ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1862

# Secured and Quality-Optimized Image Steganography using K-LSB and AES with RGHS Enhancement

Sravan Kumar Reddy M[1]; Sai Suma L[2]

[1]Associate professor, Department of Computer Science and Engineering.
[2] Computer Science Department, Rajeev Gandhi Memorial College of Engineering and Technology Nandyal, 518501.

Publication Date: 2025/05/29

**Abstract: Image steganography is the process of hiding a message under a cover image. The main objective is to hide the secret text or image into an image by using k- Least Significant Bit (LSB) algorithm, improvise the visual quality by using Relative Global Histogram Stretching (RGHS) based on adaptive parameter acquisition. The secret message is protected and secured using the Advanced Encryption Standard (AES) method. The data is encrypted using pseudo-randomly generated keys to further improve security. Efficiency of the algorithm is estimated by Peak Signal to Noise Ratio (PSNR), where higher PSNR value gives the higher quality image.**

***Keywords:*** *Image Steganography, K-LSB, RGHS, AES, PSNR.*

**How to cite:** Sravan Kumar Reddy M; Sai Suma L (2025). Secured and Quality-Optimized Image Steganography using K-LSB and AES with RGHS Enhancement. *International Journal of Innovative Science and Research Technology*, 10(5), 2313-2317. https://doi.org/10.38124/ijisrt/25may1862

## I. INTRODUCTION

The “Goal of Steganography” is to keep sensitive information secret from prying eyes. In this essay, we will look at the goal steganography set itself for achieving through the proposed algorithm best possible visual quality principle. Information is secured using both steganography and cryptography, however their methods are different. The goal of steganography is to conceal the communication's existence. It hides information in other data, such as music, video, or photographs [1]. Another name for steganography is "covered writing." It is derived from two geek words “stegano” which means “covered” and “graphos” which means “to write”. Whereas cryptography involves encoding the message to make it unreadable without the proper key [2]. Among them, Steganography has an edge compared to cryptography as the secret message is hidden inside the image and is not easy to notice. Attacker can easily suspect whenever he sees encrypted message. In terms of security cryptography has an advantage over steganography but steganography has more probability of not being suspected. Thus, the fusion of cryptography and steganography has proven to be robust approach for concealing sensitive information within digital media.

A good steganographic technique is the one which aims for three aspects: payload capacity (maximum data that can be hidden inside the cover image), visual quality of stego image must remain unchanged so that the image does not exhibits noticeable visual artifacts or alterations which may attract attention and raise suspicion (imperceptibility), and security. Keeping compatibility and efficiency in mind, this work employs the k-LSB method as a steganographic technique and AES as a cryptographic methodology.

In the rapidly evolving digital landscape, the challenges of security and visual quality in image steganography have become paramount concern. This research delves into the advancement of security and visual quality in image steganography by the addition of another layer of encryption using pseudo randomly generated keys. However, the Relative Global Histogram Stretching approach is used to improve the visual look and quality. This paper presents a comprehensive analysis of the proposed methodology, evaluating its effectiveness in safeguarding confidential information while preserving the visual integrity of the cover image.

## II. RELATED WORK

Prior research has witnessed the integration of steganography and cryptography to fortify information hiding techniques. Many steganographic methods have been proposed in the recent years, such as [2] In this paper, PVD (Pixel Value Differentiating) is proposed as steganographic method which compresses and embeds information in pictures at the difference in pixel values between two successive pixels. [2] This work introduces the use of Discrete Cosine Transform (DCT) augmentation for image steganography on

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1862

both colour and greyscale images. [3] This paper deals with understanding and implementation of steganography using two different techniques: Least Significant Bit method in which secret message is hidden using the bits at least significant level of the cover image and Discrete Wavelet Transform (DWT), which alters the wavelet coefficients of the cover image in order to hide the secret message. And also, there are various cryptography methods such as [4] [4] Data Encryption Standard (DES), Advanced Encryption Standard (AES), and so on. For the enhancement of visual quality of an image RGHS (Relative Global Histogram Stretching) seems to be the best choice [6]. Relative Adaptive Parameter Acquisition-Based Global Histogram Stretching for Enhancing Images of Shallow Water was used in this study accomplish this. The two components of the suggested approach are colour correction and contrast adjustment.

