Image Steganography Using Pixel Manipulation and Shuffling

Vikas Sharma, Utkarsh Srivastava and Shubham Aggarwal

Abstract—Security of the information or any sort of data is crucial for the transmission and reception from end to end without any risk of breach in privacy. Steganography is the safest data hiding technique deployed that gives almost an invisible form of information exchange method on the web using different data concealing techniques. It takes numerous digital images for hiding any information in the form of text via pixel manipulation. Here, a user thinks that an image is shared and it doesn't even look like an information that has been exchanged. In this paper we will elaborate about steganography technique of pixel manipulation we have deployed and its forthcomings.

Keywords - Steganography, Pixel manipulation, Embed Text, Encryption, Scramble, Extract Text and Decryption.

1 INTRODUCTION

The intruders can be successful in invading a system and its files as the vast amount information obtained from a system is kept in a readable form. Intruders may expose the information to others, mold it to misquote anyone, or use it to assault. Possible rectifications to this condition is use of image stenography. Steganography is a mechanism of hiding facts in digital medium. Here our goal is to keep information safe and retrievable and don't project it if anything secret exists in front of by manipulating pixels of an image. Steganography has become more essential as masses have joined the revolutionary model of privacy. Steganography is the art of masking facts in ways that doesn't let the hidden facts get detected. Steganography include a string of forbidden transmission ways of concealing any message from detection. With improvements in ICT, Steganography became helpful in providing mechanisms to secure information.

An ideal Steganography technique embeds data into images in a way that forms modified images which visually don't look encrypted or manipulated. As the domain of the application embeds data in image, the data hiding techniques are deployed in terms of security, storage and invisibility. The performance of a steganography system is measured by difficulty in determining the existence of a hidden message.

2 METHODOLGY

The basic modules of image steganography used are Embed Text, Encryption, Scramble, Extract Text and Decryption. [1]

Embed Text: The place where text has to be added in the image.

Encryption: Here, the text added is encrypted with a password.

Scramble: Here, the image file is added and text is encrypted in it and the new image file is saved.

Extract Text: In this module, the text is extracted from the new image file (pixel manipulated) that is uploaded.

Decryption: Now, the decryption is completed with the text displayed.

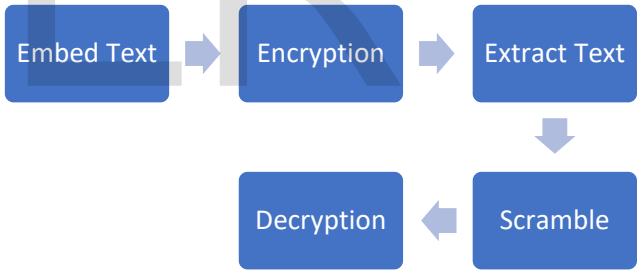

Fig 2.1 Process Deployed for Image Steganography with Pixel Manipulation

3 LITERATURE SURVEY

Steganography is the process of concealing delicate information within something that looks like nothing but is unusual. Steganography is mostly preferred for essential data protection. The process of steganography includes concealing information such that it makes its appearance not hidden at all. If a person views the image, the information concealed inside won't create an iota of doubt or signify its presence and the person will not try to decrypt any info within. What steganography importantly focuses on exploitation of human perception as they can't simply look for information concealed beyond their knowledge. Although this software is capable in doing Steganography. [2]

Mostly steganography is used to keeping an info from the person inside another file using Pixel Manipulation. Image Steganography consists of linguistic forms of concealed writing. Earlier obscure ink was used to hide info manually. One drawback of steganography based on language was that users must be equipped with a good understanding of linguistics. Recently, digitization is trending to a great extent and with the progress of the web technology, digital media transmission has become convenient over the net. Henceforth, message can be discreetly sent on digital platforms by using the steganography techniques, and further transmission through the internet rapidly. [5]

Various file formats are potentially used but digital images are the most renowned as their large presence on the internet. To hide confidential information in images, there exists a numerous range of steganography mechanisms which are very complicated than others. Most of them have their own pros and cons. So we can up with this application, to make the information hiding more foreseeable.

There are several historic references of Secret use of Steganography for communication of information among people. [6]

Here are some examples of how Steganography was used earlier:

1. During World War 2 invisible ink was used to write information on paper to make it look like nothing to a common man. Drinkable fluids such as milk, Acetic acid and fruit extracts were used, because when they were heated they darkened and become perceptible to human vision.

