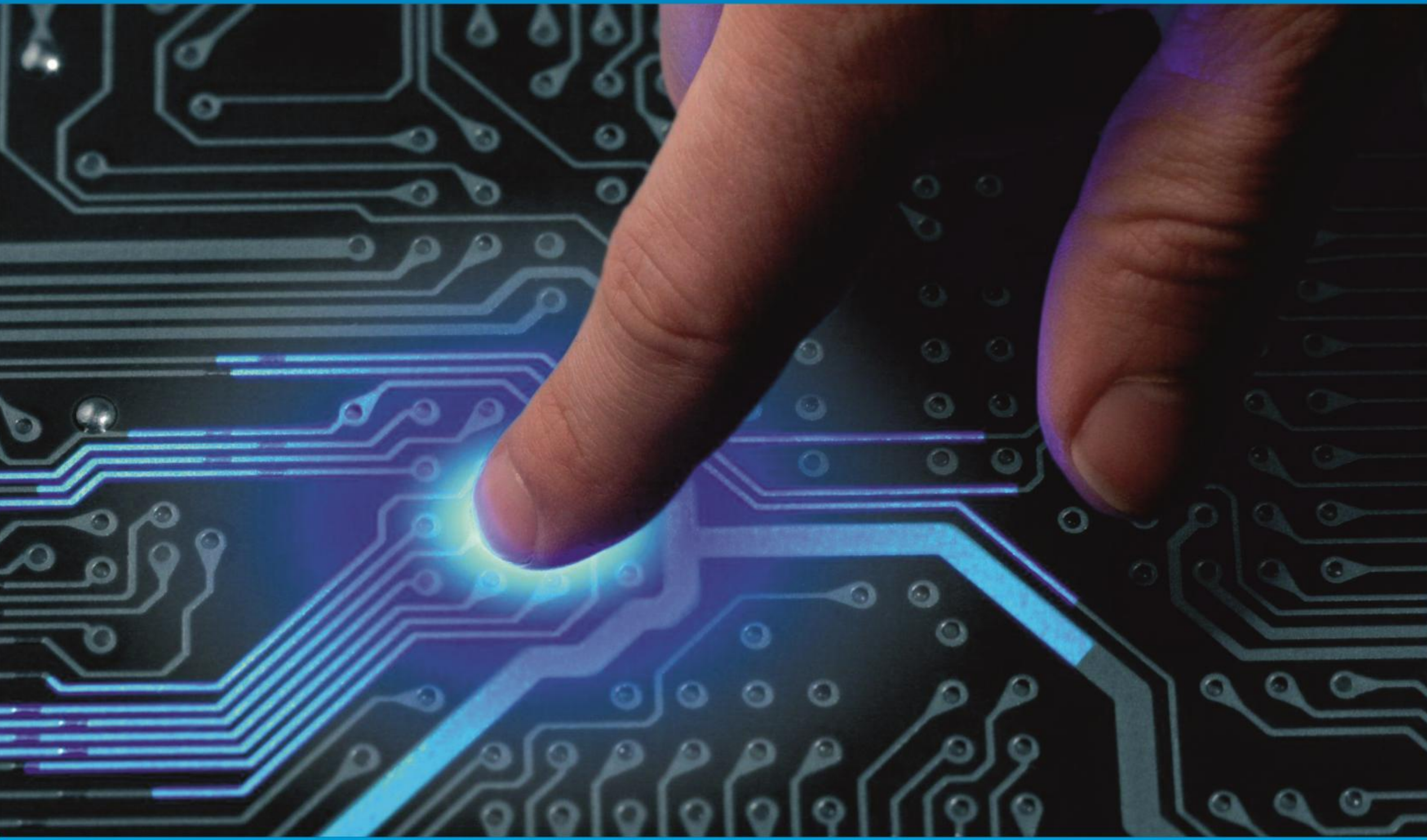
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

Improving Steganography with Two Levels of Security

T.Suba Nachiar, A.M.Sabhari, T.R.Sesha Prasan Kumaran, S.Sudharshan

Assistant Professor, Department of CSE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India

