Robust Reversible Watermarking in Encrypted Image with Secure Multi-Party Based on Lightweight

Mr. k. Sreenivasa Reddy[1],Ms. Vaishnavi Badvane[2], Ms. Teja Sree Rugada[3], Ms. Sowmya Avula[4]
[1,2,3,4]*Sridevi Women's Engineering College*

Abstract- **Initially, the image is taken as input and pre-processing is performed by using the Pixel Repetition Method. Visual quality, payload capacity, and security against attacks. LSB information hiding algorithm of image using secret key is be proposed combining information hiding and cryptography, increasing the human eye visual features, and the identity authentication based on digital signature and encryption technology to improve the security of information hiding. It is based on hidden data is extracted by the receiver through the reverse process of System Using A* Algorithm. Finally through the experiment and the comparison of the peak signal-to-noise ratio (PSNR) and safety. The improved LSB image steganography algorithm using the encryption technology is better than general LSB image steganography method with better security and higher PSNR.**

Index Terms- **Encryption, Decryption, LSB.**

I. INTRODUCTION

Image steganography comprises of transform domain, model relied steganography, spatial domain and spread spectrum. The spatial domain and transform domain contrasts with one another. Pixel value is directly used to embed a secret message in spatial domain. On the other hand, transform domain techniques accomplish embedding by initially transforming the particular image from STF (Spatial to Frequency) domain. The recent progress in the communication and information technology generates easy and simple accessible data. In addition, establishing secure communication is the most important requirement.

II. PROBLEM STATEMENT

The main aim of this project is to provide better recovery of the secret bits than previous steganographic methods.

III. PROPOSED SYSTEM

In proposed several techniques to accomplish image steganography. Initially, the image is taken as input and pre-processing is performed by using the Pixel Repetition Method. In the pre-processing technique, various unwilling distortions are suppressed and the significant image features are used for further processing. Then, recommended AES cryptosystem is used for data encryption. This process helps in achieving communication security. Proposed new LSB embedding is utilized to hide the secret data inside an image. Finally, the hidden data is extracted by the receiver through the reverse process of the A* Algorithm proposed system. The proposed system in analyzed to validate its performance efficiency.

IV. ADVANTAGES

- Low Encryption and Decryption Time.
- Key Generation will be easy using AES algorithm.
- The hidden data is extracted by the receiver through the reverse process using A* algorithm
- It is based on analyzed to validate its performance efficiency.

V. SYSTEM DESIGN

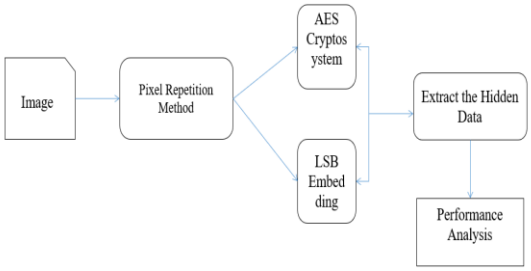

Fig 1. System Architecture for Robust Reversible Watermarking in Encrypted Image With Secure Multi-Party Based on Lightweight Cryptography.

VI. SYSTEM COMPONENTS

There are three system components or modules in this project. The three system modules are:

- Input Image
- Pre-processing
- AES Cryptosystem
- LSB Embedding
- Extract the hidden data
- Performance Analysis
- **Input Image:** The data selection is the process of selecting and loading the input images from dataset.
- **Pre-processing:** The image taken as input is scaled-up by the use of PRM (pixel repetition method). The (X*Y) input image is scaled-up by converting the individual pivot or seed pixel into a block (2*2) by reiterating the pixel.
- **AES Cryptosystem:** The AES (advanced encryption standard) is utilized for textual data encryption in an unconceivable way.
- **LSB embedding:** the LSB (Least Significant Bits) of few or all the bytes within an image is substituted with a bits corresponding to the secret message. Hence, the raw data is encrypted prior to embedding process to achieve more security.
- **Extract the hidden data:** from cover image it is going to extract the hidden text.
- **Performance Analysis:** It evaluates the performance.

