IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007198|

Secured Communication through the Application of Steganography

Ashwini R. Patil[1], Prof. S. S. Mhaske [2], Dr. C. M. Jadhao [3]

P.G. Student, Dept of Electronics &Telecomm. Engg.,MGI-COET, Shegaon, Maharashtra, India[1]

HOD &Assistant Professor, Dept. of Electronics &Telecomm. Engg., MGI-COET, Shegaon, Maharashtra, India[2]

Principal & Professor, MGI-COET, Shegaon, Maharashtra, India[3]

ABSTRACT:Developments in the technology brings the convenience and comfort in all fields. In communication field alsoit offers lots of choices for modes through which the information can be transferred. During the transfer of confidential data, the important aspect which is of great concern is the security of the data. Data scrambling and data hiding have come into the attention because of simplicity in implementation it offers. A combination of both would suffice for the intended requirements with security being primary, amount of data that can be embedded as a secondary issue. Hiding the data by embedding it into another file format while hiding the traces of existence of the message is the process of Steganography. This paper presents a methodology for providing security in the communication by hiding the information in the JPEG, PNG or Bitmap images. The system uses Least Significant Algorithm that modifies the pixel values of images according to the information to be hidden into the image. This technique creates the object at the sender side which is transmitted over the network. At the receiver end, the information is extracted using the same algorithm which is used at the side of sender.

KEYWORDS:Steganography, Cryptography, Microdots, Least Significant Bit,Python, Stego object.

I. INTRODUCTION

Advancement in the communication technology throughout the time makes the confidentiality an important aspect. Incommunication whether it is carved in stone, written on paper or sent over the Internet, correspondence between sender and receiver is exposed to interfering or eavesdropping. Therefore, it becomes necessary to provide a mechanism that protects the sent information. One of the most commonly used methods of securing transmitted data is cryptography.

The purpose of cryptography is to cover plaintext in such a way that it becomes unreadable. The resulted text after encryption called cyphertext can then be safely transmitted to the destination. Knowing the algorithm used for encryption, only the receiver will be able to get the original message. In cryptography, no matter how powerful the encryption algorithm is, encrypted data will always create suspicion. This is where steganography can help.

Steganography is the science and art of communicating in a way thatconceals the existence of messages in the communication. Although cryptography and steganography are considered to be the same, they are essentially different. The cryptography technique scrambles a message so that it cannot be understand whereas the steganography hides the message so that it becomes invisible. Thus, application of the steganography technique can provide a way to make the communication secured.

II. LITERATURE SURVEY

Steganography is derived from the Greek steganos (covered or secret) and graphy (writing or drawing). Steganography can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds. Steganography is actually an ancient practice used for the communication in the various way like shaving and tattooing, writing messages on wood and covered it with wax, use of invisible ink, Microdots and null ciphers.

In digital communication, this concept of data hiding is used by many researchers in their work by applying different techniques for providing security. Some of the researches are discussed in this section.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007198|

SteganoCNN: Image Steganography with Generalization Ability Based on Convolutional Neural Network, et al. [1] proposes a Steganography Convolution Neural Network (SteganoCNN) model which embeds two images in a carrier image and that reconstruct two secret images. Hiding data in images using cryptography and deep neural network, et al. [2] propounds a method where an encryption layer added provides an additional layer of security with deep neural networks. K. Arun Kumar, et al. [3] gives the detail analysis of data hiding using image encryption based on image. But due its visibility problems it is possible to tamper some sensitive data by the simple attacks, detection disabling and ambiguity attacks or removal attacks. Hence there is need of some constructive, robust secured method of data hiding in encryption.Habiba Sultana, et al [4] has presented a comprehensive survey of steganography and its classification. In this paper, the classification of steganography techniques is given based on the various aspects, carrier file and key used. Kevin Curran in their article, et al. [5] proposes an eventual design in which the application logic and validation occur within the base classes (controllers) and the data is provided within the embedded database system.

III. METHODOLOGY

This project presents a system that uses Graphical User Interface (GUI) to provide the interface for the user to access the system. The system implementation is based on the Python programming language. The system checks the authentication of the user accessing the system using login credentials. The operation of system has mainly two functions concealing and revealing. The proposed model conceals the confidential message in an image format so that it is difficult for the intruder to suspect the presence of the message inside the image.

