IMAGE STEGANOGRAPY

A PROJECT REPORT

Submitted by

Pradeep Kumar Chaudhary

Computer Science and Engineering

AUGUST 2022

ABSTRACT

The messages which are to be kept private and to be transmitted without getting interpreted by the attacker is really a challenging task. For instance, the secret information which is very important for trading between nations should not be compromised in any case. Steganography helps to transmit the message by getting embedded in the image, audio or video file. The algorithm and its effectiveness plays a vital role in preventing the embedded message from being hacked. This project report contains the implementation of image steganography using traditional lsb algorithm, adaptive lsb algorithm, filtered lsb algorithm and the novel approach called as advanced filtered algorithm. The advanced filtered algorithm helps to minimize the disadvantages available in other mentioned algorithms. The mean square is the matric considered to measure the error between the cover(original) image and the stego image(image with message bit).

1. INTRODUCTION

Using a private key, the data is encrypted to create cipher texts in cryptography, but the existence of the message is still shown to others.Steganography, on the other hand, hides the secret information in a conventional, non-secret file in order to avoid visual detection. Confidential information is hidden inside a picture using just a few chosen image pixels. Different types of cover media are available where we can apply Steganography. By using Steganograpy we can hide messages in the different cover media available like audio, video, image, text, etc.

A few potential cover media are shown in Figure 2 that we can easily utilize steganography on. The photograph, however, is the most popular and efficient way to get helpful information. It is well known that brightness is more sensitive to human vision than chrominance. Steganography therefore makes use of the limits of how the human eye can read image files to convey information.

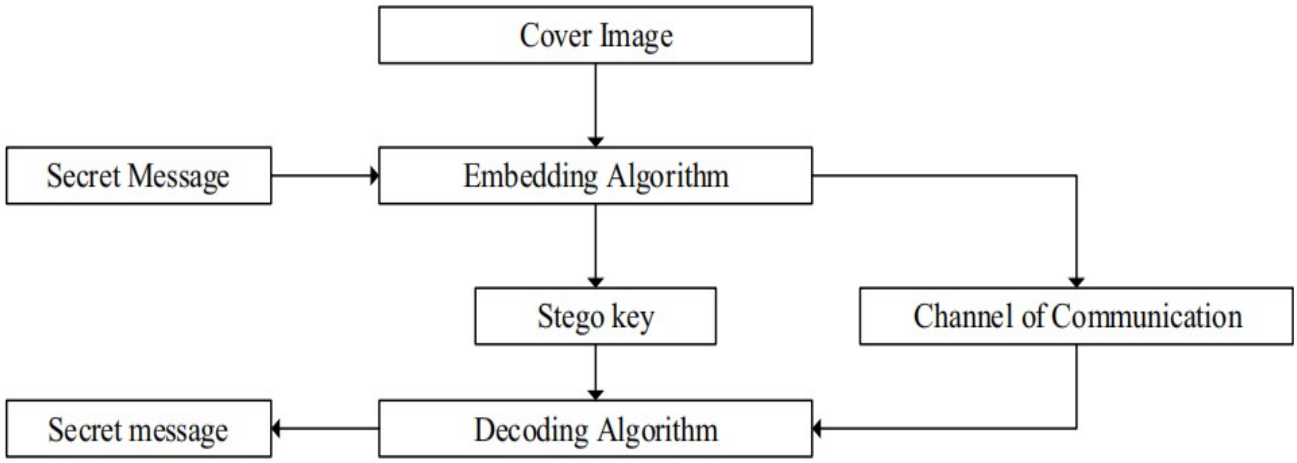

Figure 1. General block diagram of steganography .

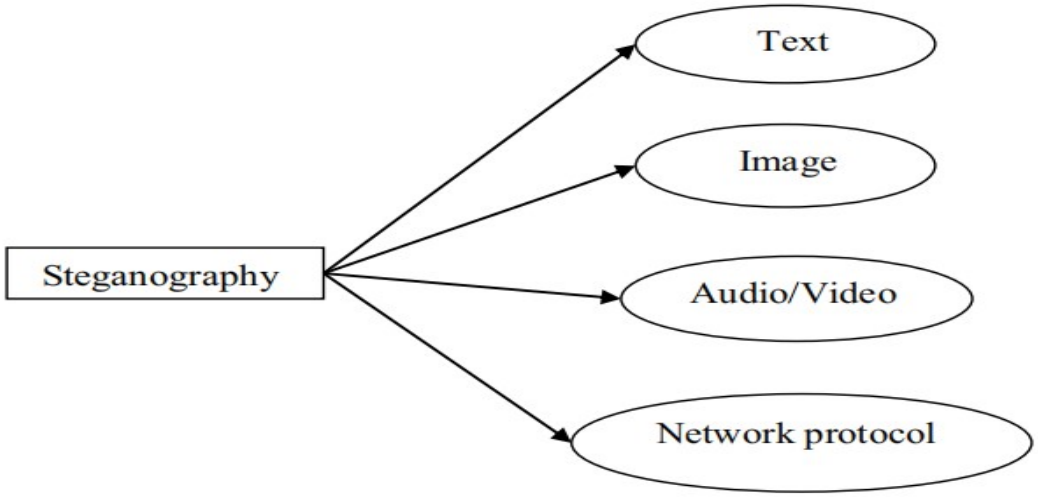

Figure 2. Types of cover media

A coded key a symmetric cipher is comparable to the steganography system, where the sender selects a cover and uses a secret key to embed the secret message inside the cover. The recipient can reverse the procedure and recover the secret message if he is aware of the secret key used in the embedding.

