Understanding Image Steganography with Practical Approach

Gautam Juvarajiya

Student, Department of Information Technology, Thakur College of Engineering and Technology, Mumbai, Maharashtra, India

---***---

Abstract - *As internet usage increases, we must be mindful to send and receive sensitive information securely. Steganography and Cryptography are two techniques used for secured data transfer and user privacy. In cryptography, the message is changed using an encryption key that is only known to the sender and the recipient. No one else can read the message without the encryption key. Steganography increases the anonymity of data communication by concealing the existence of data such that no one can identify its presence.*

Key Words: internet, privacy, encryption, steganography, cryptography

1.INTRODUCTION

The Greek words steganos (covered) and graptos (writing) are the origin of the word steganography (meaning covered or hidden writing)[1]. In the modern world, everyone shares data and information with one another. As electronic devices for sharing data and information have developed and become more widely used, the need for data security has become critical[2]. With so many publicly available technologies capable of exploiting the privacy, data integrity, and security of the data being communicated, malicious threats, eavesdropping, and other malicious actions have become commonplace. Various techniques, including Steganography, Cryptography, etc have been made accessible for the security of this information and data[3,4]. Although the goals of steganography and cryptography are identical, there is a little distinction or there is a thin line of difference between these two. In Cryptography, plain text or original data is first converted into Cipher text in encryption while conversion of cipher text to original text is known as Decryption. The cipher text can be seen by human eyes, but encryption renders the data unbreakable and unreadable. While in Steganography the data or the secret message is concealed in such a way in some form but the hidden data or secret message here is not visible to any of the party unless it is decrypted properly[3].

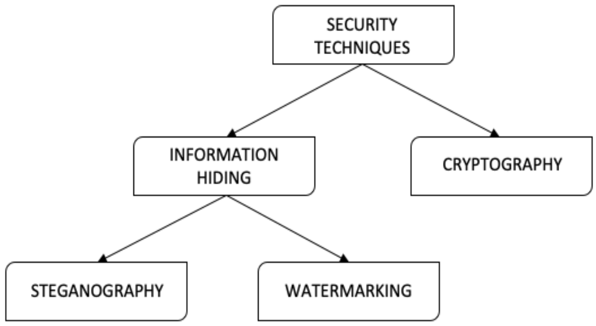

Fig -1.1: Security Techniques [5]

Steganography and watermarking are two examples of information-hiding domains; both are employed to conceal the hidden message[3]. These two approaches are closely related to one another, although they each have different goals. While steganography refers to the act of concealing information by hiding the secret message in a public cover media without any indication of its existence, watermarking aims to maintain the integrity of the secret data by preventing outsiders from knowing the existence of the communication[3,5].

Steganography techniques conceal sensitive information or a secret message in unassuming cover material to prevent attracting the attention of attackers. Words can be inserted inside of images, audio files, video files, etc. Contrarily, the study of mathematical techniques related to information security components like secrecy, data integrity, entity authentication, and data origin authentication is referred to as cryptography[3]. There are numerous varieties of steganography, including those for images, text, audio, and video.

2. TYPES OF STEGANOGRAPHY

Few types of steganography technique to encrypt or hide data which are common: Image Steganography, Video Steganography, Audio Steganography, Video Steganography, etc.[1,5,6,7].

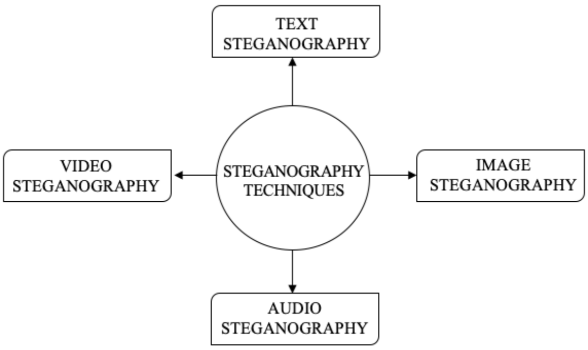

Fig -2.1: Types of Steganography

2.1 Image Steganography

The secret image is hidden inside the cover image in a way that makes the secret data or secret message disappear and the main picture appear to be the original. By changing the pixels in the primary image, the secret message is concealed.

FIG -2.1.1: Image Steganography

2.2 Audio Steganography

Audio steganography is the process of using digital sound files to obscurely alter a sound file's binary sequence, which can be used to conceal messages. It supports various audio files like wave, mpeg, mp3, etc. to conceal the data in it.

