International Journal of Research in Engineering, Science and Management
Volume 4, Issue 1, January 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Obscurity of Data Using Steganography with Encryption

Amreen Rahman*
Department of Electronics and Communication Engg., Institute of Technology & Management, Aligarh, India

***Abstract*: The purpose of this paper is to demonstrate the implementation of data security using two techniques that is obscurity and encryption. The role of Steganography is to hide the message that is in graphical form, the technique that we are using in this system is LSB then after this we encrypt the message of which key is dynamic from both the ends each time the message send, AES 256 encryption technique is being implemented. So it is basically a data security implementation that consists hiding too.**

***Keywords*: Data security, encryption, graphical password, programming languages, textual password.**

1. Introduction

As the name of the topic "The Obscurity of Data using Steganography with Encryption" illustrates, the motive of the report is to secure the data or provide the strong security to the data that is being sent or transmitted between two users under the same network or the different network using Steganography. The word Steganography is derived from the Greek word "Stegno's" which means covered or concealed and "graphic" means writing, combining these means becomes an art of concealing the message that has been sent from the source with an image, text or protocol to the receiver to avoid the hacking of message from the intended user. Here we use encryption and decryption as well.

Technology we use:
A) AES-256
B) NET beans -IDE
C) Hiding/Obscurity: LSB Technique

2. History

The uses of Steganography was first recorded in 440 BC in Greece. It was named as Steganographia by a German abbot name Trithemius. Histaiaeus an ancient Greek tried to provoke fomenting revolt against the King of Persia and he wanted to pass along the message securely and secretly, so he shaved the head of one of his trusted vassal and marked the tattoo on his head's scalp on which the alert has been written secretly and sent him on his way when his hair grew back. And the recipient on the other end shave his head to read the secret message or an alert(information). The same way Greek used the same trick writing the message on the rabbit's belly to convey the secret message.

3. Literature Review

The word Data, the modern computing world revolves around this word. The data explosion is like never before, as today the world is witnessing. "How much data do we create every day?", the Forbes article, it states that there is about almost 2.5 quintillion bytes of data is created every day at our current pace and it's only accelerating with the growth of internet of things (IoT). And the interesting thing that is worth reading is that in just last 2 years the 90% of data has been generated. So data alternates the matter of security is first thing that should place under consideration.

So we are putting light on some already proposed methods and at the end we will be presenting the advantage of using the proposed system over the existing system. So obscurity, is basically the quality of data of being difficult to understand. Steganography as we have already discussed used to conceal the desired message into other file, the file is of various types. In the same way we can describe steganography in different forms. Though there are many types of steganography, in this paper we are taking

Let's discuss the types of Steganography;

A. Types of Steganography

Fig. 1. Steganography types

Image steganography: Image commonly use cover file. The cover file can be of the format png, jpg, jpeg, etc.

Video Steganography: As we know that video is the combination of many still frames of images and audio as well. The hiding method of video steganography is same as that of the audio and the image steganography. The advantage of using video steganography is that large amount of data can be stored in cover file and we can conclude it is the reason that there is flow of sounds and images.

Audio Steganography: The Audio Steganography is the technique in which the intended data/secret information is to be

*Corresponding author: amreen6rahman@gmail.com

embedded in audio cover file that must be resistant to malicious attacks and robust. This results in slender shifting of binary sequence of the equivalent audio file. Methods involved in this type of steganography are as follows;

- Phase coding
- LSB Coding
- Spread Spectrum
- Echo Hiding, etc.

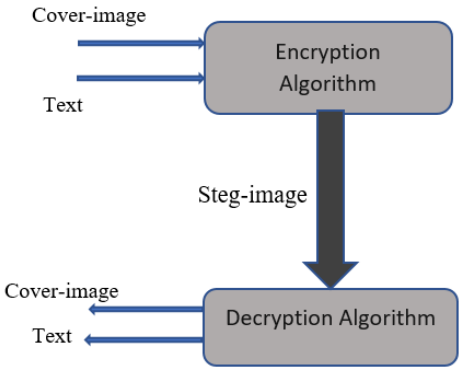


Fig. 2. Process of image steganography

Text Steganography: In this type of steganography the process takes place just by formatting or changing the characteristics of some textual element and it consists of Line Shifting Coding, Word Shift Coding and the Feature Coding.

Protocol: The Network protocol Steganography is the new approach for data hiding and in this type of steganography network layer protocol of TCP/IP suite are used for hiding of data.

B. Understanding the image Steganography using LSB (Least Significant Bit) Method

The digital image is made up of the group of digital values which we call as pixels, these are the smallest individuals with which the image is made up of. Pixels of an image decides the brightness level of the given color at any specific point.

