LAUTECH Journal of Engineering and Technology 16 (2) 2022: 54-63

FILE ENCRYPTION AND HASH SYSTEM USING JAVA PROGRAMMING LANGUAGE FOR IMAGE STEGANOGRAPHY

***[1]Adejumobi, O. K., [2]Ayeni, M. O., [3]Adeyeye, A.H., and [3]Ogundeji, O.A.**

[1]Computer Engineering Department, The Polytechnic, Ibadan, Oyo State
[2]Electrical Engineering Department, The Polytechnic, Ibadan, Oyo State
[3]Electrical Engineering Department, Adeseun Ogundoyin Polytechnic, Eruwa, Oyo State
*kolastar@yahoo.com,+2348055136497

ABSTRACT

Due to the rapid development and rapid popularization of the information technology, internet and digital media have become an important tool for military, commercial, individuals and many other organizations to obtain and transmit information. However, digital communication via the Internet is vulnerable to eavesdropping, malicious interference and other activities. As a result, data transmission protection and information security issues become a bottleneck than ever before. This paper presents file encryption and Hash system (Image Steganography) via Least Significant Bit (LSB) approachto increase the amount of text file the cover image can conceal. The software used consists of two sections: the Encode section (embedded text file by using an image as cover) and the Decode section (extract the embedded text from the cover image) which is implemented through NetBeans IDE using Java Programming Language.The different results obtained when the proposed device was tested revealed that it worked according to the design specifications.

Keywords: *Information security, Data encryption, Image steganography, Least Significant Bit.*

INTRODUCTION

Cryptography and steganography are one of the research fields in information security that had been around for several years. However, these technologies is aimed at protecting data confidentiality and information security. Cryptography involves protection of data transmission by encrypting data before being sent or shared to third party without hiding the encrypted data, which may leads to the interception of the data. Steganography, is the practice of hiding information in the audio, text, image or video, this method ensures that data protection is well managed.In digital image setganographic, confidentiality of data can be concealed in the appropriate cover image(Pascal M. et al (2019).

A number of related studies have proposed different approach, due to the high degree of redundancy encountered in digital image, several steganographic methods that hides data in digital image are presented in the literature review.A gray-valued cover image using a new and effective steganographic technique was proposed by Da-Chun W. et al (2003) to hide message. In this research, a cover image is divided into non-overlapping blocks of two consecutive pixels in order to embed a secret message. The two pixels in each block's value are used to calculate the difference and each conceivable difference value falls into one of several categories. Based on the features of human vision's sensitivity to changes in gray-value, from smoothness to contrast, the range intervals were chosen. The value of a sub-stream of the secret message is then embedded by replacing the difference value with a new value. The breadth of the range to which the difference value corresponds determines how many bits can be

stored in a pair of pixels. In conclusion, the modification is never outside of the range interval.

Hemalatha, S. et. al (2013) presented a novel image steganography method that uses discrete wavelet transforms (DWT) and integer wavelet transforms (IWR) to conceal both the image and the key in a colour cover image. The cover image and the stego image are identical on the surface. The retrieved image and the hidden image are comparable,the high Peak Signal to Noise Ratio(PSNR) values for both the recovered secret image and the stego serve as evidence for this. The results are contrasted with those of comparable procedures, the proposed technique is more straightforward and produces higher PSNR values than others.

An overview of popular Steganography techniques was given in the work of Abbas, C. et al (2008). This approach identifiesgaps in the current research in this field and explores how his own research methodology might address some of these gaps. The authors suggested forming an adaptive environment for an edge operator utilizing human skin tone recognition in colour photos, which will offer a great secure site for data hiding.

Masoud, A. etal (2010) proposedAdaptive More Surrounding Pixels Using(A-MSPU) method. Majority of steganographic proposed by these authors are not used, only three or four adjacent pixels around a target pixel are used.However, the suggested methodology can use up to eight nearby neighbours, increasing the imperceptibility value. The research proves that discovering the best capacity value brings about an improvement in terms of imperceptibility.

