Scientific Research Publishing

Journal of Information Security, 2024, 15, 355-377
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Novel LSB Steganography Technique for Enhancing Cloud Security

Ahsan Ullah, Md. Inzamul Haque, Md. Mokarom Hossain, Md. Sadman Ahammad, Mst. Nishita Aktar

Department of Computer Science and Engineering, World University of Bangladesh, Dhaka, Bangladesh
Email: ahsan.ullah@cse.wub.edu.bd, inzamulhoque321@gmail.com, mokarom10384@gmail.com, sadmanshawon23@gmail.com, nishita.mumu@gmail.com

How to cite this paper: Ullah, A., Haque, Md.I., Hossain, Md.M., Ahammad, Md.S. and Aktar, Mst.N. (2024) A Novel LSB Steganography Technique for Enhancing Cloud Security. *Journal of Information Security*, **15**, 355-377.
https://doi.org/10.4236/jis.2024.153021

Received: March 14, 2024
Accepted: July 14, 2024
Published: July 17, 2024

Abstract

Steganography is a technique that is frequently used to hide hidden information in multimedia artifacts including music, video, and images. In order to protect data saved in the cloud, this paper presents a steganography method for encrypting sound utilizing LSB-based computation. By using the least significant bit (LSB) of a byte to represent a message and then substituting each LSB bit with a binary message and encrypting a significant quantity of data. The proposed system uses the LSB technique of picture steganography, Multi-Level Encryption Algorithm (MLEA) and Two-Level Encryption Algorithm (TLEA) data encryption to give the highest level of cloud security. Compared to other current schemes, the performance of the suggested method is 1.732125% better on average.

Keywords

Steganography, LSB, Cloud Computing, Security, Cryptography, TLEA, MLEA

1. Introduction

The concept of steganography emerges as a compelling solution. Steganography, the art and science of concealing information within other data, offers a covert means of communication that complements encryption techniques. By embedding secret messages within innocuous carrier files, steganography enables the transmission of sensitive information without drawing unwanted attention. In this method, we use a cover image which is changed to the flipped cover image, and the pixel state of the image is changed. Changing the pixels causes the image to flip and change from left to right. Then the cover image is converted to RGB. Here among the three-color channels, we selected the green color. Then this

image is divided into 16 equal parts in 4 × 4 matrix. Each part is called a sub image. Then these sub images are shuffled. Shuffling changes the position of each sub image and results in a scrambled image. On the other hand, a secret key is selected and changed to the encrypted secret key through TLEA. Here the encrypted secret key and secret message are hidden in the shuffling sub-image by converting the decoding LSB to binary bits by MLEA. Then the reset changes to the encrypted sub-image. And the stego image is obtained by changing the reshuffle image to the combining RGB channel. The image obtained after embedding the secret information is called stego image although it carries a secret message, the stego image is identical to the cover image. So, no unauthorized person can receive the secret message. As a result, data security is maintained. Two algorithms are applied like TLEA and MLEA. TLEA is a robust method designed to improve security by encrypting a secret key. It has two main functions bit-XOR and secret pattern-based bit shuffling. On the other hand, MLEA is encrypted using the original secret beta, which makes it more challenging for an attacker to extract the secret message from the stego image. MLEA has four operations bit XOR, block division of secret bits, secret key based shuffling and encrypted secret key based encryption.

This novel LSB steganography technique not only aims to bolster the confidentiality and integrity of data stored in the cloud but also addresses the challenges posed by the distributed and dynamic nature of cloud environments. By seamlessly integrating steganographic capabilities into the cloud architecture, this technique offers a versatile and robust solution for securing sensitive information against unauthorized access and cyber threats.

Related Works

An elegant processing of image steganography for how to securely store data in the cloud, focusing more on List Significant Bits. Here 8 bits of each data are dealt with. And shuffling the cover image by dividing it into 3 × 3 metrics ensures data protection. Also applied RGB color method. Here data security is ensured by using TLEA and MLEA algorithms so users can easily store their data in the cloud. By reading this we can get a better idea about steganography. But if we were working with 16 bits here. That would be better. Moreover, the matrix size could also be increased. It would ensure the security of stored data [1].

A proposed system design and development provides data privacy, authenticity, and integrity for information held in cloud and IoT environments. This system's main goal was to increase security protection for both IoT devices and cloud-stored data when it was crucial [2].

A smooth cryptographic hashing algorithm based on the Merkle-Damgard construction structure and Matyas-Meyer-Oseas compression function which generates hashes through 16 rounds where each block contains 256 bits of data. The algorithm they used, which processes blocks of data using existing and new methods, generates hashes as high as SHA-512 and MD5 [3].

The paper proposes to develop a new symmetric algorithm, which ensures the security of personal information. Apart from online shopping, we also provide a lot of information on the internet, which can lead to cybercrime. By using this symmetric algorithm, it is possible to protect personal information from cybercrime [4].

A cloud computing is a shift from traditional server-based models to package as service, which has gained popularity over the past decade. It aims to improve performance, scalability, and resource consumption while addressing security concerns with data stored in the cloud. The next decade will see increased smartphone-based work from anywhere. The paper mentions the importance of cloud and the increasing use of cloud day by day, but no clear idea is given about how to provide security of information in the cloud [5].

A strategy to improve a distributed intrusion detection structure within Cloud Computing, is a secure tool that lets customers develop and deploy security terminals at their digital sources and the Cloud infrastructure. The structure used is an exploratory implementation of an IDS controller deployed in the cloud [6].

A novel steganography paradigm that is impervious to detection and secret extraction and transparent to all attackers was proposed. We are able to accomplish these aims because of two characteristics: the secret is spread over multiple clouds and the data is not altered. The environment enables us to conceal the covert channel's existence between the parties involved in the conversation. Information in related works is usually kept secret in underground media. The hidden media in this work indicates the content. As a result, the data is still there in the file and can only be accessed with the key. Experiments indicate that as the value of the chosen base increases, the secret distribution in the clouds diminishes. The author of this work has provided an idea of how to securely communicate data to the receiver. But no clear idea is given on which algorithms or steganography can be used to store data securely in the cloud [7].

The aim is to examine the key steganographic strategies utilized in cloud computing data security reported in this paper between 2016 and 2018. The author suggested a steganographic technology that is currently accessible to improve cloud data security. The matrix of location (MoF) is used in the suggested approach to improve security. Furthermore, this text file uses the steganographic technique to encrypt the message, producing a natural text file. People are therefore unable to read the wording that obscures the message inside. In this paper the author only mentions text steganography. Did not mention any other steganography. There exist various image based steganographic techniques are present to insert data securely from unauthorized users. The image-based techniques can be classified into two categories of domains: spatial and frequency domains. In most of the spatial domain, steganography techniques are based on the least significant bit (LSB) substitution in which the LSB of the pixels is selected to embed the secret message. In this, we have two different classifications: LSB replacement and LSB matching. In LSB replacement technique, the LSB bit of each pixel is replaced with secret data. In LSB matching, the LSB bit is re-

placed with the next bit of the LSB; if those are not matched, we cannot insert the data. In both the techniques, we have multiple combinations of LSB bit; finally, we have multiple ways of an embedded secret message [8].

A brand-new approach that makes use of multilayer steganography using the Hash–LSB methodology and the AES cryptography algorithm for sharing and storing private data on cloud storage. This allows customers to improve the confidentiality of personal information kept on cloud servers, such as bank, health, and employment records. Every saved file is concurrently accessible at all times and from any location. There is no reasonable way to prove how much of the data is on the way, and there is no mention of any specific steganography [9].

An intrusion detection and prevention system (IDPS) to enhance data security in the cloud. The authors discussed various types of cloud-based IDPS. By keeping an eye on configuration options, log files, network activity, and user actions to spot typical attack patterns, IDPS can offer additional security safeguards for cloud-like environments [10].

A highly successful technique for guaranteeing data integrity. In this technique, the information sent to the server is stored behind the images. Unauthorized access is prevented from accessing the data since it is hidden. In the suggested architecture, image steganography is an excellent technique to safeguard data integrity; however, there is no discussion of data security during transmission. This makes it a novel method, but if data integrity and confidentiality could have been managed while the file was being uploaded to a cloud server, it may have been much better [11].

A cross-system and carried out a comparative study of the two several strategies for fusing steganography and cryptography into one system were investigated. Information contained in an image was safeguarded using the LSB steganography technique and an enhanced version of the K-Strange Clustered Algorithm. In this paper, the author mentions data security but does not mention any cloud storage. And what algorithm to use to protect the data also could not give a clear idea [12].

The author's Cloud data security is enhanced by the use of hashing algorithms, encryption, and information hiding. During the data encryption step, the author coupled the RSA asymmetric encryption algorithm with the AES256 symmetric encryption method to generate hybrid encryption. The encrypted information was then concealed within an image using the LSB technique. Data validation involved the use of the SHA hashing algorithm. Although LSB is mentioned here, it does not mention how many bits to work with and image shuffling, which is a limitation of this paper [13].

Reviewing some of the steganography techniques put forth in multiple studies suggests strengthening cloud data security and fortifying it against cyberattacks and eavesdropping. Most people agree that steganography is one of the best ways to protect cloud communication. The process of creating hidden messages using steganography ensures that only the sender and recipient can securely access and transfer the data via a communication channel. But here Mustafa Abdullah could

not talk about any clear algorithms and data protection of image steganography [14].

Security risks associated with cloud computing systems and how to prevent them. In this instance, data was secured using steganography and cryptography. Compared to other algorithms, RSA is a more secure algorithm. In this paper the author has used only the RSA algorithm. No separation is used for data encryption and decryption [15].

