuring reliable message retrieval in adverse conditions.

# Conclusion

In Conclusion, the proposed strategy for reversible data hiding in encrypted pictures (RDHEI) that combines key-based encryption with block-based XOR operations offers a reliable way to embed and extract messages within digital images. This method's key characteristics involve dividing the original image into blocks for message embedding and then encrypting it using a randomly generated matrix. Data hiding is ensured by carefully integrating the message bits into the encryption process using XOR operations with key matrices. By breaking the image up into smaller parts, the embedding process is made easier and helps to integrate extra information seamlessly while preserving the general structure and quality of the original image.

The analysis's findings, which show error-free data extraction and lossless image recovery, show how effective the suggested method is. The consideration of the Hamming distance between the embedded message and the recovered message is another feature of the suggested methodology. The accuracy of the data extraction process can be checked by calculating the Hamming distance. The success of the reversible data hiding technique is highlighted by the Peak Signal-to-Noise Ratio (PSNR) value equal to INF dB, which shows the retention of image quality throughout the operation.

# Future Work

**Selecting Adaptive Block Size:**

Adaptive block size selection techniques are a promising area of research that aims to dynamically modify block sizes according to the properties of input images. By using an adaptive technique, the data embedding efficiency is guaranteed to be optimal for a wide variety of images, which may enhance the overall performance of RDHEI.

**Capacity to Embed Messages Dynamically:**

Considering the content and features of images, it is crucial to have the ability to incorporate dynamic messages. By using an adaptive technique, RDHEI will be able to modify its data embedding capacity in response to the intricacy of the content, guaranteeing effective data hiding while maintaining the recovery of high-quality images.

**Actual Time Execution:**

The practical deployment of RDHEI requires optimization for real-time applications. In order to meet the expectations of applications where immediate data embedding and extraction are crucial, future work should concentrate on enhancing processing speed, resource efficiency, and latency. It is also possible to expand the algorithm to support color images.

# References

1. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006, Link: [Google Scholar](https://scholar.google.com/scholar_lookup?title=Reversible%20data%20hiding&author=Z.%20Ni&author=Y.-Q.%20Shi&author=N.%20Ansari&author=W.%20Su&publication_year=2006)
2. B. Ou, X. Li, Y. Zhao, and R. Ni, “Reversible data hiding using invariant pixel-value-ordering and prediction-error expansion,” *Signal Processing: Image Communication*, vol. 29, no. 7, pp. 760–772, 201, Link: [Google Scholar](https://scholar.google.com/scholar_lookup?title=Reversible%20data%20hiding%20using%20invariant%20pixel-value-ordering%20and%20prediction-error%20expansion&author=B.%20Ou&author=X.%20Li&author=Y.%20Zhao&author=R.%20Ni&publication_year=2014)
3. 3.Z.-L. Liu and C.-M. Pun, “Reversible data-hiding in encrypted images by redundant space transfer,” *Information Sciences*, vol. 433-434, pp. 188–203, 2018, Link: [Google Scholar](https://scholar.google.com/scholar_lookup?title=Reversible%20data-hiding%20in%20encrypted%20images%20by%20redundant%20space%20transfer&author=Z.-L.%20Liu&author=C.-M.%20Pun&publication_year=2018)
4. 4.P. Tsai, Y.-C. Hu, and H.-L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” *Signal Processing*, vol. 89, no. 6, pp. 1129–1143, 2009, Link: [Google Scholar](https://scholar.google.com/scholar_lookup?title=Reversible%20image%20hiding%20scheme%20using%20predictive%20coding%20and%20histogram%20shifting&author=P.%20Tsai&author=Y.-C.%20Hu&author=H.-L.%20Yeh&publication_year=2009)
5. X. Zhang, "Reversible data hiding in encrypted images", IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255-258, Apr. 2011, <https://scholar.google.com/scholar?as_q=Reversible+data+hiding+in+encrypted%0Aimages&as_occt=title&hl=en&as_sdt=0%2C31>
6. K. Ma, W. Zhang, X. Zhao, N. Yu and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 3, pp. 553-562, March 2013, doi: 10.1109/TIFS.2013.2248725. <https://ieeexplore.ieee.org/document/6470679/references#references>