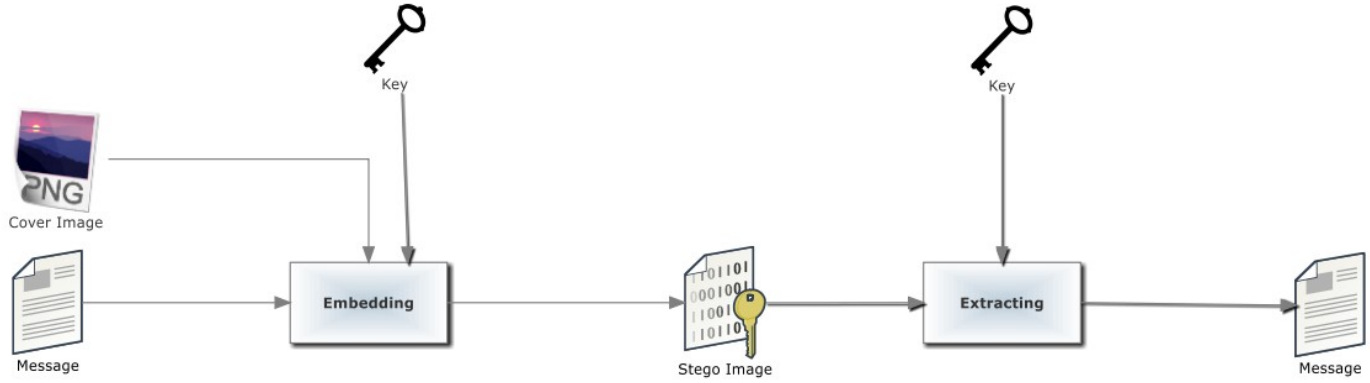

Figure 3. Secret Key Steganography

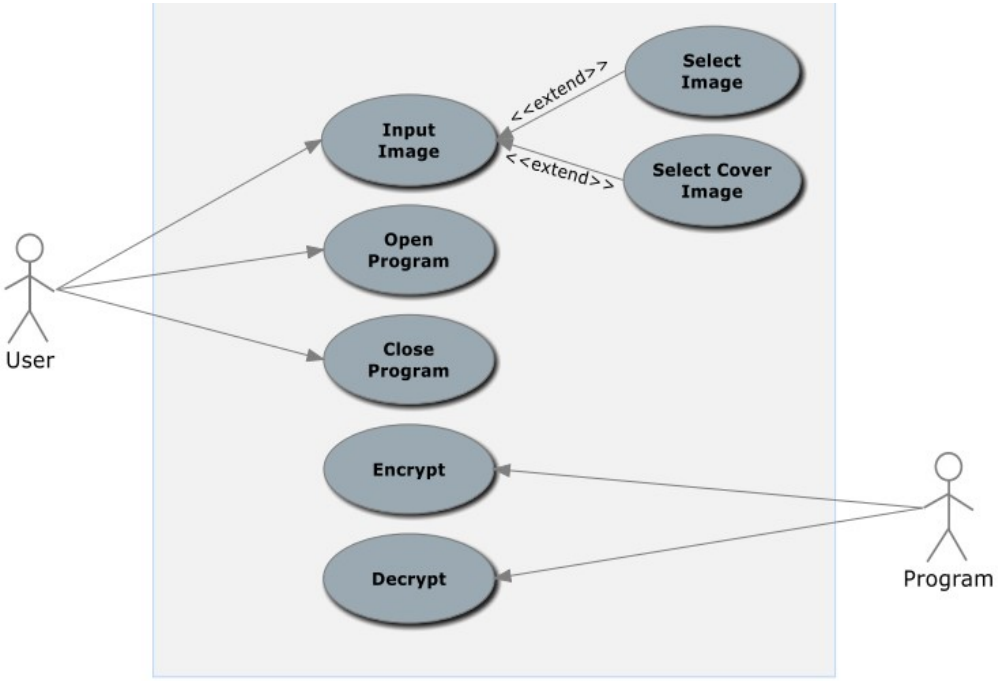

Figure 4: Use case diagram

A user or any other system that interacts with the subject is referred to as an actor in the Unified Modeling Language (UML). An actor "models a type of role played by an entity that interacts with the subject but is external to the subject" (e.g., via exchanging signals and data).

There are two actors in our application:

1. User
2. Program

A use case is a collection of scenarios that illustrate how a user and a system interact. The connection between actors and use cases is shown on a use case diagram.