In this work, Data Encryption and Hash system (Image Steganography) via Least Significant Bit (LSB) approach is proposed to increase the amount of text file the cover image can conceal. The software consists of two sections; the Encode section (embedded text file by using an image as cover) and the Decode section (extract the embedded text from the cover image) which is implemented through the NetBeans IDE using Java Programming Language. The results obtained revealed that the proposed methodeffectively hides message viaLSB and was able to retrieve message. This method would also generatea passkey automatically toincrease the amount of data the cover image can conceal.

Methodology

A friendly graphical user interface that hides and retrieve same message effectively via LSB approach has two operations/processes: the Encode process and the Decode process is presented in the flow chart in Fig. 1.

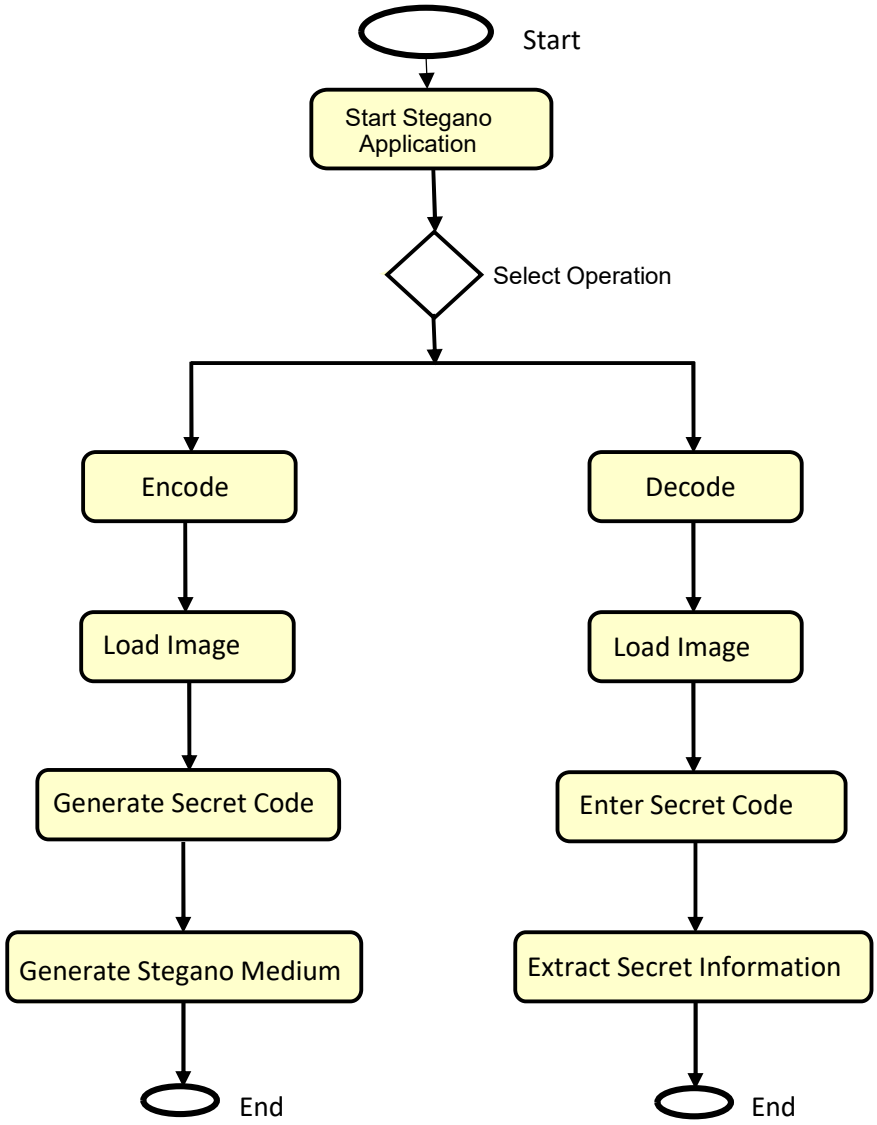


Fig 1: Flow Chart of the Development of File Encryption and Hash System

Encode Process

The object of Buffered Image uses ImageIO.read method, the original image and the text file are taken as input (with the aid of Text Area provided in the encode module) and separated into a stream of bytes. Each bit of these bytes is encoded in LSB of the next pixel. The final image that contains the encoded message is achieved and it is saved at the specified path given by the user in PNG format using ImageIO.write method.

