International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(April),2026
Received: 18-02-2026 Accepted: 23-03-2026 Published: 01-04-2026

SECRET SHARING BASED REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

Dr. S. Lakshmikanth Reddy,
Associate Professor,
Dept. of Electronics and Communication Engineering,
Annamacharya Institute of Technology and Sciences,
Kadapa, India.
Kanth.srec@gmail.com

Mantha Mohan,
Dept of Electronics and Communication Engineering,
Annamacharya Institute of Technology and Sciences,
Kadapa, India.
mohanmona2156@gmail.com

Shaik Mohammad Arif,
Dept of Electronics and Communication Engineering, Annamacharya Institute of Technology and Sciences, Kadapa, India.
shaikarifarif32@gmail.com

Posa Varun Sai,
Dept of Electronics and Communication Engineering, Annamacharya Institute of Technology and Sciences, Kadapa, India.
varunsaiposa@gmail.com

Nagineni Raviteja,
Dept of Electronics and Communication Engineering, Annamacharya Institute of Technology and Sciences, Kadapa, India.
yadavteja9347@gmail.com

Abstract—The main focus of this project is on a data hiding technique, that enables several users to hide their data in a secure way. The main concept of this technique is to use a combination of secret sharing and homomorphic encryption, which enables the embedding of data directly into an encrypted image without the use of the original image. This enables we to work with our data without revealing the content of the data.

It ensures the NO loss recovery (100% recovery) of the raw image after the extraction.

Keywords — Lossless data hiding, secure images, information sharing, data protection.

I INTRODUCTION

In the past few years, numerous digital images are being generated due to an increase in cloud storage and easy online communication. These digital images may carry vital information, which is why it is becoming a major problem to secure these images. In many applications, data hiding and encryption are used to attain data security.

Data hiding is an approach in which data is embedded inside an image. In conventional data hiding schemes, it has been found that sometimes an image is slightly altered after data is embedded. In some areas, such as medical science and military science, it is not possible to allow an image to be slightly altered. In order to solve this problem, reversible data hiding came into existence, in which data can be perfectly extracted without any loss of data [1]. Because of this

property, it is highly suitable for applications in which accuracy is high.

To enhance security, the research integrated RDH with encryption, which gives us reversible data hiding in encrypted images. This technique involves encrypting an image, followed by embedding the data in the encrypted image, such that the data in the image is protected [2]. This technique can be used in cloud environments, where data privacy should be maintained for both storage and processing [3].

The majority of the conventional techniques for RDHEI concentrate on single data hider, which is a significant drawback of the conventional techniques. For instance, in practical scenarios, there can be a number of users who can hide their data in an image. Therefore, to overcome this drawback, some recent research works have proposed various techniques for multi-user data hiding using secret sharing [4].

Secret sharing is an important technique used to enhance security as well as reliability. It divides the image into several shares, which can only be reconstructed by the authorized user to get the embedded data [5]. Some recent techniques have used distributed systems, which can be used for efficient multi-user data hiding [6].

There is a way of doing this but we still have a lot of problems to fix with encrypted images, for example, how much data we can hide, how long it takes to do it, and how we can make it work for lots of people. To fix this, new ideas have been tried with sharing and other fancy encryption techniques.

For our project, we want to make something that will allow people to hide data, in an encrypted image that is safe, reverses easily, and lots of people can use. We have made something that uses sharing and other techniques of encryption so that we can safely hide data without using the original image. We also have something that lets us retrieve the data we hide and the original image perfectly [7]. We can do this with storing data in the cloud secret messages and other digital data.

There are ways to do this, but we still have a lot of problems to solve, such as how much data we can hide, how long it takes to do it, and how to make it work for a lot of people. To solve this, some new ideas have been tried, using things such as sharing in order to make it work better.

II EXISTING SYSTEM

In the existing system, reversible data hiding (RDH) is used only for plain (unencrypted) images, which means that the images are not encrypted. Reversible data hiding is done by modifying the pixel values of the images [8]. Some of the existing methods used for reversible data hiding include difference expansion, histogram shifting, prediction error, etc. these methods make use of the natural redundancy of images to hide the data, which can be extracted perfectly without any distortion [9]. The above methods are not secure enough, as the image is not encrypted. Anyone who gains access to the image. For better security, reversible data hiding in encrypted images (RDHEI) was introduced [10]. In this method, the image is encrypted, and then the data is embedded in the image. This way, the image remains secure both in storage and transmission.