2. LITERATURE REVIEW

There are numerous ways to apply steganography techniques to various cover media. Islam et al. (2014) have suggested a technique that combines visual steganography and cryptography. Here, the AES encryption method is used to encode the secret message before embedding it in the image. They also employed the idea of filtering, in which not all image pixels are used to conceal data. In order to ensure security, Mukhedkar et al. (2015) have suggested a method that uses both message encryption and image concealing to conceal personal information during communication. According to a method proposed by Broda et al. (2015), data can be concealed as text by using an image color model. The information is not lost while switching between RGB and YCbCr.

A method to conceal sensitive information in a color image using a 3,3,2 LSB substitution algorithm has been put forth by Charan et al. (2015). The confidential data is first encrypted using the Caesar cipher algorithm, and then it is embedded into the image. A strategy that includes both the segmenting and the data masking methodology has been put forth by Khalaf and Sulaiman (2011). The private information pertaining to the third channel is obscured using two RGB channels.

The other channels determine the number of ones within the chosen index path by using the benefits of one channel as an index path. A steganography algorithm that encrypts the LSB bits has been proposed by Emad et al. (2018). The approach applies the integer wavelet transform's (IWT) approximation coefficients to the grayscale images.

A digital watermarking technique employing ANN and LSB approach to conceal the secret information was proposed by Deeba et al. in 2020. In order to accomplish this, they first conceal a digital image within another digital image using the LSB approach, and then they reveal the hidden information using ANN.

Steganalysis is a technique for determining whether data is embedded in an image or not and for locating any hidden messages. In order to prevent anyone from deciphering the information hidden in the image, Rajendran and Nairm presented a novel encryption method that relies on raising the security level. To attain this degree of security, they combined a variety of strategies.

Steganalysis is avoided by combining encryption, visual cryptography, and image steganography. Using LSB steganography, they transformed the secret message into an encrypted image and integrated it into the cover image. As a result, the Stego image generated can be safely transmitted to the receiver side via an unreliable channel.

By concentrating on grayscale photos and straightforward LSB steganography, Ker introduced a novel method for locating the hidden data concealed inside a stego image. To determine where improvements may be made, they performed a high-speed computation of steganalysis statistics over enormous image libraries. Their experimental findings point to a variety of LSB techniques that could be improved.

3. PROPOSED METHODOLOY

We want to use conventional, adaptive, and filtered LSB image steganography to embed and extract the message. In addition, we'll look for new LSB image steganography to help us get around the drawbacks of the aforementioned methods. Finally, using new steganography, we will also attempt to embed and extract the message.

3.1 Traditional LSB

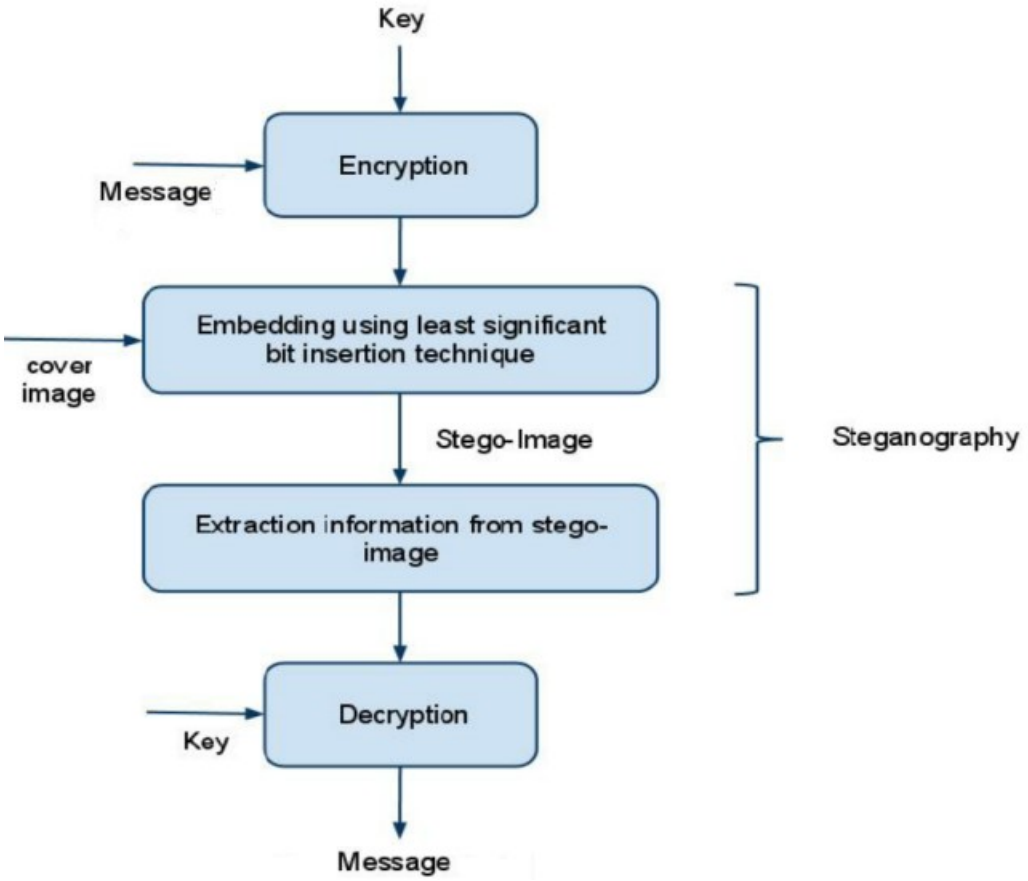

Figure 5. Flowchart showing encryption and decryption of the message using traditional LSB

