Digital Image Steganography based on Least Significant Bit method

MD. Alamgir Kabir

Abstract—Steganography is the art of concealing the data into the other data in a manner that the concealed data gives off an impression of being nothing to the human eyes. It plays a significant role for effective undercover contact. There are numerous approaches to shroud data inside an image,audio/video, archive and so forth. But Image Steganography has its own particular preferences and is most prevalent among the others.In this paper, an information concealing system that depends on digital image steganography is proposed to secure information exchange between the sender and receiver. Computerized picture with different file formats are utilized for the steganography and an LSB (Least Significant Bit) algorithm is utilized to encode the message inside the picture record. The proposed framework was assessed for viability and the outcome demonstrates that, the encryption and decryption techniques utilized for building up the framework make the security of the proposed framework more effective in securing information from illicit access.

Key Terms: - Steganography, Image Domain, Data Compression, LSB (Least Significant Bit) algorithm, Encryption, Decryption

1.INTRODUCTION

In the course of the most recent decades, the quick advancement of the internet requires secret data that should be shielded from the unapproved clients. This can be accomplished by concealing the data. It is a strategy for concealing mystery messages into a cover medium, so that an unintended spectator won't know about the presence of the shrouded messages. This is accomplished by steganography.

There are several kinds of technique exists that seems so much similar with steganography. These are cryptography, watermarking and fingerprinting. The similitude amongst those techniques is that, all of them are utilized to disguise data. Yet, these systems sounds to be same and give same ultimate objectives, however, these are altogether different in the way they are working [8][10]. However, the distinction is that the steganography does not uncover any suspicious about the shrouded data to the client. Along these lines the aggressors won't attempt to decode data. This paper audits the technique of steganography to shroud the data into computerized picture.

2.STEGANOGRAPHY TYPES

In this paper the fundamental point is to conceal data into the carrier file. The file that contains the implanted data within it, called as stego record. Essentially, we can cover up various sorts of file formats, for example, video, sound, picture and so on.

There are principally two sorts of steganography. They are Fragile and Robust.

2.1FRAGILE

In Fragile steganography, if the record is altered, then the concealed data is pulverized. For instance the data is concealed into the .bmp file format. If the file format is changed into .jpeg or some other format then the concealed data will be obliterated. Delicate steganography procedures have a tendency to be less demanding to execute than strong techniques.

2.2 ROBUST

Robust steganography means to insert data into a document which can't be easily pulverized. Albeit no mark is really indestructible, a framework can be viewed as vigorous if the measure of changes required to evacuate the check would render the file pointless. In this manner the mark ought to be covered up in a part of the file where its expulsion would be effectively seen[13].

3. DATA COMPRESSION

There are several kinds of data compression techniques available in a digital image. Mainly there are two compression techniques used more than any others. The first one is lossless compression and the second one is lossy compression.

In lossy compression it will be done by losing some information specially the redundant bits while compressing. That means after compressing the file few information will be discarded. JPEG (JOINT PHOTOGRAPHIC EXPERTS GROUP) is the image format that follows Lossy Compression [1].

And In lossless information it will never discard the information from the original file even after decompressing. GIF (GRAPHICAL INTERCHANGE FORMAT) and BMP (BIT MAP FILE) are image format that follows Lossless Compression[1].

4.IMAGE STEGANOGRAPHY

Image steganography is characterized into two spaces: Transform Domain (Frequency Domain technique) and Image Domain (Spatial Domain technique).Transform Domain applies image transformation and manipulation of algorithm[1].Image Domain applies bit insertion and noise manipulation of a covered image[5][7]. This paper gives a reviewof Spatial Domain Technique.

4.1IMAGE DOMAIN(Spatial Domain Technique)

4.1.1.LSB (Least Significant Bit)

The Least Significant Bit (LSB) addition technique is the most widely recognized, basic and least demanding strategy for embedding messages in a picture.LSB strategy depends on modifying the excess bits that are the minimum essential with the bits of the secret data. The point of the LSB is to transmit the concealed data to the receiver without knowing to the gatecrasher that the message is being passed.