This completes the encoding process as shown in Fig 2.More so, user space is created for preserving the original file, so that all the modifications are done in the user space.

Fig 2: Encode Module

Decode Process

The User space created consists of the following buttons; Open Button (jButtonOpen), Decode Button (jButtonDecode), Save Button and Reset Button (jButtonReset). Using ImageIO.read, the carrier file (image) is taken, by using Byte class the image is taken into byte Aray which is then converted into String (text) and the output is displayed with the aid of Text Area (TA) provided in the decode module as shown in Fig 3.

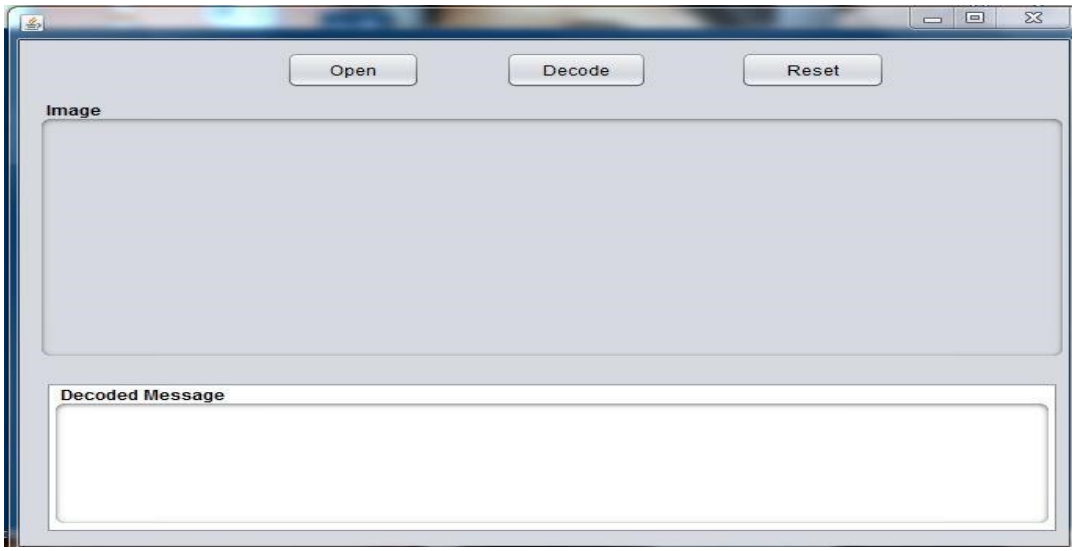


Fig 3: Decode Module

Least Significant Bit (LSB)

Each pixel typically has three numbers associated with it, one each for red, green, and blue intensities, and these values often range from 0-255. In order to hide the message, data is first converted into byte format and stored in a byte array. The message is then hidden by replacing each pixel least significant bit of the image with the bits of the messages to be hidden as presented in Fig. 4.