There are various methods used in the reversible data hiding in encrypted images, which include bit-place, most significant bit prediction, etc. These methods make use of the correlation between two pixels to increase the embedding capacity of the images, maintaining the quality of the images [11]. Some of the methods make use

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(April),2026
Received: 18-02-2026 Accepted: 23-03-2026 Published: 01-04-2026

of recursion to increase the payload of the image.

Although these techniques offer security, most of them are only suitable for use by a single data hider. This is a drawback, as in most cases, there is a requirement for the use of more than one user for hiding their data in the same image. These techniques make use of the relationship between pixels to offer enough space for hiding data without compromising the quality of the image [12].

With the latest developments in the field of the data hiding, some of the techniques make use of models such as secret sharing, LWE, and adaptive coding, which are helpful in improving the security of the image with the maximum amount of data hiding without compromising the quality of the image, ensuring that the image is restored in the correct manner [13]. Moreover, some of the techniques make use of the multi-sever system, which is helpful in the case of hiding in the cloud environment.

Due to all these reasons, it is still necessary to develop a better technique that can be helpful in meeting the requirements of multiple users, ensuring security, and hiding the maximum amount of data in the image without compromising the quality of the image [14].

Limitations

- One common issue is that some methods cannot store more data. If we try to increase the data, the image quality may get affected [15].
- Another problem is that most of the systems allow only one user to hide data. But in real situations, more than one user may need to use the same image [16].
- Some methods are a bit complicated and take more time to process. Because of this, they are not easy to implement [17].
- There is also a problem with maintain both image quality and data capacity. If one increases, the other may decrease [18].
- In some cases, security is not strong enough, especially when the image is not encrypted properly [19].
- Handling multiple users is also not easy. It becomes difficult to manage data from different users while keeping everything secure [20].
- Some methods depend on keys or image shares. If any key or share is missing, then recovering the original image becomes difficult [21].

III PROPOSED SYSTEM

Problem statement

In many real world applications, we don't just need to protect an image. We also need to embed confidential information within the image. However, many existing data hiding methods tend to permanently after the image, which is not acceptable in sensitive fields such as medical imaging, where maintaining the original image quality is extremely important. So, we need a method that can both secure the image and allow data hiding without losing original quality.

System overview

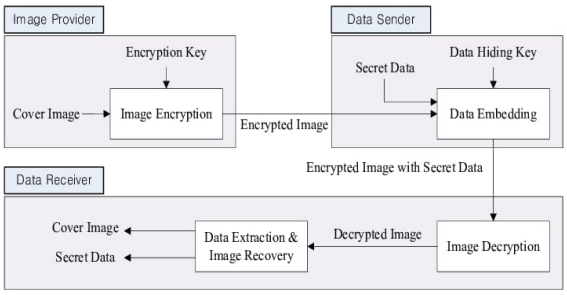
Our system works in several steps:

1. First, we prepare the image
2. Then, we encrypt it
3. Convert secret data into binary form
4. Split the data(secret sharing)
5. Embed the into the image
6. Extract the data at the receiver side
7. Finnally, recover the original image

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(April),2026
Received: 18-02-2026 Accepted: 23-03-2026 Published: 01-04-2026

Block Diagram



1. Image Preprocessing

We first convert the input image into grayscale and resize it to 256 * 256.

Why we do this :

- It reduces complexity
- Makes processing faster
- Keeps image size comsistent

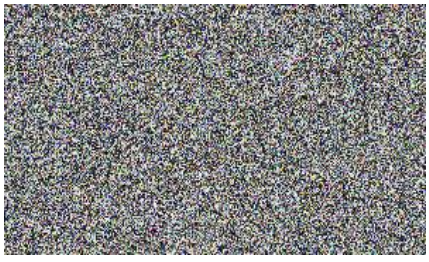
Each pixel in the image has a value between 0 and 255.

2. Image Encryption

To protect the image, we encrypt it using an XOR operation.

How it works :

- We generate a random key matrix
- Each pixel is XORed with the key



Result:

- The image looks like random noise
- No one can understand the original image without the key

3. Secret Data Preparation

The secret messege(like text) is converted into binary form.

Process :

- Each character converted into 8-bit binary
- All bits are combined into a sequence

This makes it easy to embed data into the image.

4. Secret Sharing

Instead of embedding the whole data at once, we split it into parts

Method :

- Separate even bits and odd bits

Why :

- One part alone cannot reveal the data
- Only combining both parts gives the original messege

5. Data Embedding (Reversible data hiding)

We embed the secret data into the encrypted image using LSB.