2.3 Video Steganography

The digital video formats that are utilized for video steganography allow for the concealment of any type of information. Video files can include a sizeable quantity of sensitive information because they are a moving stream of images and sounds. MP4, AVI, and other video formats are used in video steganography.

2.4 Text Steganography

In its simplest form, text steganography describes the information that is concealed in text files. Text steganography can be used to generate legible messages by altering context, modifying words within the text, constructing and generating random sequences, and more.

3. IMAGE STEGANOGRAPHY WORKING

Firstly, user needs to select whether to encode the image or decode the image. If a user wants to encodes, he/she needs to select the image from their system and enter the secret message then click on "Encode" button and save it on the system. To decode the hidden text from the image, user needs to select the encoded image and click on "Decode" button and the output Hidden message will be displayed.

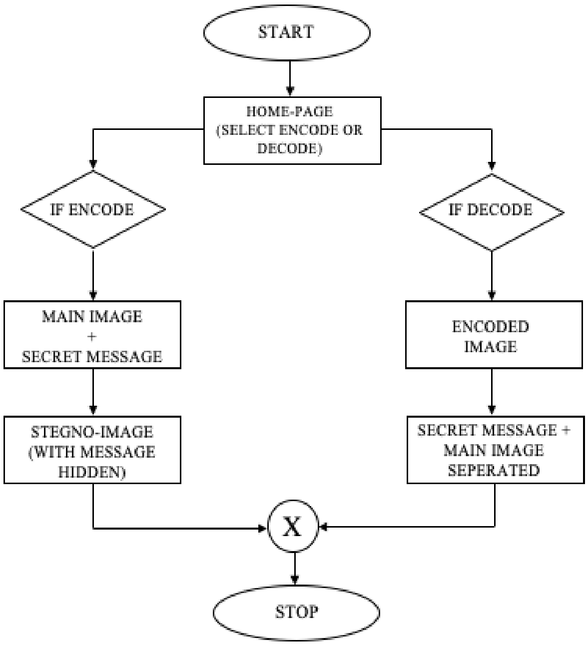

FIG -3.1: Flow Chart for Image Steganography

3.1 Algorithm :

STEP 1 : Start

STEP 2 : Select Encode/Decode

STEP 3 : If Encode,

Select image & write text to be encoded & save at particular directory

STEP 4 : If Decode,

Select encode image & hidden message will be displayed

STEP 5 : Stop

4. RESULTS AND ANALYSIS

The initial screen, or the default homepage, that the user sees when the application is launched asks whether they wish to encrypt or decrypt the image. The application's home page features two buttons, Encode and Decode. The secret message is encoded using the original image and decoded using the encoded image using the Encode and Decode buttons, respectively.

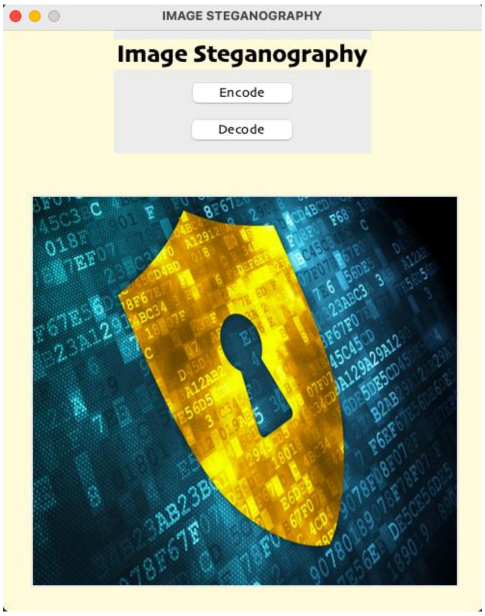

FIG -4.1: Home-Page of Application

4.1 Encode Page

The user is then taken to this screen after clicking the "Encode" button on the homepage, where they must choose an image from their system or computer.

