ISSN: 2455-1848
International Journal of Innovative Research & Growth
A Peer Reviewed & Referred International Journal
Volume-9 Issue-4 February-2020
Impact Factor-3.0
www.ijirg.com, editor@ijirg.com

# Practical RGB Layered Method Of Data Hiding Using Image Steganography

**[1]G. W. Wagaye, [2]F. M. G. Yohans**
Ethiopian Institute of Technology – Mekelle (Eit-M) School of Electrical and Computer Engineering, Mekelle University, Mekelle, Ethiopia
Email- geberemedhn.wubet@mu.edu.et, wubetger@gmail.com

***Abstract***
*Hiding information with technique of steganography provides that security of the data. The huge challenge here for computer users is security and confidentiality of the message transfers through different media. Therefore, this paper proposed red-green-blue (RGB) layer method for security of information which includes encryption and decryption algorithm (DES) and LSB techniques. LSB stands for least significant bit (LSB) coding is the simplest way to embed information. Image steganography is a techniques used to transmit hidden information by combining with cover image to give stego-image that provides a new way of securing the information to avoid disruption in transmission over network and implemented in MATLAB. So, the result implies the security of hiding information process.*
***Keywords:-*** *Steganography, Cryptography, DES, Image, LSB, RGB.*

## 1- INTRODUCTION

In this highly digitalized world, the internet serves as an important instrument for data transmission and sharing. However, since it is a worldwide and exposed medium, some confidential data might be stolen, copied, modified, or destroyed by intended or an unintended observer. Therefore, security issue becomes an essential concern.

Security of data is decisive part of any society and it provides confidentiality and authentication as well. The information should be hidden by image steganography technique to protecting from corruption and unauthorized access over the communication network as shown in figure 1. The focus behind data security is to ensure privacy while protecting personal or corporate data. Steganography is one of the ways used for secure transmission of confidential information. Data hiding techniques have been widely used for transmission of hiding secret message for long time.

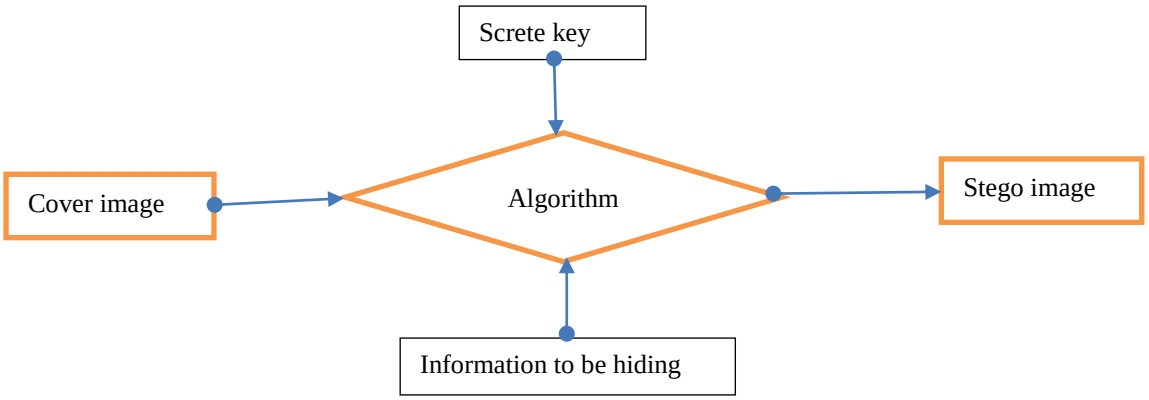


Figure.1. steganography principle [1]

Steganography is an art and science of writing hidden message in such a way that no one apart from the intended recipient knows the existence of the message .In steganography, the message used to hide secret message is called host message or cover message. Once the content of the host message or cover message are modified the resultant message is known as stego message is known as stego message [2]. Cryptography scrambles messages so it can't be understood. It defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attackers. Cryptography is the study of methods of sending message in disguised from so that only the intended recipients can remove the disguise and read the messages. Image steganography is the techniques of hiding data in cover image [2, 3, 4].