Process :

- Divide pixels among different data hiders
- Each hider embeds their share into LSB

Benefits :

- Changes are invisible
- Image remains encrypted

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(April),2026
Received: 18-02-2026 Accepted: 23-03-2026 Published: 01-04-2026

- Original image can be recovered later

6. Data Extraction

At the receiver side :

- Extract LSB bits
- Recover each share
- Combine shares to get orignal messege

Important point :

- Image is still encrypted during this process

7. Image Recovery

After extracting data, we recover the original image using XOR again.

Result :

- Perfect recovery
- No data loss
- No distortion

IV CONCLUSION

In this project, we successfully combined emcryption, reversible data hiding, and secret sharing. This ensures :

- High security
- Hidden data protection
- Perfect imagew recovery

It is especially useful in applications where both privacy and data integrity are critical.

V FUTURE IMPROVEMENTS

The system can be further enhanced by making a few improvents :

- Using stronger encryption like AES
- Randoming pixel selection
- Using authentication to detect tampering
- Improving secure transmission

VI REFERENCES

[1] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible Data Hiding: Advances in the Past Two Decades," *IEEE Access*, vol. 4, pp. 3210–3237, 2016.

[2] P. Puteaux and W. Puech, "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1670–1681, 2018.

[3] P. Puteaux and W. Puech, "A Recursive Reversible Data Hiding in Encrypted Images Method With a Very High Payload," *IEEE Trans. Multimedia*, vol. 23, pp. 636–650, 2021.

[4] C.-Y. Weng and C.-H. Yang, "Reversible Data Hiding in Encrypted Image Using Multiple Data-Hiders Sharing Algorithm," *Entropy*, vol. 25, no. 2, 2023.

[5] H. Yu, J. Zhang, Z. Xiang, B. Liu, and H. Feng, "Lossless Reversible Data Hiding in Encrypted Image for Multiple Data Hiders Based on Pixel Value Order and Secret Sharing," *Sensors*, vol. 23, 2023.

[6] L. Xiong, X. Han, C.-N. Yang, and Z. Xia, "Reversible Data Hiding over Distributed Encrypted-Image Servers Based on Secret Sharing," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 19, no. 1, 2023.

[7] G. Fang, F. Wang, C. Zhao, C. Qin, C.-C. Chang, and C.-C. Chang, "Reversible Data Hiding With Secret Encrypted Image Sharing and Adaptive Coding," *IEEE Internet of Things Journal*, vol. 12, no. 13, pp. 23933–23945, 2025.

[8] Y.-Q. Shi et al., "Reversible Data Hiding: Advances in the Past Two Decades," *IEEE Access*, 2016.

[9] X. Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE Signal Processing Letters*, 2011.

[10] P. Puteaux and W. Puech, "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images," *IEEE TIFS*, 2018.

[11] P. Puteaux and W. Puech, "A Recursive Reversible Data Hiding in Encrypted Images Method With a Very High Payload," *IEEE Trans. Multimedia*, 2021.

[12] C.-Y. Weng and C.-H. Yang, "Reversible Data Hiding in Encrypted Image Using Multiple Data-Hiders Sharing Algorithm," *Entropy*, 2023.

[13] Z. Saeidi and S. Mirzakuchaki, "Reversible Data Hiding in Encrypted Images Using LWE-Based Secret Sharing," 2025.

[14] L. Xiong et al., "Reversible Data Hiding over Distributed Encrypted-Image Servers Based on Secret Sharing," *ACM TMM*, 2023.

[15] Y.-Q. Shi et al., "Reversible Data Hiding: Advances in the Past Two Decades," *IEEE Access*, 2016.

[16] X. Zhang, "Reversible Data Hiding in Encrypted Image," *IEEE Signal Processing Letters*, 2011.

[17] H. Yu et al., "Lossless Reversible Data Hiding in Encrypted Image for Multiple Data Hiders," *Sensors*, 2023.

[18] P. Puteaux and W. Puech, "A Recursive Reversible Data Hiding in Encrypted Images Method With a Very High Payload," *IEEE Trans. Multimedia*, 2021.

[19] C.-Y. Weng and C.-H. Yang, "Reversible Data Hiding in Encrypted Image Using Multiple Data-Hiders Sharing Algorithm," *Entropy*, 2023.

[20] L. Xiong et al., "Reversible Data Hiding over Distributed Encrypted-Image Servers Based on Secret Sharing," *ACM TMM*, 2023.