5. IMPLEMENTATION USING LSB ALGORITHM

5.1 ENCRYPTION TECHNIQUE

When the image data is accessed as a series of bytes. Depending on the image format, a pixel may be represented by one or more bytes [12][13]. In a 24-bit PNG file format which utilized a byte each for the red (R), green (G), and blue (B) channels.

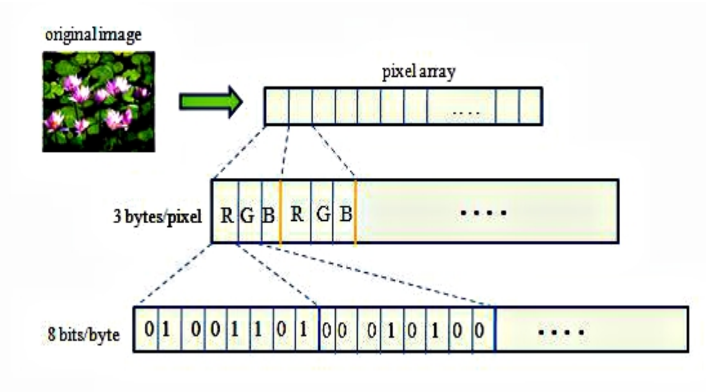


Figure 1. Accessing the Bits of a PNG image.

The next stage is to read in the text file, and access its bits, as shown in Figure2.

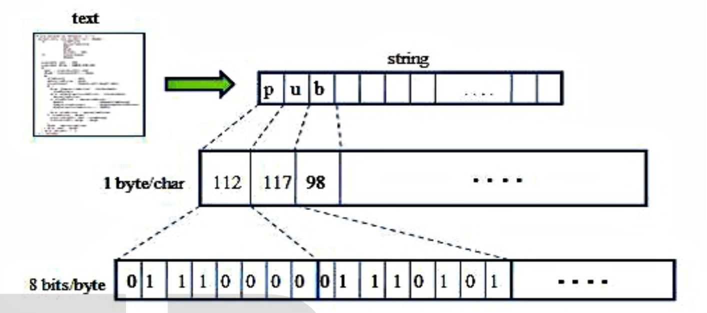


Figure 2. Accessing the Bits of a Text File.

Presently its opportunity to embed the bits of the content record into the picture. The LSB approach just changes the slightest noteworthy piece of every picture byte, as delineated by Figure 3.

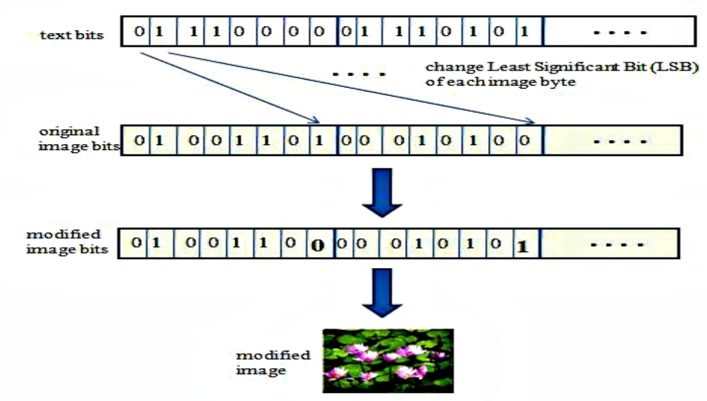


Figure 3. Inserting the Text Bits into the Image.

5.2 DECRYPTION TECHNIQUE

Separating the text from the image at a later time includes replicating the LSBs of the adjusted picture's bytes, and recombining them into bytes in a text document, as in Figure 4.