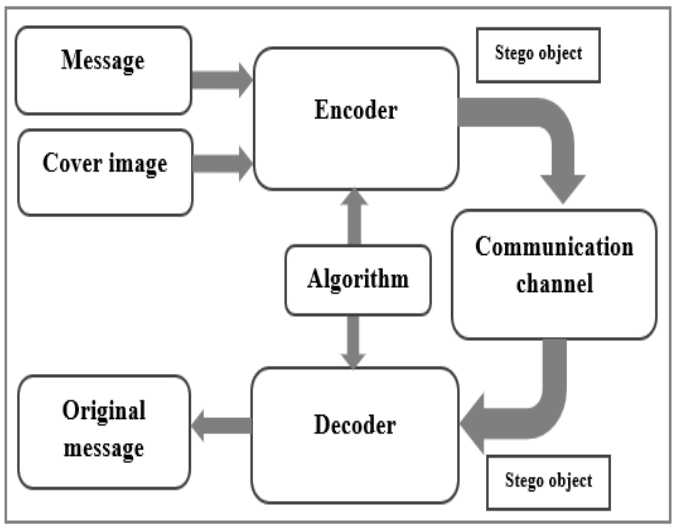


Fig. 1. Block diagram of proposed model

As shown in the fig.1, the secret message to be hidden and the cover image are applied as input to the encoder i.e., steganographic encoder. The encoder will use Least Significant Bit (LSB) algorithm to embed the message into the cover image. The encoder will generate the Stego objectwhich consist of the message embedded into the cover image.This stego image is thensent over the communication channel to the intended receiver.

On receiving the message at the receiver end, the decoder i.e.steganographic decoder will use the same algorithm to extract the message from the stego object. The receiver is having the information of the exact algorithm and technique hence can correctly decode the message concealed into the image. The extraction of the original message embedded into the image will be carried out by the decoder. Thus at the output of decoder, the original message will be generated. Only the receiver having the knowledge of technique used at the transmitter end can successfully reveal the information from the received stego image at the receiver side. Hence, the system provides security in the communication. The cover image and the generated stego image can be JPEG, PNG or Bitmap file format depending on the type of image selected by the user.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007198|

IV. EXPERIMENTAL RESULTS

The implemented system can conceal the secret message in one of the image file formats like JPG, PNG or Bitmap. After embedding the message into the image, it will generate the new file called as stego object in the same file format. In this section, the output of the implemented system is discussed.

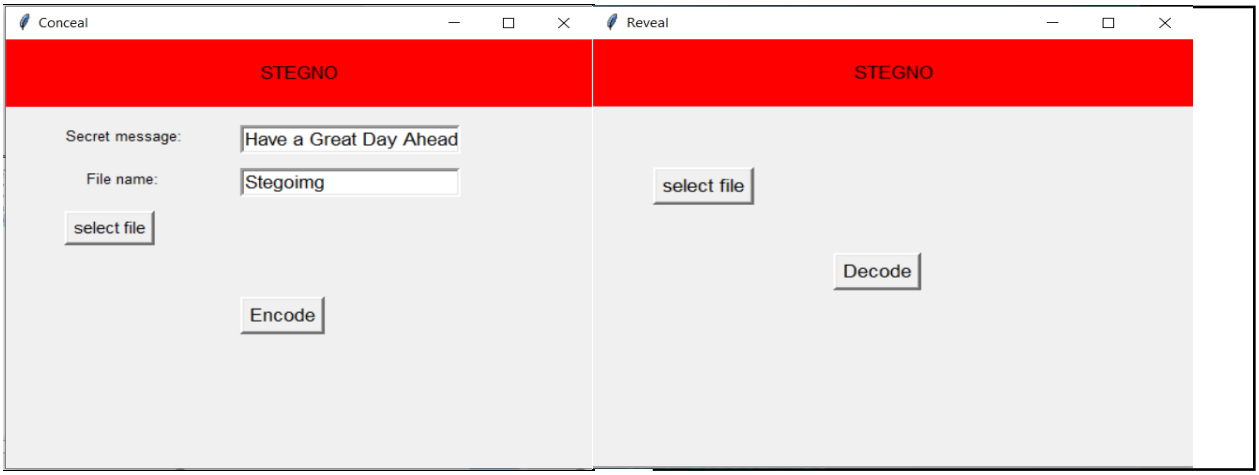
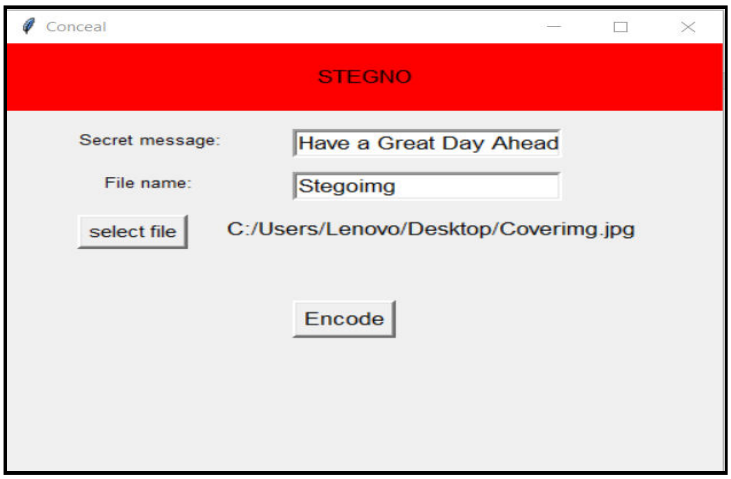


Fig.2. (a) GUI for conceal function(Encoding) Fig.2. (b) GUI for reveal function (Decoding)

The graphical user interface for conceal and reveal function is as shown in fig. 2. (a) and (b) respectively. The secret message and cover image are selected using the GUI window as shown in the fig. 3 (a). The appearance of selected JPG cover image and resulted stego image is shown in fig. 3. (b) and (c) respectively.