VII. RESULTS AND DISCUSSIONS

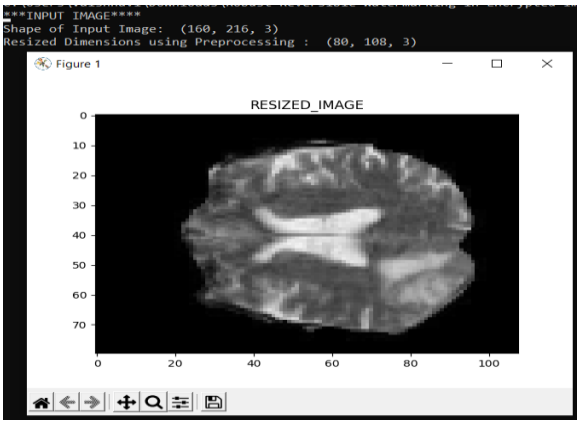

Fig 2. Resized Image

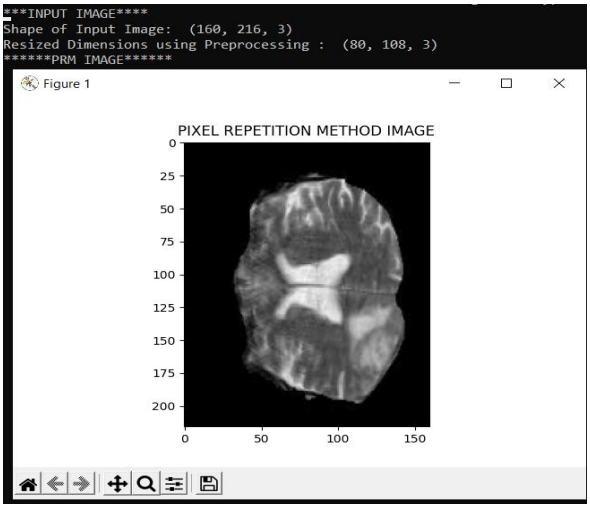

Fig 3. Pixel Repetition Method Image

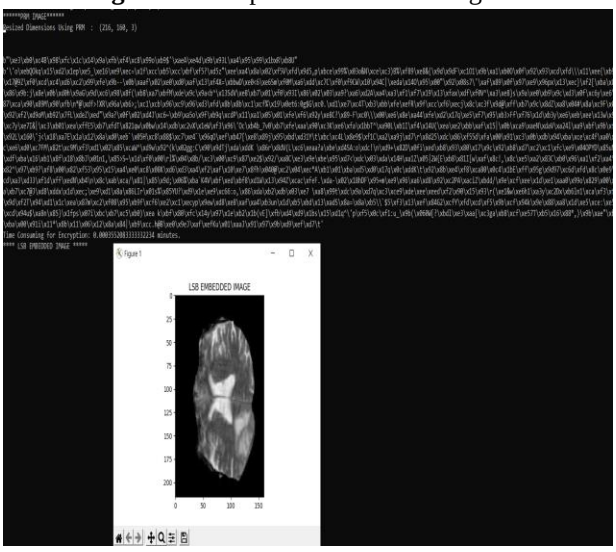

Fig 4. LSB Embedded Image

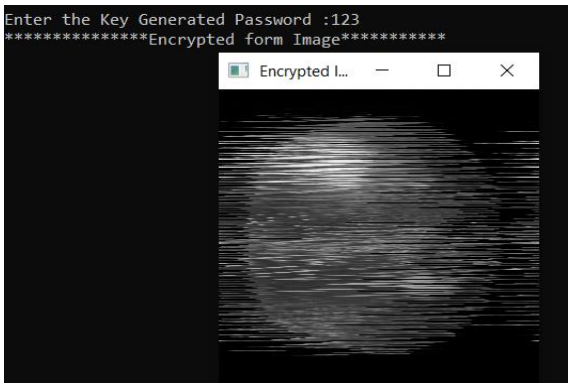

Fig 5. Encrypted Image

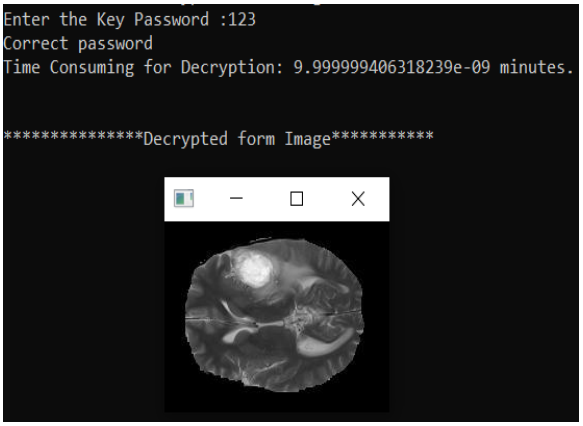

Fig 5. Decrypted Image

VIII CONCLUSION

In this process, image encryption and decryption process. The image is taken as input and pre-processing is performed by using the pixel repetition method. Various techniques are used to achieve image steganography through encryption and decryption. Pixel repetition method is used to perform pre-processing. Later, proposed AES system is used to encrypt the data and LSB embedding is utilized for embedding the data thereby performing image enhancement through the so as to extract the hidden data. To perform on analysed to validate its performance efficiency.

IX FUTURE ENHANCEMENT

The future work on this project is to improve the compression ratio of the image to the text. This project can be extended to a level such that it can be used for different types of image formats like .bmp, .jpeg, .tif, etc., in the future. The security using Least Significant Bit Algorithm is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption.

REFERENCES

[1] s. Karakus and E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images," medical hypotheses, vol. 139, pp. 109691-109691, 2020.

[2] c. Y. Roy and M. K. Goel, "visual cryptographic steganography with data integrity," lovely professional university, 2017.