2. Research Design and Analysis

2.1. Research Design

Description of Proposed Method (Figure 1 and Figure 2)

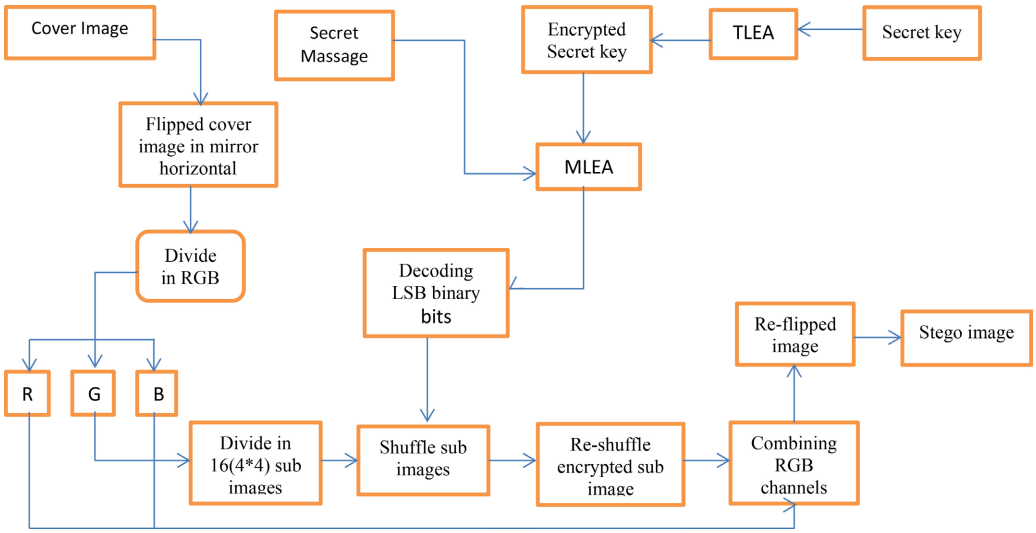

Figure 1. Proposed encryption method.

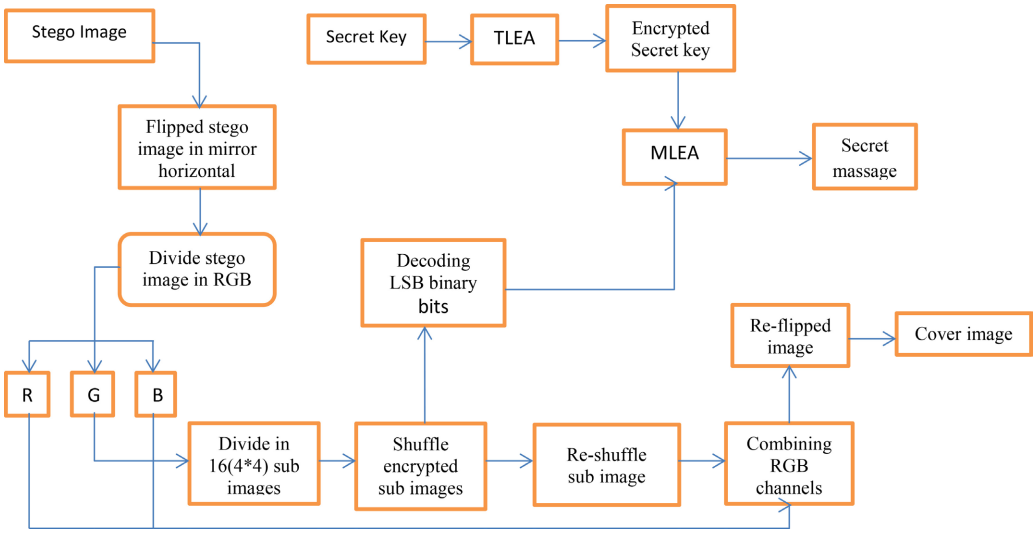

Figure 2. Proposed decryption method.

Cover Image: The image selected for hiding data into it is called a cover im-

age (Figure 3).

Figure 3. Cover image.

Flipped Cover Image in mirror Horizontal: When an image is flipped, its pixel positions are altered. When a picture is flipped, it changes from left to right and the horizontal axis is inverted. That's shown in Figure 4.

Figure 4. Flipped cover image.

Divide in RGB: Four color channels are present in color images: red, green, and blue. Choosing the green channel for the cover image is known as "dividing in RGB," which divides the image (Figure 5) into these three-color channels.

Figure 5. Green channel of cover image.

Divide into 16 Sub-Images: Dividing the entire image into sixteen equal por-

tions using a 4 × 4 matrix, or four rows and four columns. Every component calls a sub-image, which are shown in Figure 6.

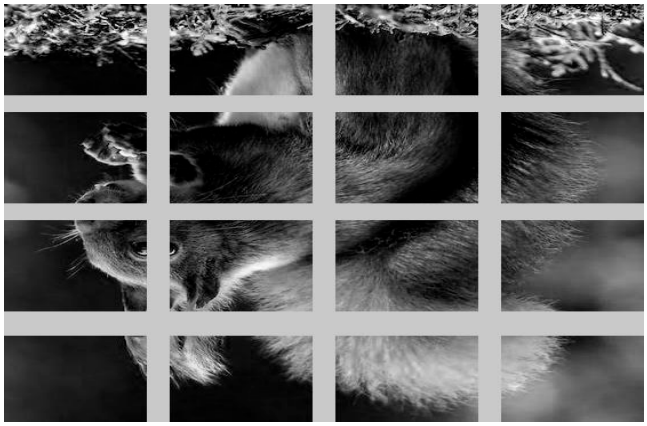

Figure 6. Divide into 16 sub-images.

Shuffle Sub-Images: The sub-images are repositioned using a coded shuffle pattern. You can use the sub-image from position 9 or 10 or any other location in place of the sub-image in position 1. The scrambled image will be obtained after each sub-image has changed positions, which are shown in Figure 7.

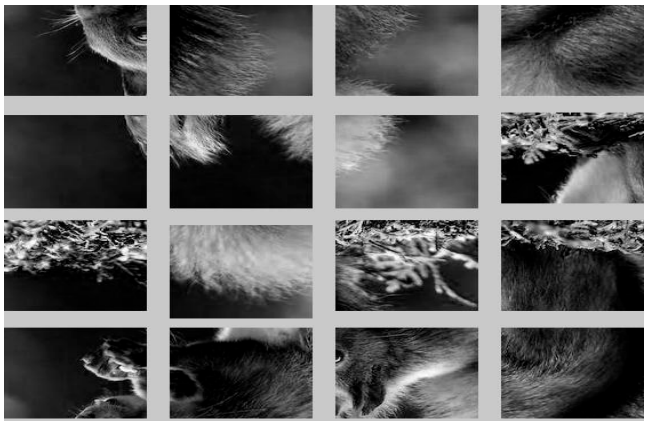

Figure 7. Shuffle sub-images.

TLEA: The Two-Level Encryption method is a straightforward yet powerful method designed to improve security by encrypting a secret key. It consists of two main functions; bit-XOR and secret pattern-based bits shuffling.

MLEA: The real secret data is encrypted using the Multi-Level Encryption Algorithm (MLEA), which makes it more challenging for an attacker to extract it from the stego picture. Its four constituent operations are bit-XOR, block division of secret bits, secret key based shuffling, and encrypted secret key based encryption.

Reshuffle Encrypted Sub-Images: Transforming every sub-image's position back to its original location, which are shown in Figure 8. Additionally, the encrypted message will be present in each sub-image.

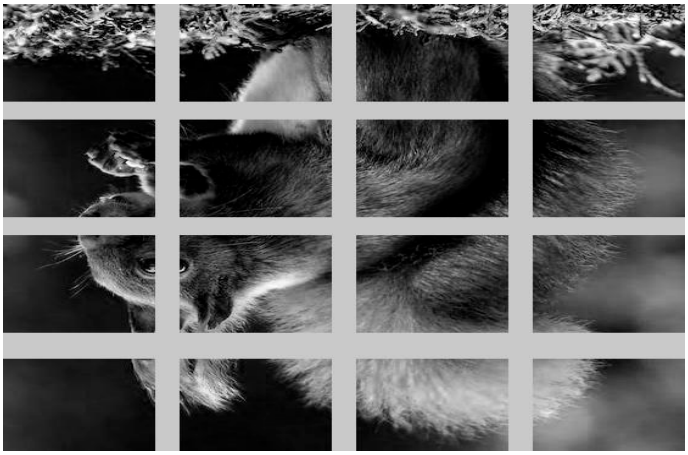

Figure 8. Reshuffle encrypted sub-images.

Combining RGB Channels: The previous colorful image is obtained by combining the Red, Green and Blue channels, which is shown in Figure 9.

Figure 9. Combining RGB channels.

Re-flipped Image: Returning the image to its original position, both vertically and horizontally, which is shown in Figure 10.

Figure 10. Re-flipped cover image.

Stego Image: The image obtained after hiding or embedding data is called the stego image (Figure 11). Though it bears a secret message, the stego image is identical to the cover image.

Figure 11. Stego image.

2.2. Encryption Algorithm

Two-Level Encryption Algorithm (TLEA)

The TLEA (Figure 12) is a straightforward method that aims to improve security by encrypting a secret key. Its two primary functionalities are bit shuffling based on secret patterns and bit-XOR. While there are a number of encryption methods available for these kinds of works, including AES, DES, and Blowfish, these methods have enormous processing costs, which prevents them from being used in real-time.