(a)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

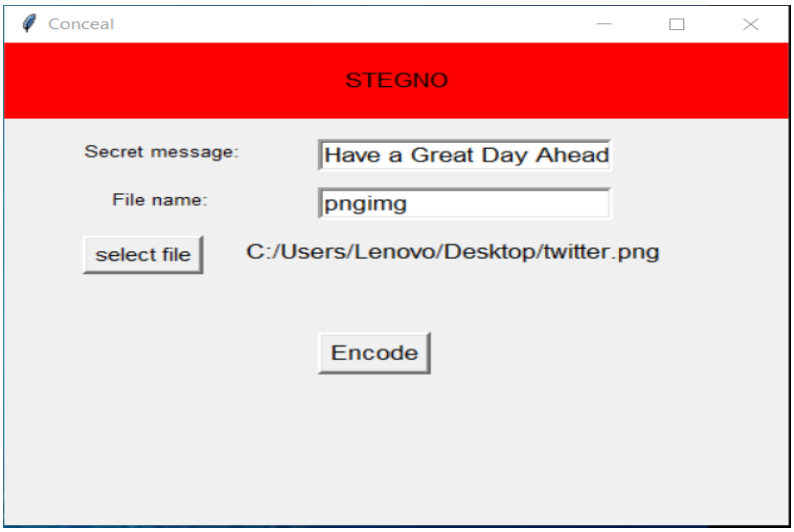
| DOI:10.15680/IJIRSET.2021.1007198|

(b)

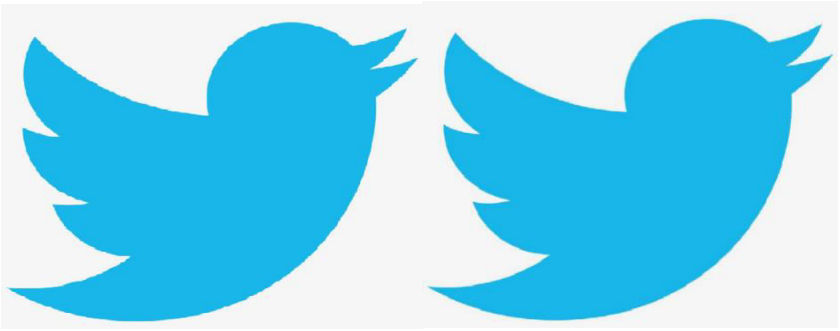
(c)

Fig. 3. Case 1:JPEG image (a) Secret message & selection of jpg image in conceal function (b) selected jpg cover image (Coverimg.jpg) (c) jpg stego image (Stegoimg.jpg)

The secret message and PNG cover image are selected using the GUI window as shown in the fig. 4 (a). The appearance of selected PNG cover image and resulted stego image is shown in fig. 4. (b) and (c) respectively.



(a)



(b) (c)

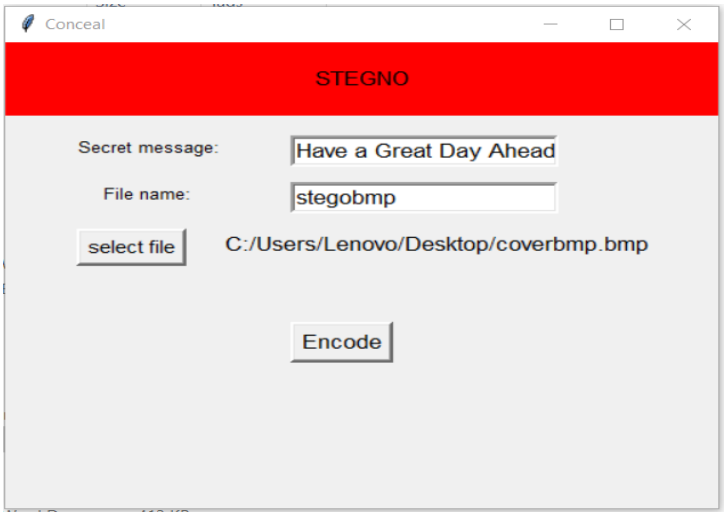
Fig. 4. Case 2:PNG image (a) Secret message & selection of png image in conceal function (b) selected png cover image (twitter.png) (c) png stego image (pngimg.png)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007198|

The secret message and BMP cover image are selected using the GUI window as shown in the fig. 5 (a). The appearance of selected BNP cover image and resulted stego image is shown in fig. 5. (b) and (c) respectively.