➢ *Disadvantages of Existing System –*

- Low payload capacity
- Limited Security measures
- Lack of Dynamic Key Management
- Detectability concerns

## III. PROPOSED METHODOLOGY

Image steganography is the process of hiding a message into a cover image, the message can be text, codes or image. Hiding secret message (text or image) into image and encrypting it with pseudo randomly generated keys is the proposed approach in this paper. The proposed method can be broadly classified into four modules – Encoding, Encryption, Decoding, Decryption. The suggested system uses the following techniques.

➢ *K-Least Significant Bit (k-LSB)*

The K-Least Significant Bit is a steganographic technique that involves replacing or substituting the least significant bits of pixel values in an image with the bits of hidden message. When a number is represented in binary, the bit at the right is the least significant since it has the least effect on the number's total value. The parameter “k” in k-LSB denotes the number of least significant bits that are used for hiding information. For instance, one least significant bit is changed if k=1, and two least significant bits are changed if k=2.

In this working principle, if the secret message that is to be hide in the cover image is text, then k value is taken as 1or 2 which means one or two least significant bit in every pixel is replaced with the message. If the secret message that is to be hide in the cover image is an image, then k value is taken as four it is because in order to embed high amount of data, we need replacement of more significant bits.

K=1 or 2 if the secret message is text K=3 or 4 if the secret message is image.

The k value also depends on other factors such as quality of a cover image and security requirements.

For illustration, let's apply LSB to any 8 bytes of three pixels from an image.

Table 1 Pixels Before

| | | |
|---|---|---|
| (11001010 | 10101101 | 00110101) |
| (11100011 | 10010011 | 01010101) |
| (00110001 | 11100000 | 10101101) |

Data to be hidden – A (10000001)

Table 2 Resultant Pixels

| | | |
|---|---|---|
| (11001011 | 10101100 | 00110100) |
| (11100010 | 10010010 | 01010100) |
| (00110000 | 11100001 | 10101101) |

Figure 1 Describes about the Encoding Process. Encoding in Image Steganography can be Defined as the Process of Embedding the Secret Information within Image.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1862