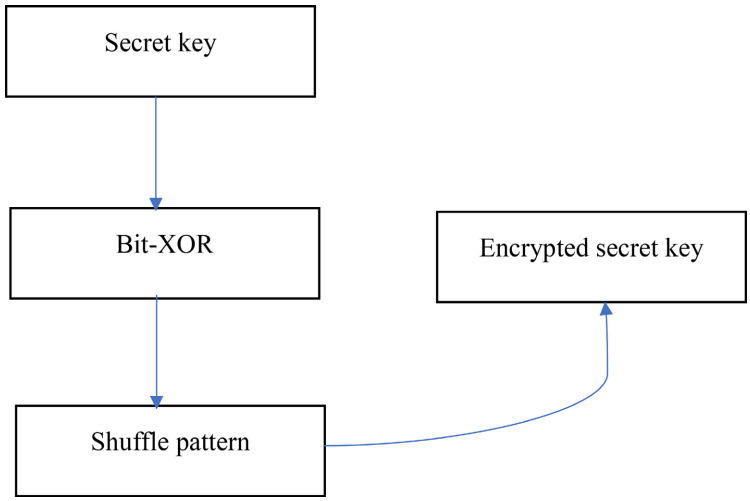

Figure 12. TLEA block diagram.

Algorithm:

Step: 01-Choose the secret key, then convert into 16 bits of binary.

Step: 02-Applying logical 1 to the XOR of every bit.

Step: 03-Taking 16-bits combination & the 1st bit is flipped with the 9th bit; 2nd bit is flipped with 8th bit; 3rd bit is flipped with 12th bit; 4th bit is s flipped with 11th bit; 5th bit is flipped with 13th bit; 6th bit is flipped with 14th bit; 7th bit is flipped with 16th bit and 10th bit is flipped with 15th bit.

Step: 04-Store all bits in ESK.1

2.3. Multi-Level Encryption Algorithm (MLEA)

The MLEA (Figure 13) was chosen because, in contrast to AES, DES, and other sophisticated algorithms, it is comparatively lightweight. It consists of four processes: bit-XOR, blocks division of secret bits, secret key based shuffling, and encrypted secret key based encryption. Encrypting the real secret data and making it more difficult for an attacker to remove it from the stego image is the goal of the MLEA.

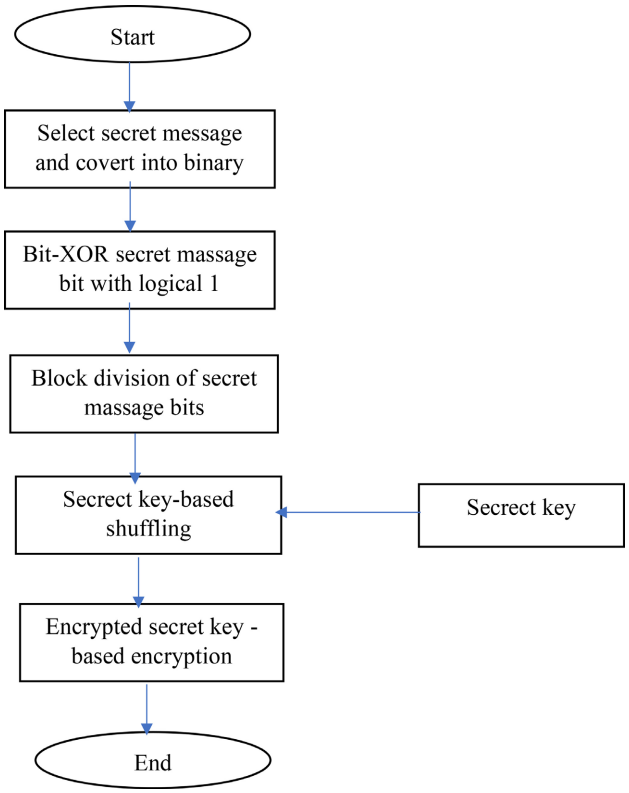

Figure 13. MLEA block diagram.

Algorithm:

Step: 01-Choose the secret key, then translate it into 16 bits of binary.

Step: 02-Applying logical 1 to the XOR of every bit.

Step: 03-Taking 16-bits combination & divide whole bits array into 8 blocks (MB1, MB2, MB3, MB4 MB5, MB6MB7, MB8). MB1 all the sixteenth and first bit; MB2 all the fifteenth and second bit; MB3 all the fourteenth and third bit; MB4 all the thirteenth and fourth bit MB5 all the twelfth and fifth bit; MB6 all the eleventh and sixth bit; MB7 all the tenth and seventh bit and MB8 all the ninth and eighth bit of each 16-bits combination.

Step: 04-Take the secret key's i^{th} digit.

Step: 05-At the i^{th} digit position, remove the secret bit from the BSMB.

Step: 06-Increase the value of i and concatenate the separated bit with SKBSM.

Step: 07-Continue from step (4) to step (6) until all of the BSMB's bits are jumbled.

Step: 08-Assume that j = 0 and k = 0 after initializing the loop counters.

Step: 09-Choose the SKBSM's j^{th} hidden bit.

Step: 10-Choose the k^{th} bit from the ESK, the encrypted secret key.

Step: 11-When the secret key ESK's k^{th} bit is 1, execute Temp = (SKBSM (j) ⊕ logical 1) ii. Combine Temperature and ESM. Otherwise, join SKBSM (j) and ESM without using bitxor. Finish

Step: 12-J and K are increased by 1.

Step: 13-Steps (9) through (12) should be repeated until all bits are encrypted.

2.4. Encryption Process

Encryption Process Block Diagram (Figure 14)

TLEA and MLEA are designed to provide robust and flexible encryption solutions to protect sensitive data against unauthorized access and advanced cryptographic attacks. They are essential tools for organizations aiming to achieve high levels of data security and regulatory compliance. TLEA typically involves three encryption layers, usually involving different keys and possibly different algorithms at each layer to increase security. MLEA involves multiple levels of encryption, but unlike TLEA, it may use more than three levels and potentially different encryption algorithms at each level.

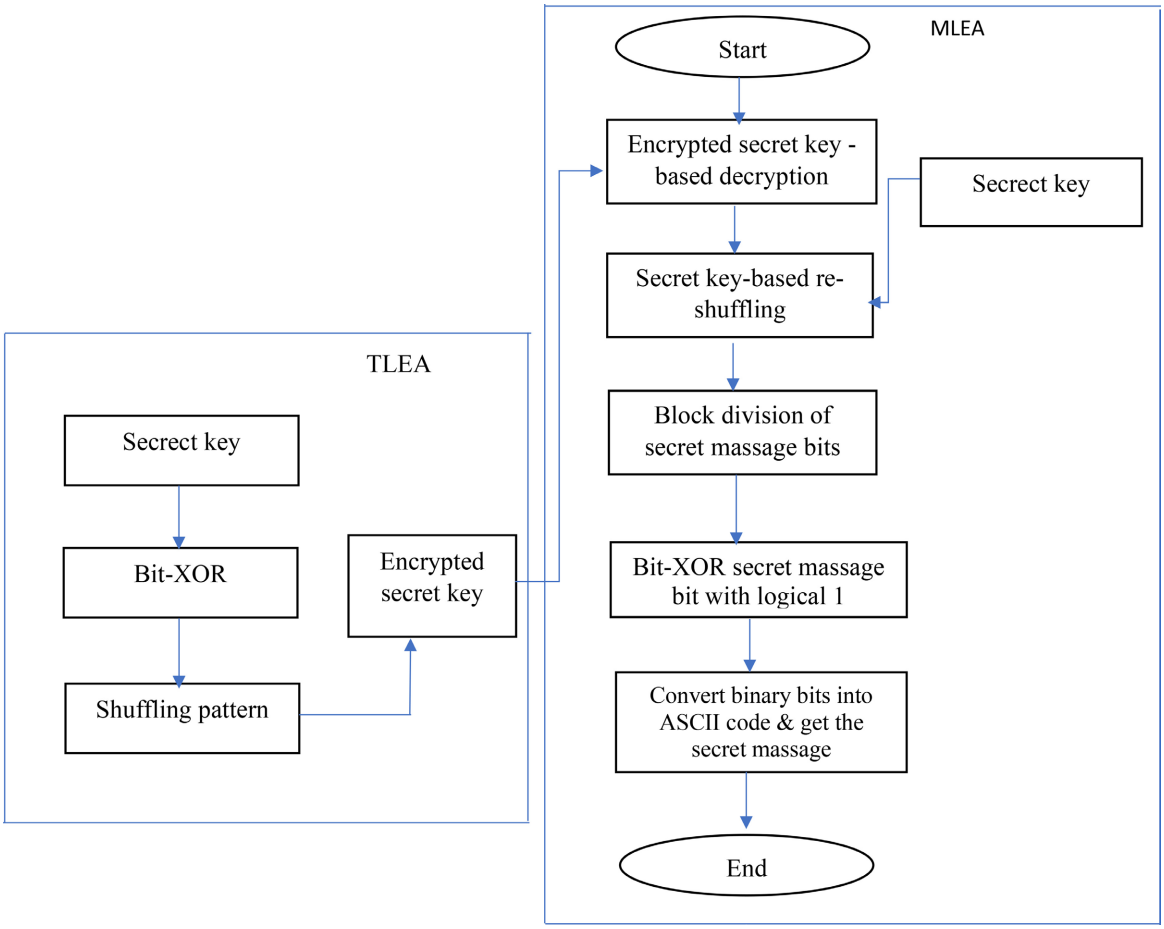

Figure 14. TLEA & MLEA encryption process block diagram.

2.5. Decryption Process

Decryption Process Block Diagram (Figure 15)

TLEA and MLEA decryption process involves reversing the encryption steps using the respective keys in the opposite order.