Only one bit from each pixel in the cover image is used by the conventional Least Significant Bit technique. Each grayscale cover picture pixel's eighth bit is changed to contain a little portion of the hidden information. Replace the 8th bit in each of the three separate color (Red, Green, and Blue) channels in each pixel when utilizing a 24-bit color image file to conceal a hidden message.

Figure 6 illustrates a classic LSB algorithm example of a character "m" being hidden with the ASCII code (109 as decimal) and (0110 1101 as binary). Here, the letter "m" serves as an illustration of a cover image and a hidden message, respectively. Only four bits from the cover image, or half the size of the hidden message, are modified, as seen by the stego image created following single bit replacement.

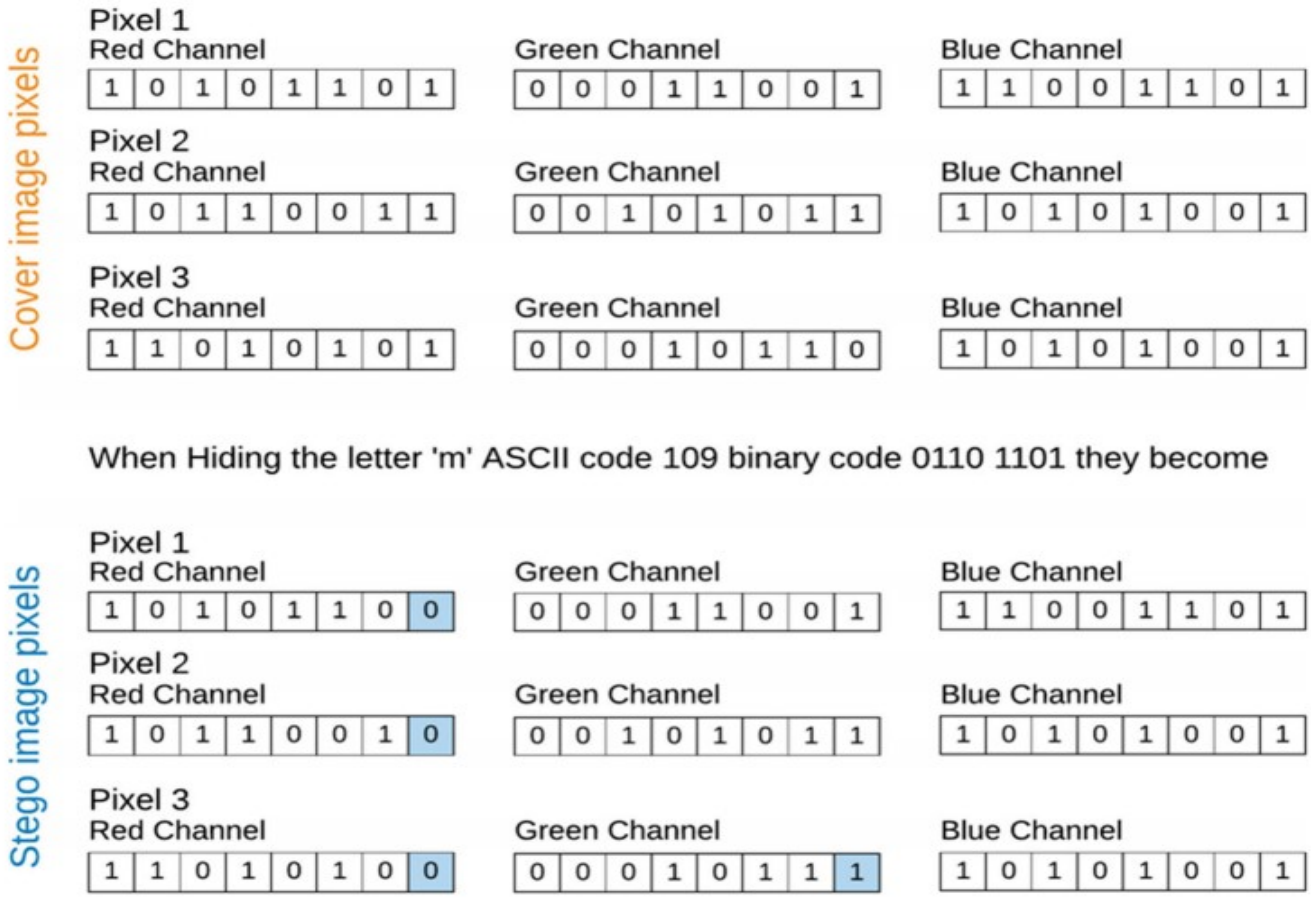

Figure 6. Example of LSB data hiding using 3 RGB color pixels

3.2 Adaptive LSB

The steganography method relies on both the visual qualities of the images and the human visual capabilities rather than various algorithms to conceal the hidden message.