So, if a pixel with a value of 1,0 and 0 would mean 1 parts of red, 0 part of green and 0 parts of blue; in essence it would turn out to be a red pixel. As we all now know that any image is made up of three colors namely red, green and blue, and each color is of 8-bit value. Now in case of an 8-bit system, a pixel can accommodate up to 8 digits and those in the form of 0's and 1's. The largest number that could be represented in 8 digits is 11111111 which is 255, and the smallest number that could be represented is 00000000 which would be 0. So we can conclude that any pixel in the 8-bit scenario accommodate any number between 0 to 255 as the value considered for each of the color among RGB.

Now, let's assume a random 8-bit grid has 3 pixels and each of the pixel having values given below for R, G and B.

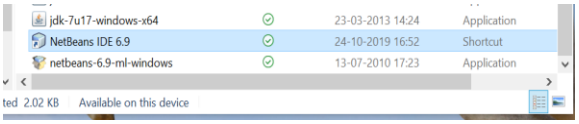
	RED	GREEN	BLUE
Pixel 1	00101101	00011100	11011100
Pixel 2	10100110	11000100	00001100
Pixel 3	11010010	10101101	01100011

Now, suppose if we want to embed the secret number 220, we get the value binary equivalent of this as 11011100. Now implementing LSB (Least Significant Bit) technique, use each digit of binary value of 220 that is 11011100 to replace the right most bit of our pixel grid, that are indicated in bold fonts. The resulting new color scheme shown in the grid given below;

	RED	GREEN	BLUE
Pixel 1	00101101	00011101	11011100
Pixel 2	10100111	11000101	00001101
Pixel 3	11010010	10101100	01100011

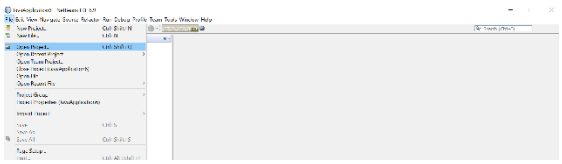
This results in the altering of the colors I the original picture in the three colors of the three pixels by the smallest amount. Similarly, if we want to insert the large message into the image the second right most bit and so on will be replaced according to the secret message inserted. But if our message is too large the attacker can notice the changes in the picture, so it is to a certain limit.

4. Working of the Software

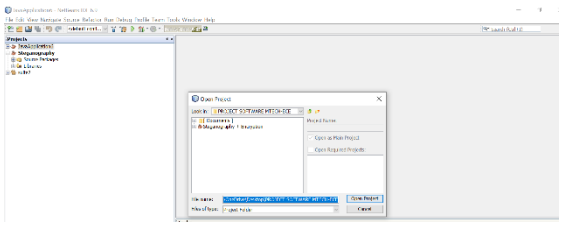


(a)

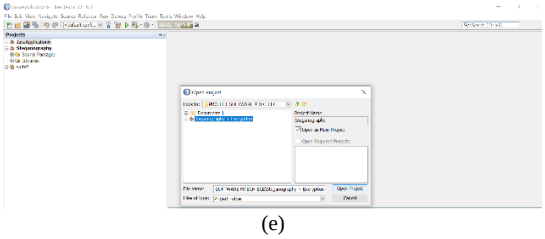
(b)



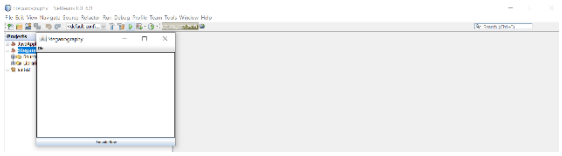
(c)



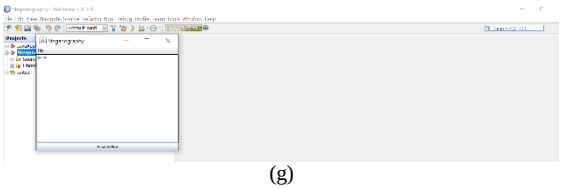
(d)



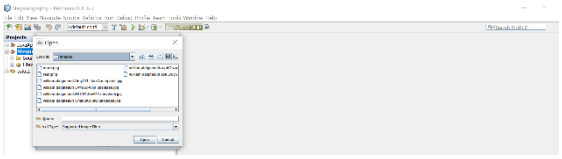
(e)



(f) Encoding commencement

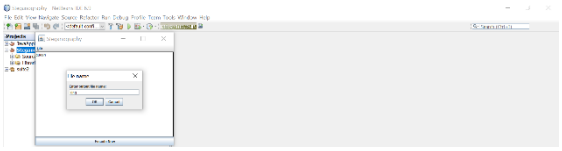


(g)



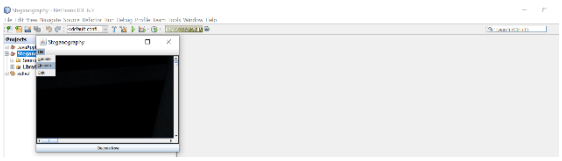
(h)

