International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 8 Issue 01 Ver. II || Jan 2019 || PP 14-21

A New Approach to Embed Confidential Data within Color Images

H. M. Shah Paran Ali[1], Mosammat Jakia Sultana[2],
Shamima Nasrin[3], and Md. Golam Moazzam[4]

[1]*Islami Bank Bangladesh Ltd.*
[2]*Department of ICT, Govt. of the People's Republic of Bangladesh.*
[3]*Shaikh Burhanuddin Post Graduate College, Bangladesh.*
[4]*Department of CSE, Jahangirnagar University, Savar, Dhaka-1342. Bangladesh.*
Corresponding Author: H. M. Shah Paran Ali

Abstract: *Data transmission is a challenging part in public communication system due to interception and improper manipulation by eavesdropper. To protect against the threat, various ways are available, one of an attractive solution is Steganography- an art of embedding confidential information within other information in such a way that it is hard or even impossible to identify the existence of any hidden information. This work is proposing an algorithm to embed data inside the file (i.e. image, pdf, audio, video etc.) using steganogrphy technique in the sender end and then recover the original message in the receiver end with a secret key. Encryption file (contains encrypted message) will be merged with the carrier file to convert into Stego file. On the other hand, receiver will decrypt the original message from Stego file using secret key. It also attempts to identify a suitable Steganography algorithm depending on the given application among alternatives.*

Keywords - *Cryptography, Decryption, Encryption, Secret key, Steganography, Stego-image.*

Date of Submission: 30-12-2018 Date of acceptance: 15-01-2019

I. INTRODUCTION

Due to upgrade of modern technology, communication of secret information between sender and receiver is a critical factor. Communication between two parties located on same secure network usually emerges limited challenges and can be considered as manageable. Advancement in technology that encourages hackers/intruders activities result in lack of security to user's confidential data. In these situations, confidentiality and data integrity are essential to protect system against unauthorized access and usage which don't rely only on technological advancement. The most popular technique for embedding confidential messages that have been used from ancient era in different ways. Cryptography is an important technique that was created for securing the communication using different methods to keep data in secret format. However, it's not enough to keep the contents of message secret, sometimes it requires doing communication between sender and receiver. For that reason, it is needed to implement more security which is called Steganography [1], [2].

Steganography is the practice of concealing private or sensitive information within the cover or carrier file and presence imperceptible and is to be reliably communicated to a receiver that appears to be nothing out to the usual. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis. In Steganography, various types of carrier are available (Text Carrier, Image Carrier, Audio Carrier and Video Carrier) [3].

The proposed algorithm will be concealed secret data within the carrier file to defend the data secrecy. Secret data means not only plain text, but also the proposed system will cover any types of file like text, doc, pdf, image etc. Every sender information and receiver information will be exactly same. No more chance to loss quality of file or other data types.

Since Steganography has different category, the paper proposed an algorithm that will be covered secure communication between two parties (Sender and Receiver) using Secret Key Steganography technique. Secret key steganography is a way of another process in steganography which uses the same procedure other than using secure keys. It uses the individual key for embedding the data into the object which is similar to symmetric key. For decryption it uses the same key which is used for encryption that has shown in **Fig. 1**.

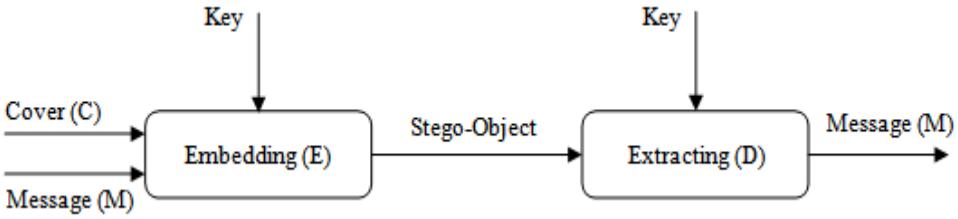

Fig. 1: Secret Key Steganography

The proposed system provides a platform to put any types of secret file as an input and some sort of cover or carrier file (i.e. Image, Audio and Video etc.) to generate a stego or embedded file. Once the proposed algorithm is accommodated, then sender will send the stego file to other parties. Since the receiver is able to retrieve data from the carrier file using the same proposed system. However, the data will be safeguarded without disclosing the contents to the intruder.

