

CRYPTOLOGY OF DATA AND STEGANOGRAPHY

A Project Report for the Evaluation 3 of Project 2

Student Name: **SEJAL APURVA**
Admission No.: **16SCSE101359**

b.tech

**School of Computing Science and Engineering Greater Noida,
Uttar Pradesh**

Under the

Supervision of

Mr. Llvendhan A (AP)



Winter

2019-2020

TABLE OF CONTENTS

1. Abstract
2. Introduction
 - (i) Overall description
 - (ii) Purpose
 - (iii) Motivations and scope
3. Implementation & diagram
4. Proposed model
5. Result
6. Conclusion
7. References

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

INTRODUCTION:

Overall Description:

Message is the data that the sender wishes to remain confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

The goal of steganography is covert communication. So, a fundamental requirement of this steganography system is that the hidden message carried by stego-media should not be sensible to human beings.

The word steganography comes from the Greek “Steganos”, which means covered or secret and – “graphy” means writing or drawing. Therefore, steganography means, literally, covered writing. It is the art and science of hiding information such that its presence cannot be detected and a communication is happening. A secret information is encoded in a manner such that the very existence of the information is concealed. Paired with existing communication methods,

steganography can be used to carry out hidden exchanges.

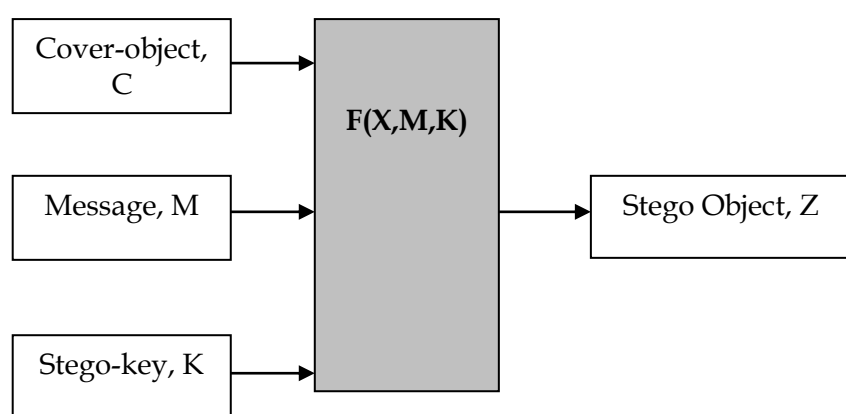
The main goal of this projects it to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hider data. There has been a rapid growth of interest in steganography for two reasons:

The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products

Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The basic model of steganography consists of Carrier, Message and password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message.

Basically, the model for steganography is shown on following figure:



ensures that only recipient who know the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the Stego-object.

Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message.

Purpose:-

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with

cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. This technique is chosen, because this system includes not only imperceptibility but also un-delectability by any steganalysis tool.

Motivation and Scope: This project is developed for hiding information in any image file. The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file

PROBLEM STATEMENT:-

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry. In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.

So we prepare this application, to make the infor

IMPLEMENTAION:-

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that alteration made to the image is perceptually indiscernible. Commonly approaches are include LSB, Masking and filtering and Transform techniques. Least significant bit (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel. The advantage of LSB-based method is easy to implement and

high message pay-load.

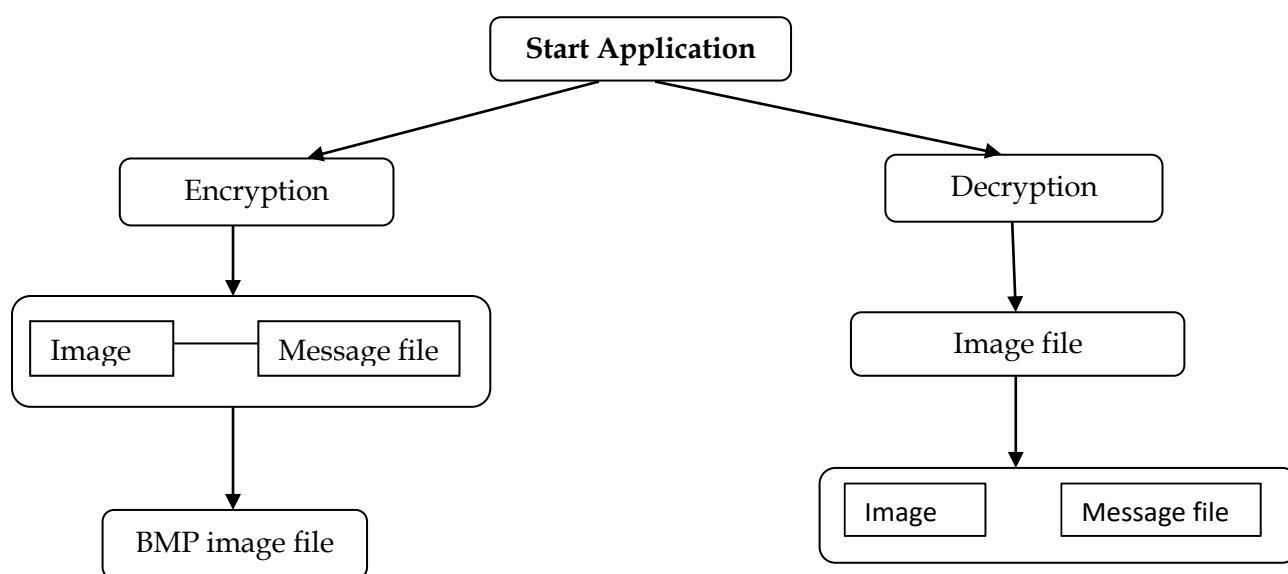
Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

