www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

# SECRETE SHARING BASED REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES WITH MULTIPLE DATA HIDERS

MR. K. RAMBABU [1], M. LAKSHMI RENUKA [2], V.V. SATYA VISWANTH [3], A. DATTA DEVI [4],
K. BHAVANI NAGA PRASADA REDDY [5], D. ADHITYA [6]

[1] Assistant Professor, Dept. Of ECE, PRAGATI ENGINEERING COLLEGE

[23456]UG Students, Dept. Of ECE, PRAGATI ENGINEERING COLLEGE

## ABSTRACT

This project proposes a novel approach for secret sharing-based reversible data hiding in encrypted images with multiple data hiders. In this method, the confidential information is hidden within encrypted image data in such a way that the original image can be perfectly recovered, ensuring data integrity and confidentiality. The proposed scheme employs a secret sharing technique, where multiple hiders collaborate to embed their individual pieces of secret data into the encrypted image, distributing the burden of hiding across multiple parties. This multi-party approach enhances security by preventing any single hider from fully accessing the original image or its concealed data. The scheme is reversible, meaning that after extracting the embedded secrets, the original encrypted image can be restored without any loss. This feature is critical for applications requiring both data security and image integrity, such as cloud storage, secure image transmission, and medical image processing. The project also investigates various data-hiding algorithms to ensure that the embedding process does not significantly degrade the visual quality of the image or introduce detectable distortions, preserving the image's usefulness in its original encrypted form.

## INTRODUCTION

With the rapid growth of digital communication and cloud storage, ensuring data security and privacy has become a critical challenge. Reversible Data Hiding in Encrypted Images (RDH-EI) is an emerging technique that allows confidential data to be embedded in encrypted images while ensuring complete recovery of both the original image and the embedded data. This technique finds applications in medical imaging, military communication, and cloud-based secure data sharing.

Traditional RDH-EI methods often rely on a single data hider, limiting flexibility and security in multi-user environments. To address this limitation, we propose a Secret Sharing-Based Reversible Data Hiding (SS-RDH) scheme that enables multiple data hiders to embed data independently without compromising security or image quality. The proposed approach leverages secret sharing techniques to distribute the encrypted image across multiple parties, ensuring secure and reliable data hiding.

## LITERATURE SURVEY

### 1. Traditional Reversible Data Hiding (RDH)

Early RDH techniques focused on embedding data into unencrypted images using methods such as:



Index in Cosmos
Mar 2025, Volume 15, ISSUE 1
UGC Approved Journal

- Difference Expansion (DE): Tian (2003) introduced a method that expands pixel differences to embed data while maintaining reversibility.
- Histogram Shifting (HS): Ni et al. (2006) proposed modifying the histogram of pixel values to create space for embedding secret data.
- Prediction-Based RDH: Hong et al. (2009) improved embedding capacity by predicting pixel values and utilizing the prediction error for data hiding.

**2. RDH in Encrypted Images (RDH-EI)**

To ensure both security and reversibility, researchers extended RDH to encrypted images. Key contributions include:

- Vacating Room After Encryption (VRAE): Zhang (2011) introduced an RDH-EI method where an image is first encrypted and then data is embedded by modifying encrypted pixels.
- Vacating Room Before Encryption (VRBE): Hong et al. (2012) improved Zhang's method by reserving space before encryption, leading to better data extraction and image reconstruction.
- Bit-plane-based RDH-EI: Liu et al. (2016) introduced bit-plane techniques to enhance embedding capacity without significantly altering encrypted pixels.

## PROPOSED SYSTEM

In this thesis, I will propose a steganography algorithm to hide textual information in digital colored images. The proposed algorithm is designed to be simple but effective to hide as much information as possible in the image without changing the image size. Also, the algorithm is intended to preserve the quality of the image and to be fast enough for being used in web applications. Another feature of the proposed algorithm is resistance to statistical attacks.

First, the algorithm converts characters to their equivalent ASCII codes, then shifts the codes m bits to the left (e.g., two bits). I use circular shift to preserve shifted bits. Circular shift can make detecting the original message difficult for attackers. I substitute n LSBs of the blue channel of the edge pixels with n bits of the message. Since n bits of the message may be uniformly distributed, their substitution in the LSBs of the blue channel of the edge pixels makes the stego image vulnerable to statistical attacks. Thus, to increase the robustness of the algorithm, I analyze the frequency of the n LSBs of the blue channel of the edge pixels to find their distribution and then generate random numbers based on this distribution. Random numbers are in the range $[0,2^n-1]$ and their number equals to the number of groups of n bits of the message. Then, bitwise XOR operation is performed on each group of n bits of the message and its corresponding random bits. The resulting bits are stored in the LSB of the blue channel of the edge pixels.