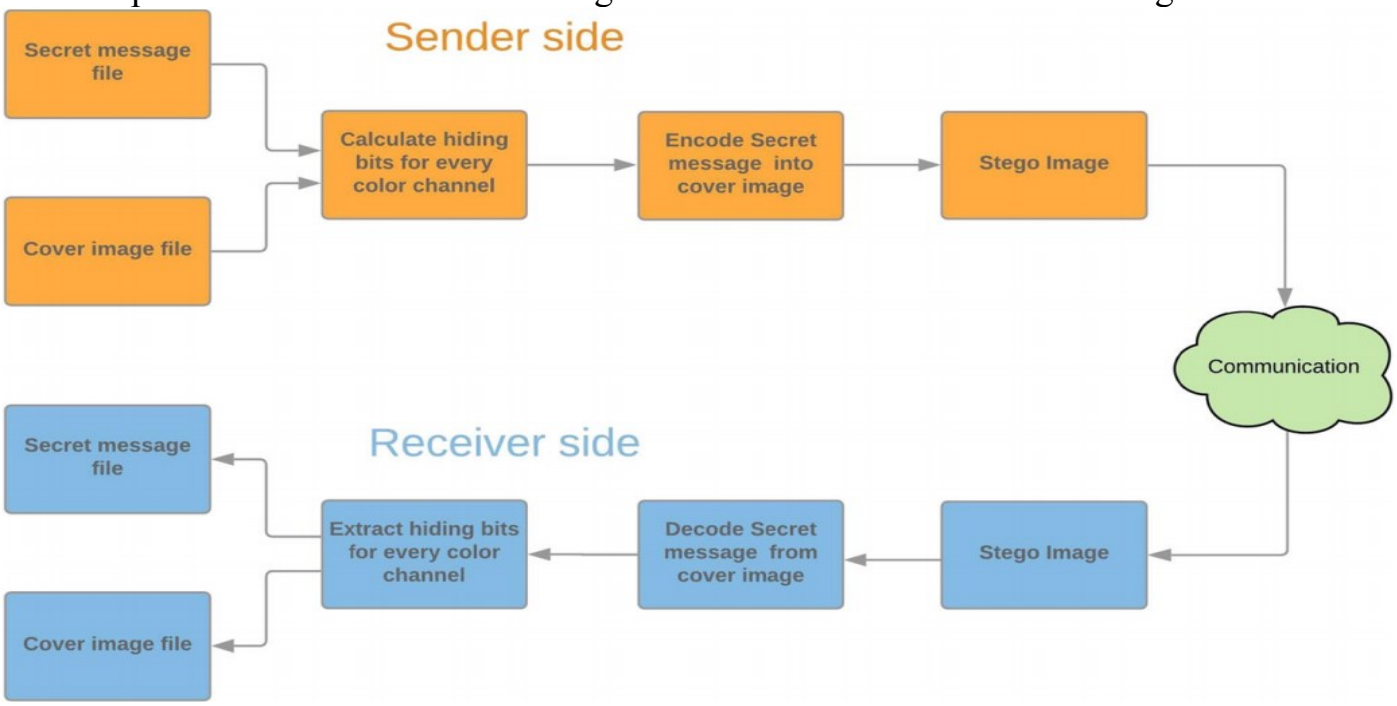

Figure 7. Adaptive Steganographic approach block diagram

If data concealing requires three bits, we will use the final bit in the Blue, Red, and Green channels. We will use the final two bits of the Blue, Red, and Green channels if we require 6 bits. In this scenario, if there are 4 bits needed for data concealing, we will use the final bit from each of the Blue, Red, and Green channels, and the final bit from the second-to-last channel of the Blue color. We will use the final two bits of the Blue if the needed bits for data concealing are 8 bits in this case. In this scenario, if the needed number of bits for data hiding is 8, we will use the final two bits from the Blue, Red, and Green channels, whereas the final two bits from the Blue and Red channels will be utilized. This technique of concealment is seen in Figure 8.

Figure 8. Adpative LSB data hiding in RGB channel bits

3.3 Filtered LSB

A digital image with a color depth of 24 bits is utilized as the cover material in the suggested steganography technique. A pixel, made up of three parts called Red, Green, and Blue, is the smallest component of an image. Not all pixels are used for embedding in this technique. In the beginning, a suggested filtering process is employed to choose the potential pixel for embedding the private messages. The MSB bit of each pixel is utilized for filtering. The entire process is carried out using a user-defined secret password, which can be any length and contain any number of characters. The password's ASCII value is then translated into a binary representation. The binary number is then split into three blocks of bits. If one or two more bits are needed as the last block, a rotational shift operation is used. As a result, each block is divided into its own decimal place, Pn.

