Design a Secure Communication Technique using Concepts of Image Steganography and Cryptography

Shashwat Kumar Dev, Kohinoor Jain, Vyshakh Sreekumar, Nikhil Bhardwaj, Manikandan K.

Abstract: With increase in the data transmission and data exchange in daily life, along with the increasing data thefts and other adversary snooping, the security and privacy of data has become an important thing to be concerned about. Throughout the years many different approach, ideas, algorithms and protocols have been developed to protect the data from snoopers and adversaries and ensure secure communication. Every approach has its own pros and cons. This project is an attempt to combine two different approaches of data protection-(Steganography and Cryptography) to develop a powerful and secured method for data exchange.

Keywords: Communication, Cryptography, security, steganography

I. INTRODUCTION

Steganography is the practice of sending the message in the way that it is hidden to third party or adversary. Using steganography, one can eliminate the risk of leaking of information of hidden message to third party and do so by hiding a confidential data in plain sight preventing the adversary from knowing the very existence of the data with his naked eye. If suspicion is raised, then this goal of steganography is defeated. Cryptography only conceal the message by substituting, re-arranging or hashing the messages. The adversary or the third party knows that a private encrypted message is present. The concept of steganography is different from cryptography; it does not let the adversary know that a secured message is in transmission. If the concepts of both steganography and cryptography are applied together, they can produce a very effective application for secure communication. In this project our main aim is to cover general concepts of steganography and implement an efficient technique with help of cryptography thus, using the concept of both domains to produce a powerful and efficient secured plain-sight communication technique. The proposed communication system is designed using python GUI consists of 2 main modules-Steganography and Cryptography.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author

Shashwat Kumar Dev, Student, Department of Computer science and Engineering, Vellore Institute of Technology, Vellore, India.

Kohinoor Jain Student, Department of Computer science and Engineering, Vellore Institute of Technology, Vellore, India.

Vyshakh Sreekumar, Student, Department of Computer science and Engineering, Vellore Institute of Technology, Vellore, India.

Nikhil Bhardwaj, Student, Department of Computer science and Engineering, Vellore Institute of Technology, Vellore, India.

Prof. Manikandan K., Associate Professor, Department of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India.

The user will be asked a secret text, a secret key through which he/she want to encrypt, a cover image to hide the data, and the format of the stego image in which he/she wants to save the file. After providing all the necessary details. The system will generate a stego image in the desired format with encrypted message encoded inside the stego image. The user can also mail the image directly to the intended recipient from the system GUI.

As for the recipient, he/she after obtaining the stego image can decrypt the message by supplying the correct image and decryption key. The security of the system is based on 2 elements – first on the encryption-decryption algorithm in use and second on the encoding algorithm used to encode the message in the image. Thus, providing a high-level secure system with an in-built feature of sending a secured mail.

II. LITERATURE SURVEY

The paper [1] surveys the topic by introducing with the basics and introduction to steganography-a data hiding technique and deals with history and uses of steganography technique. Paper [2] talks about steganography in a consisted and to the point manner. The author starts with text steganography and explains the methods like Line-shift coding, word shifting etc. to implement on the text. The paper deals with image steganography and introduces methods like LSB, filtering and transformations. The [3] paper mainly deals with the survey and analysis of the most widely-used steganography techniques and qualitative assessment of these techniques. The author describes the steganography as a multidisciplinary discipline and its application and comparison with cryptography. The [4] paper introduces the steganography through a different perspective and model the approach in the paper view the steganography technique as a problem of hypothesis testing and test it by viewing from an adversary point of angle by his ability and his capability to distinguish between an innocent cover message and a modified message containing the private hidden information. The [5] paper describes the overview of the steganography by introducing the need, the key features and differences with cryptography. The [6] paper deals with defining the border between steganography and steganalysis. The paper also deals with improving the steganographic strategies and schemes and enhancing the steganalytics capabilities along with possible research trends. [7, 8] gives an overview of the image steganography and different techniques of image steganography. The paper describes the keywords and elements related to image like image matrix, image compression etc. Paper also tells about the steganographic system robustness of the applied algorithm and the security of the system.

Retrieval Number: E2786039520/2020©BEIESP
DOI: 10.35940/ijitee.E2786.039520
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In [9] the author deals with most common method-based steganography i.e. LSB method. The paper describes and defines the LSB, its significance in image processing and steganography and various algorithms to hide the data. In [10] author gives an analysis of the LSB based steganography techniques on various file formats like GIF, PNG, JPEG etc. The paper deals with the efficiency and the ability to hold the secret message in case of an attack or any other vulnerabilities associated with implementation to a file format.