Student, Department of CSE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India

Student, Department of CSE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India

Student, Department of CSE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India

ABSTRACT: Steganography is the process of hiding secret data within an ordinary, non-secret file or image in order to avoid detection from intruders. A huge number of messages circulate through the social media, and many of these messages carry personal information. The least significant bit method of data steganography is effective in hiding messages, but it is not much secure. Our proposed system will present a way to raise the security in the method of hiding data without affecting the effectiveness of the method. The proposed method will be based on breaking an image into pixels and selecting a block, the secret message will be embedded into this block which acts as a covering media. After inserting the message, the block will be returned to the image. In addition to this, the covering image will be encrypted at the dispensing end using cryptography and decrypted at the receiving end.

KEYWORDS: Steganography, least significant bit method, pixel, block, covering image, cryptography

I.INTRODUCTION

Text messages are considered one of the most common types of data circulating through social media, which requires protection as they contain confidential information or information of a person that no unauthorized person is allowed to see. So the process of hiding secret messages is important. And to implement this process, it is necessary to search for a medium that carries confidential data so that this medium is large and that a concealment process does not result in a message from affecting the covering media and that change is not noticed by naked eye. The color digital image is considered as one of the best options to hide message for various reasons. The most important among them are

- Color images are a massive medium due to their high resolution
- Color images are widely available and can be easily obtained
- Easy to process color digital image
- A specific part of the image can be used to hide the message

Thus color images can be used as suitable media to hold text messages, providing a high secure environment to hold and cover secret data. This paper is organized as follows: Section II describes the related study, Section III describes the proposed system, Result and discussion is presented in Section IV and Conclusion in SectionV.

II.RELATED STUDY

Two techniques steganography and cryptography are used to ensure that user's confidential and important data will be safe. Cryptography is the method of storing and transmitting data in a particular form so that it can be read and used only by those for whom it is intended. But with the generated cipher text, one can identify that a secret message has been encrypted and on finding it the attacker may try to recover the secret message by performing a series of attack on the cipher text. And if attacker couldn't succeed, there might be a possibility that encrypted secret message may be destroyed during the attack. Steganography is an art of covering secret information within a carrier which could be an image file. This technique provides an invisible form of communication since the image file which has the secret information embedded within it is delivered to receiver instead of secret information itself. It hides the existence of secret message, only the sender and receiver can suspect the existence of secret information**.** Image steganography is a very interesting and important technique which attracts many researchers to perform research on it to find and suggest new and better solution to make important information more secure, and developers to make dreams of researcher true by developing useful applications and tools for desktop computer and smart phones. Few projects regarding image steganography are:

- Android application developed by White and Martina that allows user to hide short text message in an audio that is recorded by user and then user can send this message to anybody
- An application called MobiStego using steganography algorithm, that only hides message into an image
- Another application called PixelKnot which only hides message into image using F5 algorithm but this application takes too much processing time

Most of these applications are developed only to hide text message into an image which must be smaller in size, not more than few words. These applications change the original image type into other type e.g. if image have jpg extension, these applications will convert it into other data type e.g. png extension after hiding text message in it. Our proposed system will take an image and hide the secret message into that image. The image in turn will be encrypted at the sender side and sent to the receiver where the image is decrypted and the secret message is retrieved.

III.PROPOSED SYSTEM

The proposed system is specially designed to improve security in transmitting a secret message from the sender to the receiver. In this proposed system, the secret message is embedded within the image and the image is encrypted using RSA encryption algorithm. This makes the intruders very difficult to decrypt the algorithm and extract the secret message. The below image shows the original image and the image that carries the secret message.

