Survey on Steganography Techniques

Rini.J

Abstract .Steganography is an effective and popular means for privacy protection for achieving data security and internet security. It can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. . Ultimate objectives of steganography which are detectability, robustness (resistance to various image process- sing methods and compression) and capacity of the hidden data are the main factors that separate it from related techniques such as watermarking and cryptography. Using steganography, information can be hidden in different embedding mediums, known as carriers. These carriers can be images, audio files, video files, and text files. The focus in this paper is on the use of an image file as a carrier and hence, current steganography techniques for image files have been presented.

Index Terms—Steganography, LSB, SSIS, DCT based steganography, Filtering based Approach

---

1. INTRODUCTION

With the boost of computer power and internet different parts of the world are connected as one global virtual world. As a result, people can easily exchange Information and distance is no longer a barrier to communication it is desired that
The communication be made secret. However, the safety and security of long distance communication remains an issue. This is particularly important in the Case of confidential data. The need to solve this problem has led to the development of steganography schemes. Steganography is a powerful security tool that provides a high level of security, particularly when it is combined with encryption.

Steganography is the technique of hiding the message in a chosen carrier such that no one except the intended recipient can figure out its existence. Steganography is different from cryptography in the way that cryptography conceals the meaning of the message while steganography conceals the existence of the message. A message in encrypted form may arise some suspicion but the risk is eliminated if the very existence of the message is hidden as done by the steganography.

Steganalysis is the cracking of stenographic messages. The purpose of steganalysis is to identify the information and determining that whether or not they have hidden messages encoded into them and if possible, extract the hidden information.

———————————————————
• Rini. J currently pursuing M.Tech Degree in Computer Science and Information technology from FISAT, Angamaly, Kerala, India
• E-mail: riniklbm@gmail.com

The performance of a stenographic system can be measured using several properties. The most important property is the statistical un-detectability (imperceptibility) of the data, which shows how difficult it is to determine the existence of a hidden message. Other associated measures are the stenographic capacity, which is the maximum information that can safely embedded in a work without having statistically detectable objects [6], and robustness, which refers to how well the stenographic system resists the extraction of hidden data.

2. IMAGE STEGANOGRAPHY

In image steganography the cover medium is always an image file. An image is defined as an arrangement of numbers and such numbers usually stand for different
Light intensities in different parts of the image images are considered as the most popular file formats used in steganography. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. Also the hidden information could remain invisible to the eye.

3. HISTORY

Throughout history, a multitude of methods are used to hide information. The word 'steganography' was basically derived from the Greek words with the meaning “covered writing”. One of the ancient stenographic methods is to peal the wax off a wax-covered tablet, then write a message and to have the application of the wax again. The one in charge to receive the message would simply need to get rid of the wax from the tablet to see the message. Use of invisible ink was another popular form of steganography Then the Microdot technique used by Germans during the Second World War. Jerome Cardin, then a scheme of secret writing using a paper mask with holes. The user of such papers needs to write his secret

message in such holes after placing the mask over a blank sheet of paper and remove the mask to fill in the blank parts of the page and in this way the message appears as innocuous text.

4. TAXONOMY

Stenographic techniques that modify image files for hiding information include the following:

- Spatial domain;
- Transform domain;
- Spread spectrum;
- Statistical methods
- Distortion techniques

Spatial domain stenographic techniques, also known as substitution techniques, are a group of relatively simple techniques that create a covert channel in the parts of the cover image. .One of the ways to do so is to hide information in the least significant bit (LSB) of the image data. This embedding method is basically based on the fact that the least significant bits in an image can be thought of as random noise and consequently they become not responsive to any changes on the image. Transform domain embedding can be defined as a domain of embedding techniques for which a number of algorithms have been suggested. They hide information in areas of the image that are less exposed to compression, cropping and image processing. In SSIS, the message is hidden in noise and then it is combined with the cover image to reach into a stego image. Statistical methods modulate or modify the statistical properties of an image in addition to preserving them in embedding process. Distortion techniques require knowledge of the original cover image during the decoding process where the decoder functions to check the differences between the original images in order to restore the secret message.

In [1] a data hiding scheme by simple LSB substitution is proposed. Here 8 bit grayscale images are selected as the cover media's substitution generally means replacing the LSBs of the cover image with secret data bits.
Here to embed n bits of the secret message into the k rightmost LSBs of the cover image, first the secret message is rearranged into k bits. Then select a subset of pixels from the cover image in a predefined sequence, which is shared by the sender and the receiver. Then the k LSBs of the selected pixels are replaced with the rearranged secret message bits. Thus the stego image is obtained.
For message extraction, the embedded message can be extracted from the set of pixels storing the secret message.

In [2] a new method for image steganography called LSB++, which reduces the amount of changes made to the perceptual and statistical attributes of the cover image.
Here first some sensitive pixels of the cover image are identified and blocked using a key. Then the secret message to be embedded are encrypted using another key, and embed them into the unlocked pixels using a third key.
At the reciever side, first the locked pixels are distinguished using the third key and message is extracted. Extracted message is then decrypted using the same key used for encryption.

In [3] a novel stenographic scheme with the allowable modifications {-2,-1, 0, +1, +2} is proposed. Here the secret message can be embedded into the LSB, second LSB and third LSB of the cover samples.
To embed data into the first LSB, the cover samples that can be modified by +1 0r -1 are chosen(c0).If the LSB of the cover image is similar to the secret message bit, then it is kept unmodified otherwise the LSB is flipped. Another method for data embedding is matrix embedding.
For data embedding into second LSBs, cover samples in C0 with adding one and subtracting one are selected(C1).+-2 modification is employed to flip the LSBs of the selected cover samples.
For data embedding in third LSBs, adding one or subtracting one on the samples in C1 are selected. Here the third LSBs are flipped.
For data extraction, the cover samples are decomposed into bit planes and according to the index, the receiver can obtain the secret data.