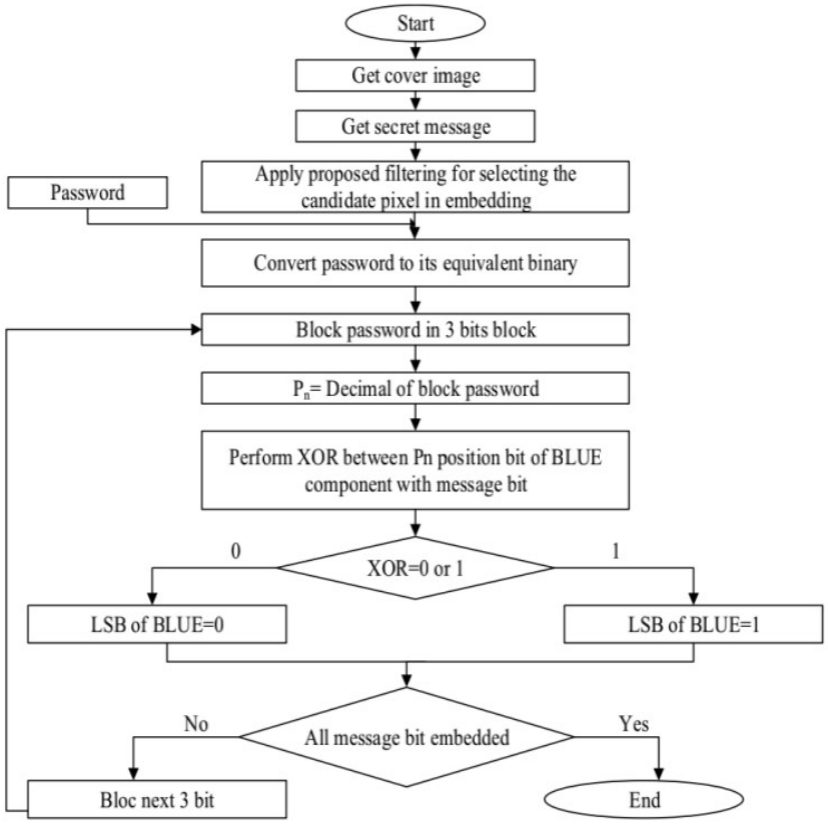

Figure 9. Embedding flowchart for filtered LSB.

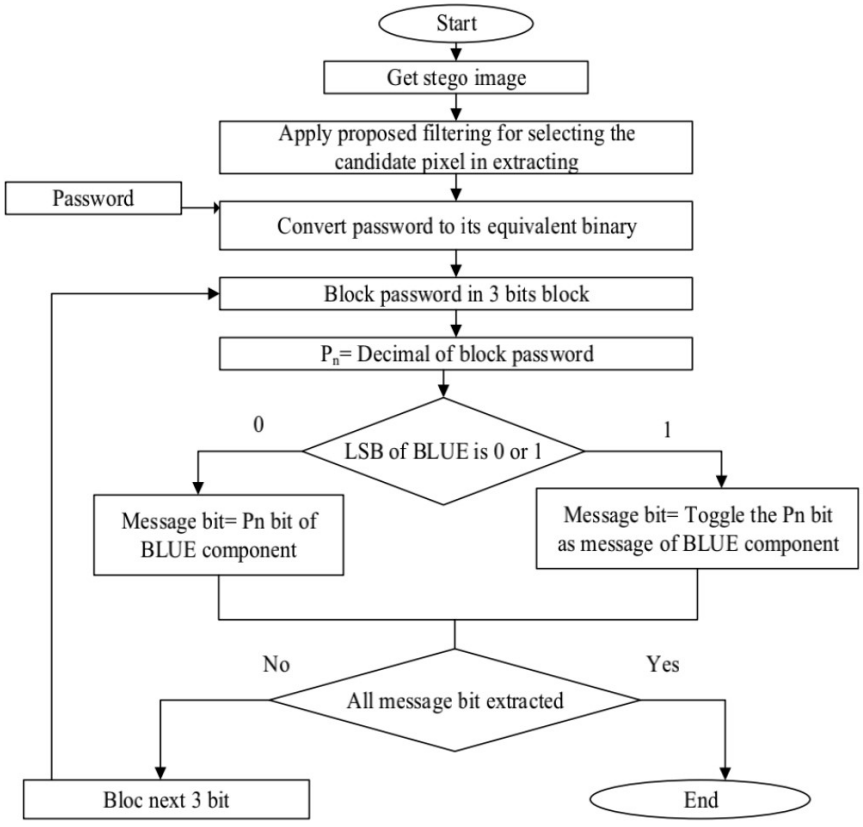

Figure 10. Extracting flowchart for filtered LSB.

3.4 Advanced filtered LSB

New approach to hide the message using image steganography. Advanced filtered LSB is the combination of traditional LSB, adaptive LSB and filtered LSB.