**1.1- PROBLEM OF STATEMENT**

Currently, in the world internet users' head ache is hiding data over network. Since the media is exposed to different hackers, then RGB layer method is proposed to hide message with colored layers combined with encryption and decryption techniques

**2- LITERATURE SURVEY**

In recent years, a number of encryption algorithms and steganography algorithms have been proposed to overcome the security problems in the open communication channel. Some of the related works to proposed technique are [5-6]. In cryptography Advanced Encryption Standard (AES) algorithm is used to encrypt secret message and then Pixel Value Differencing (PVD) with K-bit LSB substitution is used to hide encrypted message into true color RGB image [7]. In cryptography AES algorithm is used to encrypt a message and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys which make this system highly secured [8].

LSB modification techniques are easy ways to embed information, but they are highly vulnerable to even small cover modifications [9]. An attacker can simply apply signal processing techniques in order to destroy the secret information entirely. Transform domain methods like DCT and wavelet transforms hide messages in significant areas of the cover image which makes them more robust to attacks than the LSB approach, even though the amount of secret data that can be hidden using this technique is very small as compared to LSB based steganography scheme. However, while they are more robust to various kinds of signal processing, they remain imperceptible to the human sensory system.

## 3- SYSTEM MODELING

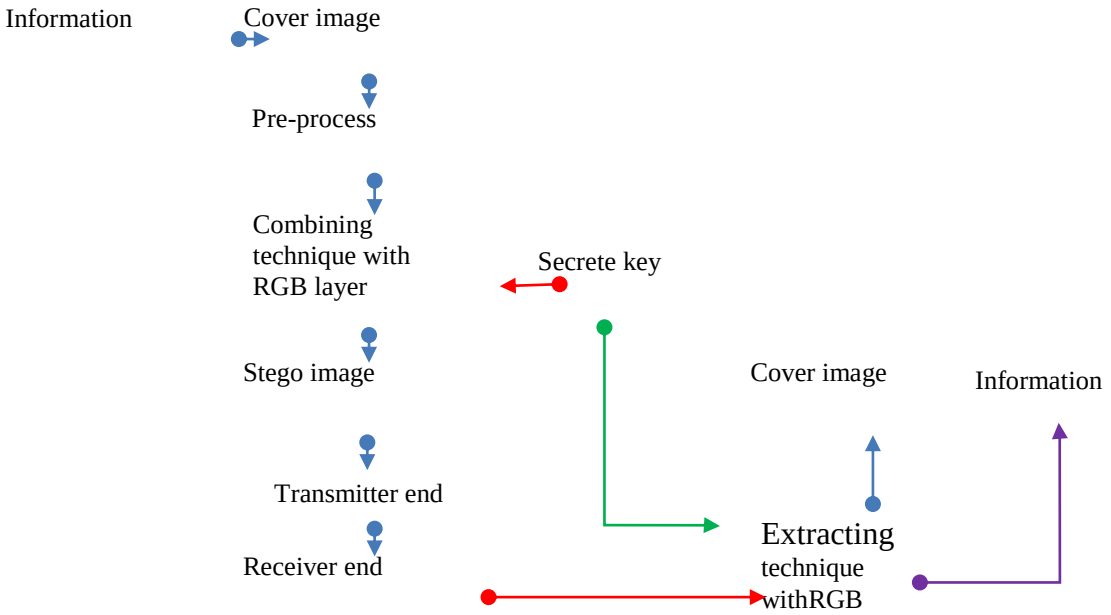


Figure 2. Block diagram of proposed system

The main objective of this paper is to develop data hiding algorithm using steganography as shown in figure 2 while incurring minimal perceptual degradation and to solve the problem of unauthorized data access. The hiding data in cover image resulting stego-image that can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganography technique to detect the message from the stego-object, he would still require the stego-secret key decoding method to decipher the encrypted message as indicated in figure 2.

## 4- RESULT AND DISCUSSION

### 4.1- HIDING PROCESS

In order to hide the data, a username and password are required prior to use the system. Once the user has been login into the system as shown in figure 3, the user can use the information (data) together with the secret key to hide the data inside the chosen image. Using the proposed algorithm, these data will be embedded and hided inside the image with smooth distortion of the original image. Once the information and the cover image are loaded the process of hiding the data within the image starts its process.