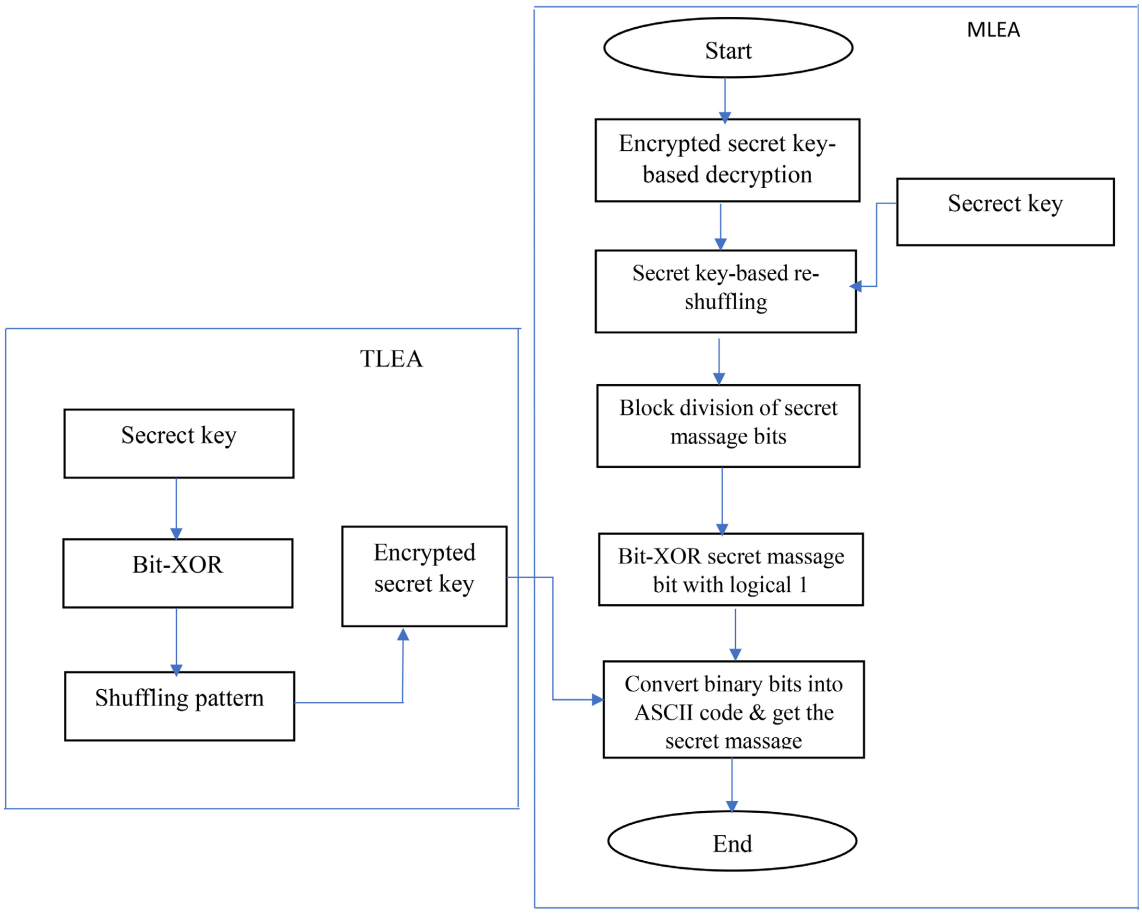

Figure 15. TLEA & MLEA decryption process block diagram.

2.6. Embedding Algorithm (Figure 16)

The RGB colour space is the basis for the embedding process in the figure. The cover picture splits into its red, green, and blue channels after being initially turned horizontally in a mirror. The secret data is concealed via the green channel. A Secret Shuffled Pattern is used to shuffle each of the 16 equal blocks that make up the green channel before it is embedded. Alternatively, the secret message, which is composed of ASCII characters, was encrypted using an MLEA, and the secret key was encrypted using a TLEA. We used the green channel to embed a hidden message that is divided into sixteen equal parts. Sixteen secret message bits are chosen, with the first two being embedded in the first block of the green channels, the second in the second block, and the third in the third. Bits into the fourth, fifth, sixth, seventh, eighth, and ninth blocks, respectively, follow this order: fourth, fifth, sixth, seventh, and ninth. tenth bit into the 10th block, eleventh bit into the 11th block, twelfth bit into the 12th block, thirteenth

bit into the 13th block, fourteenth bit into the 14th block, fifteenth bit into the 15th block, and sixteenth bit into the 16th block of the green channels separately. After rearranging the blocks and combining the RBG channels, every bit is embedded into the image's green channel. The image was refilled. Finally getting the Stego Image was obtained.

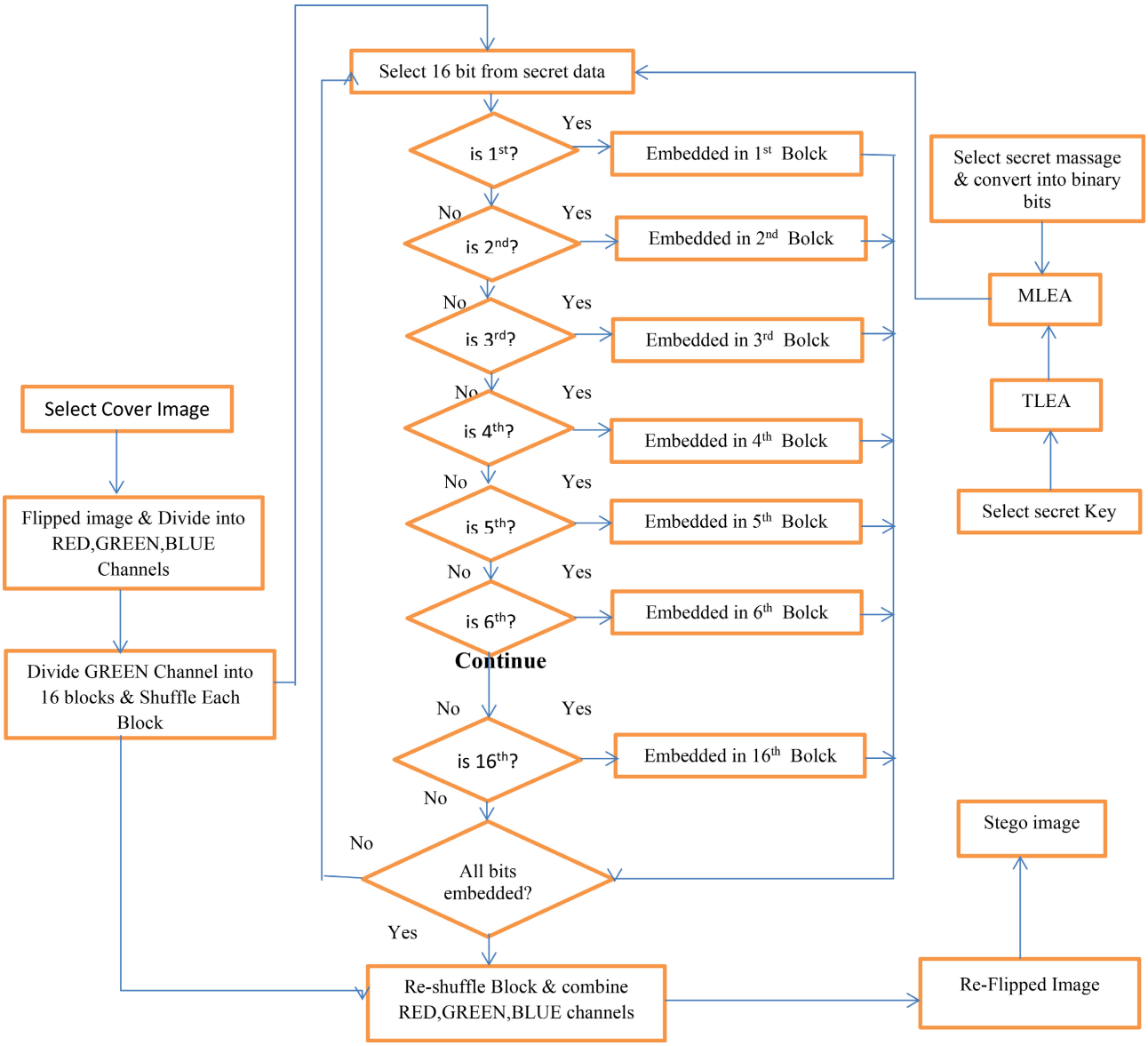

Figure 16. Embedding algorithm.

2.7. Extracting Algorithm (Figure 17)

The embedding process is executed in reverse order in Figure, which depicts the extraction algorithm. The stego-image is split into the red, green, and blue channels after first being turned back horizontally and mirrored. Next, the green channel is split into sixteen equal blocks, and a Secret Shuffle pattern is used to shuffle each block. Up to the end of the embedded data, the leading-side bit

(LSB) of each block is extracted cyclically. After that, the recovered data is decoded using TLEA and MLEA. Next, each sixteen-bit combination is converted to an ASCII value, obtaining the massage in secret at last.