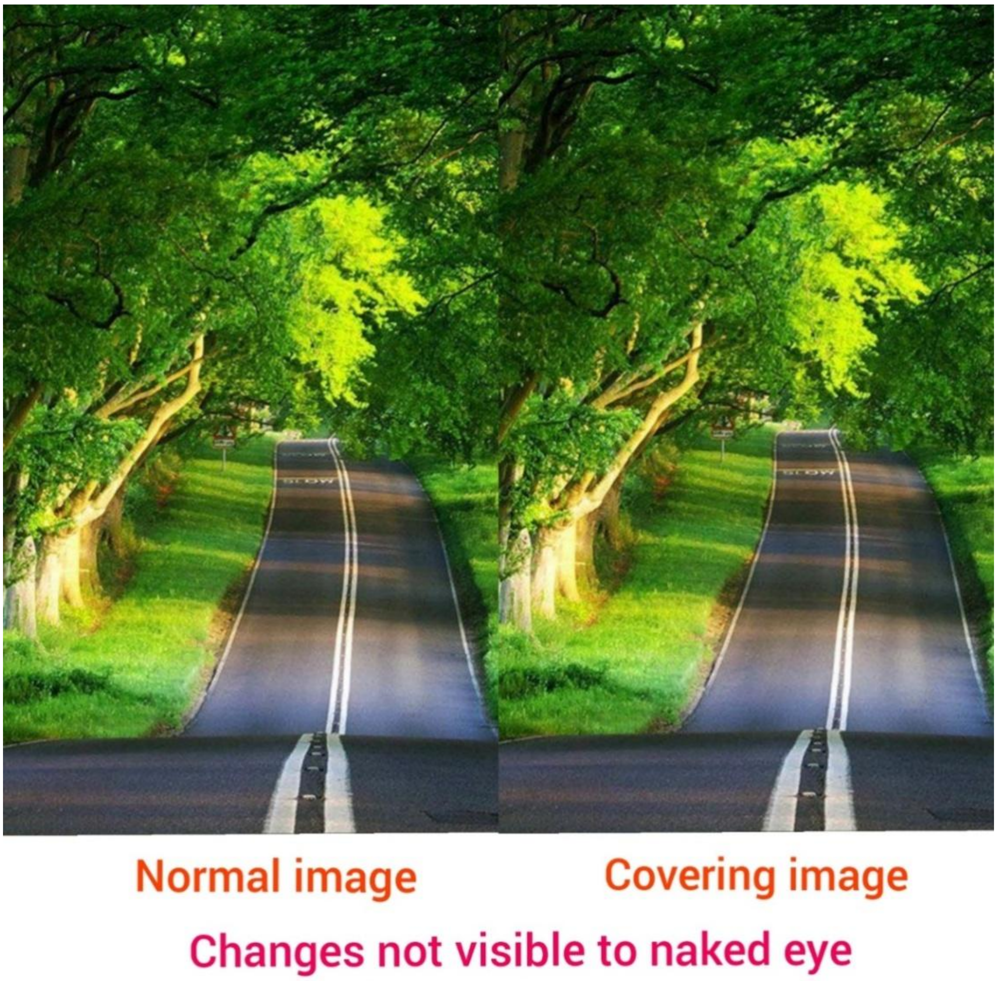


Figure 1: Original and carrier images

Least significant bit (LSB) method is one of the commonly used method to hide secret data. In the proposed system, the system has three main units. The first is a sender unit which is used by the sender. This unit consists of choosing the operation to encode. The customer will select the image into which the secret message is going to be embedded. After selecting the image the sender shall choose the encode option to initiate data transfer. The second unit is the data transfer unit. The system divides the image into blocks and selects a particular block to hide the data. The least significant bit of the pixels are used to hold the data. Eight pixels values are required to store a single symbol of the secret message. After successful embedding the block is returned back to the image. Once the block is returned back, the whole covering image is encrypted using the RSA algorithm of cryptography and set for transmission to the receiver. The third unit is the receiver unit. The receiver on receiving the image decrypts it using the key and performs decoding operation to retrieve the secret data from the image.

The process of hiding the message into the color image causes slight changes in the image but these changes are impossible to be noted with naked eye, and these changes in the value of each pixel range between -1 and +1.The mean square error (MSE) between the original image and the covering image must be closed to zero. The peak signal to noise ratio (PSNR) between the original image and the covering image must be very high.