To ensure data security, the system has integrated multi layer security that will be strongly protected from intruder and unauthorized access. During the sending session system will be converted every secret file to encoded file and then converted it into encryption file using symmetric key. Encrypted message file will be merged with the cover file to process embedded file. On the other hand, receiver will extract the embedded file using the symmetric key. The proposed system block diagram is given below in **Fig. 2**.

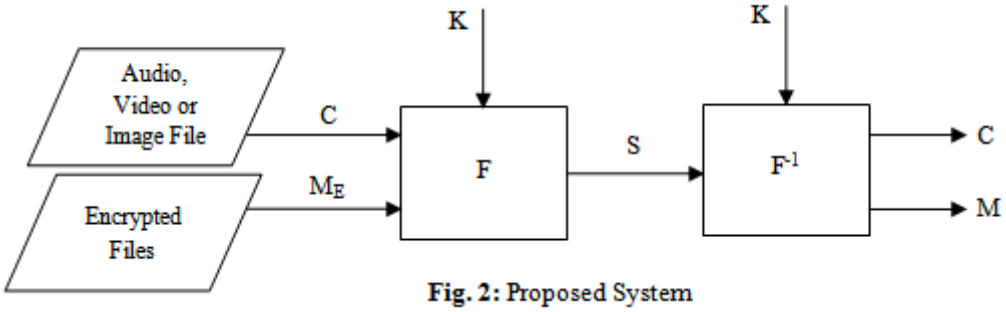

Fig. 2: Proposed System

Major components of the proposed system Steganography are:

- The cover media (C) that will hold the hidden data.
- The secret message (M) may be plain text, cipher text or any type of data.
- Convert the secret message (M) using encryption technique for two level security (M_E).
- Using symmetric key (K) to embedded Cover media with Encrypted data.
- The stego function (F) and its inverse (F^{-1}).
- Stego-key (K) or password may be used to hide and unhide the message after decoding.

II. RELATED WORKS

To implement the secret message during the communication of sender and receiver has been established in various techniques. Steganography is defined as covering writing in Greek. Many researchers' has explored their innovative idea to implement it. The most famous method of traditional steganography technique around 440 B.C. is marking the document with invisible secret ink, like the juice of a lemon to hide information [4], [5].

Another method is to mark selected characters within a document by pinholes and to generate a pattern or signature [6].

Warkentin proposed an algorithm to hide data inside the audio visual files. Secret message will be hidden in a carrier file [7].

On the other hand, El-Emam [8], has proposed an another algorithm to hide a huge amount of data that can be audio, image and text file inside of a color bitmap image where has maintained high security. He has filtered and segmented of image file instead of bits replacement is used on the appropriate pixels. Moreover, another researcher Chen has given concept to hide data inside of image edge portions that is modified method of El-Emam [9].

Rosziati Ibrahim and Teoh Suk Kuan [10] proposed an algorithm to hide message inside image. In the system data has been taken from input box as a text then converted it to binary codes. After converting, binary

code is compressed as a file and then hide inside of Image. This steganography technique is used as an Image Steganography.

III. PROPOSED METHOD

The proposed algorithm is using two layers of security to maintain the privacy, confidentiality and accuracy of the data that is secret type of Steganography. The algorithm is able to hide the data inside the digital data (i.e. image, audio, video) as well as to retrieve the data from the digital data (i.e. image, audio, video). The pictorial representation of the proposed system is given below in **Fig. 3.**