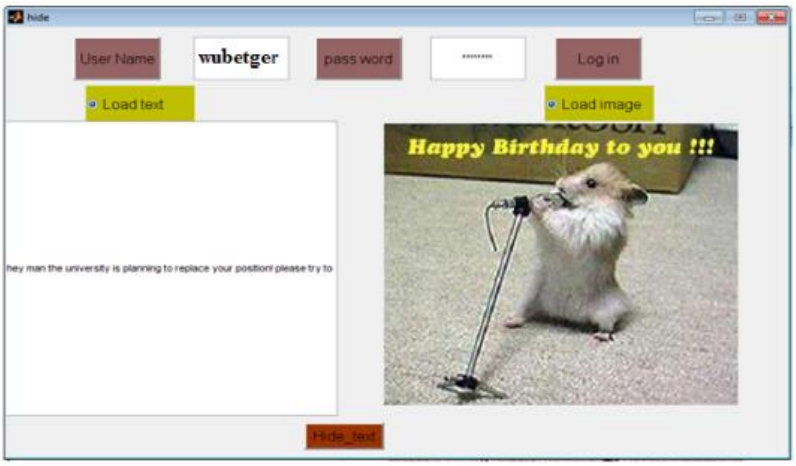

Figure 3. Hiding process

## 4.2- COVER MAGE

A sample image used in this system is shown in figure 4. Since the cover image is a JPEG image the pixel values vary from 0 to 255. The pixel values of the cover image for red layer, green layer and blue layer are shown graphically in figure 5, figure 6 and figure 7 respectively. In these graphs the plots show the variation of pixel values for each column.


Figure 4. The sample image used as a cover image

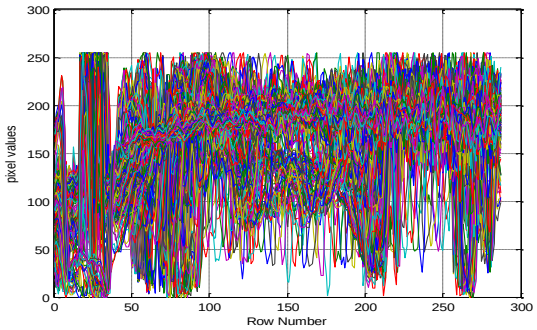


Figure 5. The pixel values of red layer

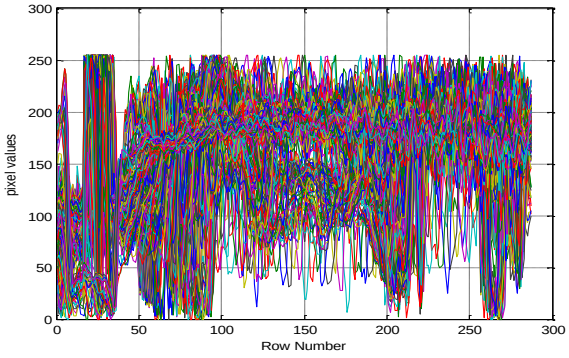


Figure 6. The pixel values of green layer

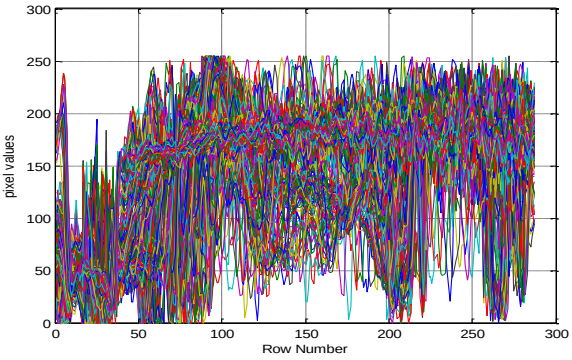


Figure 7. The pixel values of blue layer

## 4.3- STEGO IMAGE

Loading the cover image and the secret message to be hidden, the matrices representing both of them are generated by loading the image to MATLAB and converting the text message in to its respective sequence. The two matrices are multiplied to yield a new matrix (stego image)$M(n) = M(i) * M(t)$ as in figure 8. The pixel values of the new matrix are shown in figure 9, figure 10 and figure 11.