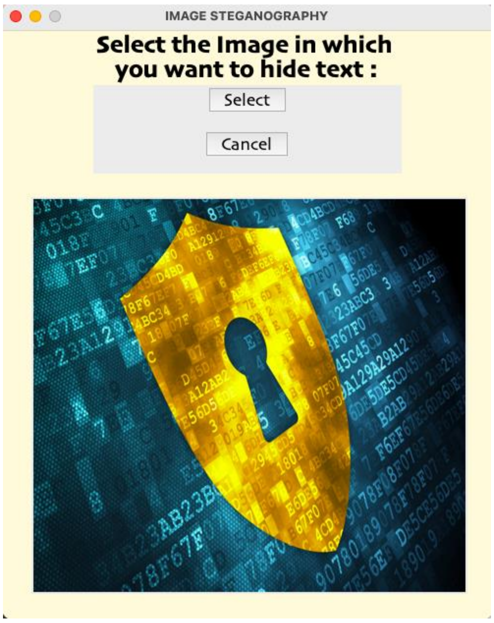

FIG -4.1.1: Encode Page

The user is then taken to this screen after clicking the "Encode" button on the homepage, where they must choose an image from their system or computer.

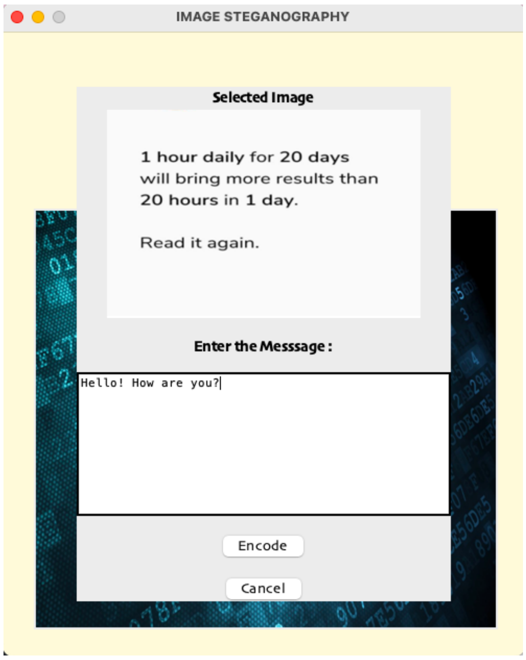

FIG -4.1.2: Selecting Image and Entering Hidden Message for Encoding image

4.2 Decode Page

The user must select the encoded image from the computer system and click the "Decode" button in order to decode the secret message or data from the image.

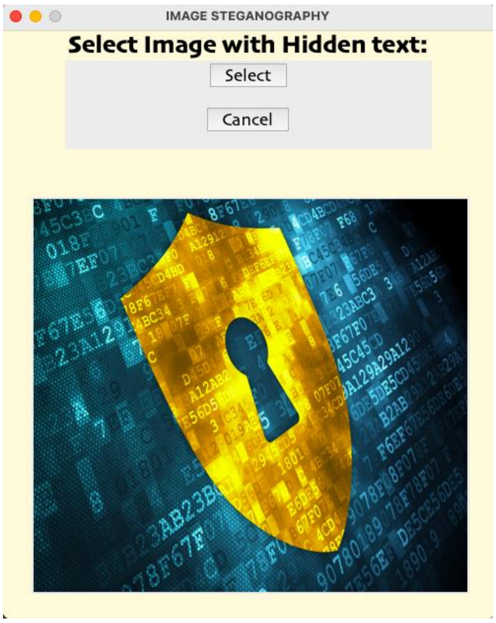

FIG -4.2.1: Selecting image for Decoding Secret Message from Encoded image

After selecting the "Decode" Button, the chosen (encoded) image's hidden message is displayed on the screen.

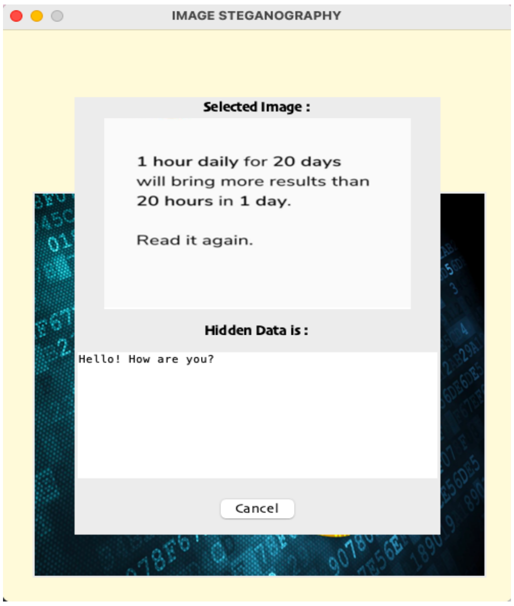

FIG -4.2.2: Successful Decryption

4.3 Observations

According to the project, the size of the image before hidden message or secret message encoding was smaller than the size of the image after encoding.