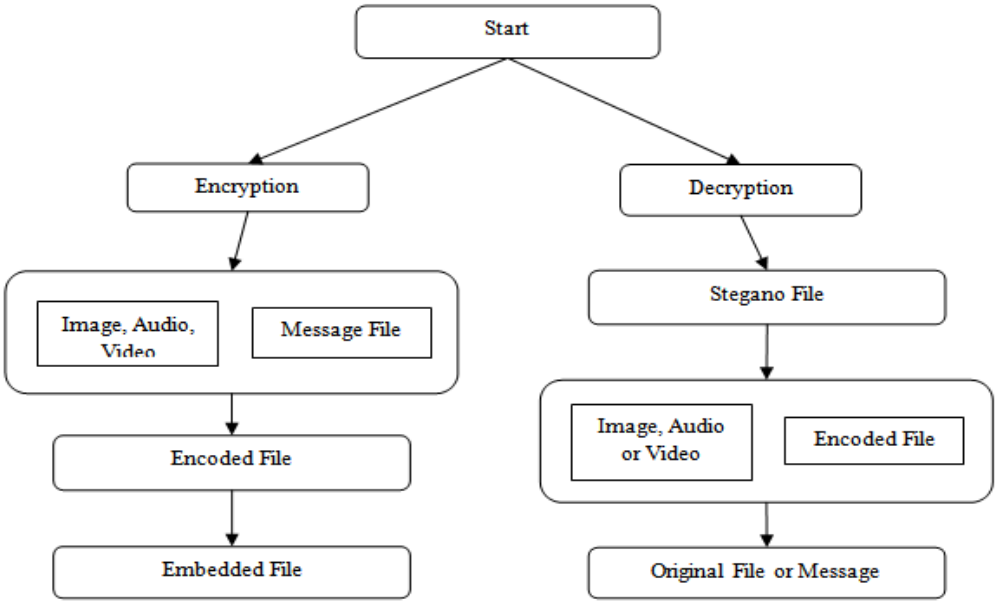

Fig. 3: Pictorial Representation of the Proposed System

3.1 Encryption

The encrypt module is used to hide information into the multimedia files (i.e. image, audio, video etc). No one can see that information or file. This module requires a carrier file and message or secret file then system will automatically generated a Stegano File which is called embedded file. Algorithm of embedding data is given below. Its flowchart is also shown in **Fig. 4**.

Begin

Input:

Cover_File (i.e. Image, Audio, Video etc)
Secret_Message File (Any Kind of file)
Secret_Key (Symmetric Key)

Conversion:

Encoded of Secret_Message
Encryption of Encoded file with secret key
Embedded Compressed File with the Cover_File to create Stego_File