The overall architecture of the proposed system is shown below:

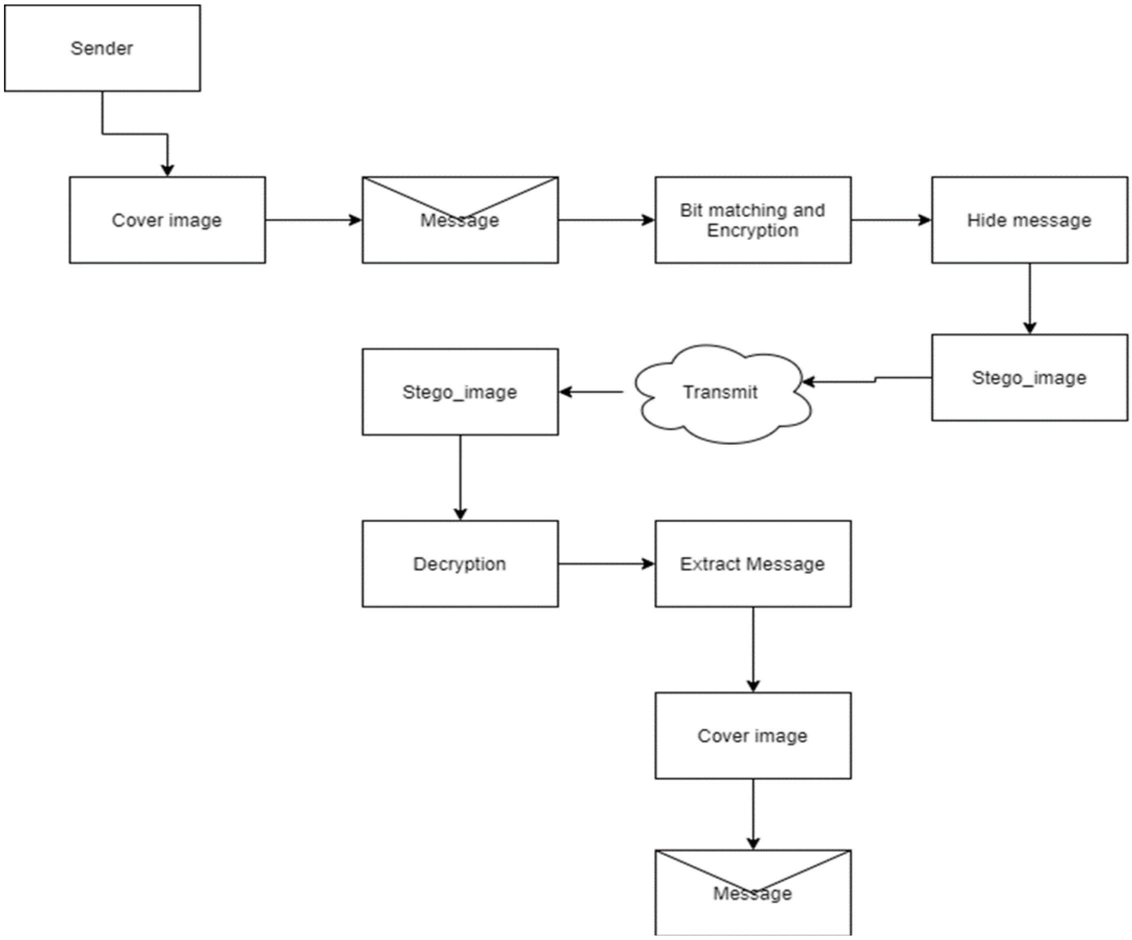


Fig 3: Overall Architecture of Proposed System

Thissystem is divided into fouroperations based on two processes:

1. Encoding Operation
2. Decoding Operation

Steganography Process

3. Encryption Operation
4. Decryption Operation

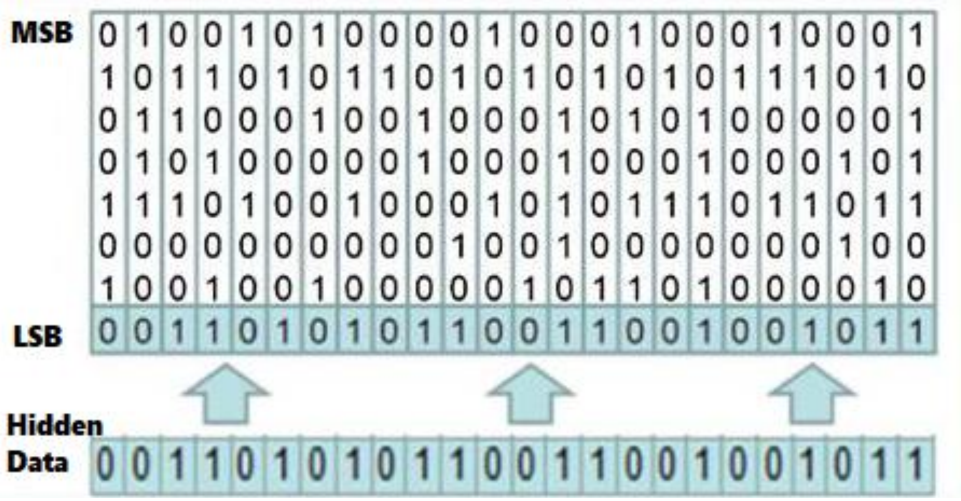
Cryptography Process

The system starts with the steganography process. This process consists of the encoding and decoding operations. The encoding operation starts when the sender selects the image to encode. The text message is converted into binary digits. The selected image is divided into blocks. One particular block is chosen from the set of blocks. That block is broken down into pixels. The least significant bit of the pixels are used to hold the secret data.

Eight pixels are required to store a single symbol from the secret message. Once the data is embedded the block is recreated and returned to the original image. Then starts the encryption operation where the image holding the secret data called the cover image is encrypted using RSA algorithm of encryption and set for transfer to the receiver.

Next the encrypted image is transferred to the receiver and that's where the decryption process starts. The encrypted image is decrypted by providing the same encryption key used in the sender side and thus the image is decrypted.

Then starts the decoding process where the decrypted image is split into blocks and the block containing the secret message is identified and the message is extracted. Thus the secret message is securely transferred.

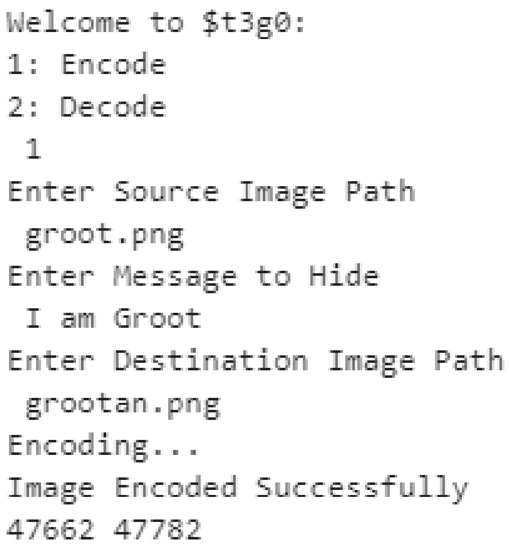


MSB	0	1	0	0	1	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
	1	0	1	1	0	1	0	1	1	0	1	0	1	0	1	0	1	0	1	1	1	0	1	0
	0	1	1	0	0	0	1	0	0	1	0	0	0	1	0	1	0	1	0	0	0	0	0	1
	0	1	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	1
	1	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	1	0	1	1	0	1	1
	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0
	1	0	0	1	0	0	1	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	1	0
LSB	0	0	1	1	0	1	0	1	0	1	1	0	0	1	1	0	0	1	0	0	1	0	1	1
Hidden Data	0	0	1	1	0	1	0	1	0	1	1	0	0	1	1	0	0	1	0	0	1	0	1	1