[3] p. Rahmani and G. Dastghaibyfard, "an efficient histogram-based index mapping mechanism for reversible data hiding in vq-compressed images," information sciences, vol. 435, pp. 224-239, 2018.

[4] m. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, "image steganography in spatial domain: A survey," signal processing: image communication, vol. 65, pp. 46-66, 2018.

[5] https://cybernews.com/resources/what-is-aes-encryption/.

[6] https://www.researchgate.net/publication/348979603_Robust_Reversible_Watermarking_in_Encrypted_Image_with_Secure_Multiparty_based_on_Lightweight_Cryptography.

[7] https://www.sciencegate.app/document/10.1109/tcsvt.2021.3055072.

[8] S. D. Ahmadi and H. Sajedi, "Image steganography with artificial immune system," in 2017 Artificial Intelligence and Robotics (IRANOPEN), 2017, pp.

[9] A.Miri and K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm," Optik, vol. 145, pp. 158-168, 2017.

[10] M. Umair, "Comparison of Symmetric Block Encryption Algorithms," ResearchGate, 2017.

[11] X. Li, S.-T. Kim, and I.-K. Lee, “Robustness enhancement for image hiding algorithm in cellular automata domain,” Optics Communications, vol. 356, no. 1, pp. 186–194, 2015.

[12] Q. Su, Y. Niu, H. Zou, Y. Zhao, and T. Yao, “A blind double color image watermarking algorithm based on QR

decomposition," Multimedia Tools and Applications, vol. 72, no. 1, pp. 987–1009, 2014.

[13] A.Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image water marking using DWT-SVD and firefly algorithm," Expert Systems with Applications, vol. 41, no. 17, pp. 7858–7867, 2014.

[14] A. Ansari, M. Pant, and C. W. Ahn, "Artificial bee colony optimized robust-reversible image watermarking," Multimedia Tools and Applications, vol. 76, no. 17, pp. 18001–18025, 2017.