Transforming the message using non-uniform distributed random numbers will increase resistance of the algorithm against statistical attacks. To extract the image, I extract the coded length of the message from the stego

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

image first. Then, I extract the seed of random generator and generate enough random numbers in the range [0,2n-1]. Until extracting all groups of n digits from the image, I extract n digits from the blue channel of the edge pixels and perform XOR operation on these n digits and the next random number. I put the result of all XOR operations together and shift it m bits to the right.


Figure.1 The interface of the steganography system

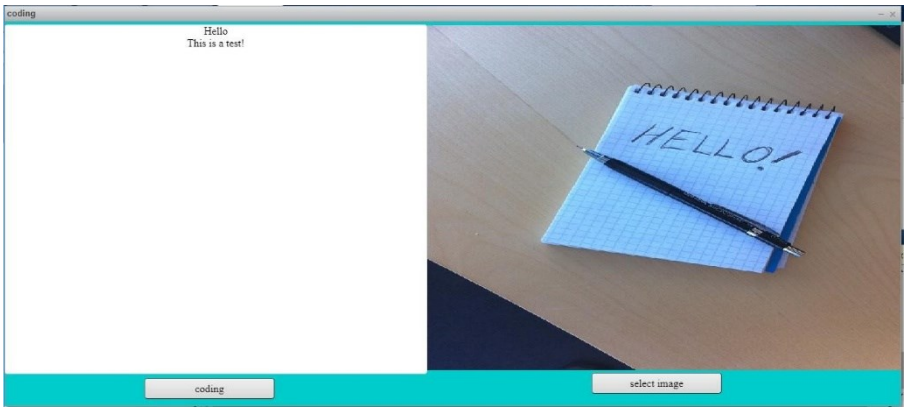
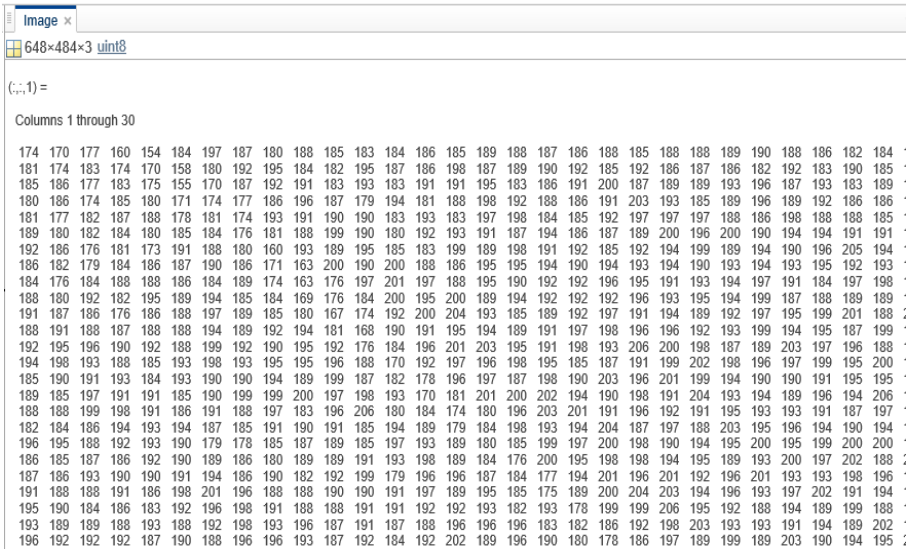



Figure.2 Hiding a message into an image






Index in Cosmos
Mar 2025, Volume 15, ISSUE 1
UGC Approved Journal

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Figure.3 The matrix of the image