Figure 2: Hidden message in LSB Method

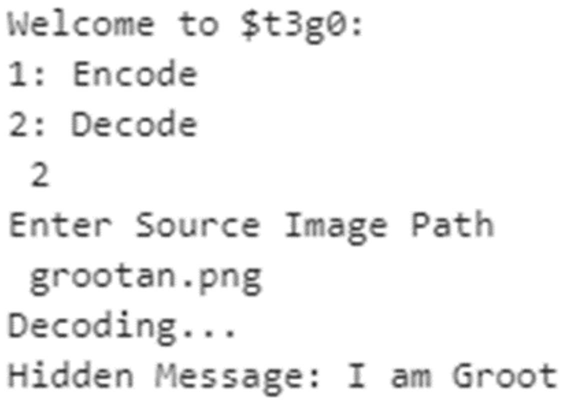
IV.RESULT AND DISCUSSION

This system is developed with a computer having a processor of 2GHz or above. The system must have a RAM memory of 2GB or above and a hard disk storage of 20GB or above. We recommend to use Windows operating system 7 or above. The below images depict a list of outputs obtained from our system.



```
Welcome to $t3g0:
1: Encode
2: Decode
 1
Enter Source Image Path
 groot.png
Enter Message to Hide
 I am Groot
Enter Destination Image Path
 grootan.png
Encoding...
Image Encoded Successfully
47662 47782
```

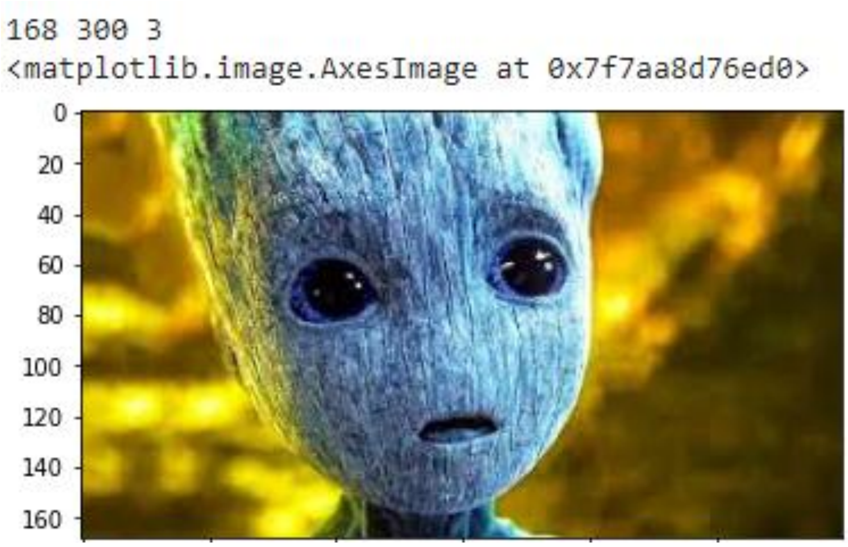
Figure 4: Encoding output in Steganography



```
Welcome to $t3g0:
1: Encode
2: Decode
 2
Enter Source Image Path
 grootan.png
Decoding...
Hidden Message: I am Groot
```

Figure 5: Decoding output in Steganography

Figure 6: Covering image before encryption



```
168 300 3
<matplotlib.image.AxesImage at 0x7f7aa8d76ed0>
```