[11] paper deals with introducing a best approach for LSB based steganography by enhancing the currently used LSB substitution technique in order to increase the certainty and reliability of covert data. [12] article proposes a different LSB based steganography technique with an addition edge detection technique. The paper shows the method by which edges of an image are used in concealing the plain text messages with the help of steganography. The method proposed conceals the message in chosen dark spots but the information is not placed straight into those pixels. The [13] paper unlike the above paper deals with a different approach towards developing a steganographic technique by hiding information inside gray-scale images. The algorithm uses FIVE MODULUS METHOD called ST_FMM. The proposed method gives a high-quality image and gives non-noticeable distortions. The [14] paper unlike above papers deals with a recently developed procedure for image steganography which improves quality of the image. The procedure advised within the paper hides the key message supported looking out regarding the similar bits between the key texts and image pixels readings. Paper [15] describes the method of evaluation of a steganographic algorithms by computing a function. The paper deals PSNR and SSIM. The author describes their ability to compute the degradation of the image which has been manipulated with. The [16] paper takes Associate in Nursing in-depth scrutinize by introducing the reader to varied ideas and a glance at number of the Steganographic technique. The [17] This paper delivers a method for enhancing security of privileged data, which is a implemented using these methods: image compression using transform, symmetric-based cryptography, LSB. Therefore, the proposed methodology provides huge reliability and certainty and standard of the restored initial image. The [18] article is telling about the fruitful execution of the new steganography approach utilizing IDEA and LSBG techniques. The IDEA and LSBG have some crucial characteristics, for example, information classification, limit and strength. It is discovered that the productivity of this system is higher than that of different strategies. The [19] paper is about instructions to make a commonsense stenographic execution to shroud message inside dark scale pictures. With the help of five Modulus methods the secret message is hidden inside the cover images. The algorithm is called ST- FMM. In the [20] paper, we clarify what are the limitations of steganography also, what it can do. We separate it with the related controls of cryptography and traffic security and diagram various methodologies of them created to cover scrambled copyright imprints or sequential numbers in advanced sound or video. It shows that open key data concealing frameworks exist and don't appear to be basically compelled to situation where superintendent is uninvolved. In the paper [21] author did research on e-healthca

III. IMPLEMENTATION

The implementation is done in two phases-:

(i)Encryption: In this phase the data is encrypted using cryptography technique like Vigenere cipher, AES, S-DES, RSA or ElGammal.

(ii) Encoding: The data is encoded in the cover image using RGB technique.

A. Platform

- Python Tkinter: for GUI development.
- OpenCV: OpenCV is a package which contains functions used for Computer Vision and digital image processing.
- SMTP (Simple Mail Transfer Protocol): It is used for generating, sending, routing and receiving mails between the servers. smtplib component of python is going to be used to initialize SMTP client session object so that a mail can be sent to any computer on the internet having SMTP or ESMTP listener daemon.
- PyCrypto: Combination of two things, hash functions and encryption algorithms. SHA256 and RIPEMD160 are secure hash functions which can be used. Different encryption algorithms such as DSA, AES, RSA can be used. Extra modules can be added without any problem using this package. Used to encrypt message using RSA.

B. System models and methods

The main architecture of the process for communication between 2 parties is as follows**:**

i. The sender (Alice) selects a cover image for encoding the message in it.

ii. The sender encrypts the confidential data with suitable cryptographic algorithm and encodes the encrypted message to image RGB technique and transmits it to the receiver (BOB) on an unreliable channel.

iii. The receiver (BOB) receives the stego-image and decodes the encrypted text from it.

iv. The encrypted text is decrypted using the same cryptographic algorithm and confidential message is obtained.

The projected and the associated GUI will be developed and implemented in Python.

C. Pre and Post processing

The input is taken as an image to encode the text into this cover image. The image can be of the format like (.jpg, .bmp, .jpeg, .png, .jpeg). These images are then processed in the following steps using PIL (Python Imaging library):

1. Image reading:

```
image = Image.open(img, 'r')
```

2. Convert into binary:

For encoding and other mathematical functioning, it is easier to interpret the image in binary format.

```
def convert_binary(data):
bin_data = []
for i in data: bin_data.append(format(ord(i), '08b'))
return bin_data
```

After encoding and decoding the data to or from the image the data is present in the binary format. The above function is used to interpret the binary data and convert it into readable format.