Output: Stego_File

End

***Flowchart of Encryption Process*:**

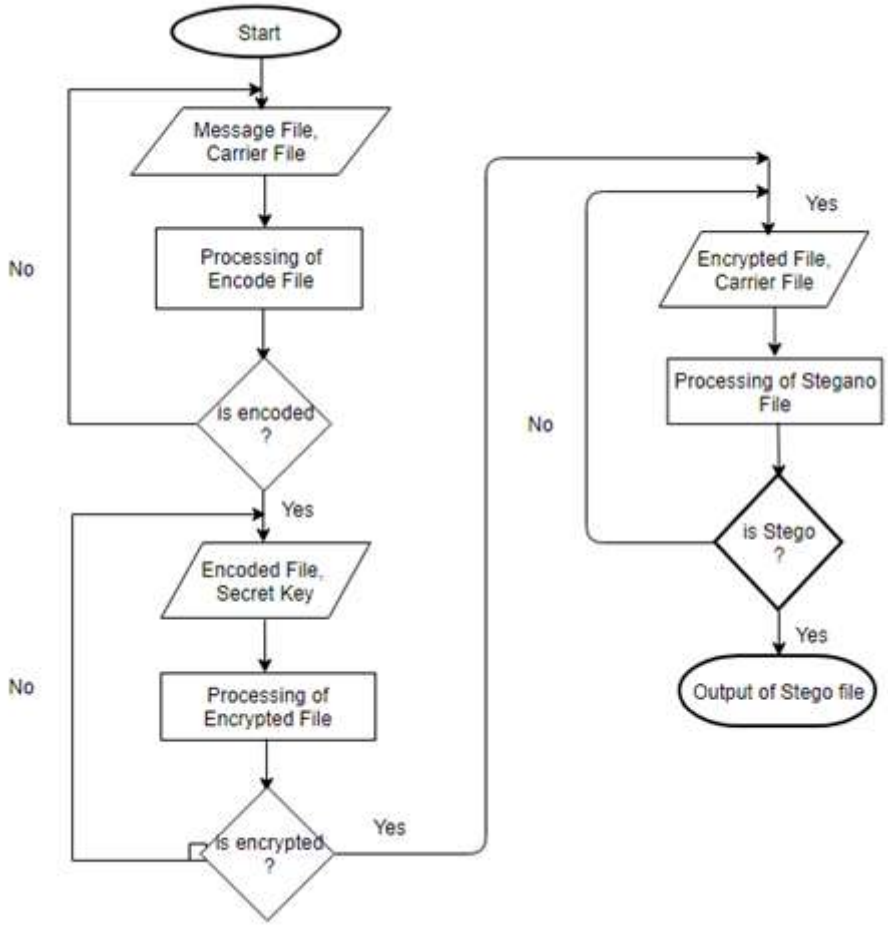

Fig. 4: Flowchart of Proposed Encryption Process

3.2 Decryption

The decrypt module is used to get the hidden information in an embedded Stegano file. It will be extracted the embedded file with the valid symmetric key where carrier and encoded message file both will be separated. Algorithm of getting original message is given below. Its flowchart is also shown in **Fig. 5**.

Begin

Input:

Stego_File
Secret_Key

Conversion:

Extract Stego_File with compare secret_key
Decrypt Secret_Message File

Output: Secret_Message

End

***Flowchart of Decryption Process*:**

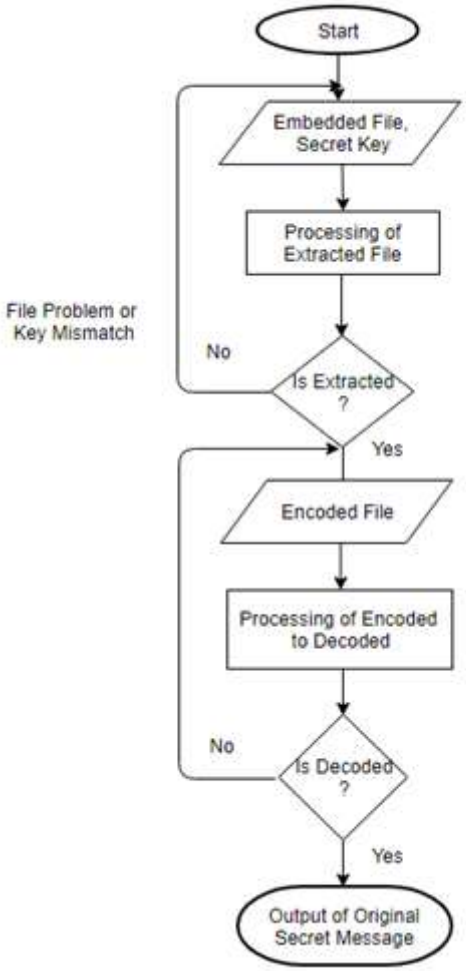

Fig. 5: Flowchart of Proposed Decryption Process

Using the system, secret message will be concealed inside the digital data (i.e. image, audio, video) with almost zero distortion. During the process of embedding the message inside the carrier file, a secret symmetric key is required for the purpose of retrieving the original secret message back or extract or separate from the Stegano file.

The secret message that has been encoded using the system, and then encrypt with the symmetric key into the zip file. The purpose of zipping the file that is more secured and the contents in the zipped file will significantly hard to be detected and read. The secret key in this proposed Steganography algorithm is playing an essential role where the key is acts as locker that used to lock or unlock the secret the message.

IV. SYSTEM IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed system has been implemented using Linux Shell Programming which is more efficient, flexible and secured. Only root user can assign role to enhance its security. By default it has access permission given to root user, other user will be rejected if no permission exists. The system has been tested using various file types with different carrier files. It has two part "Encryption" and "Decryption" that appear in the following **Fig. 6**.

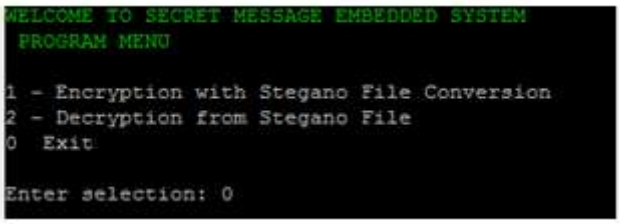

Fig. 6: Start Application

For encryption, select **option 1** that will ask for secret message, carrier file and secret key. Moreover, it has another optional parameter after generating embedded file to send another internal server that has shown in the following **Fig. 7**.