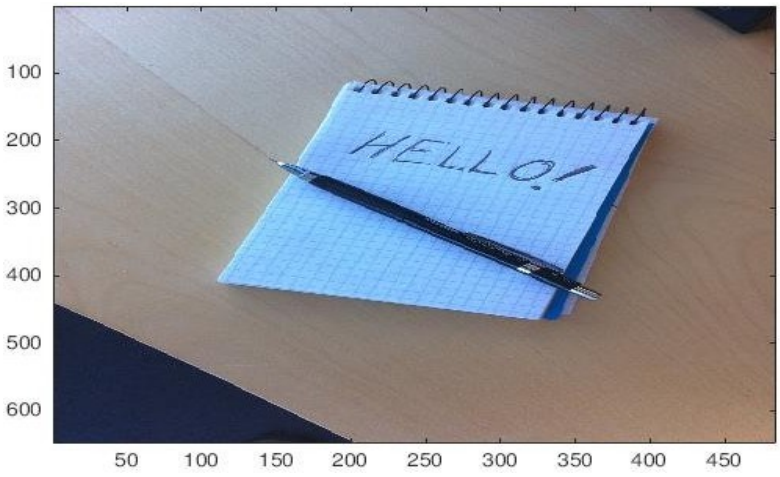



Figure.4 The stego image

I evaluated the proposed algorithm using the following metrics:

Capacity: The number of bits that can be embedded in each image.

Signal-to-noise ratio (SNR) and peak signal-to-noise ratio (PSNR), which indicate the quality of the picture and are defined as (Horé & Ziou, 2010):

$$SNR = 10 \times \log_{10} \frac{\sum_{i=1}^{W} \sum_{j=1}^{H} (O_{ij})^2}{\sum_{i=1}^{W} \sum_{j=1}^{H} (O_{ij} - D_{ij})^2}$$

$$PSNR = 10 \times \log_{10} \frac{\max(O_{ij})^2}{\frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (O_{ij} - D_{ij})^2}$$

where W is the width of the image and H is the height of the image. Oij and Dij are the values of the pixel in row i and column j in the original and stego image, respectively.

## STIMULATION RESULTS



Index in Cosmos
Mar 2025, Volume 15, ISSUE 1
UGC Approved Journal

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Figure.6 Lenna

Figure.5 Barbara Number of edge pixels222867 :