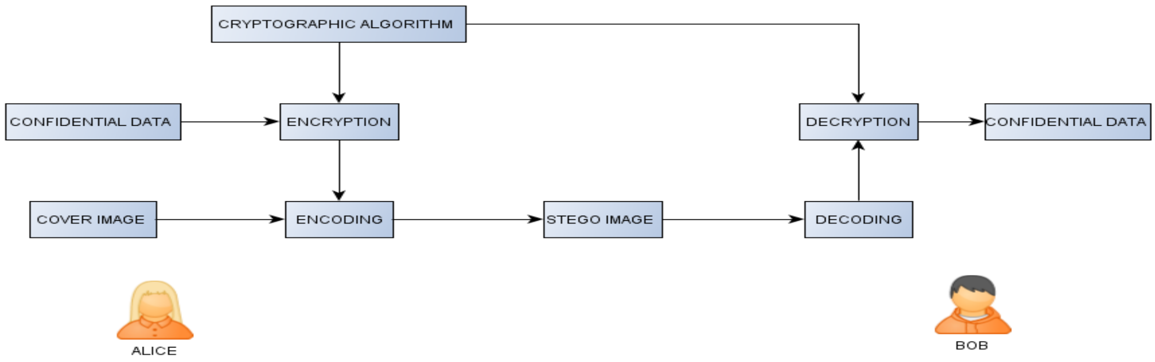

Fig. 1.Flow diagram of proposed approach

Pre and post processing of the text include just to convert it into binary format and encrypt and decrypt it using AES algorithm as follows:

```
def encryption(rawmsg, pass):
private_k  =  hashlib.sha256(pass.encode("utf-8")).digest()
rawmsg = pad(rawmsg)
iv = Random.new().read(AES.block_size)
cipher = AES.new(private_k, AES.MODE_CBC, iv) return
base64.b64encode(iv + cipher.encryption(rawmsg))
def decryption(encrypted, pass):
private_k                                                  =
hashlib.sha256(password.encode("utf-8")).digest()
encrypted = base64.b64decode(encrypted)
iv = enc[:16]
cipher = AES.new(private_k, AES.MODE_CBC, iv) return
unpad(cipher.decryption(enc[16:])
```

Stenography technique which is proposed here can be evaluated with the help of performance metric which is called PSNR. It assists in measuring the distortion prior to the encoding and later in the encoded image. The ratio between peak signal and noise ratio depicts the performance of algorithm. PSNR is used in calculation of peak signal to noise ratio which is used as a parameter to evaluate the quality among the two images. If it is high, images are of best quality.

Human eye should not be able to see any visual artifacts. To check whether the image is of good quality or not PSNR value will be used. Following equation can be used to calculate the PSNR value.

PSNR= 10 log2((255)2 / MS) db

$MS = (1/A*B)\sum P-1$

$\sum B-1(A(x, y) - A'(x, y))2$

Where, image size is represented by A and B. Original value of pixels is represented by A(x,y) and the pixel value of stego image is represented by A'(x,y).

Higher the value of PSNR, better will be the quality of the image. This is shown as when PSNR reached to infinity MS leads to zero. On the other hand there will be large difference between the images for low PSNR value.