(a)

(b) (c)

Fig. 5. Case 3:BMP image (a) Secret message and selection of bmp image in conceal function (b) selected bmp cover image (coverbmp.bmp) (c) bmp stego image (stegobmp.bmp)

The message “Have a Great Day Ahead” is embedded in three image file formats as shown in above figures. It is observed thatfor same message if the selection of type of cover image changes, the percentage change in the size of the resulted stego image compared to original cover image changes. Table 1. given below shows the variation in the sizes of stego image compared to that of cover image for the same size of message embedded into it.

Table1. Effect of selection of file format

Sr. No.	File format	Size of Image		Percentage change in the image size
		Cover Image	Stego Image	
1	JPEG	179KB	208KB	+16.20%
2	PNG	57.9KB	20KB	-65.45%
3	Bitmap	2.13MB	2.13MB	No change

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007198|

V. CONCLUSION

The main goal of this project is to provide the security in the communication through the application of Steganography technique. Implementing the project using Python programming language gives the outputs from which it is observed that through LSB Substitution method, the results obtained in data hiding are pretty impressive as it utilizes the simple fact that any image consist of pixel values and the modifications in the LSB bits of the pixels doesn't makes the huge change in the appearance of the image. Also, on comparing various researches, it is found that the Least Significant Bit Algorithm is advantageous in imperceptibility, payload capacity and complexity. This technique is useful for colour as well as gray scale images. This technique can be used for JPEG, PNG or bitmap images. From the resulted images, it is observed that there is no change in the selected bitmap cover and stego image. The percentage change in the size of cover image and stego image for JPEG image is less compared to the PNG image. The appearance of resulted image doesn't give the traces of message embedded into the image. Thus, the method provides security through the application of steganography technique.

REFERENCES

[1] Xintao Duan, Nao Liu, Mengxiao Gou, Wenxin Wang and Chuan Qin, "SteganoCNN: Image Steganography with Generalization Ability Based on Convolutional Neural Network", Entropy 2020, 22, 1140; doi:10.3390/e22101140.

[2] Kartik Sharma, Ashutosh Aggarwal, Tanay Singhania, Deepak Gupta, Ashish Khanna, "Hiding Data in Images Using Cryptography and Deep Neural Network" Journal of Artificial Intelligence and Systems, 2019, 1, 143-162 AIS ISSN Online: 2642-2859.

[3] K. Arun Kumar & S.M. Riyazoddin, "Analysis of Data Hiding Techniques in Encrypted Images - A Survey" Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4, (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

[4] Habiba Sultana, "A study on steganography and steganalysis", International Journal of Scientific & Engineering Research, Volume 9, Issue 12, December-2018 ISSN 2229-5518.

[5] Kevin Curran, "Text based steganography" International Journal of Information Privacy Security and Integrity, January 2017 DOI: 10.1504/ IJIPSI.2017.088700.

[6] Namrata Singh, "High PSNR based Image Steganography", International Journal of Advanced Engineering Research and Science (IJAERS), Vol-6, Issue-1, Jan- 2019 https://dx.doi.org/10.22161/ijaers.6.1.15 ISSN: 2349-6495(P) | 2456-1908(O).

[7] Pengfei Xue, Hanlin Liu, Jingsong Hu, Ronggui Hu, "A multi-layer steganographic method based on audio time domain segmented and network steganography" AIP Conference Proceedings 1967, 020046 (2018); https://doi.org/10.1063/1.5039018 Published Online: 23 May 2018.

[8] G. Kalaiarasi, A. S. Narmadha, J. Nandhini, "Encryption And Decryption Of Data Hiding In Audio Signal Using LSB Algorithm", International Journal of Advanced Research and Publications ISSN: 2456-9992, Volume 1 Issue 4, Oct 2017.

[9] Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth, "Review Paper on Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016 ISSN: 2277 128X.

[10] Huseyin Bilal Macit, Arif Koyun, Orhan Gungor, "A Review And Comparison Of Steganography Techniques", https://www.researchgate.net/publication/330162221· Conference: INES 2018 , Antalya, Turkey.

[11] C. P. Sumathi, T. Santanam and G. Umamaheswari," A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[12] Niels Provos, and Peter Honeyman. "Hide and Seek: An Introduction to Steganography" IEEE Security & Privacy Magazine, May-June 2013.

[13] Bharat Sinha, "Comparison of PNG & JPEG Format for LSB Steganography", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 ,2013.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details