2. In Greece, masses used to select messengers with shaven heads to write a message on their head. After writing the message hair was grown back again. After that the messenger went to provide the message, the receiver would shave the messenger's hair again to view the concealed message.

4 PROPOSED SYSTEM

We did amplification of the image stenography system using AES (Advance Encryption Standard) approach for efficient and safe communication and using a pixel manipulation during embedding the message into the new image. The main job of this software was to modify any type of image to bitmap or png and diminish quality and text to hide. After the manipulating bits of the pixels in the image and adding document or any information, we will encrypt the image by shuffling the pixels of the image according to a specified module by providing password security to our data. [4]

Due to advancements in technology, the safety of info has become a major concern. Steganography can be deployed to obtain info like audio, video and images. Steganography hides the forbidden message within the host image and keep its

presence unviable and reliable for transmission and communication with the receiver. The host image is covertly modified and damaged to keep it invisible to any attacker. Henceforth the manipulating the images using pixels and their distortion is the idea behind encryption and decryption of the images. [3]

5 OUTPUT

The Output is focused at selecting an image, encrypting it with an information (with password protection), then the image is uploaded and information is added. Thereafter the encrypted image is saved and then it is used again to retrieve the information required. The following Screenshots of our work is depicted below:

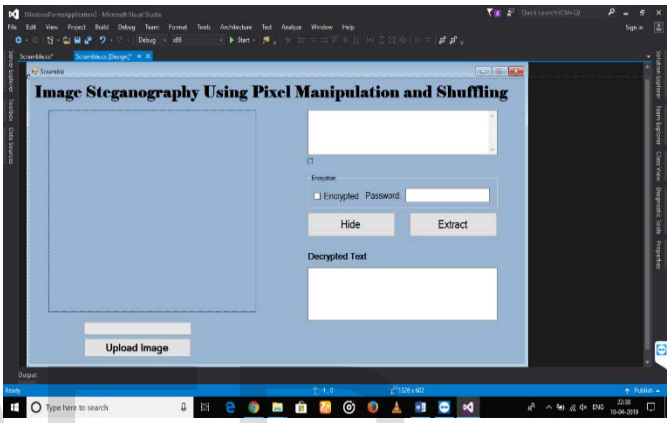

Fig 5.1 GUI depicting the fields required for upload and information hiding.

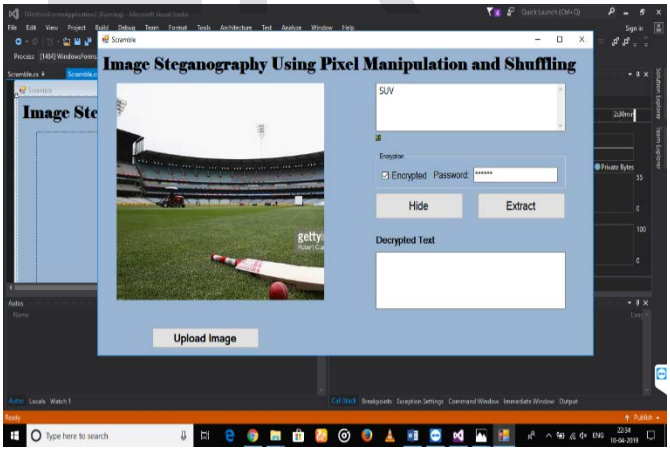

Fig 5.2 Image uploaded for Pixel Manipulation and the text entered with password.

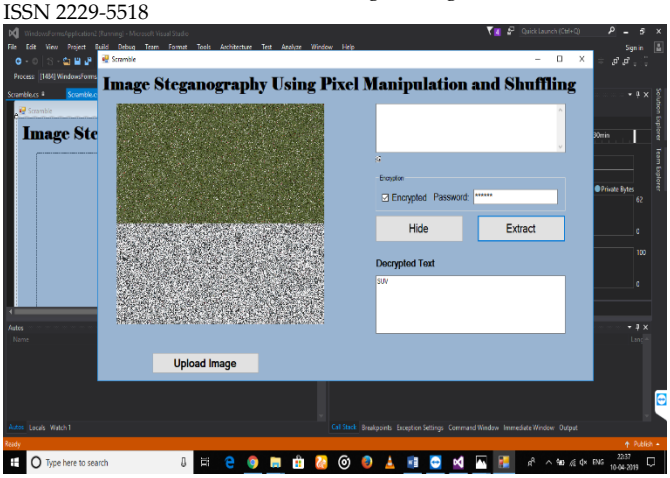

Fig 5.3 Image after Pixel Manipulation and Encryption and the extracted information with password depicted.