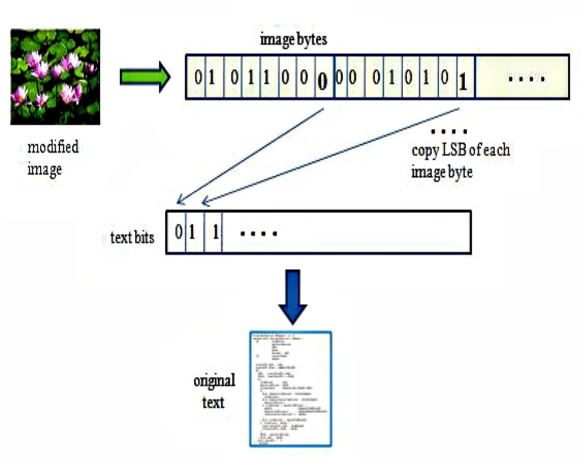


Figure 4. Extracting the Text from the Modified Image.

6. STEGANALYSIS

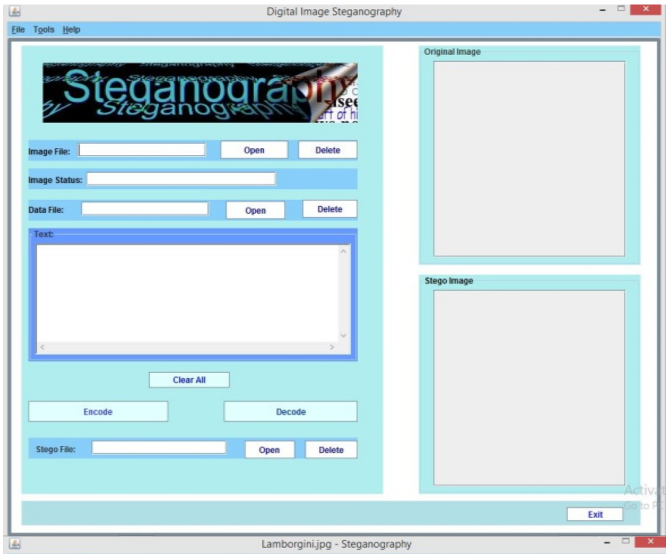
Steganalysis strategy is utilized to assault the steganographic techniques by extracting,separating or distinguishing the inserted data. For various application distinctive steganalys is techniques are utilized. The distinctive assaults are:

1. Stego only – extract only stego image
2. Known carrier – extract carrier and stego image
3. Known payload – known the protected message in the embedded file
4. Chosen stego – extract by using tool
5. Chosen payload – it is a most powerful and efficient tool among other different attacks [1][2][3].

7. APPLICATION OF DIGITAL IMAGE STEGANOGRAPHY

There are different applications in steganography; it depends, among the user requeirements, for example, copyright control, incognito correspondence, smart ID's, printers and so forth. But in here I have completed my research project and made a Digital Image Steganography application which will encode and decode the message in an image.