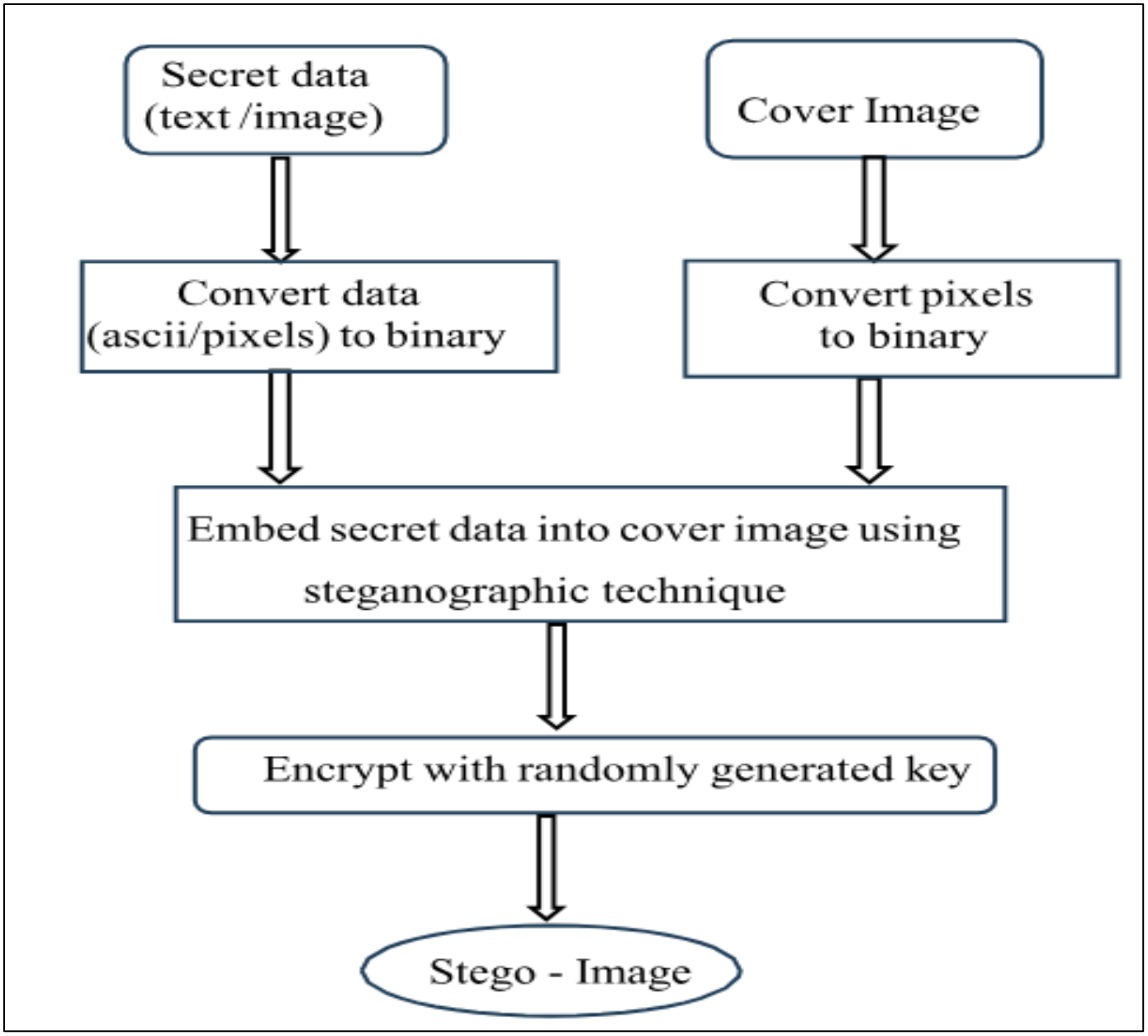


Fig 1 Process of Encoding

➢ *AES (Advanced Encryption Standard)*

In this research, Advanced Encryption Standard is employed as a cryptographic technique to secure the hidden information within the stego image. It uphold key sizes of 128, 192, and 256 bits with fixed-size data blocks. In that order, rounds 10, twelve, and fourteen are completed. One of the most potent algorithms is AES because it is symmetric, meaning that the same secret key may be used for both encryption and decryption, enhancing the system overall.

➢ *Usage of Randomly Generated Keys* –

To fortify the security further an additional layer of protection is introduced through the AES in conjunction with randomly generated keys. Its unpredictable nature contributes to the robustness of the encryption process.

Every stego picture has a different set of randomly generated keys. This variability ensures that even if one stego image is comprised, the security of other stego images remains intact.

The use of AES with randomly generated keys aligns with industry best practices for secure information hiding.

Figure – 2 describes about the Decoding process where the hidden information is extracted for stego image.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1862