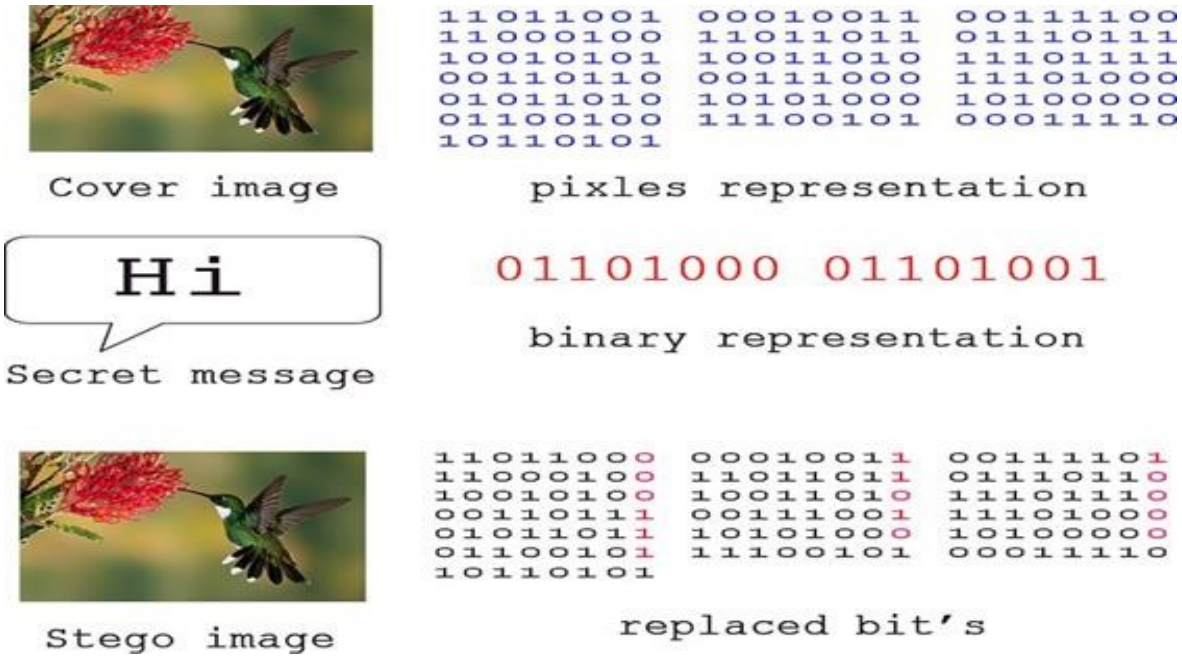


Fig. 4:LSB Operation

The interface was developed using Netbean IDE which is an integrated development environment for Java is as shown inFig. 5

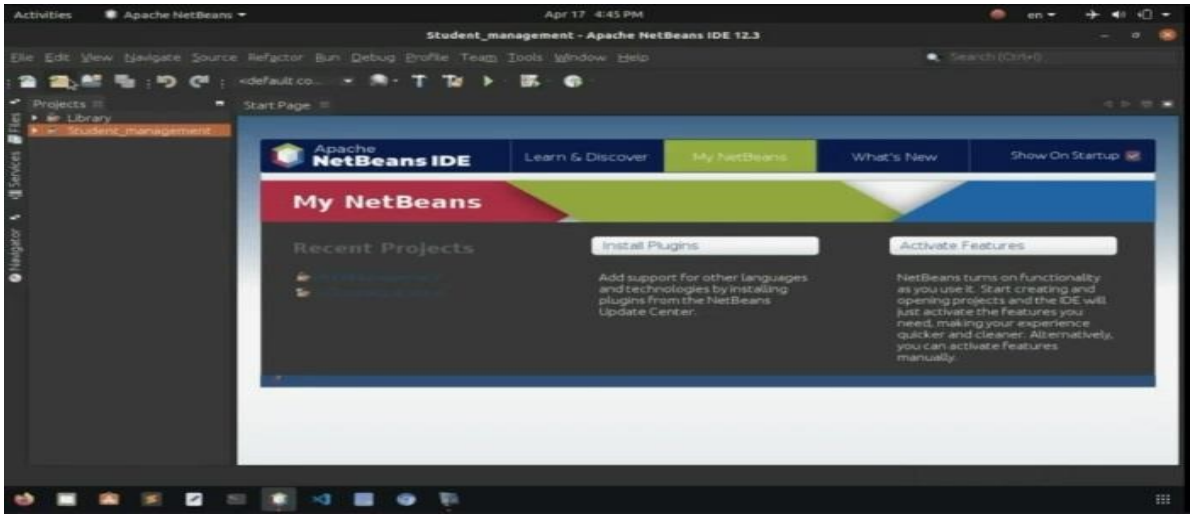


Fig 5: NetBean IDE

Testing

After the development of the software, the system worked as expected by embedding a text using a cover image and the embedded text was extracted in the decode process.

Result

Fig.6 shows the main menu of the developed application.

Fig. 6: Main menu interface

Encode Section: Fig. 7 shows the encode interface of the application.