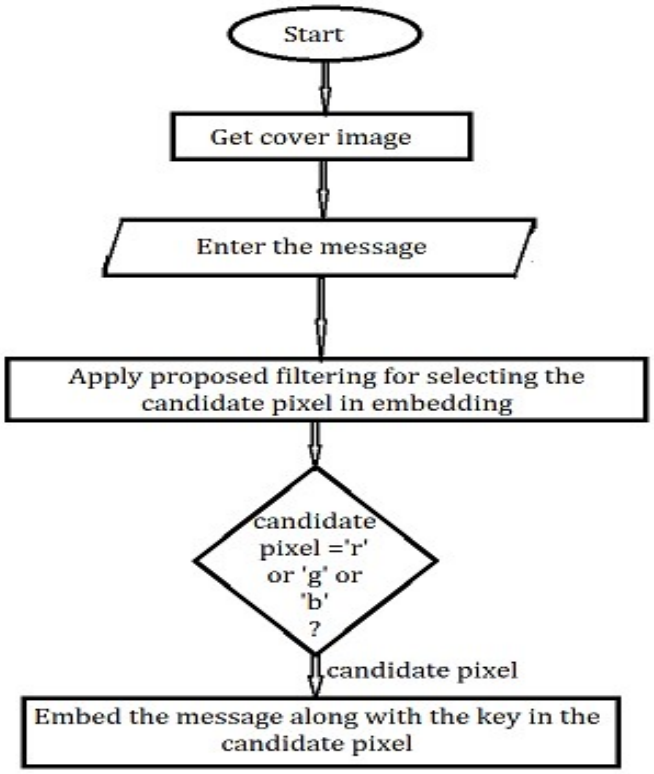

Figure 11. Embedding flow chart for advanced filtered LSB

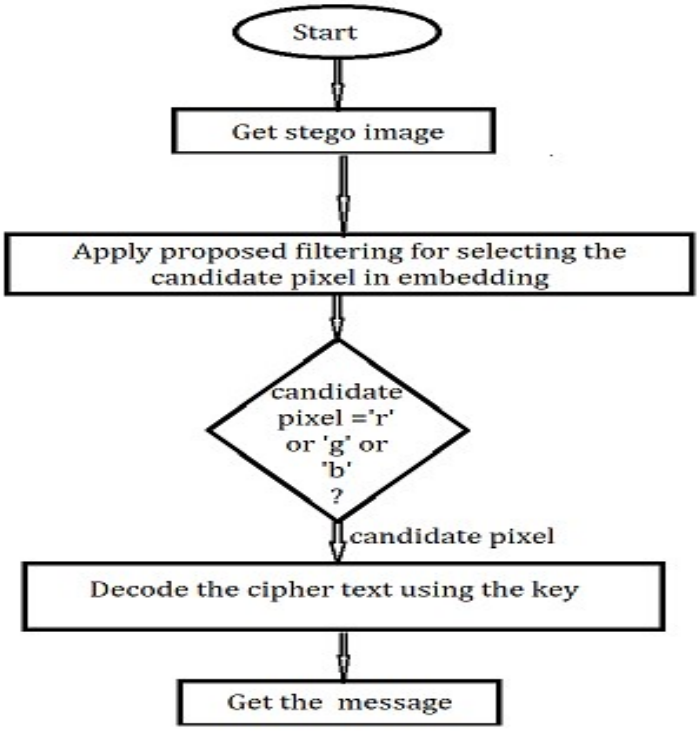

Figure 11. Extracting flow chart for advanced filtered LSB

3.5 Performance metrics

MSE is a performance metric used to compare the two images' quality. The MSE is a measurement of the squared cumulative error between the cover and stego images. where the image's width and length are M and N, respectively. The cover image is C, while S is the stego image. The two images must be the same size in order to calculate MSE. C and S calculate the square of the difference between each pixel in C and its corresponding pixel in S, add those values together, and divide the result by the total number of pixels. Excellent similarity between C and S is indicated by an MSE value of 0, and similarity declines as the MSE value rises.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}([S(i,j) - C(i,j])^2$$

4. IMPLEMENTATION

4.1 Tools used

- Visual Studio Code
- Python 3
- Jupyter Notebook

4.2 Platform

- Windows OS
- 4GB RAM
- 64 bits processor

4.3 Screenshot of the output using Traditional LSB

```
Image stegnography
       1.encode
       2.decode

 enter your choice:1
Enter your message: Mobile phones are used for a variety of purposes, such as
keeping in touch with family members, for conducting business, and in order t
o have access to a telephone in the event of an emergency. Some people carry
more than one mobile phone for different purposes, such as for business and p
ersonal use.
mse: =  13955.633665167416

enter 1 for continue otherwise 0:1

Image stegnography
       1.encode
       2.decode

 enter your choice:2

 your message:Mobile phones are used for a variety of purposes, such as keepi
ng in touch with family members, for conducting business, and in order to hav
e access to a telephone in the event of an emergency. Some people carry more
than one mobile phone for different purposes, such as for business and person
al use.


enter 1 for continue otherwise 0:
```