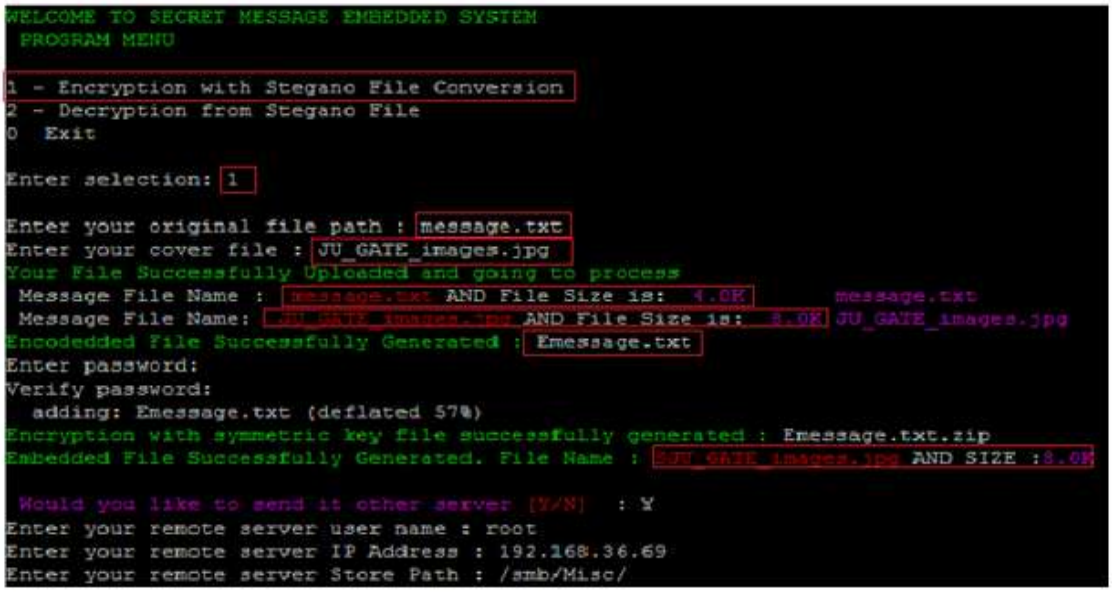

Fig. 7: Encryption Process

Fig. 7 shows the encryption process of original text file (***message.txt***) with image carrier file (***JU_GATE_images.jpg***). However, the system is not fixed only for Image Steganography, it also supports other Steganography techniques for carrier Audio and Video. Secret message (***message.txt***), carrier image (***JU_GATE_images.jpg***) and stego image are shown in **Fig. 8**.

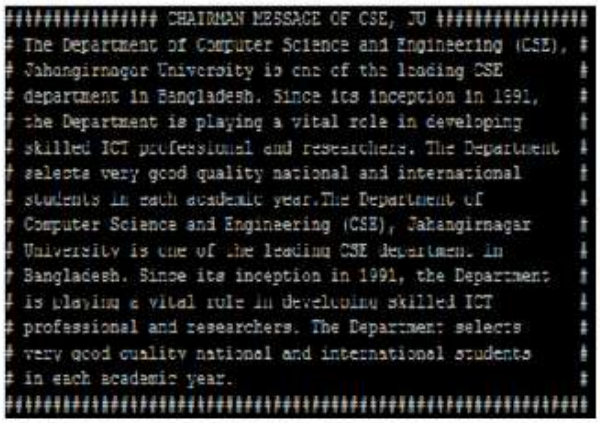

Fig. 8 (a): Secret message (***message.txt***)

Fig. 8 (b): Carrier image (***JU_GATE_images.jpg***)

Fig. 8 (c): Stego image

Another module is decryption process that asks to put Stego file. The pictorial representation of decryption process is shown in **Fig. 9**.