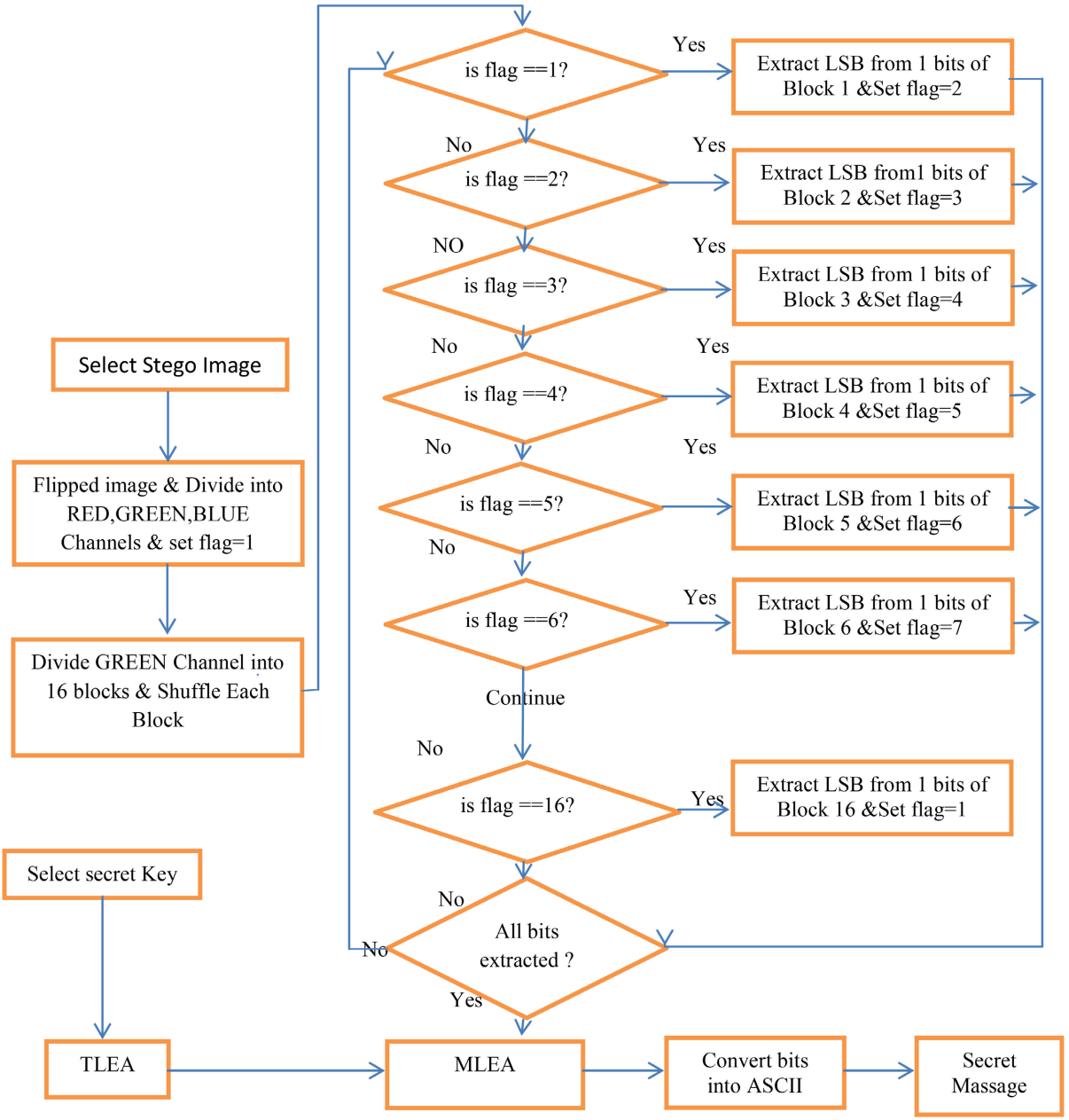

Figure 17. Extracting algorithm.

2.8. Implementation of the Algorithm in Python

The following **Figure 18** shows the message embedding & extraction in Python.

Users must select one of the three options on the panel Type 1 for Embedding Data in Cover Image, Type 2 for Extraction Data from Stego Image, or Type 3 for Exit from the Panel—when they wish to Embedding Data in Cover Image or Extract Data from Stego Image.

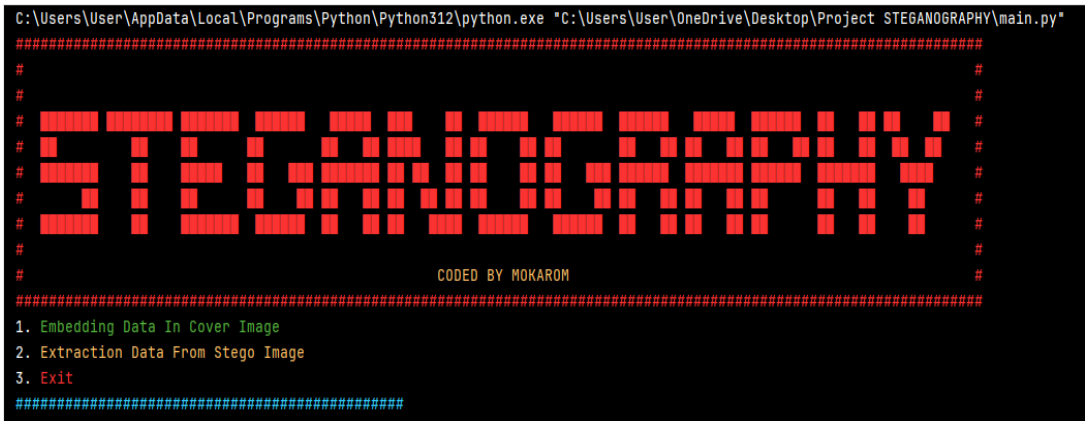

Figure 18. Message embedding & extraction in python.

2.9. Embedding Data in Cover Image

The following **Figure 19** shows the message embedding process in python.

The cover image, secret key, and secret massage required to be entered by the user. After encryption is complete, the user will receive an output file named "Stego_Image.png."

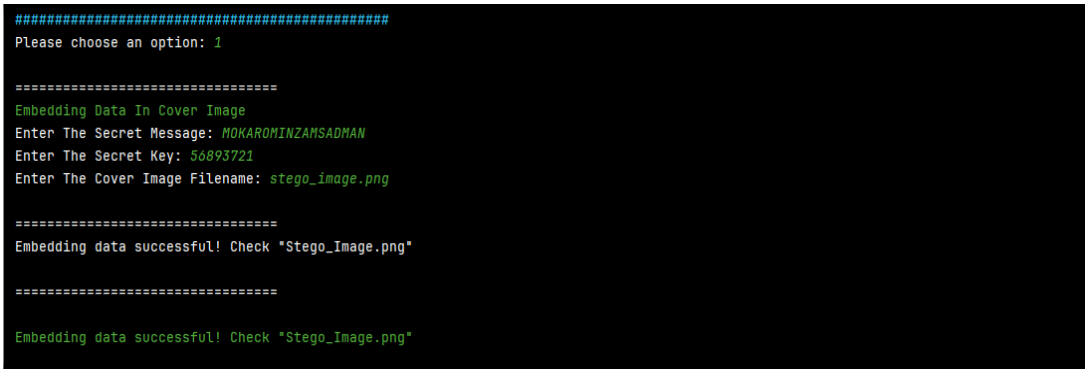

Figure 19. Message embedding process in python.

2.10. Extraction Data from Stego Image

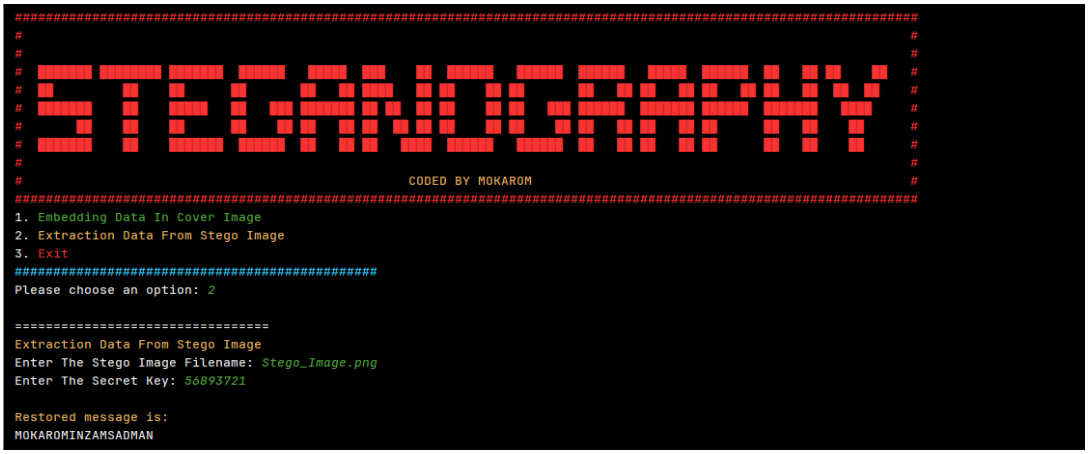

Figure 20. Message extraction process in python.

Figure 20 shows that Stego Image and the same Secret Key have to be entered by the user in order to extract data from the image. The original message will then be sent to the user upon completion of the decryption procedure.

