INFORMATION SECURITY USING IMAGE BASED STEGANOGRAPHY

Dr. T.Pandikumar [1] Tesfay Gebreslassie [2]

[11] *Phd, Department of Computer and Information Technology, Defence University, College of Engineering, Debre Zeyit, Ethiopia*

[2] *M-tech, Department of Computer and Information Technology, Defence University, College of Engineering, Debre Zeyit, Ethiopia*

---***---

Abstract - *Over past few decades, with the advancement of communication technology the use of internet has grown extremely to exchange information without any distance barrier. However, such network is most popular for fast and easy process to exchange information over the long distance but still the message transmissions over the Internet have face all kinds of security problems. Steganography is the art of hiding the fact 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. This research seminar is on a secured, robust approach of information security using image based steganography. It presents two component based Least Significant Bit (LSB) steganography methods for embedding secret data in the least significant bits of blue components and partial green components of random pixel locations in the edges of images. A hybrid feature detection filter is also proposed that performs better to predict edge areas even in noisy conditions. Advanced Encryption Standard (AES) and random pixel embedding is incorporated to provide two-tier security. The comparison analysis of output results with other existing techniques is giving the proposed approach an edge over others. To improve the quality of encryption as well as the size of data to be encrypted with a single image (cover image) using the combination of cryptographic algorithm and steganography is helpful.*

***Keywords**: Steganography, Advanced Encryption Standard (AES), Least-Significant Bit (LSB)*

1.INTRODUCTION *(Size 11 , cambria font)*

A long time ago ancient Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.
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. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images.

Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. So by taking these weaknesses and strength of these algorithms you can take your own choice which algorithm to apply to maximize the capacity which is the size of data that can be secretly transferred, Robustness, perceptual transparency (quality of image after embedding), temper resistance(difficulty for cryptanalysis) and computational complexity (cost of encryption and decryption).

This document is template. We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace(copy-paste) the content with your own material. Number the reference items consecutively in square brackets (e.g. [1]). However the authors name can be used along with the reference number in the running text. The order of reference in the running text should match with the list of references at the end of the paper.

1.1 Steganography

Steganography is a Greek word which means concealed writing. The word "steganos" means "covered " and "graphy " means "writing" . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, and stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia objects like audio, video, images are used as a cover sources to hide the data.

1.2 Text steganography

It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are

- Format Based Method
- Random and Statistical Method
- Linguistics Method

1.3 Image steganography

Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

1.3 Audio steganography

It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are

- Low Bit Encoding
- Phase Coding
- Spread Spectrum.

1.4 Video steganography

It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

1.5 Network or protocol steganography

It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc. as cover object. In the OSI layer network model there exist covert channels where steganography can be used.

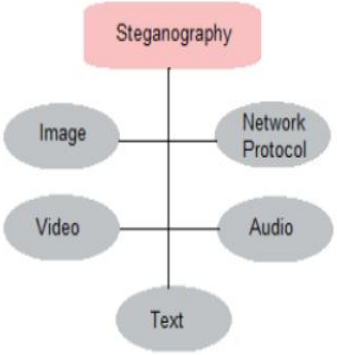


Fig. 1 Steganography types

2. IMAGE STEGANOGRAPHY TERMINOLOGIES

Image steganography has the following terminologies [5]

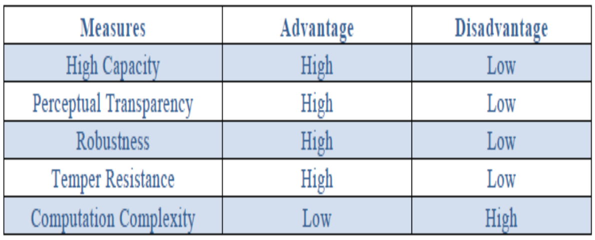
- Cover-Image: - Original image which is used as a carrier for hidden information.
- Message: - Actual information which is used to hide into images. Message could be a plain text or some other image.
- Stego-Image: - After embedding message into cover image is known as stego-image.
- Stego-Key: - A key is used for embedding or extracting the messages from cover-images and stego-images.

2.1 Image steganography classifications

Generally image steganography is categorized in following aspects and Table-1 below shows the best steganography measures.

- High Capacity: - Maximum size of information can be embedded into image.
- Perceptual Transparency: - After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover-image.
- Robustness: - After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.
- Temper Resistance: - It should be difficult to alter the message once it has been embedded into stego-image.
- Computation Complexity: - How much expensive it is computationally for embedding and extracting a hidden message.