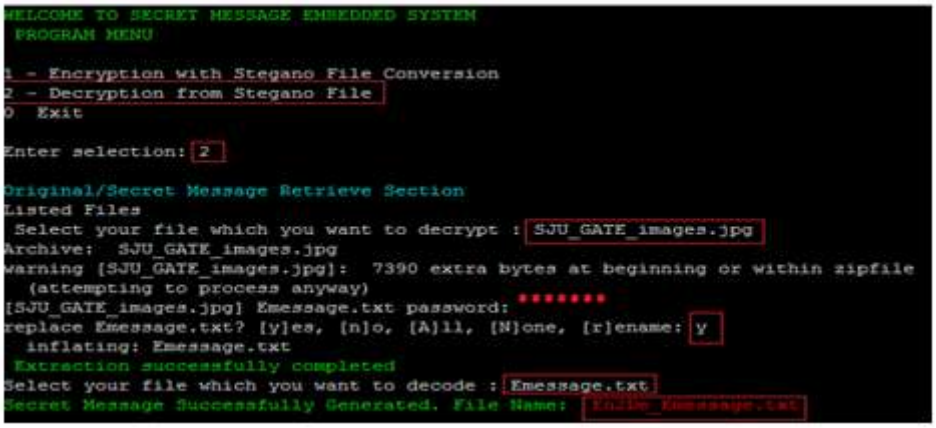

Fig. 9: Decryption Process

After performing the decryption, it separates two files (*Cover file* and *Secret Message file*). It is mentioned that, symmetric secret key must be required to perform decryption process.

Table 1 shows the output of the proposed technique for different sizes and types of files used by Steganography algorithm.

Table 1: Comparison of different size files from sender to receiver.

Cover Image	Cover Type	Message Size	Message Type	Encrypted File	Stego Image	Hide Message	Retrieve Message
11 MB	Video	28KB	JPEG	20 KB	11 MB	OK	OK
8 KB	JPEG	4 KB	Text	4 KB	8 KB	OK	OK
20K	JPEG	40K	Doc	28 KB	48 KB	OK	OK

Table 2 shows comparative study between existing system and proposed system for different parameters.

Existing System	**Proposed System**
1. Depends on OS.	1. Virtually it can be managed from any OS platform using putty
2. Developed using various softwares.	2. Developed using Linux default package and Bash Programming
3. Existing system used third party software to develop the system	3. There is no software installation required (using only default package)
4. Most of the existing system has been developed for individual specific carrier.	4. Developed for general purpose (i.e. Image, Audio, Video Steganography)
5. Developed on different OS	5. Developed on Linux platform which is most secure.
6. Single layer or double layer security	6. Two level security maintained.
7. Configuration has some dependency.	7. Configuration is more flexible and smooth.

V. CONCLUSION

This work has proposed a new algorithm on Steganography to hide secret data inside a cover file. It finds that the embedded or Stego file doesn't have a salient distortion on it. The system has been tested using the PSNR value. Based on the PSNR value of each images, the stego image has a higher PSNR value. Hence, the proposed technique is more efficient to hide the data inside an image or audio or video file. The system has maintained privacy, confidentiality and accuracy of the data.

REFERENCES

[1]. Kahate, A., "Cryptography and Network Security", 2nd Edition, Tata McGraw-Hill, 2008.
[2]. Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications, pp. 1-11.
[3]. Khare, P., Singh, J. and Tiwari, M., "Digital Image Steganography", Journal of Engineering Research and Studies, Vol. II, Issue III, pp. 101-104, 2011, ISSN: 0976-7916.
[4]. Rabah, K., "Steganography – The Art of Hiding Data", Information Technology Journal, Vol.3, no.3, 2004, pp. 245-269.
[5]. Curran, K. and Bailey, K., "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2.
[6]. Laskar, S.A. and Hemachandran, K., "An Analysis of Steganography and Steganalysis Techniques", Assam University Journal of Science and Technology, Vol.9, No.II, 2012, pp.83-103, ISSN: 0975-2773.
[7]. M. Warkentin, M.B. Schmidt, E. Bekering, Steganography and steganalysis, Premier reference Source-Intellectual Property Protection for Multimedia Informaiton technology, Chapter XIX, 2008, pp. 374-380.
[8]. N.N. El-Emam, Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.
[9]. P.Y. Chen, W.E. Wu, A modified side match scheme for image steganography, International Journal of Applied Science & Engineering 7 (2009) 53-60.
[10]. Rosziati Ibrahim, Teo Suk Kuan, Steganography Algorithm to Hide Secret Message inside an Image, Computer Technology and Application 2 (2011) 102-108.

H. M. Shah Paran Ali" A New Approach to Embed Confidential Data within Color Images" International Journal of Engineering Science Invention (IJESI), vol. 08, no. 01, 2019, pp 14-21