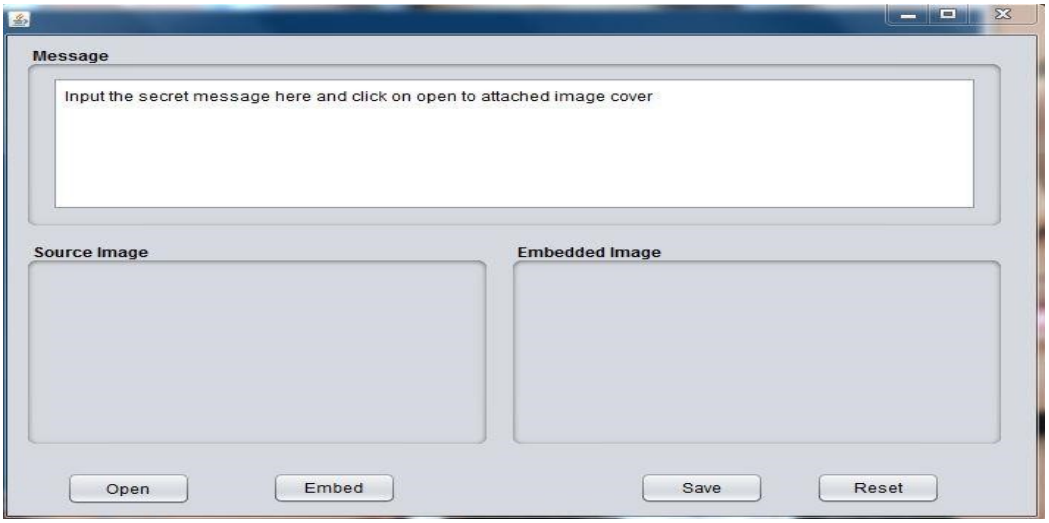


Fig. 7: Encode Section Interface

Open Button

Fig. 8 showsthe open button allowsthe user to selects the cover image that needed to be processed

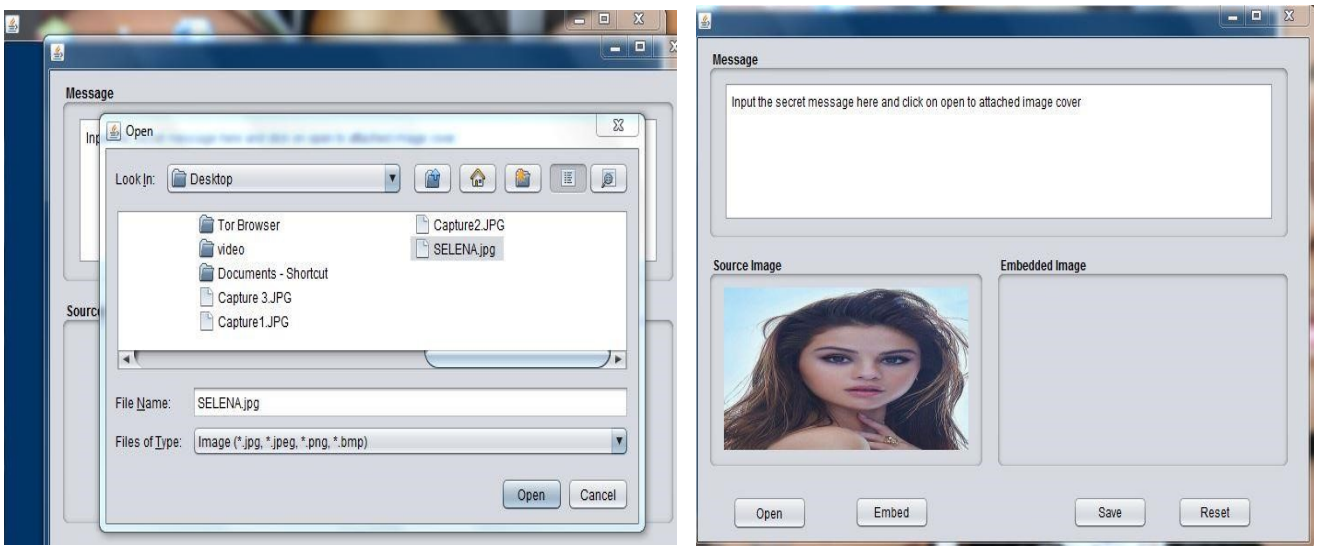
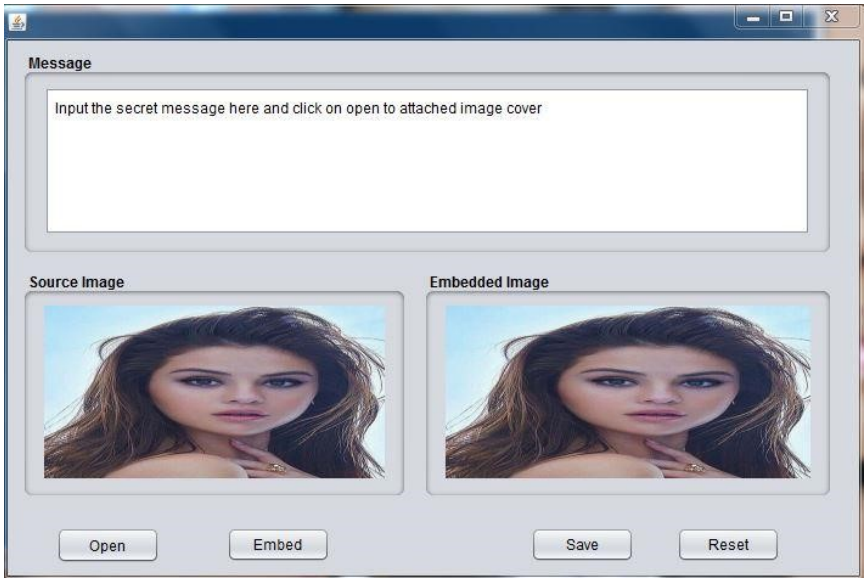


