A NEW METHOD USED IN IMAGE STEGANOGRAPHY WITH ENHANCED CONFIDENTIALITY

[1]Aparajita, [2]Prof Ajay Rana

[1]Assistant Professor, Dept. of MCA,Galgotia Institute of Management and Technology/ UPTU, Greater Noida, Uttar Pradesh, (India).
[2]Program Director, Amity School of Engineering and Technology, Amity University, Uttar Pradesh, (India).

ABSTRACT

Steganography is the only answer for secure and secret communication. Existing methods in image steganography focus on increasing embedding capacity of secret data. According to existing methods, the experimental results indicate that two pixels are required for one secret digit embedding. In direction of improve the embedding size of secret data, a novel method of Pixel Value Modification (PVM) by modulus function is proposed. The proposed PVM method can embed one secret digit on one pixel of cover image. Thus, the proposed PVM method gives good quality of stego image. The experimental outputs validate that good visual perception of stego image with more secret data embedding capacity of stego image can be achieved by the proposed method. In this paper we are presenting the techniques and a problem statement how we can encrypt the text message in the image file.

Keywords: Steganography, Cipher text, Plain text, Hiding information, Steganalysis, Stego types.

I INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. The purpose of Steganography is covert communication—to hide the existence of a message from a third party. Generally, a steganographic message will appear to be something else: a picture, an article, a shopping list, or some other message.

This apparent message is the cover text. For instance, a message may be hidden by using invisible ink between the visible lines of innocuous documents. Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces

unused or insignificant bits with the secret data. Steganography is not as robust to attacks since the embedded data is vulnerable to destruction.

The advantage of Steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in some countries encryption is illegal. **[1]**

1.1 Techniques

Insertion-Based

Using this technique, you store the data you want to hide in sections of a file that are ignored by the processing application. By doing this you avoid modifying those file bits that are relevant to an end-user—leaving the cover file perfectly usable.

For example, with some files there is an EOF or end-of-file marker. This flag signifies to the application that is reading the file that it has reached the end of the file and the application can stop processing the file. Hidden information can then be inserted after the EOF marker.

The end-user may not even realize that the file contains additional hidden information. However, using an insertion technique changes file size according to the amount of data hidden and therefore, if the file looks unusually large, it may arouse suspicion.

Substitution-Based

Using this approach, you replace the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion.

The main advantage of that technique is that the cover file size *does not change* after the execution of the algorithm. There is, however, a limit to the amount of data you can hide with this approach as there is a limited amount of insignificant data in any given file.

Generation-Based

Unlike insertion and substitution, this technique doesn't require an existing cover file—this technique generates a cover file for the sole purpose of hiding the message. The main flaw of the insertion and substitution techniques is that people can compare the stego file with any pre-existing copy of the cover file (which is supposed to be the same file) and discover differences between the two. You won't have that problem when using a generation approach, because the result is an original file, and is therefore immune to comparison tests. [2] [3]

1.2 Common Media for Steganography

Image Files

Image files are probably the most common medium for hiding files. Most of the stego techniques that use image files involve manipulation of the image's colour tables.

8-bit images use a colour table of 256 RGB values. Each pixel is represented by a byte, which is then used to pick out the pixel's RGB value from the colour table. In order to hide data in 8-bit images, S-Tools modify the image to only use a 32-colour palette instead of 256. These 32 colours are duplicated 8 times in order to fill the colour table. The duplicate entries are then used to store the secret message in the three least significant bits for each RGB entry. This all means that each colour in the modified image can be represented in eight different ways, which leaves redundant representations in which information can be hidden. [7]

Audio Files

Audio files are also a popular medium. As with image files it is very difficult to detect hidden information without a detection tool and just by listening. S-Tools uses least significant bit insertion to hide information in a sound file. This involves replacing the least significant bit of each byte with one bit of the message we are trying to hide. There is no way for anyone to detect the difference simply by listening to the file. [7]

Text Files

Data can also be hidden in text files. There are several methods available, including the template technique, deliberate misspelling, changes in spacing, or the use of slightly different fonts (such as Courier and Courier New).