Figure 7: Image while processing

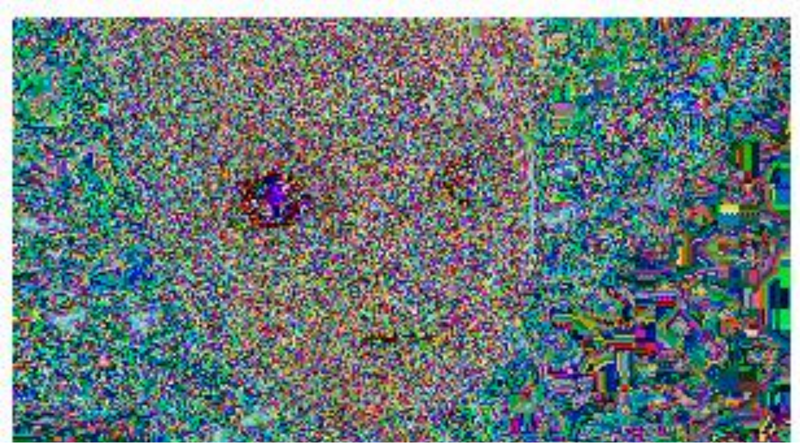


Figure 8: Image after encryption

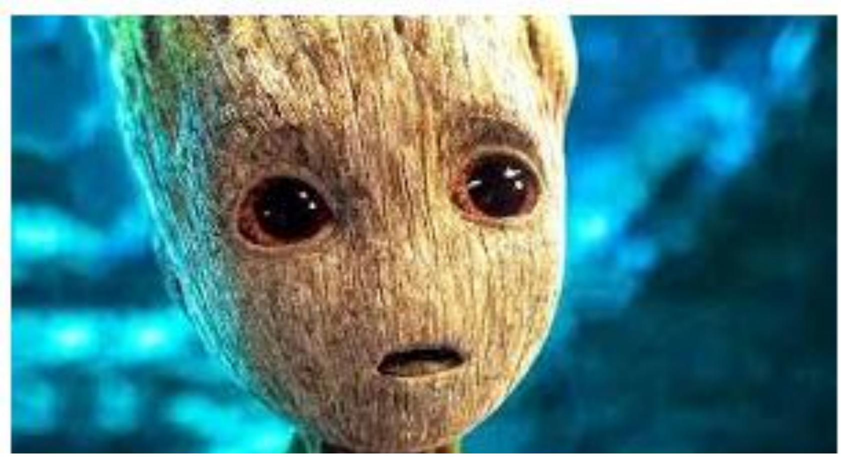


Figure 9: Covering image after decryption

V.CONCLUSION AND FUTURE SCOPE

Image steganography allows two individuals to communicate privately. LSB method of data steganography was implemented, security issues were added to make this method more secure, an extra operation was added to this method. Instead of using the whole image we focus only on a single block in the image, the block size and the selected block number must be kept in secret to form a private key. The proposed method was implemented and the obtained experimental results showed that using the image block does not negatively affects the LSB parameters.Our future works are aimed at incorporating the following features into the application. A customized user interface will be provided to the system and will be launched as an app with some additional features. The app will be extended to make it compatible to serve a large number of users. In order to make the app more productive, hosting it on cloud platforms will be investigated.

REFERENCES

[1]. ZiadAlqadi, ”Image Blocking to Hide Secret Message”, International Journal of Computer Science and Mobile Computing, Vol. 9, Issue. 11, November 2020, pg.21 – 27

[2]. AzmatUllah, MohsinIjaz, ”Stego App: Android based Image Steganography Application using LSB Algorithm”, International Research Journal of Engineering and Technology, Vol. 5, Issue.9 , September 2018

[3]. YousifEltous, Majed Omar Dwairi, Mohammad S. Khrisat, Saleh A. Khawatreh, ZiadAlqadi,”Secure Secret Message Steganography”, International Journal of Computer Science and Mobile Computing, Vol. 9, Issue. 6, June 2020, pg.1 – 9

[4]. Rushdi Abu Zneit, Jamil Al-Azzeh, ZiadAlqadi, BelalAyyoub, Ahmad Sharadqh,”Using Color Image as Stego-Media to Hide Short Secret Messages”, International Journal of Computer Science and Mobile Computing, Vol. 8, Issue. 6, June 2019, pg.106 – 123

[5].ZiadAlqadi, Mohammad S Khrisat, Yousif El Tous ,”Message Segmentation and Image Blocking to Secure Data Steganography”, International Journal of Computer Science and Mobile Computing, Vol. 9, Issue. 8, August 2020, pg.75– 82

[6]. ZiadAlQadi, M Elsayyed Hussein, “Window Averaging Method to Create a Feature Victor for RGB Color Image”, International Journal of Computer Science and Mobile Computing, vol. 6, issue 2, pp. 60-66, 2017

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details