STEGANOGRAPHY: APPLICATIONS, TECHNIQUES AND SECURITY CHALLENGES AND OPPORTUNITIES

Dr. Ashwini Chavan Associate Professor, Dr./ D. Y. Patil Institute of Management and Entrepreneur Development , Varale , Pune
Dr. Ashwini Brahme Associate Professor, Yashaswi Education Society's, International Institute of Management Science (IIMS), Chinchwad, Pune
Dr. Sachin Misal Associate Professor, Yashaswi Education Society's, International Institute of Management Science (IIMS), Chinchwad, Pune

Abstract
Steganography is the science and art of secret communication between two sides that attempt to hide the content of the message. It is the science of embedding information into the cover image without causing a loss in the cover image after embedding Steganography is the art and technology of writing hidden messages in such a manner that no person, apart from the sender and supposed recipient, suspects the lifestyles of the message. It is gaining huge attention these days as it does now not attract attention to its information's existence
Keywords— *DCT, LSB, DWT, steganography, stegano – image*

INTRODUCTION

Is defined as "the art of hiding messages inside media files", in other words, it is the way in which we can hide any message the development of computer and the fast growth of internet usage over high bandwidth and low cost computer hardware to control the quickly growth of the steganography. In the recent years, hidden and secure communication is the primary requirement of people. Steganography is a form of security technique through obscurity; the science and art of hiding the existence of a message between sender and intended recipient. Steganography has been used to hide secret messages in various types of files, including digital images, audio and video. The aim of steganography is hiding the embedded information in the cover image. Cryptography converts secret data into an unreadable form. Normally only one security approach is used at a time by the users either combination steganography and cryptography techniques are the most useful and powerful security techniques, also they can play a very important role in this field

LITERATURE REVIEW

Author :Tseng, Y.C

This paper presents a secure steganography scheme which makes sure that if any modified bit in the cover image should be adjacent to another bit that has the same value as the former's new value. By this way the detection becomes extremely difficult. But for achieving this, data hiding space has to be reduced.

Author: Jessica Fridrich

This paper proposes a highly accurate steganalysis technique which can even estimate the length of secret message embedded in LSB method. In this method, the test image is divided into groups of n consecutive or disjoint pixels. This method exploits the modified pixel values to determine the content of secret message. A discriminating function is applied on the group of pixels. This discriminating function determines the regularity or smoothness of pixels. Then a permutation function called flipping is applied on the pixel groups. By using discriminating function and flipping, Pixels groups are classified in to three categories, i.e. Regular groups, Singular groups and Unused Groups. For a given mask, fraction of Regular groups Rm and fraction of singular groups Sm are calculated. Presence of noise in the image causes Rm to be greater than Sm.

Author: A. Arya, Sarita Soni[2018]

In this paper we review different Steganography techniques which not only hides the message behind the image but also provides security. Data is generally in the form of text, audio, video and image steganography algo can be applied to audio, video, and image file. Hiding secret information in image

file is known as image steganography and in video file is known as video steganography. In this paper have been discussed various techniques & steganography like spatial domain transform domain, vector embedding, and statistical technique, distortion technique, masking and filtering techniques.

Author: Akhtar, N.; Johri, P.; Khan, S [2013]

Implemented a variation of plain LSB (Least Significant Bit) algorithm. The stegano-image quality has been improved by using bit-inversion technique. LSB method improving the PSNR of stegano image. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message.

Author: S. M. M. Karim [2011]

Proposed a new approach that provides very good security to secret data. They use LSB approach with secret key. This secret key is used to hide the sensitive information and this information is stored on different LSB bits of image. This steganography technique use RGB true color images for embedding process. This technique embeds the secret information inside in LSB of the cover image and secret key is used to encrypt the secret information to avoid unauthorized access. Depending upon the secret key used, secret information is randomly stored on different location of LSBs of cover image which make this system more robust and make difficult for attacker to extract the hidden secret information.

Author: Thenmozhi S. and Chandrasekaran, M. [2012]

The optimal pixel change process has been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter.

BASIC MODEL

The basic steganography proposed model as shown in Figure 1 contains two files: First one is a cover image and second is the secret file which will be hidden by a private key to encrypt the secret file. As shown in Figure 1 there are two steps, the first one hide data (embedding technique) and the other to compress it to reduce the spaces and the size of data. The end result of the system is the stegano-image which is the digital image that has the secret message hidden interior. Stegano-image is sent to the receiver via the public communication channel (internet) where the receiver will get the secret data out from the stegano-image by applying an extracting set of rules with the secret password. LSB Substitution: the LSB is one of the first useful coding techniques in steganography.