The template method [4] involves a set of preselected locations on a page to hide a message. Consider the note:

> THE MOST COMMON WORK ANIMAL IS THE HORSE. THEY CAN BE USED
> TO FERRY EQUIPMENT TO AND FROM WORKERS OR TO PULL A PLOW.
> BE CAREFUL, THOUGH, BECAUSE SOME HAVE SANK UP TO THEIR
> KNEES IN MUD OR SAND, SUCH AS AN INCIDENT AT THE BURLINGTON
> FACTORY LAST YEAR. BUT HORSES REMAIN A SIGNIFICANT FIND. ON
> A FARM, AN ALTERNATE WORK ANIMAL MIGHT BE A BURRO BUT THEY
> ARE NOT AS COMFORTABLE AS A TRANSPORT ANIMAL.

Applying a template or rule as to which words to read to this message might yield the following:

HORSE
FERRY
SANK
IN BURLINGTON
FIND
ALTERNATE
TRANSPORT

1.3 Steganlysis

Steganalysis is the science of detecting messages hidden using steganography. The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them and, if possible, recover that payload. [5]. Unlike cryptanalysis, where it is obvious that intercepted data contains a message (though that message is encrypted), steganalysis generally starts with a pile of suspect data files, but little information about which of the files, if any, contain a payload.

One case where detection of suspect files is straightforward is when the original, unmodified carrier is available for comparison. Comparing the package against the original file will yield the differences caused by encoding the payload-- and, thus, the payload can be extracted.

However, this is only part of the problem, as the payload has often been encrypted first. Encrypting the payload is not always done solely to make recovery of the payload more difficult. Many encryption techniques have the desirable property of making the payload appear much more like well-distributed noise, which can make detection efforts more difficult, and save the steganographic encoding technique the trouble of having to distribute the signal energy evenly. [6]

II PROBLEM STATEMENT

Currently many cryptography and steganography techniques have come into existence. Encoding of plaintext is achieved using DES, AES, Triple DES, RSA and many other algorithms. Any individual can use his/her one's own approach as encryption method.

Many algorithms such as JSteg, JPHide and JPSeek, OutGuess, F3, F4 and F5 were invented for the purpose of embedding images. These algorithms follow a certain principle to embed and retrieve hidden contents. All the existing approaches have their own disadvantages as they can easily be compromised using steganalysis. It means that one way or another, an intruder can figure out the existence of hidden data which results in him/her compromise of sensitive data. Currently, no integrate dcryptography and steganography approach in one application exists for image based information security. There are encryption and embedding approaches present that work with plaintext only.

2.1 Motivation

As described above all the available techniques used in early tools are old and follow some specified process with some improvements to previously proposed techniques. This makes the intruders work easy. The intruder may try a counter attack by making some changes to counter existing techniques. None of the existing techniques offers protection through multiple levels. That is one of the reasons why an intruder is able to view/obtain hidden data with just one or two attacks.

2.2 Scope

The primary idea behind developing this project is to protect confidential data from an intruder's counter-attacks and to block the intruder through various levels in his/her attacks. A new tool has been developed with a combination of cryptographic encryption and stegangraphic encryption for its implementation .The developed steganographic tool has a sender's segment that can take a message, a password and a cover image as input and give a stego-image as output that has message embedded in it. On the other hand, it also has a receiver's segment where the receiver inputs the stego-image and the same password is used by the sender as input to get the sender's message as output. The project is tested with various inputs and made sure that the generated stego-image has no noise are data loss.

2.3 Functionality

The developed steganographic tool is a very useful to any user who shares confidential data through a network .The developed model has a customized access that gives more freedom to users. An interface has been developed that helps the user to interact with the tool. The interface is very user-friendly with different modules implemented to encode and decode the secret message. The developed tool was tested for various input conditions.

III WORKING PRINCIPAL

In this project we will use new encryption/decryption method for text file encryption/decryption for increasing data confidentiality.

Steps involved in our Method

1. Encrypt text file by using new encryption method.
2. Cipher text file merge in to jpeg Plain Image file.
3. Stego Image transfer via communication channel.
4. Retrieve Cipher Text File from Stego Image and regenerate Plain Image.
5. Decrypt Cipher text file using new developed method.