Test image 1

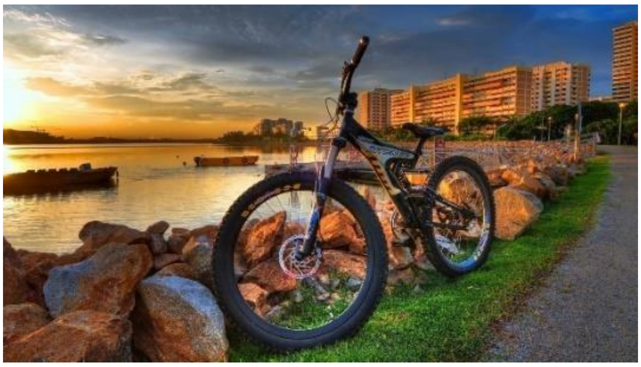

Fig. 2.Cover Image

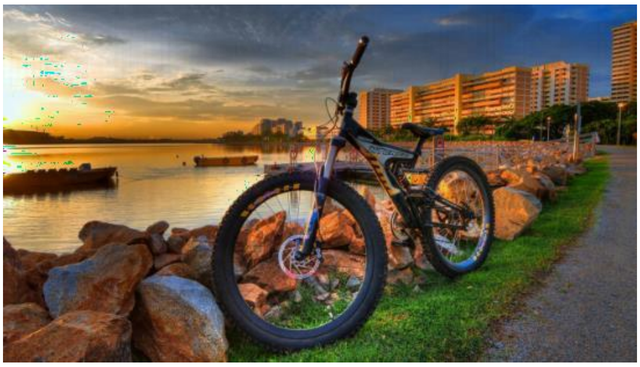

Fig. 3. Stego image

Test image 2

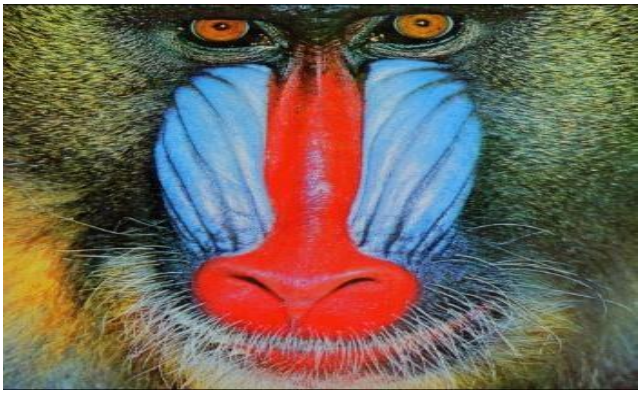

Fig. 4.Cover image

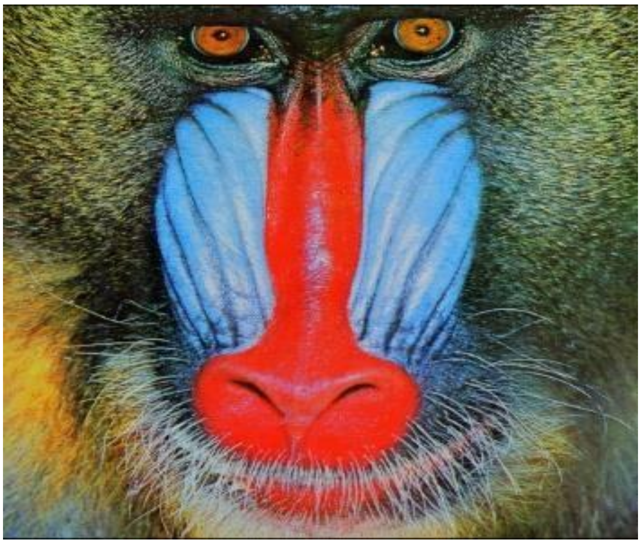

Fig. 5. Stego image

Test image 3

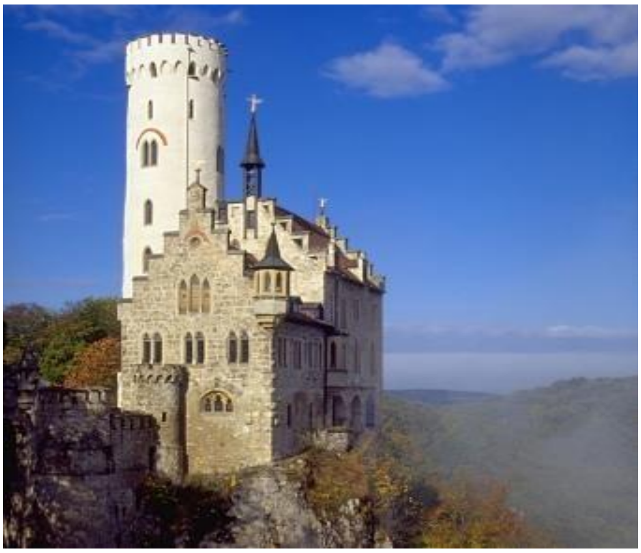

Fig. 6. Cover image

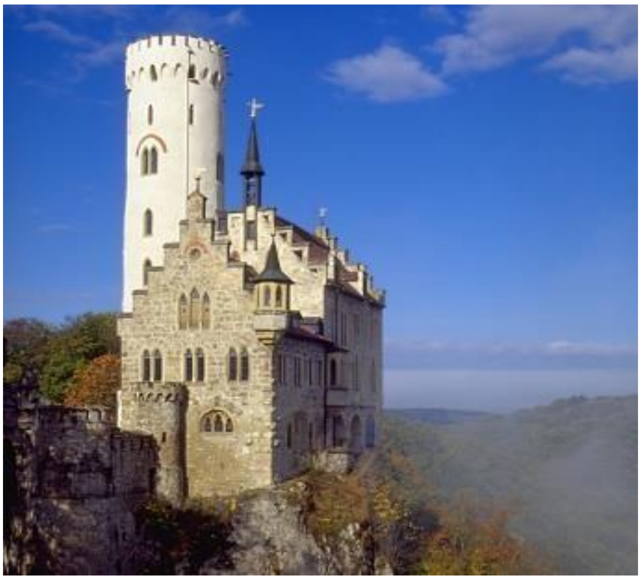

Fig. 7. Stego image

Test image 4

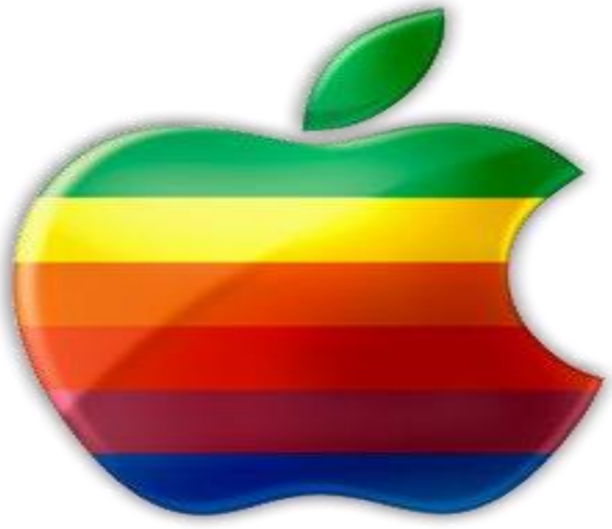

Fig. 8 Cover image

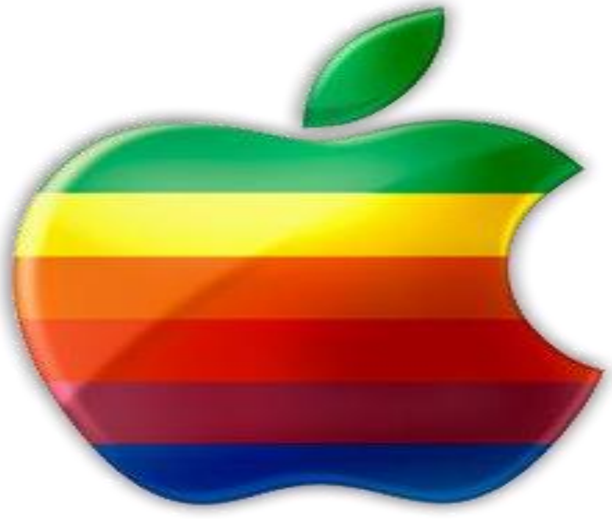

Fig. 9. Stego image

Test image 5

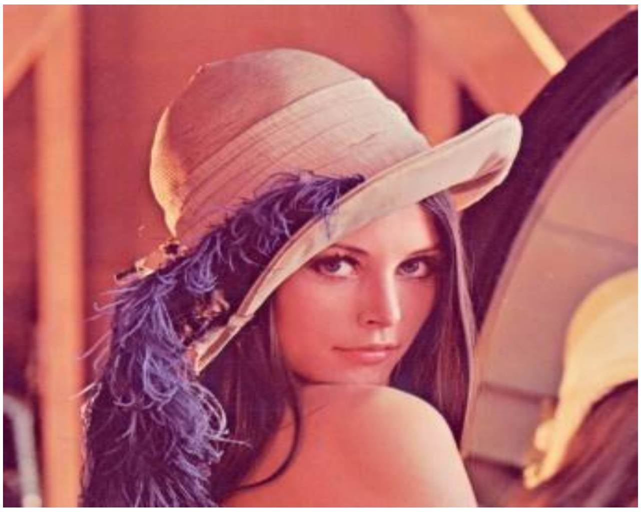

Fig. 10. Cover image

Fig. 11. Stego image

IV. RESULT AND DISCUSSION

According to the calculated PSNR values the proposed RGB steganography technique has proved to be an effective and efficient technique. High PSNR values are prove to the minimum distortion of the images and thus are not visible to a normal human eye. Thus, the steganography technique used is highly secure. The AES encryption further adds security to the system providing symmetric encryption. The mail feature in the system provides an extended utility to the user to communicate secret message to another person.