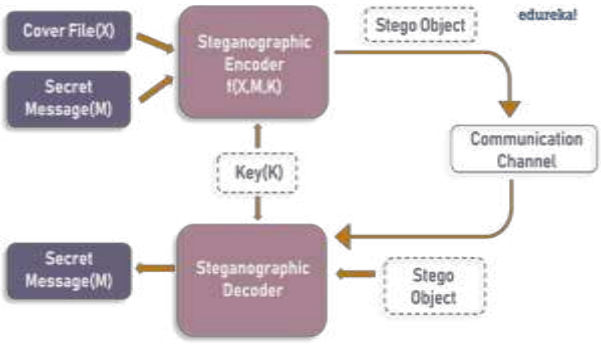

Fig. basic model of steganography

TYPES OF STEGANOGRAPHY

Depending on the nature of the cover object steganography can be divided into four types this type is will be as follows:-

- **Text Steganography**
- **Image Steganography**
- **Audio Steganography**
- **Video Steganography**

TEXT STEGNOGRAPHY

Text steganography is a mechanism of hiding secret text message inside another text as a covering message or generating a cover message related with the original secret message. The structure of text documents is identical with what we observe, while in other types of documents such as in picture, the structure of document is different from what we observe. Therefore, in such documents, we can hide information by introducing changes in the structure of the document without making a notable change in the concerned output. Text steganography can be broadly classified into three types: Format based Random and Statistical generation, Linguistic methods.

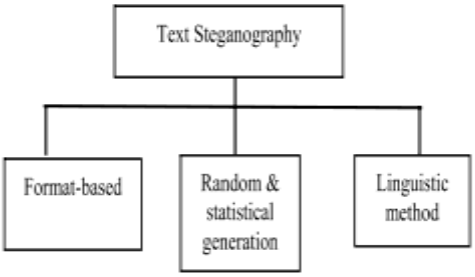

Fig. Text Steganography

IMAGE STEGNOGRAPHY

In image steganography, a message is embedded into an image by altering the values of some **pixels**, which are chosen by an encryption algorithm. The recipient of the image must be aware of the same algorithm in order to known which **pixels** he or she must select to extract the message by looking at repetitive patterns, you can detect hidden information in stegano - images. These repetitive patterns might reveal the identification or signature of a steganography tool or hidden information. Even small distortions can reveal the existence of hidden information.

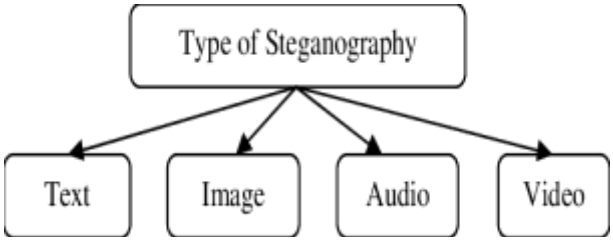

Fig. types of steganography

AUDIO STEGANOGRAPHY

Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is the science of hiding some secret text or audio information in a host message. In this type of steganography we can embed secret messages into digital sound in audio steganography. It is more complex process as compare to embedding messages in other media. This steganography method can embed messages in WAV, AU And even MP3 sound files

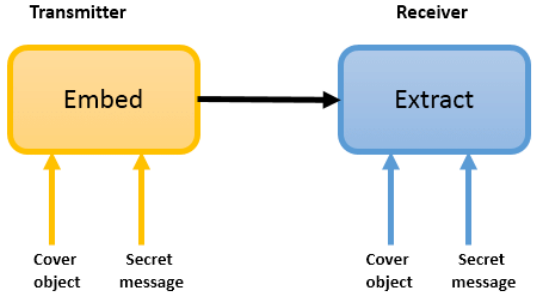

Fig block diagram of audio steganography

VIDEO STEGANOGRAPHY

Video Steganography is a technique to hide any kind of files into a cover Video file. The use of the video based Steganography can be more secure than other multimedia files, because of its size and complexity. Steganography technique refers to methods in which data. hiding is performed directly on the pixel value of cover. image in such a way that the effect of message is not. visible on the cover image.