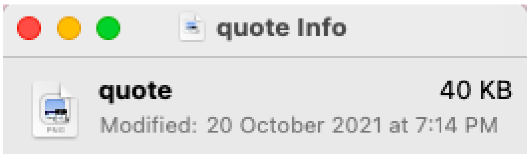

FIG -4.3.1: Image Size Before Encoding

The size of the image was 40KB before the secret message was encoded, and it was 44KB after the hidden or secret message is encoded in it.

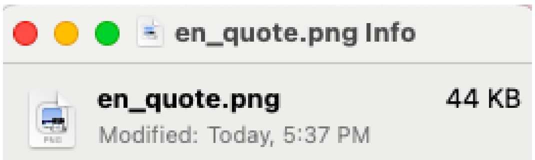

FIG -4.3.2: Image Size After Encoding

Following encoding and decoding procedures, the 4KB difference was noticed.

5. CONCLUSIONS

Each of the main formats has a unique way of encoding messages, each with different advantages and disadvantages. Where one strategy falls short in one area, the other does too in another. The strategy presented in this research makes use of image steganography, a well-known method of steganography. The personal information is contained inside the cover file image that the application creates as a stegno image. Steganography is different from cryptography, but combining the two can increase the security of the data that is being safeguarded and keep the covert communication from being discovered. The main advantages of implementing steganography to mask data over encryption is that it makes it harder to detect if private information is hidden within a file or other piece of content. In contrast, anyone may see the cipher text in cryptography.

ACKNOWLEDGEMENT

This paper was prepared with the help of a number of research papers on steganography techniques and their overview, and I want to express my gratitude to the authors for their commitment and hard work.

REFERENCES

[1] International Refereed Journal of Engineering and Science (IRJES) ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 6, Issue 1 (January 2017), PP.68-71, Survey Paper on Steganography Namrata Singh Computer Science and engineering ABES Engineering College, Ghaziabad A.K.T.U.

[2] International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April, 2020 1549 Published By: Blue Eyes Intelligence Engineering & Sciences Publication © Copyright: All rights reserved. Retrieval Number: D8760049420/2020©BEIESPDOI:10.35940/ijeat.D8760.049420 Journal Website: www.ijeat.org Information Hiding using Steganography Ritu Sindhu, Pragati Singh.

[3] International Journal of Scientific & Engineering Research, Volume 6, Issue 6, June-2015 1580 ISSN 2229-5518, Review Paper On Image Based Steganography By Indu Nehra, Rakesh Sharma.

[4] SteganoGAN: High Capacity Image Steganography with GANs Kevin A. Zhang,1 Alfredo Cuesta-Infante,2 Lei Xu,1 Kalyan Veeramachaneni1 1 MIT, Cambridge, MA - 02139, USA kevz,leix,kalyanv@mit.edu 2 Univ. Rey Juan Carlos, SpainK. Elissa.

[5] Journal of Theoretical and Applied Information Technology 15th March 2022. Vol.100. No 5 2022 Little Lion Scientific A LITERATURE REVIEW OF VARIOUS STEGANOGRAPHY METHODS RANA SAMI HAMEED, 2,3 ABD RAHIM BIN HJ AHMAD, 1MUSTAFA MUNEEB TAHER, 1 SITI SALASIAH MOKRI 2 College of Computing Science & Information Technology, University of Tenaga, Malaysia 1 Faculty of Engineering & Built Environment, Universiti Kebangsaan Malaysia 2 College of Law and Political Science, University of Kirkuk Iraq.

[6] JARCCE ISSN (Online) 2278-1021 ISSN (Print) 2319-5940 International Journal of Advanced Research in Computer and Communication Engineering Vol. 7, Issue 9, September 2018, Image Steganography Techniques - A Review Paper Mohammed A. Saleh College of Sciences and Arts in Ar Rass, Qassim University, Kingdom of Saudi Arabia.

[7] International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2016,A Survey Paper on Steganography Techniques Dr. Rajkumar L Biradar1, Ambika Umashetty2 Associate Professor, Dept. of Electronics and Telematics, G. Narayanamma Institute of Technology & Science, Hyderabad, India1 Dept. of Computer Science & Engineering, Appa Institute of Engineering & Technology, Kalaburagi.