Table 1: Images and their respective PSNR values (in decibel)

IMAGES	PSNR values (in decibel)
Image 1	94.577075
Image 2	85.0606
Image 3	83.022014
Image 4	79.72578
Image 5	83.339932

V. CONCLUSION

Cryptography is a crucial part of information sharing through networked networks. This application provides an efficient method to pass messages in a safe manner using cryptography and stegnography. The application can be further improved by adding some more utilities and designing a better UI. Some features like providing more crypto algorithm like DES, Blow Fish, RSA etc. for encryption of the message can provide more utilities to the application. Overall, the present application is very handy, secured and interactive providing sufficient utilities to the users.

REFERENCES

1. Kumar, A., & Pooja, K. (2010). Steganography-A data hiding technique. International Journal of Computer Applications, 9(7), 19-23.
2. Hariri, M., Karimi, R., & Nosrati, M. (2011). An introduction to steganography methods. World Applied Programming, 1(3), 191-195.
3. Dumitrescu, D., Stan, I. M., & Simion, E. (2017). Steganography techniques. IACR Cryptology ePrint Archive, 2017, 341.
4. Cachin, C. (1998, April). An information-theoretic model for steganography. In International Workshop on Information Hiding (pp. 306-318). Springer, Berlin, Heidelberg.E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.
5. Kaur, H., & Rani, J. (2016). A Survey on different techniques of steganography. In MATEC Web of Conferences (Vol. 57, p. 02003). EDP Sciences.
6. Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2(2), 142-172.
7. Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In ISSA (pp. 1-11).
8. Umamaheswari, M., Sivasubramanian, S., & Pandiarajan, S. (2010). Analysis of different steganographic algorithms for secured data hiding. IJCSNS International Journal of Computer Science and Network Security, 10(8), 154-160.
9. Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography techniques. In Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205) (Vol. 3, pp. 1019-1022). IEEE.
10. Thangadurai, K., & Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In 2014 International Conference on Computer Communication and Informatics (pp. 1-4). IEEE.
11. Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In 14th International Conference on Computer and Information Technology (ICCIT 2011) (pp. 286-291). IEEE.
12. Jain, N., Meshram, S., & Dubey, S. (2012). Image Steganography Using LSB and Edge–Detection Technique. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 223.
13. Jassim, F. A. (2013). A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv:1307.0642.
14. Al-Shatnawi, A. M. (2012). A new method in image steganography with improved image quality. Applied Mathematical Sciences, 6(79), 3907-3915.
15. Hore, A., & Ziou, D. (2010, August). Image quality metrics: PSNR vs. SSIM. In 2010 20th International Conference on Pattern Recognition (pp. 2366-2369). IEEE.
16. Bhadra, J., Bojamma, A. M., CN, P., & Nachappa, M. N. An Insight to Steganography.
17. Saxena, A. K., Sinha, S., & Shukla, P. (2018). Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach. International Journal of Image, Graphics and Signal Processing, 10(4), 13.
18. Shanthakumari, R., & Malliga, S. (2019). Dual-layer security of image steganography based on. IDEA and LSBG algorithm in the cloud environment. Sādhanā, 44(5), 119.
19.] Jassim, F. A. (2013). A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv:1307.0642.
20. Anderson, R. J., & Petitcolas, F. A. (1998). On the limits of steganography. IEEE Journal on selected areas in communications, 16(4), 474-481.
21. Gopichand G., Kohinoor Jain, Shashwat kumar Dev (2019). Research on E-healthcare Security Evaluation in Cloud-Based System. International Journal of Recent Technology and Engineering, 8, 2277-3878.

AUTHORS PROFILE

Shashwat Kumar Dev is a third-year student at Vellore Institute of Technology, Vellore, India and will be graduating in 2021. His research interests include Health care, cloud computing and data security.

Kohinoor Jain Student at Vellore Institute of Technology, Vellore, India. He is currently pursuing B. tech in Computer science and Engineering. A paper has been published by him in the field of cloud security. His research interests include cloud security, artificial intelligence, and cyber security.

Vyshakh Sreekumar, Student at Vellore Institute of Technology, Vellore, India. He is an undergraduate student within the Computer Science program. He will graduate with Btech. Computer Science in 2021. His research interests include cyber security and digital forensics.

Nikhil Bhardwaj, Student at Vellore Institute of Technology, Vellore, India. He is currently pursuing Bachelor of Technology Degree in Computer Science and Engineering. His research interests include cyber security and IOT.

Prof. Manikandan K., is an Associate Professor, -School of Computer Science and Engineering-Vellore Institute of Technology, Vellore, India. He is faculty coordinator cyber security department. His research interests include cyber security, Deep learning, Artificial intelligence