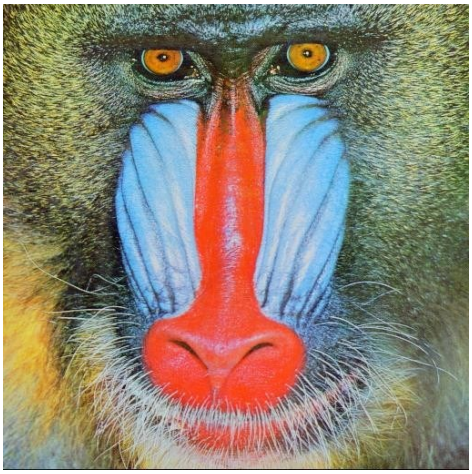


Figure.6 Baboon Number of edge pixels: 177135

Figure.7 Peppers Number of edge pixels: 44481

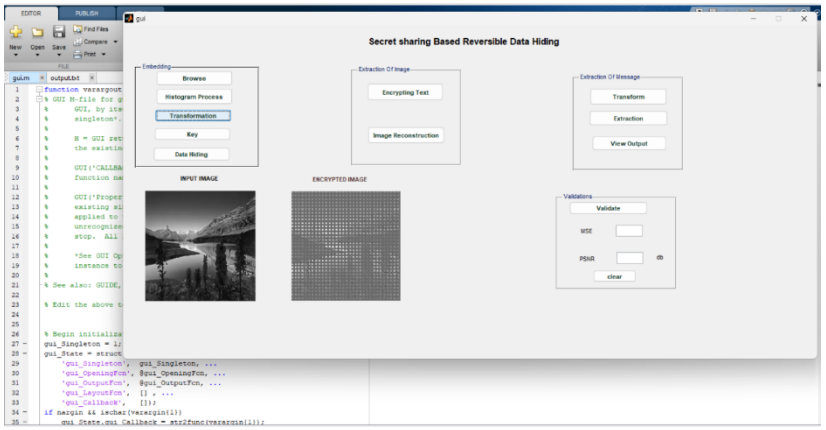



Figure.8 The Input Image is Encrypted

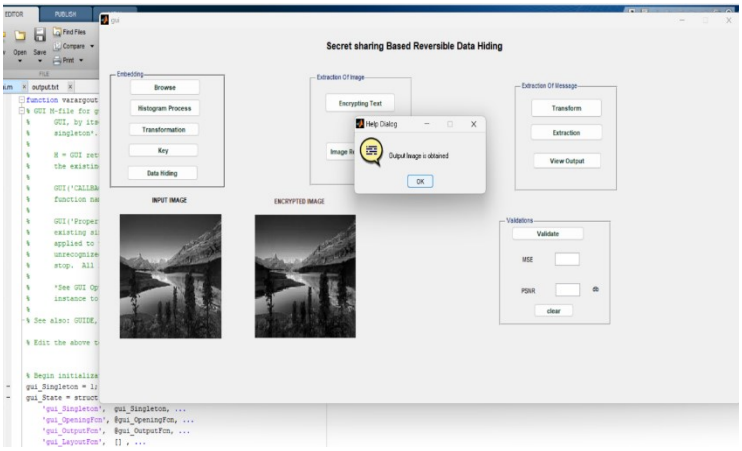



Figure.9 Conversion of Encrypted Image Similar to Input Image



Index in Cosmos
Mar 2025, Volume 15, ISSUE 1
UGC Approved Journal

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

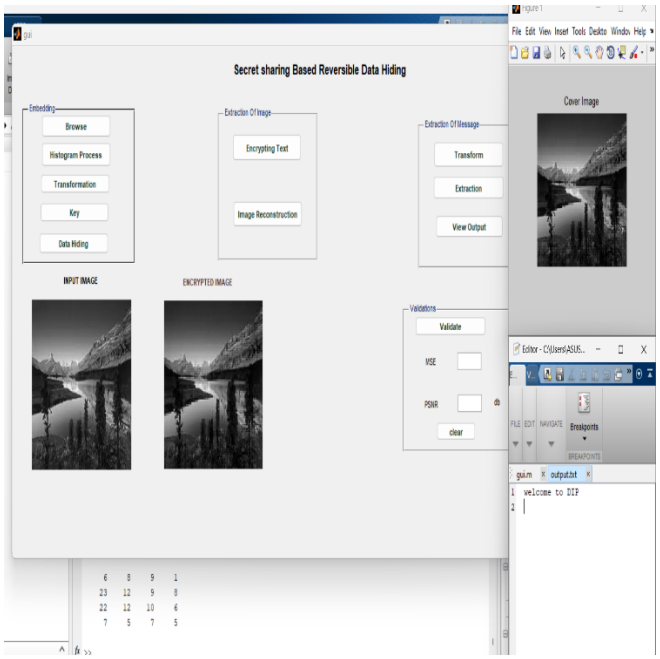



Figure.10 Encryption, Decryption of Image & Secrete Message Shared in Image in text file.

## ADVANTAGES

- The advantage of steganography is that messages do not send consideration to themselves. Clearly detectable encrypted message no matter how tough will stimulate suspicion, and may in themselves be compromising in countries where encryption is illegitimate.
- In steganography, cryptography secures the contents of a message, steganography can be said to secure both messages and connecting parties.
- This approach featured security, capacity, and robustness, the three needed element of steganography that creates it beneficial in hidden exchange of data through text files and creating secret communication.
- There are some important files carrying confidential data can be in the server in and encrypted form and No intruder can receive some beneficial information from the initial file during transmit.
- With the need of Steganography Corporation government and law enforcement agencies can connect privately.
- The major objective of steganography is to connect privately in a completely imperceptible aspect and to prevent drawing uncertainty to the transmission of a hidden information. It is not to maintain others from understanding the hidden data, but it is to maintain others from thinking that the data even exists. If a steganography approach generates someone to suspect the carrier medium, thus the method has unsuccessful.

## APPLICATION

**Hidden Communication**

Text hiding could be utilized to communicate hidden information over public networks such as the Internet. One may embed secret bits into an unnoticeable text message/file which is routinely transmitted over such networks: a greeting, joke, story, etc. Since the text messages/files are sent using unsecured communication channels such as SMS, social media and so on, they are exposed to attacks

**Network Covert Channels**

Text hiding can be used to make covert channels that provide unexpected stealthy communication over the networks. Recently, covert channels were employed by cyber-attacks, i.e., to permit a covert transmission of malware data. Nevertheless, they could also be applied for legitimate goals, such as transmitting illicit information under Internet censorship.

**Unauthorized Access Detection**

Text hiding could also be employed to detect unauthorized access to sensitive documents over private networks. For example, sensitive/confidential documents in a governmental or commercial organization can be marked with identifiers that are difficult to detect. The aim is to trace unauthorized access/use of a sensitive document to a specific user who may have obtained a copy of the marked document. The receiver of such documents should not be aware of the existence of the identifiers [12,40,64].