STEGANOGRAPHY TECHNIQUES

Steganography technique refers to methods in which data. hiding is performed directly on the pixel value of cover. image in such a way that the effect of message is not. visible on the cover image. The most common method is by embedding information into digital images the steganography techniques is as follows:-

- Least Significant Bit
- Discrete Cosine Transform
- Discrete Wavelet Transform
- Speed Spectrum
- Palette Based

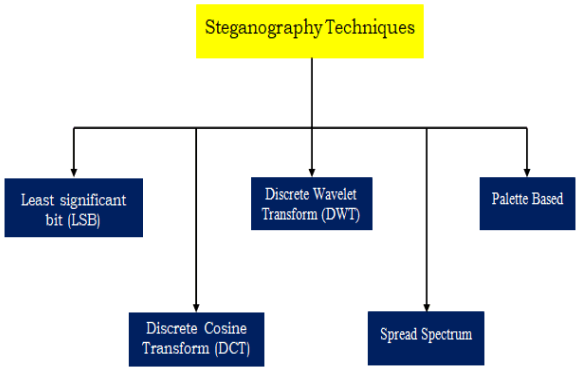

Fig. Steganography Techniques

Least Significant Bit

LSB is the one of the oldest and simplest algorithms that allows users to hide their information using spatial domain [16; 38]. The human eye cannot recognize the difference that occurs in the two first bits in each pixel. In other words, the change in the least significant bit does not affect the image's quality. Least Significant Bit steganography is one such technique in which least significant bit of pixels of the image is replaced with data bits. This approach has the advantage that it is simplest one to understand, easy to implement and results in stegano -images that contain embedded data as hidden. For example, two pixels of an RGB image color will provide six bits for watermarking. To encode a message

Discrete Cosine Transform(DCT)

In this tool the data will divide into some blocks often 8 by 8 or 16 by 16 blocks. Then, applying a discrete cosine transform on each block will convert the signal into high, middle and low frequencies. Low frequency is very close to original data while the middle and high frequencies are more details of the data. is proposed which embeds secret image in frequency domain of cover image with high matching quality.

Discrete Wavelet Transform(DWT)

It is a tool to transform the signal or data from one domain which is a spatial to another domain which is a frequency. In the frequency domain the signal splits into the two half one of them is high frequency and another is low frequency. Four parts or sub bands of decomposed signal are LL, LH, HL and HH frequencies which are low-low, low-high, high-low and high-high frequencies. Converting the spatial field in the frequency domain usually done using Wavelet transform. The use of wavelets in the form

of shorthand model lies in a statement that the wavelet transform is obviously splits the high from the low-frequency information based on pixels

Spread Spectrum

There are many algorithms using original data, such as video, image, audio, and text, to hide specific information like logos or personal signatures in a spatial domain. In other words, if the original data is an image, processing would be into the pixel values without changing the data into another domain. Our method of spread spectrum image steganography (SSIS) is a steganography communication method that uses digital imagery as a cover signal. ... The fundamental concept is the embedding of the hidden information within noise, which is then added to a digital cover image.

Palette Based

Embedding messages into the palette; embedding into the image data. The advantage of the first method is that it will probably be easier to design a secure method under some assumptions about the noise properties of the image source. Palette based or Indexed colours image that enables 8 bits per pixel or less to look almost as good as 24 bits per pixel. The technique determines the 256 most frequently used colours in the image and creates a colour lookup table, also called a colour map or colour palette, which is stored with the image. Rather than each pixel in the image having all three RGB colours (one 8-bit red, one 8-bit green and one 8-bit blue), each pixel contains one 8-bit number that indexes into the 256-color lookup table, which contains the RGB values. This is reducing images to their smallest size and these images are most commonly used on Web pages, as they are small and quick to load. The 256-color palette is mapped for best results on the Internet. Result shows that the method outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity.

CONCLUSION

This paper presents a various steganography technique and steganography types. It was also seen that the most of the papers used by the LSB Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. In the near future, the most important use of steganography techniques will probably be lying in the field of digital watermarking. The possible use of steganography technique is as following:-

- Hiding data on the network in case of a breach.
- Posting secret communications on the Web to avoid transmission.
- Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.

REFERENCES

1. https://en.wikipedia.org/wiki/Steganography
2. Afrakhteh, M., & Ibrahim, S. (2010, 25-27 June 2010). Adaptive steganography scheme using more surrounding pixels. Paper presented at the Computer Design and Applications (ICCDA), 2010 International Conference on
3. https://youtu.be/xepNoHgNj0w
4. https://youtu.be/By4TM8ikAps
5. https://www.researchgate.net/publication/278329938_A_Review_on_the_Various_Recent_Steganography_Techniques
6. https://www.researchgate.net/publication/308646775_An_introduction_to_steganography_methods
7. https://www.researchgate.net/publication/292310394_Image_Stegography_Techniques_An_Overview