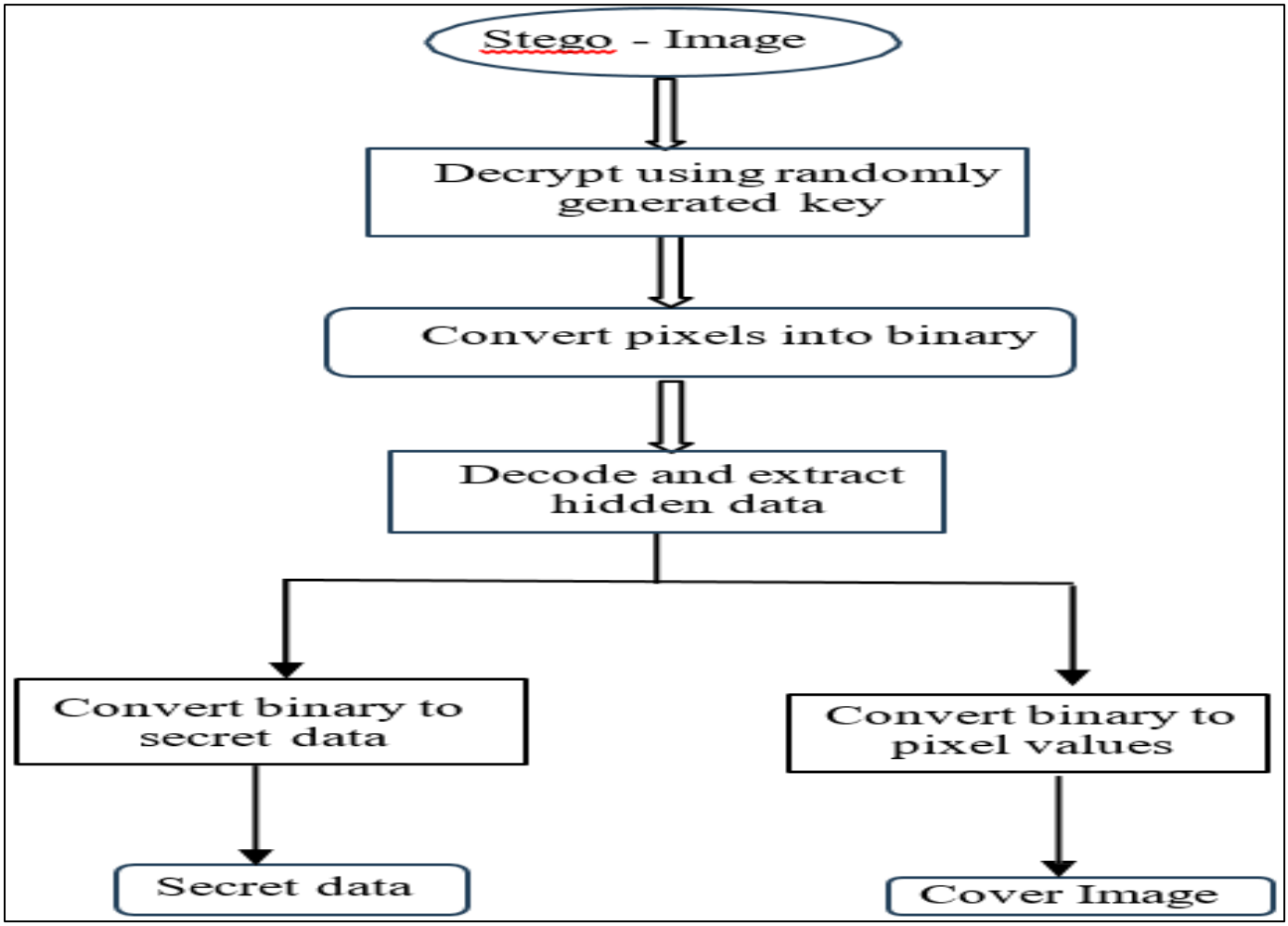


Fig 2 Process of Decoding

➢ *Enhancement of Stego- Image Quality*

After the process of encoding, stego-image is obtained. This stego image is created by combining the cover image and the secret data. Due to this the quality of cover image can be affected and can lead to certain level of visual degradation, especially if the large amount of information is being concealed.

Therefore, to minimize this, in this paper Relative Global Histogram Stretching (RGHS) based on adaptive parameter acquisition method is employed. This method improves the visual quality of images by enhancing the contrast and overall distribution of pixel intensities. One method might not adequately address the variety of stego-image properties, which is why adaptive parameter acquisition was introduced to RGHS. The adaptive approach allows for dynamic parameter adjustment ensuring optimal enhancement related to the unique statistical properties of individual stego – images.