In [4] the secret data is encrypted and then convert the encrypted data and LSB of the cover image into bit stream. Then divide the data bit streams and image bit streams into segments (number of segments is shared by the sender and the receiver).Compare each segment of the data bit by bit with each segment of the cover image. If both segments are the same, then the cover image bits are kept unchanged. Data segments are inserted using LSB insertion method based on a random sequence.
For extraction, receiver should enter the number of segments. Data segments are extracted and rearranged after obtaining the length of the data and random sequence of the data segments. Finally decrypt the extracted data to obtain the secret data.

In [5] first the secret message is encrypted using a key and encoded to obtain an encoded message. After that a real valued noise sequence is produced. Embedded signal is composed by combining encoded message and the noise sequence. Embedded signal is input to an interleaver using a key and added to the cover image to obtain the stego image.
During extraction, estimate of the original image is obtained and the difference between estimate of the stego image and cover image are fed into the de-interleaver to construct an

estimate of embedded signal. Then the noise sequence is regenerated and encoded message is demodulated and its estimate is constructed. The obtained output is decoded and decrypted to obtain the secret data.

In [6], cover image is passed through a filter to separate high and low frequency components. Then inverse transform of both the frequency component is found out as HFSI (High Frequency components Spatial Image) and LFSI. Message is embedded into HFSI image. Both the modified HFSI and unmodified LFSI are added to form stego-image.

For data extraction, Subtract LFSI from stego-image. Thus modified HFSI is obtained. Message id decoded from the modified HFSI image using the stego-key.

In [7], it reduces the distortion between the cover object and the stego object. If the distortion is sufficiently small, then the stego object will be indistinguishable from the noisy cover object. Tree based parity check matrix construct a complete N-array tree called the master tree, to represent the LSB of the cover object. That is the nodes of the master tree is filled with the LSBs of the cover object level by level from top to bottom and left to right. Then Tree based Parity check algorithm derives an L-bit binary string called master string. Toggle tree is constructed from toggle string which is obtained by performing bitwise XOR of message and master string.

Finally, stego tree is obtained by performing XOR of toggle tree and master tree.

In [8], LSB matching revisited image steganography is extended and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image's based approach is a popular type of stenographic algorithms in the spatial domain. LSB matching revisited uses a pair of pixels as an embedding units of the first pixel carries one bit of secret message. In data embedding stage, the scheme first initializes some parameters which are used for subsequent data preprocessing and region selection. To obtain the stego image, first the cover image is divided into non-overlapping blocks. Then each small block should be rotated by a random degree, as determined by the secret key. The resulting image is rearranged as row vector and divided into non overlapping embedding units.

After data hiding, the resulting image is divided into non overlapping blocks and then rotated by a random number of degree based on key. Then two parameters are embedded into a preset region. During extraction, the embedded parameters are extracted from the stego image and it is partitioned into blocks and rotated by a random degree based on the key. The resulting image is rearranged as a row vector. Finally the embedding units are obtained by dividing row vector into non overlapping blocks.

In [9], Ginseng Zhang a novel scheme for separable reversible data hiding in encrypted images. This scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases.

In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data.

With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large.

As an enhancement, I modified this paper to an analysis work that performs the performance analysis of various cryptographic algorithms on encrypted images.

Also an additional encryption of the secret data is included to enhance the security of the existing system.

5. COMPARISON

	Merits	Demerits
LSB	•Simple to implement. •High payload capacity. •Low computational complexity.	•Vulnerable to corruption. •Vulnerable to detection techniques.
LSB++	•Prevents histogram attacks. •Low distortion.	•Does not support lossy compression after embedding
DCT based steganography	•Enhanced security. •Preserves the quality of images. •Stays undetected by the well known steganalysis	•Low embedding capacity. •Amount of secret data that can be hidden is very small.
SSIS	•Robust against statistical attacks. •High capacity.	•Determined attacker is capable of compromising the embedded data using some digital processing.
Filtering based approach	•Uses both global and local image features. •High embedding capacity. •Enhanced security.	•Techniques can be applied only to gray scale images.

6. CONCLUSION

Steganography has its place in security. It is not intended to replace cryptography but supplement it. In this paper I have explored a tiny fraction of the art of steganography. Each method has a procedure of embedding for itself. Each method has some advantages, and also disadvantages in comparison with other methods of steganography. So it is not possible to say that a specified method is the best and best off all. It is impossible to determine the worst one. We can just compare them form different aspects, which results in determining a suitable method for a specific usage.

REFERENCES

[1].Chi-Kwong Chan "Hiding data in images by simple LSB substitution".
[2].Kazem Ghazanfari,Shahrokh Ghaemmaghami "LSB++:An improvement to LSB+ steganography."
[3].Xinpeng Zhang "Efficient data hiding with plus-Minus one or two."
[4].Robust data hiding technique based on LSB matching.
[5].Spread spectrum image steganography.
[6].A filtering based approach to adaptive steganography.
[7].Chung-Li Hou,ChanChun Lu,Shi-Chun Tsai and Wen-Guey Tzeng"An optimal Tree Based Parity Checking".
[8].Weiqi Luo,Jiwu Huang "Edge adaptive image steganography based on LSB matching revisited."
[9].Xinpeng Zhang "Separable reversible data hiding in encrypted messages"