Fig. 8: Open Button interface

Embed Button



The button embedded the text file inside the selected cover image is as shown inFig. 9**.**

Fig. 9: Embed Button Function

Save Button

The button automatically generates a password andsaves the carrier file (image) to the selected path or directory specified by the user as shown in Fig. 10

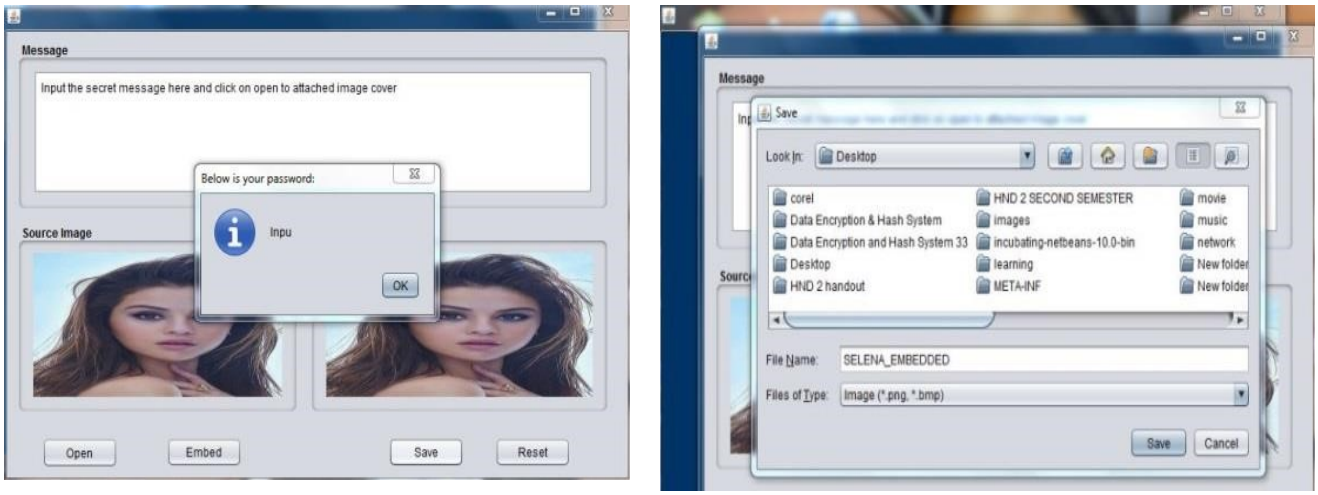


Fig. 10: Automatic Password Generation Dialog box

Decode Section