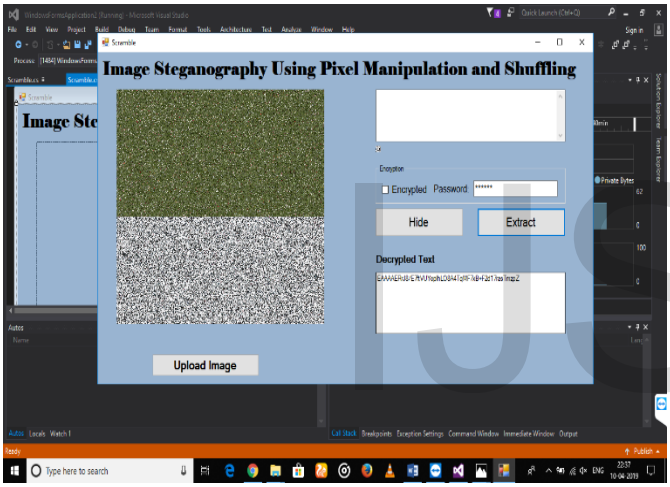

Fig 5.4 Decryption Complete.

6 CONCLUSIONS

The proposed method is fast and effective to conceal the forbidden info. It diminishes the image quality reduction and keeps its features intact. It is highly secure from the attackers as they can't even spot what was being done to keep it from them. Other than hiding info for esotericism. The approach of information concealing can be stretched to copyright protection for digital medium i.e. for audio, video and images if required. [7]

The growing needs of data transmission with security makes it mandatory to be able to secure the exchanged data on the internet. Therefore, the esotericism and integrity are required for protection against unverified access. It has led to a boom of the field of information hiding. Steganography aims to hide the secrete message within the host image and presents to be unviable and reliably transmits it to the receiver.

ACKNOWLEDGEMENT

We feel extremely glad to submit this research paper on our project report on **"IMAGE STEGANOGRAPHY USING PIXEL MANIPULATION AND SHUFFLING"**. The contentment and delight that comes along with the successful completion of this paper would be patchy without the accreditation of those who provided constant guidance and motivation to give right direction to our efforts. Firstly, we are very thankful to our guide, **Ms. Ruby Singh** for her invaluable guidance and cooperation throughout the work.

We also extend my heartfelt gratitude to **Mr. Shashank Yadav**, Project Coordinator, for constantly motivating and supporting us to keep our enthusiasm right from the beginning of our work.

We feel compelled to articulate my thankfulness to **Dr. Anand Pandey, HOD, Department of Information Technology,** for his encouragement which was a source of inspiration.

We would like to express my heartiest gratitude to **Dr. (Prof) D. K Sharma**, **Dean,** SRM Institute of Science and Technology, NCR Campus, Ghaziabad for his assistance and help throughout the work. Also, providing the desired setup to carry out the work.

Last but not the least we are very obliged with all the faculty members of our university for aiding us directly or indirectly by all means possible during the entire course of our study, research work and project work.

REFERENCES

[1] *https://github.com/Digiex/MCLauncher.NET/blob/master/MCLauncher.net/Crypto.cs*

[2] *X. M. Li and Lin Dai, "A Novel Approach for Double Image Encryption" in Proceedings of IEEE Region 10 Conference, pp. 697-701, 2010*

[3] *Meghdad; M. B Parmida, and M. H. Hesam, "Chaos-Based Medical".*

[4] https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1

[5] https://pdfs.semanticscholar.org/04f8/028c9b047538a69cb63e71eee7de92075a35.pdf

[6] https://airccj.org/CSCP/vol2/csit2211.pdf

[7] *Image Encryption Using Symmetric Cryptography," in Proceedings of "International Conference on Information and Communication Technologies: From Theory to Applications".*