International Journal of Scientific Research & Engineering Trends
Volume 5, Issue6, Nov-Dec-2019, ISSN (Online): 2395-566X

Image Encryption using Steganography

Srinvas Nishant
Computer science and engineering
VIT University ,Vellore
nishantvishwanadha@gmail.com

Sarath Dasari
Computer science and engineering
VIT University , Vellore
sarathdasari99@gmail.com

Anisha M Lal
Computer science and engineering
VIT University , Vellore
anishamlal@vit.ac.in

***Abstract* -steganography is the art of hiding information within other information in such a way that it is hard or even impossible to identify the existence of any hidden information. There are many different carriers for steganography. Of which, most popular ones are digital images. Due to recent developments in steganalysis, providing security to personal contents, messages, or digital images using steganography has become difficult. His paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good stenographic algorithm and briefly reflects on which stenographic techniques are more suitable for which applications.**

***Keywords* -algorithm, encryption, decryption, stenography, (key words).**

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Different kinds of steganograph almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this for the requirement, while research has also uncovered other file formats that can be used for information hiding. The figure shows the four main categories of file formats that can be used for steganography.

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every n the letter of every word of a text message. It is only since the beginning of the Text Images Audio/ video Protocol Internet and all the different digital file formats that is have decreased in importance. Text steganography using digital files is not used very often since text files have a very small amount of redundant data. Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography. This paper will focus on hiding information in images in the next sections. To hide information in audio files similar techniques are used as for image files.One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information.

Although nearly equal to images in stenographic potential, the larger size of meaningful audio files makes them less popular to use than images. The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used.

An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used. Lately, exponential growth of technology in every aspect ofLife is observed. Improvement of technology provides facilities to both users and hackers/intruders too. Advancement in technology that encourages hackers/ intruders activities result in lack of security to user's confidential data. The most common and popular techniques for data hiding that have been in use since long time are cryptography and steganography. Cryptography: There are many possible definitions for cryptography. One of which is, "The computerized encoding and decoding of information" to define cryptography. This is a process of converting a message from a human readable or understandable form (plaintext) to non-understandable Format (cipher text) to enable secure sending and back to original format at other receiving end. The cipher text in cryptography always reveals static information of plaintext. Many methodologies were introduced that follow their own strategy, but all the methodologies use some patterns. The underlying idea in pattern based approach is to decode the encoded message, that is, using a pattern of one's own choice or a standard pattern, a sender encodes the message and thus generates a cipher text. The receiver uses the same pattern and decodes the cipher text to generate message (plaintext). Over a period, cryptographic approaches evolved over phases.

It is suggested that a key should be used in the process of encoding and decoding a message. Based on this concept of keys, cryptography is further classified into two types, symmetric- key cryptography and public-key cryptography. In case of symmetric key cryptography, same key has to be used by both sender and the receiver while encoding and decoding respectively. In contrast, in the case of public key cryptography, the keys used by the sender and the receiver are different. Steganography: It can be defined as "The art and science of communicating in a way which hides the existence of the communication".

A stenographic model facilitates hiding or embedding of sender's secret message in a file (carrier) that does not give out a clue about the existence of secret message in it when viewed. For this, any media format or file format like .bmp, .doc, .gif, .jpeg, .mp3, .ppt, .txt and .wav is taken as a carrier that can act as cover for the sender's message, that is, a message here is hidden in a carrier and that carrier is transmitted. The underlying operation of this methodology is both logical and technical. In general, a steganography algorithm takes a secret message and a carrier as input and gives a carrier message as output (in which the message is embedded). In the process of steganography, the carrier which hides the message in it will be sent to the receiver.

The carrier gives the receiver no information about the message but reveals it only after using the tool or algorithm that is used by the sender. Both cryptography and steganography have found usage in many applications. For example, transmission of attack plans by military teams to hide information about their strategies. Many other applications of data hiding techniques other than its original objective, have gained importance, which include authentication and identification, watermarking and transmitting passwords etc.

II. PROPOSED METHOD

1. Flow of Execution

The purpose of this project is to hide an image in other image, so a secret image would be an input. At first, the secret image is converted to a text file using Base64 conversion. Then the generated text file is encrypted with a password based encryption algorithm to generate an encrypted text file called cipher text. Using a customized embedding algorithm, cipher text is embedded on to a cover image. The output is the stegno-gram (a cover image with a secret message embedded in it).