2.11. Proposed Method for Cloud Environment

1) Proposed encryption method for Cloud using proposed Encryption Algorithm (Figure 21):

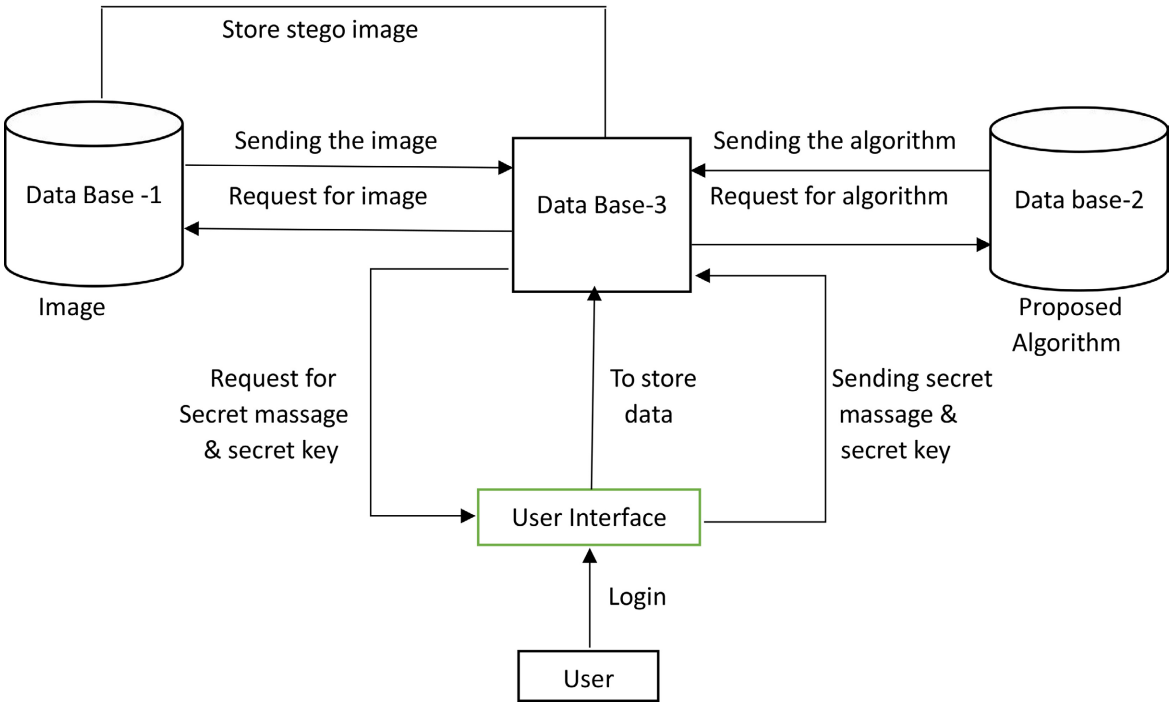

Figure 21. Proposed encryption method for cloud.

A model of using the suggested algorithm on a cloud platform, where data is encrypted using the suggested technique, is shown in Figure 21. The procedure that follows when a user wants to store data in the cloud is as follows: In order to log into the User Interface, the user utilizes User. The user asks for cloud data storage. Data Base-3 asks Data Base-1 for an image. Data Base-1 gives Data Base-3 a legitimate image. The data concealing encryption technique, which is kept in Data Base-2, is requested by Data Base-3. Data Base-3 uses the encryption algorithm that Data Base-2 supplies. Data Base-3 asks the user for their secret message and secret key. The user gives Data Base-3 their secret key and secret message. The encryption technique states that the data are stored in the image's pixel values, which are derived from the Data Base-1. Lastly, Data Base-1 will house the stego picture.

2) Proposed decryption method for Cloud using proposed Decryption Algorithm (Figure 22):

The suggested technique will be used to decrypt data in the model depicted in the picture, which shows how to use it in a cloud platform. Following are the

procedures that will occur when a user wishes to see or acquire their data: Firstly Logging into the user interface (UI) requires the user to provide their password and user ID. Access to or viewing of cloud data is requested by the user. Data Base-1 asks for the Stego Image associated with the secret message that users want to read or retrieve. Data Base-3 asks for the data retrieval decryption technique that is in Data Base-2. Data Base-2 gives the decryption algorithm to Data Base-3. Data Base-3 requests the secret key from the user. Data Base-1 provides the related Stego picture to Data Base-3.

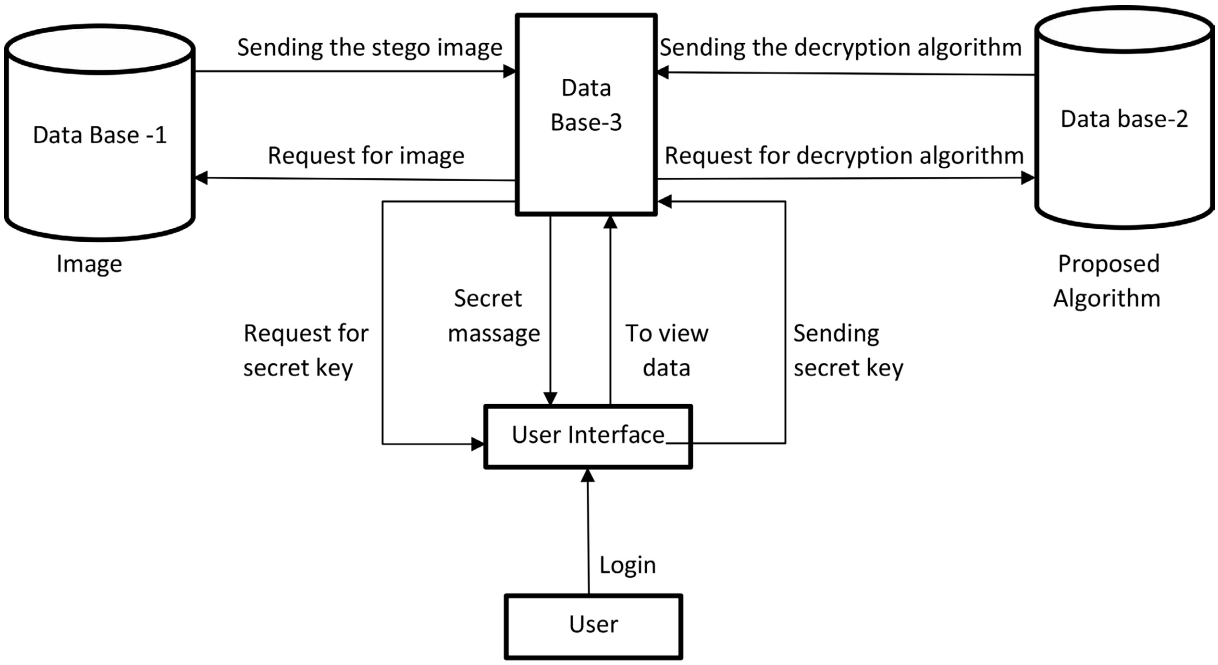

Figure 22. Proposed decryption method for cloud.

3. Result Discussion

The data provided should be used to evaluate the effectiveness of each steganographic system being considered.

The cover image is the main image that has the concealed information in it. The resulting image is referred to as the stego image. To evaluate the quality of a stego image, one can compute the Peak Signal-to-Noise Ratio (PSNR). The quality of digital photos or movies is assessed using a statistical indicator known as PSNR. Using the mean squared error (MSE) of two $M \times N$ monochrome pictures, "f" and "g", where one of the images is taken to be a noisy approximation of the other images, is the simplest method for calculating PSNR.

Mean Squared Error (MSE):

The following **Figure 23** represents graphical displays of the MSE value for the same image at different size.

$$\text{Where, MSE} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}\left[f(x,y) - g(x,y)\right]^2$$

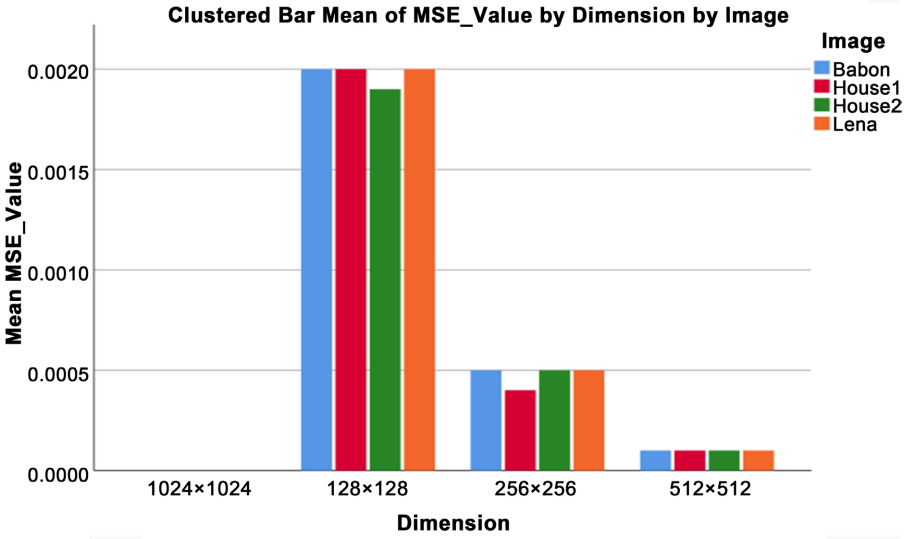

Figure 23. Graphical displays of the MSE value for the same image at different size.

Peak Signal to Noise Ratio (PSNR):

The quality difference between the $M \times N$ stego-image g and cover picture f is quantified by PSNR as follows:

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}}$$

$$\text{MSE} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}\left[f(x,y)-g(x,y)\right]^2$$

The PSNR is measured in decibels (dB), which is important to note. Since it suggests less distortion or noise in the reconstructed signal as compared to the original, a higher PSNR value typically denotes greater reconstruction quality.

Table 1. Comparing the suggested approach to previous mention approaches, inserting a secret message of the same size into a few typical photos of varying sizes depending on PSNR.