<u>**Encryption:**</u>



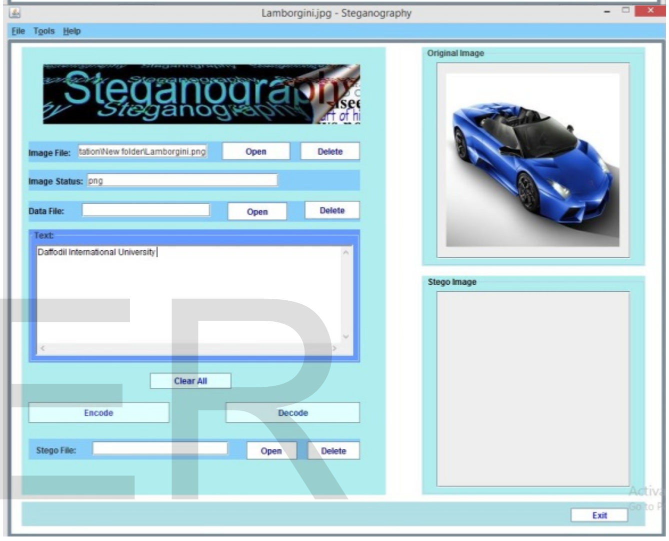


Image File: tation\New folder\Lamborgini.png

Image Status: png

Text: Daffodil International University

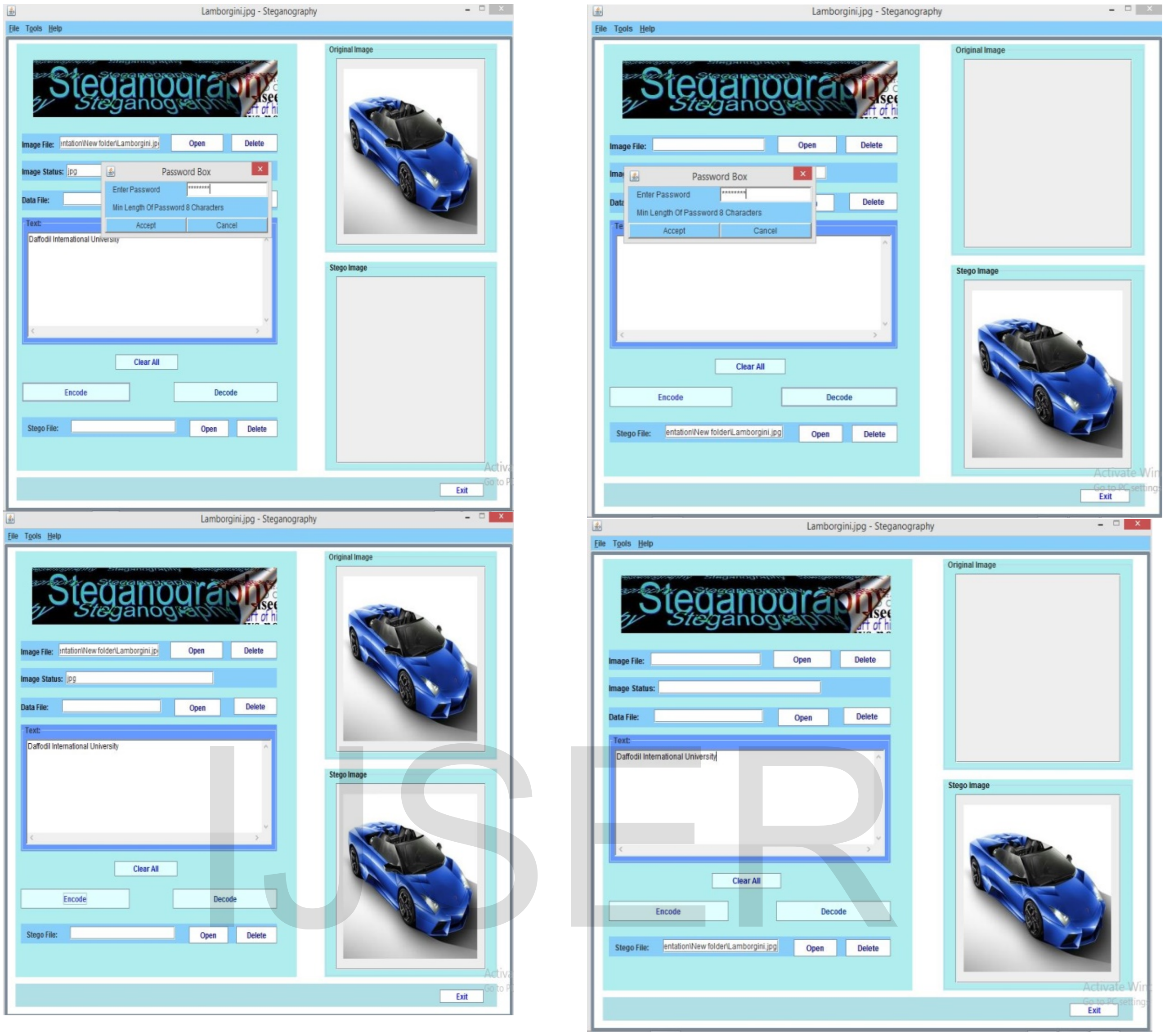


Image File: ntation\New folder\Lamborgini.jpg

Image Status: jpg

Enter Password: ********

Text: Daffodil International University

Stego File: entation\New folder\Lamborgini.jpg

Figure.5. Screen Shots of digital image steganography application.