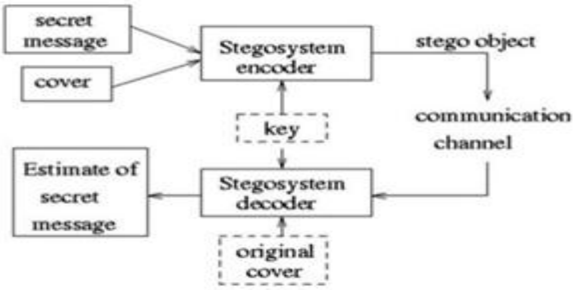

Fig. 1 Work Flow

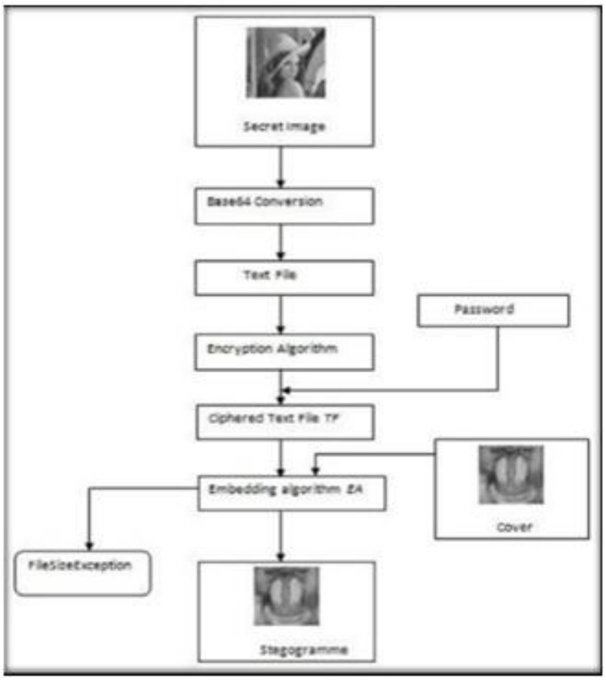

Fig.2 Flow Chart

2. Flow of execution of Sender's Operation

Read the hidden message (secret image), the stegogramme has to be decrypted. So, the stegogramme is used as input to the retrieving algorithm. If the retrieving algorithm is not the same as the embedding algorithm, there is no way that the correct output can be obtained. The correct output from retrieving algorithm is the cipher text is used as input to the decryption algorithm. This decryption algorithm is the same as the encryption algorithm; otherwise the secret message cannot be determined. And also the decryption algorithm takes a key (password) to generate plaintext.

III. RESEARCH AND DISCUSSION

Our base paper is “Secure Image Steganography Algorithm Based on DCT with OTP Encryption”. The base paper implemented a Discrete Cosine Transform method to encrypt data into an image.DCT algorithm is not a lossless method to encrypt data. The image quality gets reduced while encoding the message which might be an issue when a user tries to send a small DCT encrypted image to another user. The quality of the encoded image drastically reduces. The algorithm works on the RGB scale only.

Our implemented model works on 6 different algorithms i.e. LSB, DCT, ZK, WDCT, Fusion and Egypt. All the mentioned algorithms can work on Grayscale as well as RGB scales. The quality of compression can be decided as well. WDCT algorithm works on 2D image wavelets and changes the waveforms of the image to store the message. It gives enhanced security and is an almost lossless method to encode and decode messages to an image. Unlike DWT method which is somewhat similar to DCT, WDCT is a compilation of both the algorithms and provides a more secure and a more lossless method to image steganography. The energy level of the DCT coefficients of real world images we see most of the energy is limited to the very few coefficients. This is what JPG does, keeps only the few dominant coefficients and throws the rest. The efficiency of DCT depends on how less coefficients are needed to describe the image in an acceptable quality.

It turns out that for WDCT, the situation is better.Namely on real world images, less coefficients are needed to describe the image with the same perceived quality. This property is called the ability to decor relate the data or being energy dense. The fusion algorithm works with an image mask which is then used to fuse the two images together to get a more secure encrypted image which can be sent to another user. This provides a 2 layered security method over the LSB and DCT methods of steganography.