Image Name	Image Dimension (In pixels)	Classic LSB Method PSNR (dB)	PIT PSNR (dB)	Karim's Method PSNR (dB)	Muhammad *et al.* [Muhammad, Ahmad, Farman *et al.* (2015)] Method PSNR (dB)	Fahad *et al.* [Fahad, Fazal, Georgion *et al.* (2020)] Method PSNR (dB)	Khorshed *et al.* [Khorshed, Samia, Amir *et al.* (2022)] Method PSNR (dB)	Proposed Method PSNR (dB)
Baboon Image	128 × 128	64.9939	48.6326	50.2716	65.6754	75.1022	73.1710	75.1340
	256 × 256	55.8862	50.2321	49.6829	62.4044	62.6587	85.3847	81.1105
	512 × 512	61.882	50.1906	50.0517	59.4242	62.8478	85.3847	87.5450
	1024 × 1024	67.8306	50.2001	50.1669	65.5012	68.9636	91.8074	93.5176
	Average	**62.6482**	**49.81385**	**50.0433**	**63.2513**	**65.9681**	**82.461575**	**84.26725**
Lena Image	128 × 128	42.4947	45.3316	42.502	58.3332	67.6532	73.7108	75.1340
	256 × 256	49.1185	50.1136	52.4134	52.4134	64.1323	79.6055	81.3355
	512 × 512	49.8277	50.0932	49.9546	57.0021	60.3323	85.5038	87.2647
	1024 × 1024	50.0299	50.1004	50.0645	59.7532	61.1322	91.5244	91.7730
	Average	**47.8677**	**48.9097**	**48.0198**	**56.8725**	**60.3125**	**82.586125**	**83.8768**

Continued

House Image-1	128 × 128	43.5487	44.34547	47.5464	63.6754	62.9882	73.4325	75.1340
	256 × 256	49.4532	49.2130	50.4567	62.4044	62.9790	79.6055	81.6220
	512 × 512	48.8743	50.1110	51.5643	59.3032	74.9110	85.7841	88.4542
	1024 × 1024	51.8974	50.4311	52.4531	65.3212	75.0467	91.4348	93.6399
	Average	**48.4434**	**48.5251**	**50.5051**	**62.6760**	**75.0467**	**82.564225**	**84.712525**
House Image-2	128 × 128	62.7293	67.5132	62.7137	69.3076	74.8999	73.2278	75.3614
	256 × 256	56.6697	54.7702	53.3682	64.8565	64.9701	79.6996	81.4289
	512 × 512	62.7405	54.754	54.3691	63.3443	64.6510	85.4737	87.6426
	1024 × 1024	68.8288	54.7901	54.6877	72.4734	72.5676	91.5158	92.2715
	Average	**62.7421**	**57.95688**	**56.2847**	**67.4932**	**69.2771**	**82.49225**	**84.1761**

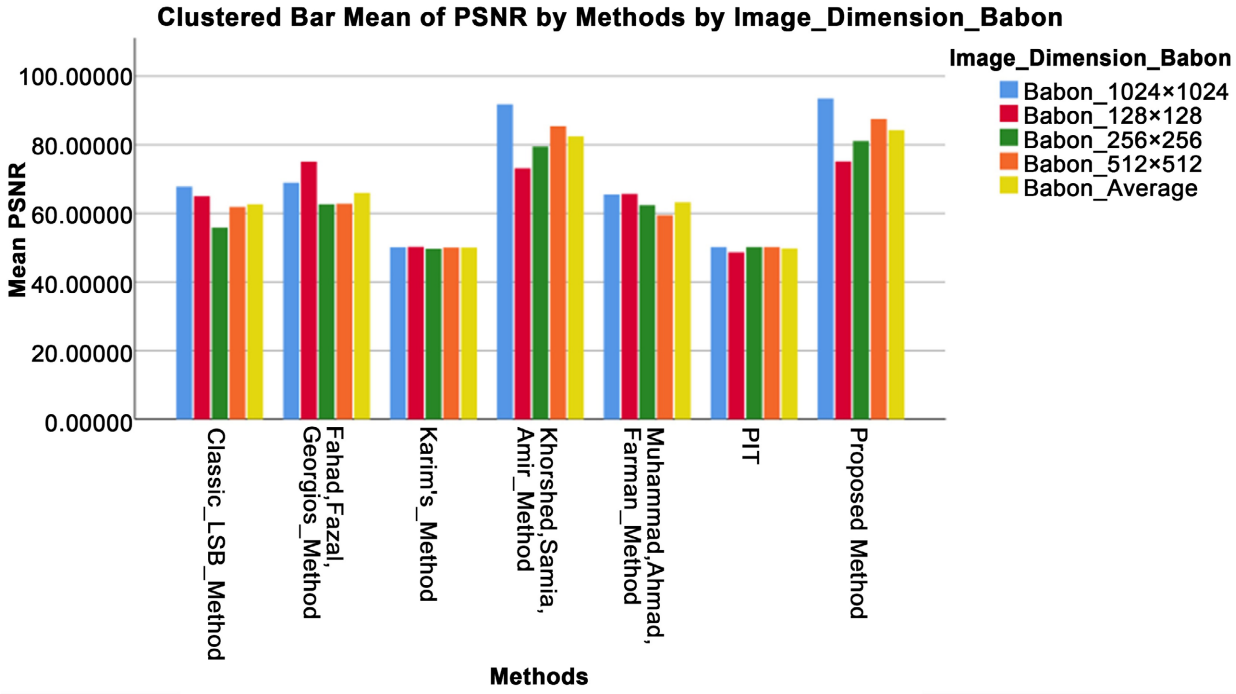

Figure 24. Graphical comparisons between the suggested approach and the current one using the same amount of data but different sized baboon picture sizes based on PSNR.

The suggested strategy and the other approaches are compared based on PSNR in Table 1. Different sizes (128 × 128, 256 × 256, 512 × 512, and 1024 × 1024) of the same photos (Lena, Baboon, House 1, House 2) are integrated with the same text. The results, which show an average improvement of 1.732125% over other current techniques, clearly show that the proposed strategy performs better. Figure 24 represents graphical comparisons between the suggested approach and the current one using the same amount of data but different sized baboon picture sizes based on PSNR. And Figure 25 shows graphical comparisons between the suggested approach and the current one using different-sized Lena photos and the same amount of data based on PSNR. Moreover, Figure 26 and Figure 27 shows graphical representations of comparison of proposed me-

thod and existing with same size of data and different size of House 1 and House 2 images based on PSNR.

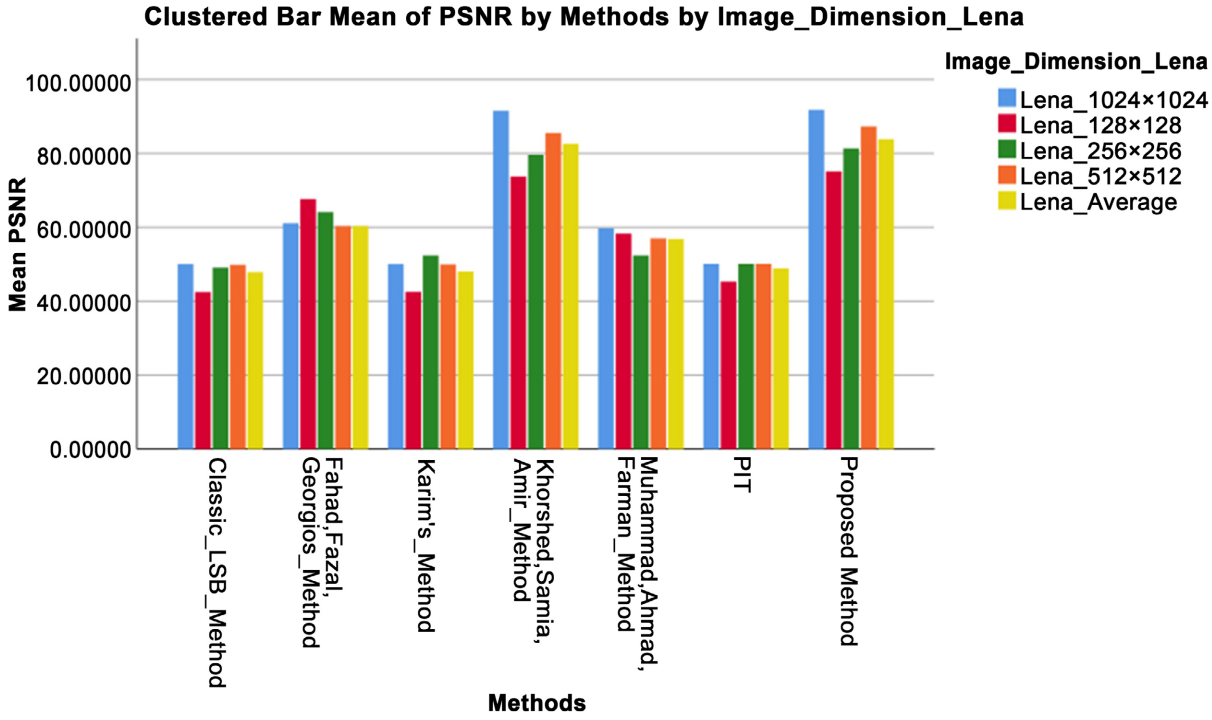

Figure 25. Graphical comparisons between the suggested approach and the current one using different-sized Lena photos and the same amount of data based on PSNR.