Decryption:

8. ACKNOWLEDGEMENT

First and foremost, we want to express our heartiest thanks and gratefulness to almighty God for his divine blessing makes us possible to complete this project successfully. And then we would like to express our heartiest gratitude to our supervisor Prof. Dr. Syed Akhter Hossain, Head, Department of CSE Daffodil International University, Dhaka, Bangladesh for his kind help to accomplish our project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice , reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

9. CONCLUSION

This paper gives the novel ways to deal with executing Digital Image Steganography, that is to hide secret data inside an image so that it seems imperceptible to the eyes. This paper gives effective steganography techniques, so that the individual can discover the assortment of picking the strategy to ensure the data. In Image Domain, we examined the most capable method called LSB to shroud data, especially inside in a PNG file format. At long last this paper closes with Application of steganography.

10. REFERENCES

[1]. R.Poornima1 and R.J.Iswarya2, AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY.

[2]. Bin Li Junhui He Jiwu Huang, A Survey on Image Steganography and Steganalysis, Journal of Information Hiding and Multimedia Signal Processing c 2011 ISSN 2073-4212 Ubiquitous International Volume 2, Number 2, April 2011,received July 2010; revised October 2010.

[3]. Angela D. Orebaugh George Mason University, A Steganography Intrusion Detection System [1]. T. Morkel 1, J.H.P. Eloff 2 and M.S. Olivier 3, an overview of image steganography, Information and Computer Security Architecture (ICSA) Research Group, vol-2, 2009.

[4]. Eugene T. Lin and Edward J. Delp, A Review of Data Hiding in Digital Images, 0165-1684/$-seefrontmatter&2009ElsevierB.V.Allrightsreserved. doi:10.1016/j.sigpro.2009.08.010.

[5]. Blossom Kaur, Amandeep Kaur and Jasdeep Singh, Steganographic Approach For Hiding Image In DCT Domain, International Journal Of Advances In Engineering & Technology, July 2011. 72 vol. 1,issue 3,pp.72-78

[6]. J. K. Mandal , A Frequency Domain Steganography Using Z Transform (FDSZT)

[7]. Jianhua Song, Yong Zhu And Jianwei Song, Steganography: An Information Hiding Method Base On Logistic Map In DCT Domain, Advances In Information Sciences And Service Sciences(AISS) Volume4, Number2, February 2012, Doi: 10.4156/AISS.Vol4.Issue2.5

[8]. Mrs. Gyankamal J. Chhajed Ms. Krupali V. Deshmukh Ms. Trupti S. Kulkarni, Review on Binary Image Steganography and Watermarking, Gyankamal J. Chhajed et al. / International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 11 November 20113645.

[9]. Mrs. Sivaranjani ,Ms. Semi Sara mani, 2011, Edge Adaptive Image Steganography BasedOn LSB Matching Revisited, Journal of Computer Applications (JCA) ISSN: 0974-1925, Volume IV, Issue 1.

[10]. Gyankamal J. Chhajed et al. Review on Binary Image Steganography and Watermarking International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 11 November 2011 3645.

[11]. S.K.Muttoo and Sushil Kumar, A Multilayered Secure, Robust and High Capacity Image Steganographic Algorithm, World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 6, 239-246, 2011 .

[12]. P. Mohan Kumar and K. L. Shanmuganathan. Developing a Secure Image Steganographic SystemUsing TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate, Journal of telecommunication and information technology 2011.

[13]. Steganography And Digital Watermarking , Copyright © 2004, Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham.

[14]. Hide and seek: an introduction to steganography published by the ieee computer society 1540- 7993/03/$17.00 © 2003 ieee . ieee security & privacy.

[15] Mohammed A.F. Al-Husain "Image Steganography by Mapping Pixels to Letters" Journal of Computer Science 5 (1): 33-38, 2009

SUPERVISOR

Dr Syed Akhter Hossain
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

AUTHOR

Email: alamgirm800@gmail.com

MD. Alamgir Kabir received his Bachelor of science degree in computer science and engineering from Daffodil international university and his research interest in Data mining, Image processing, computer networking, programming language, artificial intelligence, image processing and algebra.