Fig.11 shows the Decode Section Interface of the application

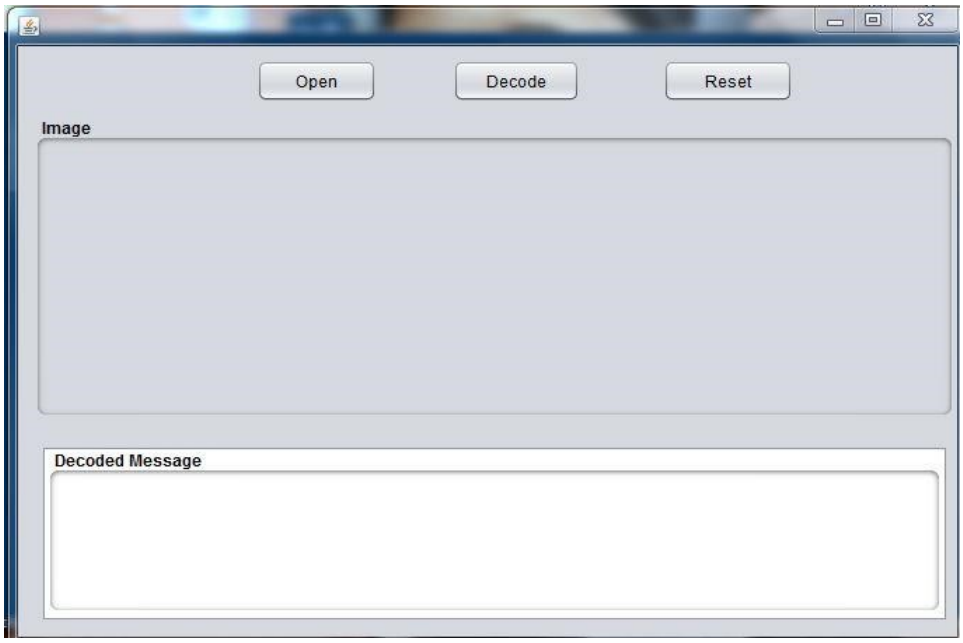


Fig. 11: Decode Section Interface

Open Button

This button is used by user to selects the encrypted file (Image) as shown in Fig 12.

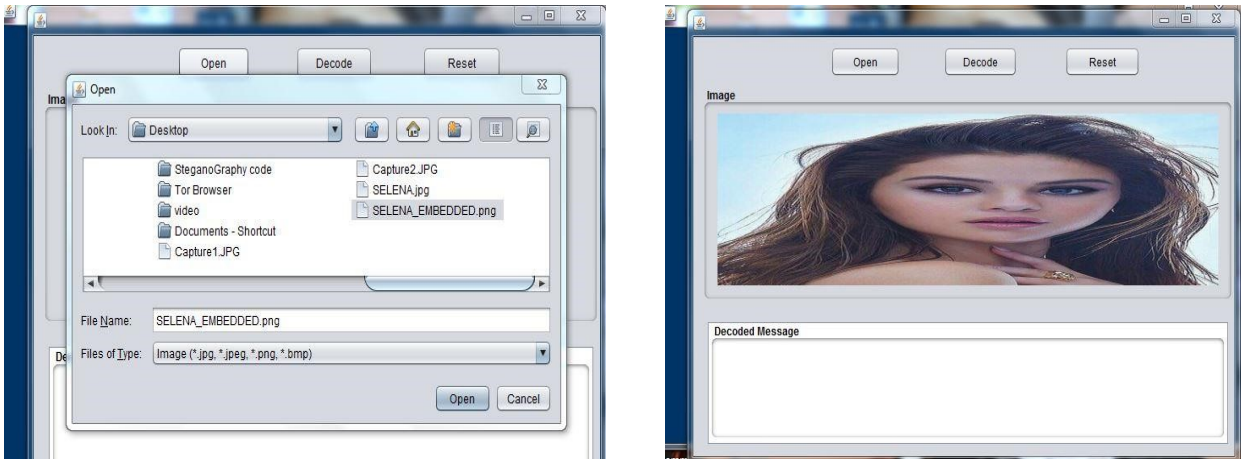


Fig. 12: Open Button Interface

(ii) Decode Button

The button extracts the text file and displays the hidden text on the Text Area field if the user inputs the correct password is shown inFig 13**.**