Table 1 Image steganography algorithm measures



Measures	Advantage	Disadvantage
High Capacity	High	Low
Perceptual Transparency	High	Low
Robustness	High	Low
Temper Resistance	High	Low
Computation Complexity	Low	High

2.2 Spatial domain methods

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. This algorithm also resists against uniform affine transformations such as cropping, rotation and scaling. The stego key is generated from the message to be embedded. The vertices of the triangle are used for embedding. Spatial domain techniques are broadly classified into

- Least significant bit (LSB)
- Pixel value differencing (PVD)
- Random pixel embedding method (RPE)
- Mapping pixel to hidden data method
- Labeling or connectivity method
- Pixel intensity based method
- Texture based method
- Histogram shifting methods

To be specific, let's discuss about only one of the above algorithms in detail. Let's select least significant bit technique and see how it works.

2.3 Least significant bit algorithm

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works well for image steganography. To the human eye the stego-image will look identical to the carrier image. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used.

To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image files to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP‟s or possibly another image format such as GIF. The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components. Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding.

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

10010101 0000110**0** 1100100**0**
10010111 0000111**0** 11001011
10011111 00010000 1100101**0**

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

2.4 The LSB algorithm

1. Select a cover image of size M*N as an input.
2. The message to be hidden is embedded in RGB component only of an image.
3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
4. After that Message is hidden using Bit Replacement method.

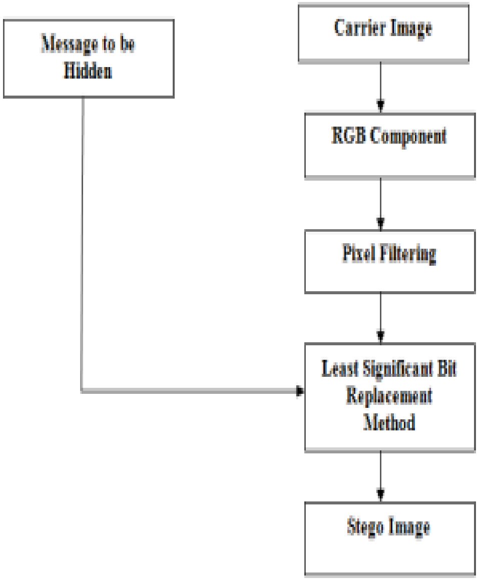


Fig. 2 Least significant bit algorithm

2.5 Transform domain technique

This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain.
Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing.
Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into
a. Discrete Fourier transformation technique
b. Discrete cosine transformation technique
c. Discrete Wavelet transformation technique

2.6 Distortion techniques

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image.
So, information is described as being stored by signal distortion. Using this technique, a stego object is created by applying a sequence of modifications to the cover image.
This sequence of modifications is use to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a “1.” otherwise, the message bit is a “0.” The encoder can modify the “1” value pixels in such a manner that the statistical properties of the image are not affected.
However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.

2.7 Spread spectrum technique

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

2.8 Statistical technique

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

2.9 Masking and filtering

These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

3. IMPLEMENTATION AND RESULTS

All of the approaches to steganography have one thing in common that they hide the secret message in the physical object which is sent. The following figure shows the steganography process of the cover image being passed into the embedding function with the message to encode resulting in a steganographic image containing the hidden message.
A key is often used to protect the hidden message. This key is usually a password, so this key is also used to encrypt and decrypt the message before and after the embedding. Secrets can be hidden inside all sorts of cover information: text, images, audio, video and more. However, there are tools available to store secrets inside almost any type of cover source. The most important property of a cover source is the amount of data that can be stored inside it, without changing the noticeable properties of the cover.
In the following figures we are going to implement steganography technique on the following images.

Fig. 3 Cover image

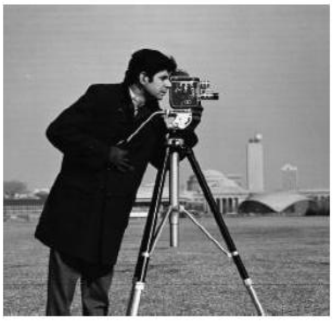


Fig. 4 Secret image

Figure 3 is our Cover Image and Figure 4 is our Secret Image. After applying this technique on it we get the image in Figure 6 which is also known as Stego Image.