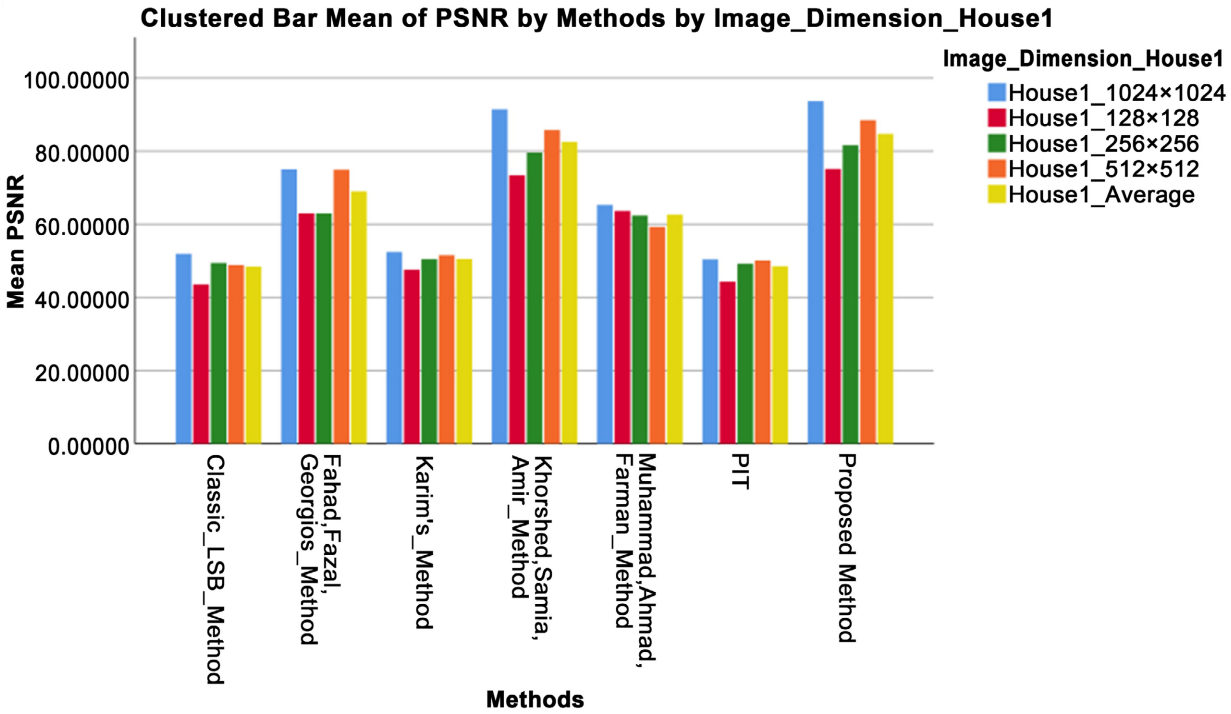

Figure 26. Graphical representations of comparison of proposed method and existing with same size of data and different size of House 1 images based on PSNR.

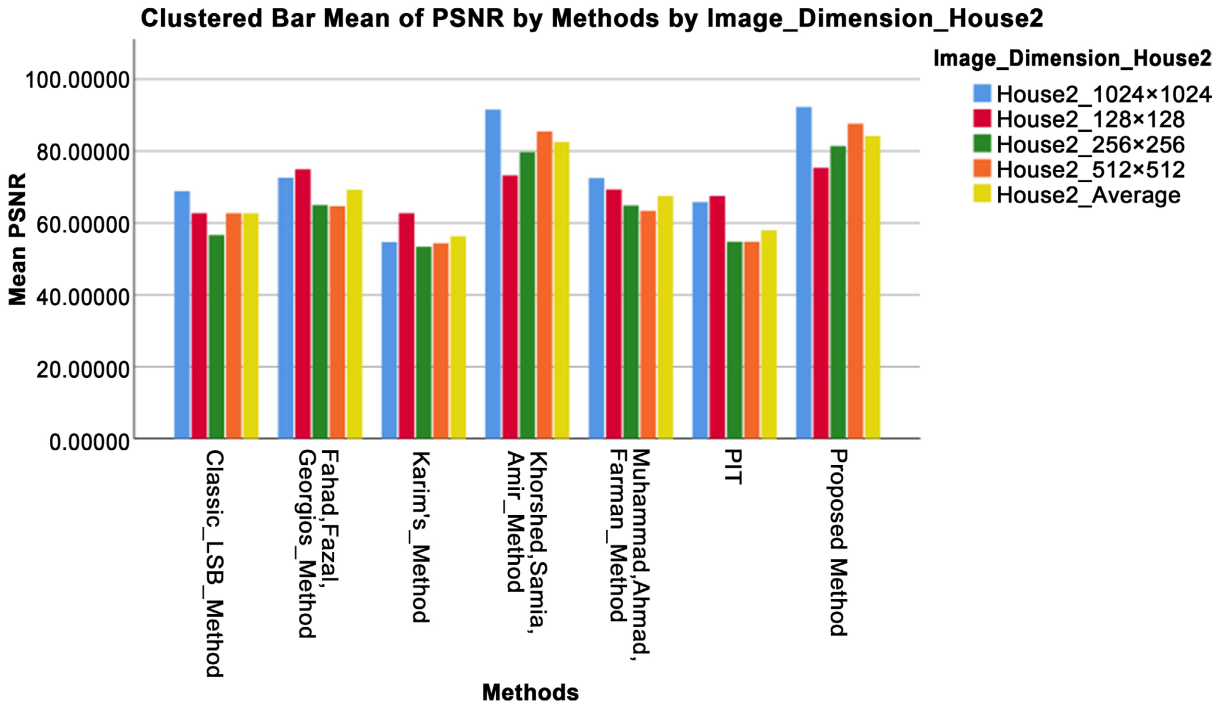

Figure 27. Graphical representations of comparison of proposed method and existing with same size of data and different size of House 2 images based on PSNR.

4. Conclusion

Our approach suggests using multi-level encryption and the LSB substitution technique to develop a security system that strikes a balance between computing complexity, security, and image quality. We investigated TLEA and MLEA, respectively, for the encryption of secret keys and secret information, and used the LSB substitution technique to embed data, increasing the difficulty of data extraction for adversaries. The new technique improves the security of current information-hiding technologies and fortifies steganography. Steganography is a method that ensures data security in cloud environments by concealing information from prying eyes. Techniques differ in how they are implemented, and each has advantages and disadvantages. We demonstrated a new and enhanced approach in the RGB shading space that is more potent and safe than earlier techniques.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Alam, K., Nushrat, S., Patwary, A.H., Ullah, A. and Robin, K.H. (2022) An Improved Approach of Image Steganography Based on Least Significant Bit Technique for Secure Communication in Cloud. *Proceedings of the Second International Conference on Advanced Network Technologies and Intelligent Computing*, Varanasi,

22-24 December 2022, 215-233.
https://doi.org/10.1007/978-3-031-28180-8_15

[2] Hossain, S., Islam, S., Ullah, A. and Hossain, A. (2022) Design and Development of a Hybrid Intrusion Detection and Prevention System for Cloud Computing and Internet of Things Environment. *Recent Innovations in Wireless Network Security*, **4**, 1-9. https://zenodo.org/records/6796201

[3] Apar, N.M., Munna, M.I., Ullah, A. and Rahman, H. (2022) Design and Development of a Dynamic Hashing Algorithm. *International Journal of Scientific Research in Computer Science and Engineering*, **10**, 8-14.
https://www.isroset.org/journal/IJSRCSE/full_paper_view.php?paper_id=2690

[4] Hossain, M.A., Ullah, A., Hossain, S., Begum, S. and Ibrahim. (2021) Design and Development of a Novel Symmetric Algorithm for Enhancing Information Security. *International Journal of Communication and Information Technology*, **2**, 49-60.
https://doi.org/10.33545/2707661X.2021.v2.i1a.40

[5] Hossain, M., Ullah, A., Khan, N. and Alam, M. (2019) Design and Development of a Novel Symmetric Algorithm for Enhancing Data Security in Cloud Computing. *Journal of Information Security*, **10**, 199-236.
https://doi.org/10.4236/jis.2019.104012

[6] Ficco, M., Tasquier, L. and Aversa, R. (2013) Intrusion Detection in Cloud Computing. *Proceedings of the* 2013 *Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Compiegne, 28-30 October 2013, 276-283.
https://doi.org/10.1109/3PGCIC.2013.47

[7] Moyou Metcheka, L. and Ndoundam, R. (2020) Distributed Data Hiding in Multi-Cloud Storage Environment. *Journal of Cloud Computing*, **9**, Article No. 38.
https://doi.org/10.1186/s13677-020-00208-4

[8] Awadh, W.A. and Hashim, A.S. (2017) Using Steganography for Secure Data Storage in Cloud Computing. *International Research Journal of Engineering and Technology* (*IRJET*), **4**, 3668-3672.
https://www.irjet.net/archives/V4/i4/IRJET-V4I4885.pdf

[9] Ranjan, A. and Bhonsle, M. (2016) Advanced Technics to Shared & Protect Cloud Data Using Multilayer Steganography and Cryptography. *Proceedings of the* 2016 *International Conference on Automatic Control and Dynamic Optimization Techniques* (*ICACDOT*), Pune, 9-10 September 2016, 35-41.
https://doi.org/10.1109/ICACDOT.2016.7877547

[10] Kumar, K. (2017) Intrusion Detection and Prevention System in Enhancing Security of Cloud Environment. *International Journal of Advanced Research in Computer Engineering & Technology* (*IJARCET*), **6**, 1138-1152.
https://www.researchgate.net/publication/320331566_Intrusion_Detection_and_Prevention_System_in_enhancing_Security_of_Cloud_Environment

[11] Sarker, M.K. and Chatterjee, T. (2014) Enhancing Data Storage Security in Cloud Computing through Steganography.
https://www.researchgate.net/publication/315850425_Enhancing_Data_Storage_Security_in_Cloud_Computing_Through_Steganography

[12] Khan, M.A. (2021) Information Security for Cloud Using Image Steganography. *Lahore Garrison University Research Journal of Computer Science and Information Technology*, **5**, 9-14. https://doi.org/10.54692/lgurjcsit.2021.0501171

[13] Abbas, M.S., Mahdi, S.S. and Hussien, S.A. (2020) Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography. *Proceedings of the* 2020 *International Conference on Computer Science and Software Engineering* (*CSASE*),

Duhok, 16-18 April 2020, 123-127.
https://doi.org/10.1109/CSASE48920.2020.9142072

[14] Ahmed, O.M. and Abduallah, W.M. (2017) A Review on Recent Steganography Techniques in Cloud Computing. *Academic Journal of Nawroz University*, **6**, 106-111.
https://doi.org/10.25007/ajnu.v6n3a91

[15] Pant, V.K., Prakash, J. and Asthana, A. (2015) Three Step Data Security Model for Cloud Computing Based on RSA and Steganography. *Proceedings of the* 2015 *International Conference on Green Computing and Internet of Things* (*ICGCIoT*), Greater Noida, 8-10 October 2015, 490-494.
https://doi.org/10.1109/ICGCIoT.2015.7380514