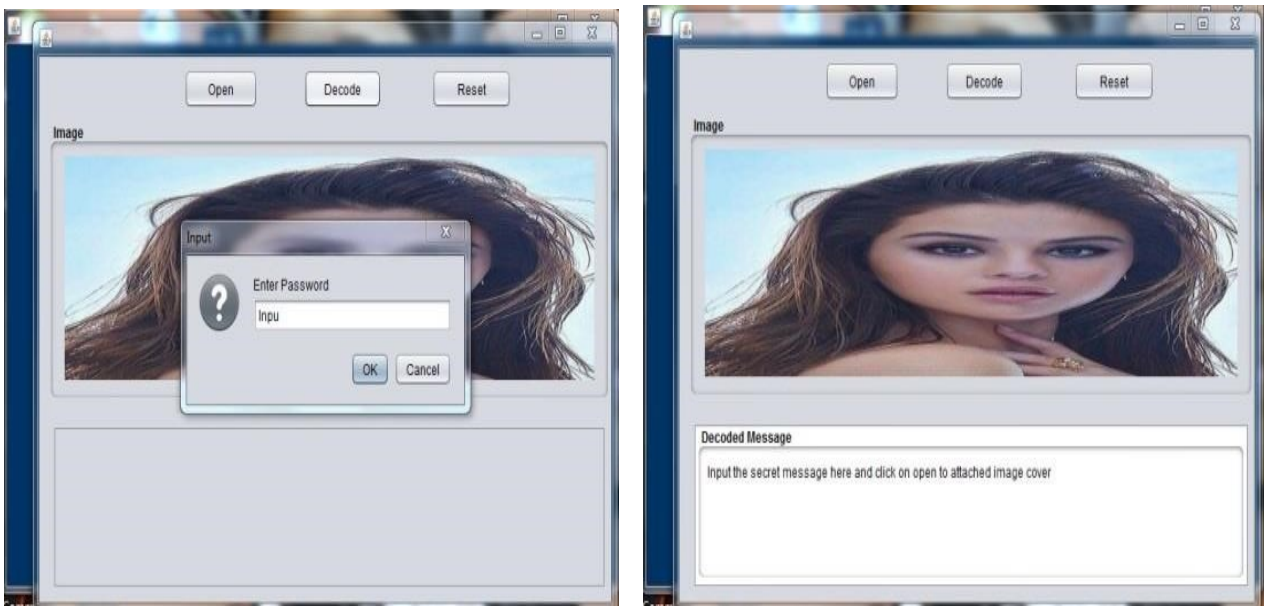


Fig. 13: Password Authentication and Decode Interface

Conclusion

This paper presents new approach to increase the amount of text file that the cover image can conceal through file encryption and Hash system (Image Steganography) via the Least Significant Bit (LSB) approach. The proposed method provides a friendly graphical user interface that effectively hides and retrieves message via LSB approach and automatically generate a passkey thereby increasing the amount of data the cover image can conceal. This model is designed for image cover files which accept only images as a carrier file.

The proposed method is recommended fordata transmission protection and information security issues such as eavesdropping, malicious interference and other cybersecurity activities. Therefore, further research can be extended to

enable it accommodates different types of multimedia files.

REFERENCES

Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt (2008). Biometric Inspired Digital Image Steganography, 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems

Da-Chun Wu and Wen-Hsiang Tsai (2003). A steganographic method for images by pixel-value differencing, ScienceDirect Volume 24, Issues 9–10, June 2003, Pages 1613-1626

Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath (2013). A Secure Color Image Steganography In TransformDomain International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1,March 2013

Masoud Afrakhteh and Subariah Ibrahim (2010). Adaptive steganography scheme using more surrounding pixels | IEEE Conference Publication | IEEE Xplore.International Conference on Computer Design and Applications

Pascal Maniriho and Tohari Ahmad. (2019). Information hiding scheme for digital images using difference expression and modules, Journal of King Saud University- Computer and Information Science, Vol. 31, Issuess 3. Pp 335-347.

Weixuan Tang, Bin Li, Shunquan Tan, Mauro Barni and (2019). CNN-Based Adversarial Embedding for Image Steganography, IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, August 2019