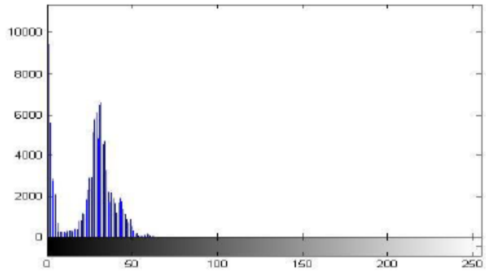


Fig. 5 Histogram of cover image

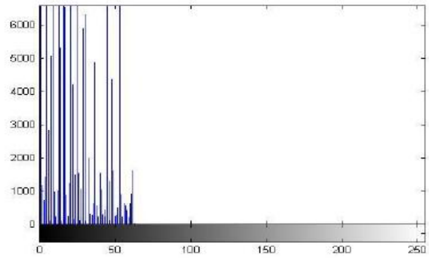


Fig. 6 Histogram of stego image

In the above two figures, Figure 6 shows the histogram of our Cover Image and Figure 7 shows the histogram of Stego Image. As we can see the difference from the histogram both the images has different histogram representation.

CONCLUSION AND FUTURE WORK

As many new application areas are identified like internet banking, mobile communication security, cloud security etc., the insight into the steganographic principles will definitely guide us to identify new areas and to improve its currently working applications in the already existing application areas also. I have tried to understand from the different proposed techniques which most of them show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods. Therefore, to improve the quality of encryption as well as the size of data to be encrypted with a single image (cover image) using the combination of cryptographic algorithm and steganography is helpful.

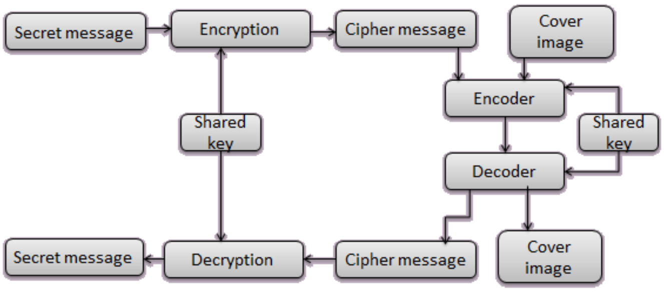


Fig. 7 Combination of cryptographic and steganography algorithms

REFERENCES

[1] Arvind Kumar Km. Pooja Assistant Professor Vankateshwara institute of computer Vidya College of engineering, Meerut, India and Km. Pooja Assistant Professor Vankateshwara institute of computer Vidya College of engineering, Meerut, India Science and technology, Meerut, India, Steganography- A Data Hiding Technique, International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[2] Mehdi Hussain and Mureed Hussain, Shaheed Zulfiqar Ali Bhutto, Institute of Science & Technology, (SZABIST), Islamabad, Pakistan. A Survey of Image Steganography Techniques, International Journal of Advanced Science and Technology Vol. 54, May, 2013 113.

[3] C.P.Sumathi, G.Umamaheswari(Department of Computer Science, SDNB Vaishnav College For Women, Chennai,India.) and T.Santanam (Department of Computer Science, DG Vaishnav College For Men, Chennai, India.) A Study of Various Steganographic Techniques Used for Information Hiding, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[4] Jasleen Kour Deepankar Verma *M-tech Student,Computer Science Assistant Professor, Computer Science R.B.I.E.B.T, India,* Deepankar Verma *M-tech Student,Computer Science Assistant Professor, Computer Science R.B.I.E.B.T, India,* Steganography Techniques –A Review Paper, *International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5) 2014.*

[5] Neha Aggarwal31 Department of computer science, Manav Rachna College of Engineering Faridabad, India,dear.sanya@gmail.com, 2 Department of computer science, Manav Rachna Collegeof Engineering Faridabad, India,Enhanced Least Significant Bit algorithm For Image Steganography, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893, www.IJCEM.org

BIOGRAPHIES

My name is Tesfay gebreslassie Hadera. I received my Bsc. Dgree in Information Technology from Mekelle Institute of Technology (MIT) Mekelle, Ethiopia in 2012. Currently am taking my M –tech in Computer and information technology from Defence University College of Engineering.

In 2012, I joined Metals and Engineering Corporation to work as a software engineer and system designer and I am still working there in this position.