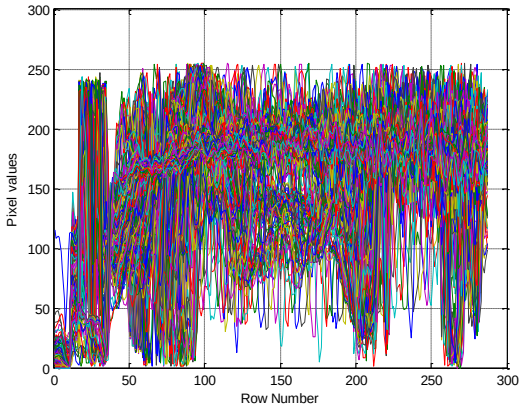

Figure 8.stego image

Figure 9: The pixel values of red layer for the new matrix

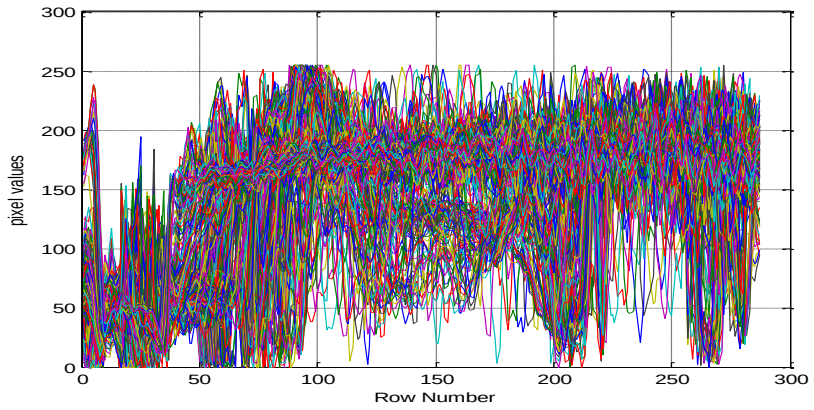


Figure 10: The pixel values of green layer for the new matrix

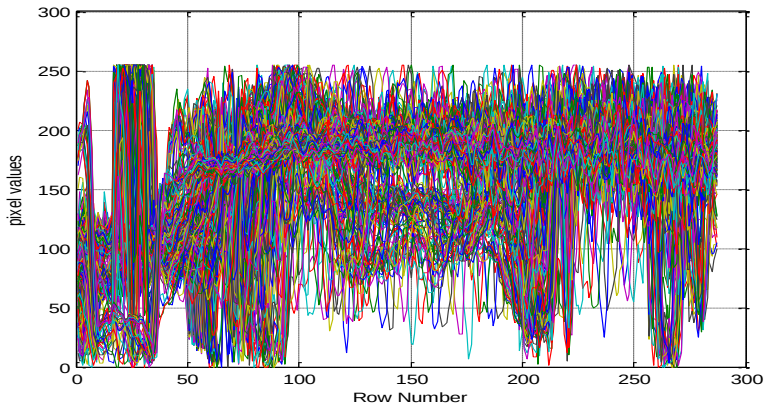


Figure 11: The pixel values of blue layer for the new matrix

**4.4- ENCODING PROCESS**

The process to encode or load the image as in figure 12, then stego-imageis given to a transmitter end and will be sent through communication channel. It is known that noise will be introduced in the path across the channel. To evaluate the peak signal noise ratio of the channel is as [4, 10]:

$$\text{PSNR} = 10\log_{10}\left(\frac{sqr(Cmax)}{MSE}\right) \qquad 1$$

Where $C_{max}$ is the maximum pixel values from 0 to 255 and MSE is defined as [4, 10]

$$MSE = \frac{1}{MN}\sum_{x\,\&y=1}^{M\&N}(Sxy - Cxy) \qquad 2$$

Where x and y are image coordinates and M&N are dimension of the image $C_{xy}$ and $S_{xy}$are cover image and stego image respectively

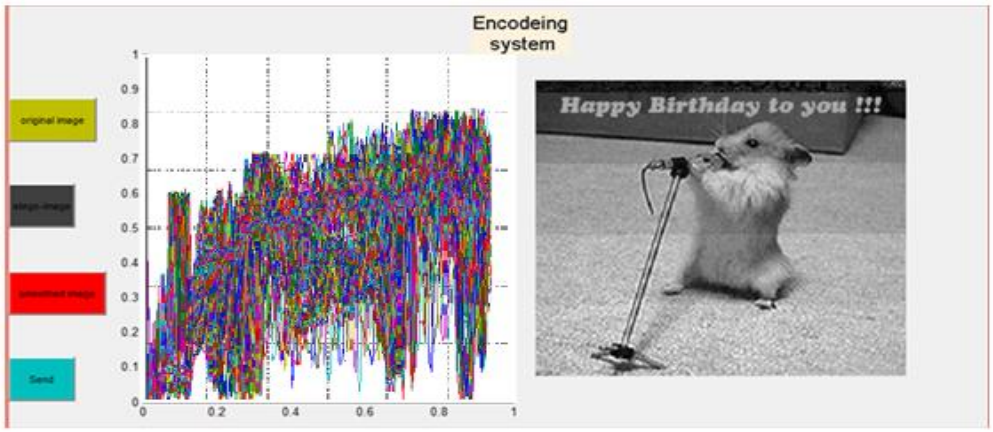


Figure 12: encoding system

**4.5- PERFORMANCE ANALYSIS**

As shown in figure 13. In this figure 'm1' and m2 represents the text matrix generated before and after transmission respectively while m3 represent the ratio of the received stego_image and the cover image.