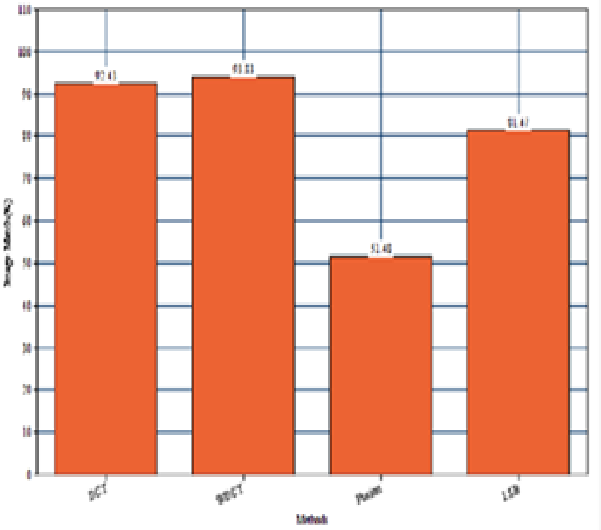

Fig.3 Comparison 1

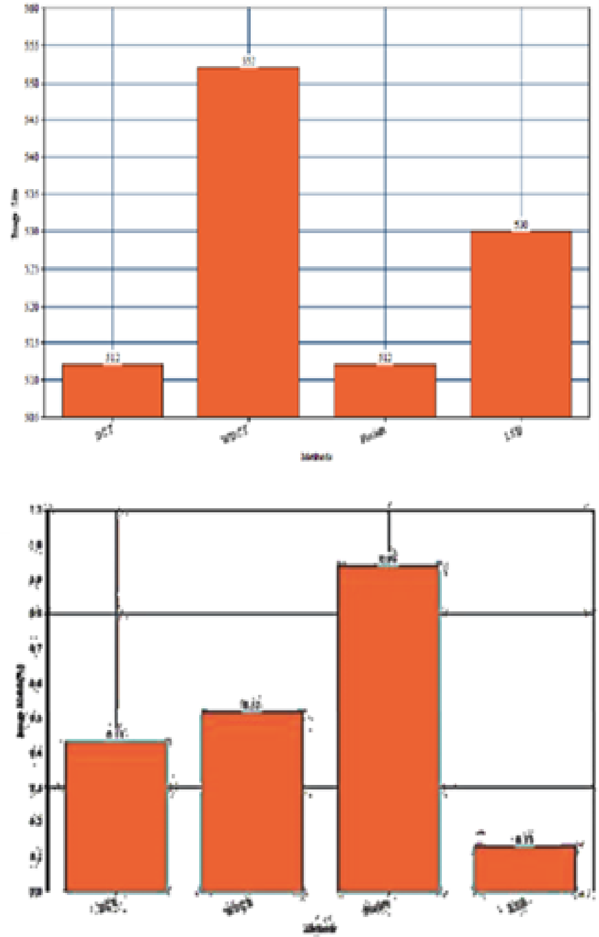

Fig.4 Comparison 2 & 3

IV. RESULTS

From the above graphs we find out that our proposed WDCT algorithm is the optimal algorithm for image steganography and can be used for any sized image along with any cipher text as it is more secure and has a good compression rate as compared to other methods of steganography.

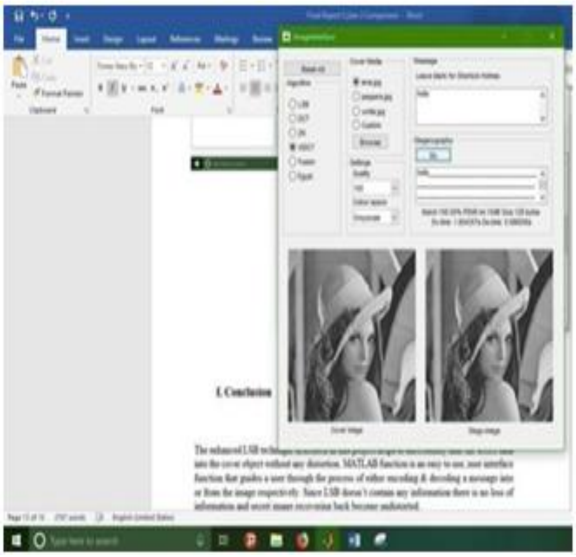

Fig.5 Result 1

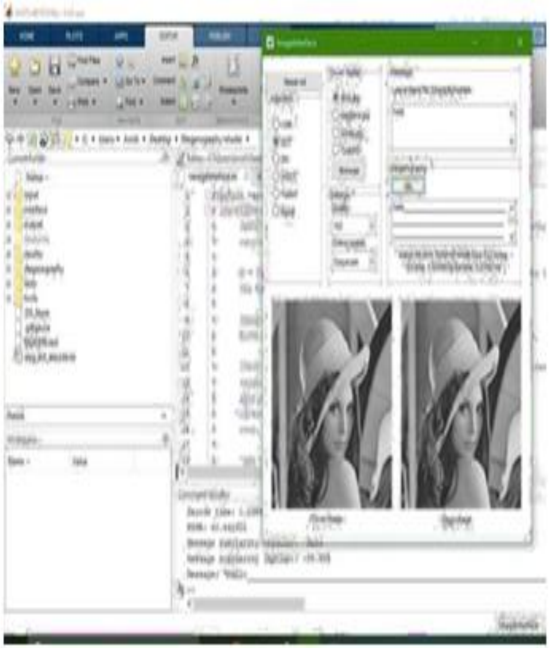

Fig.6 Result 2

V. CONCLUSION

The enhanced LSB technique described in this project helps to successfully hide the secret data into the cover object without any distortion. MATLAB function is an easy to use, user interface function that guides a user through the process of either encoding & decoding a message into or from the image respectively. Since LSB doesn't contain any information there is no loss of information and secret image recovering back become undistorted. Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images.

All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.

Thus for an agent to decide on which steganographic algorithm to use, he would have to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others. WDCT offers both - security as well as a good compression rate as compared to other algorithms which can be used for further test purposes.

REFERENCES

[1]. Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Significant Bit Algorithm", International Journal of Engineering Research and applications, vol.2, issue 3, pp.338-341May- June2012.

[2]. Vijay kumar Sharma, Vishal Shrivastava, "A Steganography algorithm for hiding image in image by improved LSB substitution by minimize technique", Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, 15th February 2012.

[3]. "OVERVIEW OF IMAGE STEGANOGRAPHY" Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa

[4]. Alaar. A, Shahrin Bin Sahib, Mazdak Zamani, "An Introduction to Image Steganography Techniques, Advanced Computer Science Applications and Technologies (ACSAT).

[5]. https://ctfs.github.io/resources/topics/steganography/ invisible- text/ README.html.