**Text Hiding Criteria**

There are many things to be considered when programmers design a text hiding algorithm. However, the fundamental criteria can be easily found in recently introduced algorithms: invisibility, embedding capacity, robustness, and security [1]. The communication channel over which the $CM_{HM}$ is transmitted can be noisy or noiseless, for the case of an active or a passive warden, respectively. Also, the steganographer capability to select the CM is often restricted if not altogether non-existent [12].

## CONCLUSION

The original image and the Stego image look identical. The human eye cannot perceive the difference because of the high PSNR result. The technique attempts to find a secret message in the higher layers of the used image and changes the last layer of the corresponding block. This will increase the degree of robustness of the Stego analysis techniques. Bit error = 0 for all experimental results; the embedded secret message is recovered correctly without any errors. The Stego system represents BLIND and PURE steganography, which means the receiving party doesn't require the original image or any secret key sent with the image. High capacity: The experimental results show that the capacity of this system is high.

## FUTURE SCOPE

In this research, RGB images have been used for the proposed steganography algorithm. Images are used in many applications on the internet. The evaluation of the proposed algorithm showed its appropriateness for online applications. There are also other media could be suitable for online steganography. For example, videos are increasingly used on the internet. 1.5 billion people use YouTube, in which 300 hours of video are uploaded every minute (Danny, 2018)! Thus, one direction for the future would be using videos as the cover media and modifying the algorithm accordingly. Since each video consists of many frames, and each frame can be considered as an RGB image, the proposed algorithm can be easily adapted for videos. For sure, the capacity of embedding information in videos is significantly more than images. However, if the algorithm is supposed to be used for online streaming, it must become more efficient to avoid any delay in playing the video.

## REFERENCES

1. Akhter, F. (2013). A Novel Approach for Image Steganography in Spatial Domain. Global Journal of Computer Science and Technology Graphics & Vision, 8(7), 1-6.
2. Andrews, C. E., & Joseph, I. T. (2013). AN ANALYSIS OF VARIOUS STEGANOGRAPHIC
3. ALGORITHMS. International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), 2(2), 116-123.
4. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. IBM System Journal, 35(3), 313-336.
5. Cheddad, A., Condell, J., Curran, & McKevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90, 727-752.
6. Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. (5th ed.). Los Angeles: SAGE Publications.
7. Danny. (2018, April 26). 37 Mind Blowing YouTube Facts, Figures and Statistics – 2018. Retrieved July 1, 2018, from MerchDope: https://merchdope.com/youtube- statistics/
8. Dooley, J. F. (2018). History of Cryptography and Cryptanalysis. Springer.
9. Ferreira, A. M. (2015). An Overview of Hiding and Detecting Stego-data in Video Streams.
10. Fouroozesh, Z. (2014). Image Steganography based on LSB in Spatial Domain. Master Thesis.
11. Fridrich, J., & Goljan, D. S. (2005). Maximum likelihood estimation of secret message length embedded using pmk steganography in spatial domain., Proc. of IST/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VII, 5681, pp. 595-606.
12. Gutub, A. A.-A. (2010). Pixel Indicator Technique for RGB Image Steganography. Journal of Emerging Technologies in Web Intelligence, 2(1), 56-64. Gutub, A., & Fattani, M. (2007). A Novel Arabic Text Steganography Method Using Letter Points and Extensions. WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE), (pp. 25-27). Vienna, Austria.
13. Hassanein, M. S. (2014). Secure Digital Documents Using Steganography and QR Code. PhD Thesis. Department of Computer Science, Brunel University.
14. Horé, A., & Ziou, D. (2010). Image quality metrics: PSNR vs. SSIM. International Conference on Pattern Recognition, (pp. 2366-2369).
15. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: seeing the unseen. *IEEE Computer, 31*(2), 26-34.
16. Kathryn, A. B. (1999). *Encyclopedia of the Archaeology of Ancient Egypt.* New York: Routledge.
17. Kaur, S., Kaur, A., & Singh, K. (2014). A Survey of Image Steganography. *International Journal of Computer Applications Technology and Research, 3*(7), 479-483.
18. Korhorn, K. (2002). *Steganography Uses And Effects On Society*. Retrieved from ComputerProfessionals for Social Responsibility: http://cpsr.org/prevsite/essays/2002/2rr3.html/
19. Lahiri, S., Paul, P., Banerjee, S., Mitra, S., Mukhopadhyay, A., & Gangopadhyaya, M. (2016).
20. Image Steganography On Colored Images Using Edge-Based Data Hiding In DCTDomain. *IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON).* Vancouver, BC, Canada.