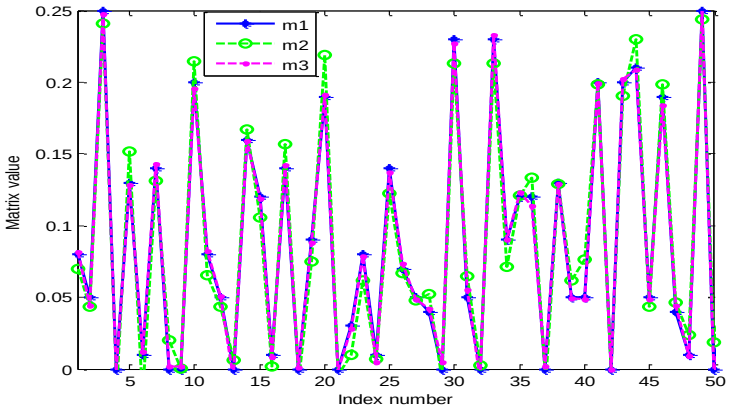


Figure 13: comparison of the ratio of received and sent matrix [10]

**5- CONCLUSION**

The Storage of secret information is a constant security concern, and the reliability and integrity of this information is important. The RGB approach is designed to protect the secrete message from intended and unintended attackers as well as the channel effect introducing during the transmission period and increases the data size to be hide in an image by having three layers (RGB) of the original image which is specified to the minimum requirement of the cover image that is the width and height of the image is 100 because in small size of images, the effect of hiding is visible, leading to suspicion.

**6- REFERENCES**

i. Johnson, N.F., Jajodia, S.(1998). Exploring Steganography: Seeing the Unseen", *Computer Journal*, 31,26-34.

ii. Thomas, S. E., Philip, S.T., Nazar, S., Mathew, A., Joseph, N.(2012). Advanced Cryptographic Steganography Using Multimedia Files, *International Conference on Electrical Engineering and Computer Science (ICEECS-2012),*Trivendum

iii. Dimyati, M., Dewanti, R. D., Kustiyo, Danoedoro,P., Hartono.(2018). Interpretability Evaluation of Annual Mosaic Image of MTB Model for Land Cover Changes Analysis, *TELKOMNIKA*, 16,934~945.

iv. Kumar,V.A.,, Dharmaraj ,C., Rao, Ch. S.(2017). A Hybrid Digital Watermarking Approach Using Wavelets and LSB, *International Journal of Electrical and Computer Engineering (IJECE)*, 7, 2483~2495.

v. Laskar, S. A., Hemachandran, K.(2012). High Capacity data hiding using LSB Steganography and Encryption, *International Journal of Database Management Systems (IJDMS)*, 4,57-68.
vi. PhadVitthal S., Bhosale Rajkumar S., Panhalkar Archana R.(2012). A Novel Security Scheme for Secret Data using Cryptography and Steganography, *I.J. Computer Network and Information Security*, 2, 36-42.
vii. Sarmah, D. K., Bajpai, N.(2010). Proposed System for data hiding using Cryptography and Steganography, *International Journal of Computer Applications*, 8,7-10.
viii. Harshitha, K. M., Vijaya, P. A.(2012). Secure Data Hiding Algorithm Using Encrypted Secret Message, *International Journal of Scientific and Research Publications*, 2,1-4.
ix. Walia, E., Jain, P., Navadeep.(2010). An Analysis of LSB & DCT based Steganography, *Global Journal of Computer Science and Technology*,10, 4 – 9.
x. Gebremedhn W. W.(2018).Performance Investigation of Channel Noise Effect in Data Transmission medium Using Signal to Noise Ratio (SNR), *Indonesian Journal of Electrical Engineering and Computer Science*, 11,419-423.