(i)

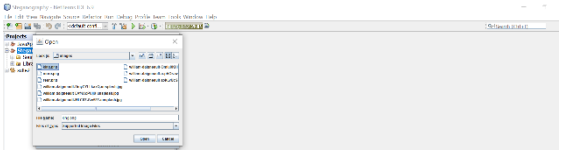


(j)

(k)

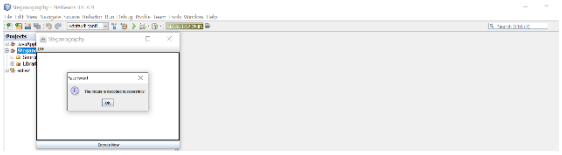


(l) Decoding commencement

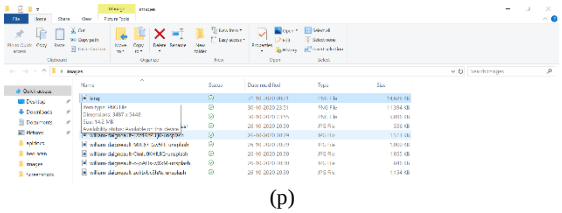


(m)

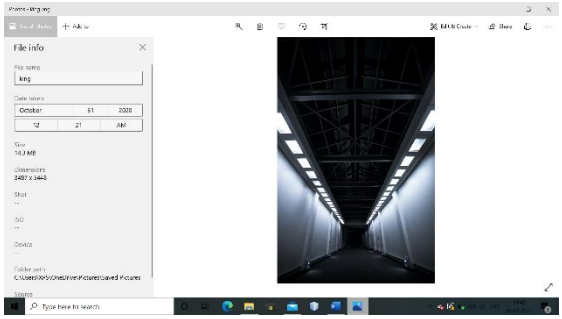
(n)



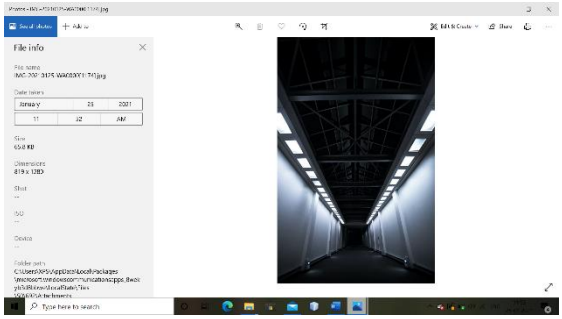
(o)



(p)



(q)



(r)

Fig. 3. Working of the software

If we could see the image 3(q) and 3(r) there is merely a difference in the image that we cannot catch the minute difference in the two images but there is the size difference, the images differ in size. The image is of bigger size the secret message is embedded this is how Steganography works using LSB Algorithm.

5. Conclusion and Future Scope

- Keeping an eye on the current scenario in the world, as days pass the data over the internet increases unexpectedly. Many individuals, business tycoons, secret agencies, information bureau, etc., use to transfer the secret information, business documents using internet.
- Because any unauthorized information while transferring the data using internet can hack the data and make that information useless/ obtain information that is unintended to him.
- In this project I used the AES-256 technique and LSB Algorithm.
- The project is GUI (graphical user interface) driven and provides the proper workflow. Encoding and Decoding dynamically possible.
- The future work that can be done into this project is that, though the LSB Technique is good but we also can improve the level as by using different encryption keys and decryption keys and no doubt by varying the carriers.

- JSteg, F5, etc., are the few Steganographic algorithms available. In this project, LSB algorithm technique is used. This algorithm works very efficiently as when we use bit map images .bmp files and the speed provided using this technique is also high as compared to other technique like JSteg algorithm.

References

[1] T. Gupta, A. A. M. Hafifau, R. Tawker, and V. Vaidhehi, "An Enhanced Approach to Steganography: Obscurity", in IJIRAE Transactions, vol. 2, no. 9, September 2015.

[2] H. A. Atee, R. Ahmad, and N. M. Noor, "Cryptography and image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding", in IDOSI publications, pp. 1450-1460, 2015.

[3] P. Tirkey, D. Kudiyam, N. Druw, D. Markam, and R. Ghosh, "Image Steganography Using LSB Along with IDEA Algorithm", vol. 5, pp. 19583-19586, Dec. 2016.

[4] Wikipedia "Image Steganography", https://en.wikipedia.org/wiki/Steganography

[5] B. Chitradevi, N. Thinaharan, and M. Vasanthi, "Data Hiding Using Least Significant Bit Steganography in Digital Images", in Statistical approaches on Multidisciplinary Research, 2017.

[6] Wikipedia "Steganography", https://en.m.wikipedia.org/wiki/Steganography