## IV. EXPERIMENTAL RESULTS

In this work, we used k-LSB technique in order to hide the secret data i.e. text or image. Further in order to provide security AES algorithm is applied along with pseudo randomly generated keys. This added another layer of protection to the system. After hiding the data into the cover image, the visual appeal of stego image can be distorted, to minimize that Relative Global Histogram Stretching (RGHS) based on adaptive parameter acquisition is employed.

Both cover and hidden images come in a variety of sizes and formats. In case of hiding image in image we encounter problem when the image that is to be hidden is greater in size than cover image and therefore leaving it to the future work. Using the above algorithms, we have hidden text or image in the cover image and are also successful in retrieving back the hidden data.

The **Peak Signal-to-Noise Ratio** (PSNR) is one metric used to evaluate an image's quality. The quality of an image is determined by the ratio of its maximal potential power to the power of corrupting noise.

10*log10(MAX^2/MSE) = PSNR

Where MAX denotes the maximum possible pixel value, MSE is Mean Squared Error.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may1862

- *Text Hidden In Image*

Table 3 Text Hidden in Image for 64 – Bit Text Length

| Cover Image (300x300) | PSNR Ratio (dB) |
|---|---|
| Dog.jpg | 53.51036890111769 |
| Fruits.png | 49.336531344548 |
| Nature.png | 49.922490438025 |
| Table.png | 49.902079446654 |

- *Image Hidden In Image*

Table 4 Text hidden in Image for 256 – Bit Text Length

| Cover Image(300x 300) | PSNR Ratio (dB) |
|---|---|
| Camera.jpg | 34.789388187611 |
| Flower.png | 32.151928169643 |
| Fruits.png | 49.216531344548 |
| Nature.png | 49.832490438025 |
| Table.png | 49.8102079446654 |

## V. CONCLUSION

In this proposed technique we hide the secret data (text/image) into a cover image using k-LSB steganographic technique. In order to provide security to hidden data AES algorithm is used with and to provide additional security, randomly generated keys are used for encoding. The keys are unpredictable because of this extra security element. PSNR values are then calculated using RGHS based on adaptive parameter acquisition, since the resolution of the stego picture may be impacted after encoding. The quality of the image is represented by a higher PSNR value.

## FUTURE WORK

In our work, while hiding image inside image, the size of secret image is taken less than or equal to the cover image. Future work can be done related to the sizes of image.

The key length used in AES can be increased.

## REFERNCES

[1] Addit Pabbi, Rakshit Malhotra, Manikandan K, “Implementation of Least Significant Bit Image Steganography with advanced Encryption Standard”, School of Computer Science and Engineering Vellore institute of technology, Published Date: March 5 2021.

[2] Amritpal Singh, Harpal Singh, “An Improved LSB Based Image Steganography Technique for RGB Images”, Guru Kashi University, Talwandi Sabo, India, Date – Mar5 2015.

[3] Omar Elharrouss, Noor Almaadeed, Somaya Al-Maadeed , “An Image Steganography approach based on k- Least Significant Bits(k-LSB) ” , 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies(ICIoT), Pages:5, Published Date: 11 May 2020.

[4] Priya Paresh Bandekar, G. C. Suguna,” LSB based text and image steganography using AES algorithm”, 2018 3rd International Conference on Communication and Electronics System (ICCES), Pages:7, Published Date: 16 oct 2018

[5] Qi Zhang, Qun Ding, “Digital Image Encryption based on Advanced Encryption Standard”, 2015 Electronic Engineering College, Heilongjiang University Harbin, China, Pages:4, Published Date: 20 Sep 2015.

[6] Huang, D., Wang, Y., Song, W., Sequeira, J. and Mavromatis, S., 2018, February. “Shallow Water Encry”, International Conference on Multimedia Modelling (pp. 453-465). Springer, Cham.