3.1 Working System Architecture

In this Working Architecture as shown in Fig 1:, we may use One Bit Stego, Two Bit Stego or Three Bit Stego as per user requirements and we will use new encryption/decryption method to make more secure our transmitted data on communication channel.

IV. APPLICATIONS

Proposed work will enhanced the following Image Steganography applications.

1) Data Transmission is more secure from attacker.
2) Confidential communication and secret data storing
3) Protection of data alteration
4) Access control system for digital content distribution
5) Media Database systems

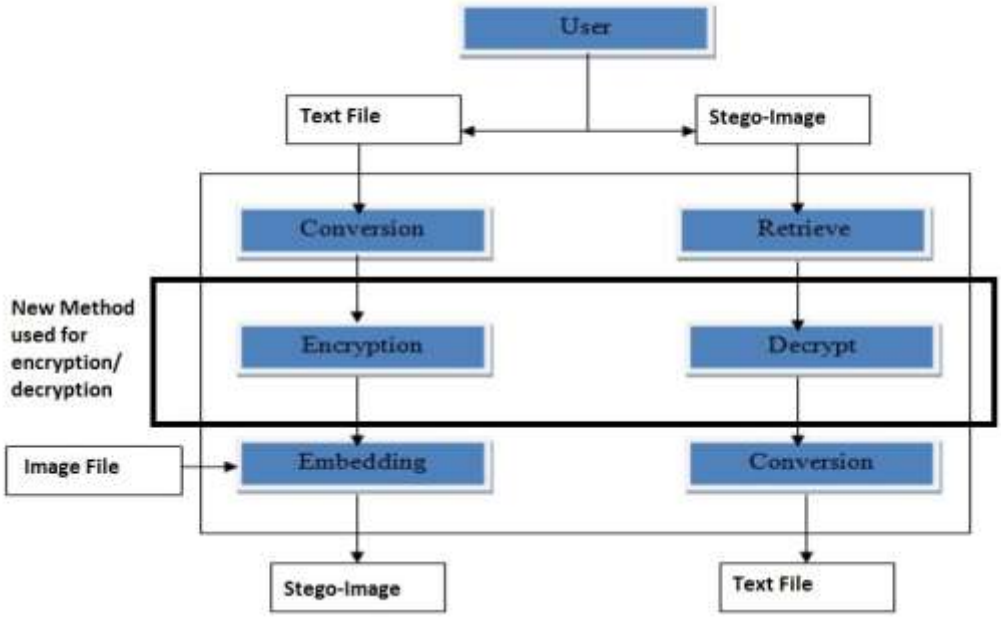

Figure 1: Working System Architecture

V CONCLUSION

From the above survey it is clear that to disguise our plain text we need some technique. In today's world Public Key Cryptography is used to hide the information and it uses the whole block instead of an individual alphabet. We have discussed the various techniques and tools and the main application areas of steganography. Another main topic was steganalysis where we look into the methods how to detect stego- objects. There is a lot of future research possible in this field. 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, and a comparison to cryptography

REFERENCES

[1] An Overview of Steganography for the Computer Forensics Examiner - http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm.

[2] Keeping Secrets Secret: Steganography with .NET – http://www.devx.com/dotnet/Article/22667

[3] Cole, Eric. - "Hiding in Plain Sight: Steganography and the Art of Covert Communication".

[4] Steganography: Hiding Data Within Data - http://www.garykessler.net/library/steganography.html

[5] Steganalysis – Wikipedia, the free encyclopaedia - http://en.wikipedia.org/wiki/Steganalysis

[6] Steganalysis of Images Created Using Current Steganography Software - http://www.jjtc.com/ihws98/jjgmu.html

[7] Steganography & Games 2005, Fitzgerald and Gallagher.

[8] STEGNOGRAPHY—"The Art of Hiding Information" A Comparison from Cryptography. Aparajita, Prof (Dr.) Ajay Rana http://www.ijirset.com/volume-2-issue-5.html#.

[9] STEGNOGRAPHY—"The Art of Hiding Information" A Study of Various Tools and Techniques along with Steganalysis. Aparajita, Prof. Ajay Rana. http://iasir.net/IJETCASpapers/IJETCAS13-587.pdf.