Figure12. Screenshot of the message output using Traditional LSB

Fig 13.a. mount.png

Fig13.b. stego_mount_traditional.png

4.4 Screenshot of the output using adaptive LSB

```
Image stegnography
       1.encode
       2.decode

 enter your choice:1
Enter the message name: Mobile phones are used for a variety of purposes, such as keeping in touch with family members, for con
ducting business, and in order to have access to a telephone in the event of an emergency. Some people carry more than one mobi
le phone for different purposes, such as for business and personal use.
mse: =  14013.124551724139

enter 1 for continue otherwise 0:1

Image stegnography
       1.encode
       2.decode

 enter your choice:2

 your message:Mobile phones are used for a variety of purposes, such as keeping in touch with family members, for conducting bu
siness, and in order to have access to a telephone in the event of an emergency. Some people carry more than one mobile phone f
or different purposes, such as for business and personal use.
```

Figure14. Screenshot of the message output using Adaptive LSB

Fig 15.a. mount.png image

Fig 15.b.stego_mount_adaptive.png

4.5 Screenshot of the output using filtered LSB

```
Image stegnography
       1.encode
       2.decode

 enter your choice:1
enter the messagehello world
mse: =  14013.330368815592

enter 1 for continue otherwise 0:1

Image stegnography
       1.encode
       2.decode

 enter your choice:2

 your message:hello world
```

Figure16. Screenshot of the message output using filtered LSB

Fig16.a. mount.png image

Fig16.b stego_mount_filtered.png

4.5 Screenshot of the output using advanced filtered LSB

```
Image stegnography
       1.encode
       2.decode

 enter your choice:1
enter the messageMobile phones are used for a variety of purposes, such as keep
ing in touch with family members, for conducting business, and in order to have
access to a telephone in the event of an emergency. Some people carry more than
one mobile phone for different purposes, such as for business and personal use.
mse: =  13836.364477761119

enter 1 for continue otherwise 0:1

Image stegnography
       1.encode
       2.decode

 enter your choice:2

 your message:Mobile phones are used for a variety of purposes, such as keeping
in touch with family members, for conducting business, and in order to have acc
ess to a telephone in the event of an emergency. Some people carry more than on
e mobile phone for different purposes, such as for business and personal use.
```

Figure17. Screenshot of the message output using advanced filtered LSB

Fig18.a. mount.png image

Fig18.b stego_mount_advancedfiltered.png

5. RESULT

S.N.	ALGORITHM NAME	MSE
1.	Traditional LSB	13955.63
2.	Adaptive LSB	14013.12
3.	Filtered LSB	14013.33
4.	Advanced Filtered LSB	13836.36

Table 1. Mean square error(MSE) obtained between the cover image and stego image while using different alogorithms for image steganography

As shown in the table 1., the MSE has increased when using traditional LSB than adaptive and filtered LSB algorithms. This is because in adaptive LSB all the bits of each component are used which increases the distraction in the stego image. The length of the message while using filtered lsb is small compared to traditional lsb because the length depends on the block size of the password. Hence, to compensate the password, we have to limit the bits of the message. The pixel used for embedding in filtered lsb is filtered before embedding starts. Hence, the component pixels used in traditional lsb and filtered lsb are different.

The advanced filtered lsb is the new approach where the MSE has decreased when compared to other algorithms because this approach combines the best portion of all three other algorithms.

6. CONCLUSION

Adaptive lsb image steganography takes longer time to decode compared to other alogrithm because the decryption involves extracting each LSB bit which is time consuming. The encoding depends on the block numbers of the password in the filtered lsb. Hence, the length of the password will be proportional to the message. Also, the algorithm is difficult to implement because of the implementation of the double security i.e., password and the secret key respectively. Traditional lsb has more mean square error than advanced filtered image steganography and it is very simple to implement. This simplicity can allow the attacker to find the message bits easily. Hence, the novel approach, advanced filtered image steganography the best among traditional , advanced and filtered lsb. The advanced filtered lsb provided pixel filtering which avoids tracking the pixel used for filtering. Also, it gives more focus on that component of the pixel which is very less visible to the human eye in the cover image used. The lsb embedding in advanced filtering helps to avoid the decrease the MSE.

References

[1] Saravanan, M., & Priya, A. (2019). An algorithm for security enhancement in image transmission using steganography. Journal of the Institute of Electronics and Computer, 1(1), 1-8.

[2] AbdelRaouf, A. (2021). A new data hiding approach for image steganography based on visual color sensitivity. Multimedia Tools and Applications, 80(15), 23393-23417.

[3] M. R. Islam , T. R. Tanni , S. Parvin , M. J. Sultana & A. Siddiqa (2020): Amodified LSB image steganography method using filtering algorithm and stream of password, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2020.1854902

[4] Nevriyanto, A., Sutarno, S., Siswanti, S. D., & Erwin, E. (2018, October). Image steganography using combine of discrete wavelet transform and singular value decomposition for more robustness and higher peak signal noise ratio. In 2018 International Conference on Electrical Engineering and Computer Science (ICECOS) (pp. 147-152). IEEE.

[5] Gaba, J., & Kumar, M. (2013, December). Implementation of steganography using CES technique. In 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013) (pp. 395-399). IEEE.