Therefore, a system named Secure Information Hiding System (SIHS) is proposed to improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the message into a set of random pixels, which are scattered on the cover-image.

Masking and filtering techniques, usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks. The technique perform analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficient in a transform domain, such as the Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other term.

PROPOSED MODEL:-

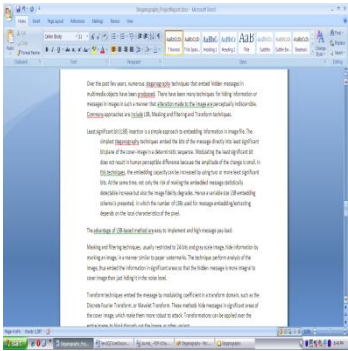


ENCRYPYION PROCESS:

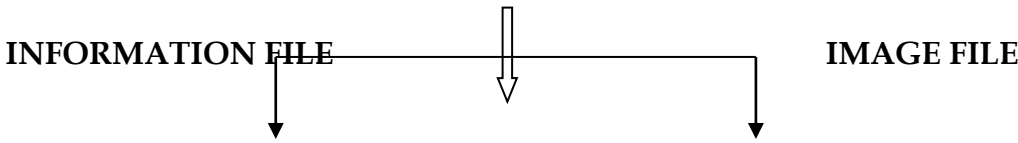
IMAGE FILE

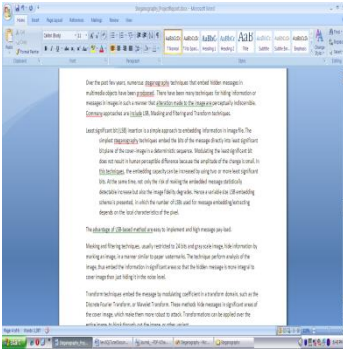
INFORMATION

FILE



DCRYPTION PROCCRESS:





RESULTS:

Steganography system requires any type of image file and the information or message that is to be hidden. It has two modules encrypt and decrypt.

Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simplify programming. One of .Net tools for pictures and images is auto-converting most types of pictures to BMP format. I used this tool in this software called “Steganography” that is written in C#.Net language and you can use this software to hide your information in any type of pictures without any converting its format to BMP (software converts inside it).

The algorithm used for Encryption and Decryption in this application provides using several layers instead of using only the LSB layer of the image. Writing data starts from the last layer (8th or LSB layer); because the significance of this layer is the least and every upper layer has double the significance of the layer below it. So every step we go to the upper layer, the image quality decreases and the image becomes more transparent.

The encrypt module is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file as the destination.

The decrypt module is used to get the hidden information from an image file. It takes the image file as an input, and gives two files as the output, one is the same image file and the other is the message file that was hidden in it.

Before encrypting a file inside an image, we must save the name and size of the file in a specific place in the image. We can save the file name and size in the LSB layer and save the file size and file name in the most right-hand pixels of the image. Writing this information is needed to retrieve the file from the encrypted image in the decryption state.

CONCLUSION:

In watermarking to protect intellectual property is evidence that steganography is

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image.

This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion o research not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

REFERENCES:-

1. <https://www.semanticscholar.org/paper/Proposed-System-for-data-hiding-using-Cryptography-Sarmah-Bajpai/6b2d7a0e22f805be7c83580a04313fa25e10ca5e>
2. <http://www.asp123.com>
3. <http://www.wikipedia.org>
4. <https://www.academia.edu/Documents/in/Steganography>