IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016.

Image Steganography: A Review

Er. Munish Katoch[1], Reenu Jaswal[2]

Assistant Professor, Computer Science and Engineering, Sri Sai University, Palampur, India[1]

Student, Computer Science and Engineering, Sri Sai University, Palampur, India [2]

Abstract*:* In the recent years, the security related to data over the internet has become a major issue. In order to solve the problem, two main techniques are used, first is cryptography and second is Steganography. Both are used for data security purpose. Cryptography changes the form of the data and Steganography completely Conceals its presence from the users, except the intended receiver. In this paper, a technique is used which combines these two methods to provide a more efficient and effective result. Therefore different cryptographic algorithms are compared on the basis of Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR)

Keywords: Steganography, Visual Cryptography, Steganography Techniques, Stego Image.

I. INTRODUCTION

Many times, users on the internet have to send, share or receive confidential information .Due to rapid development in both computer technologies and Internet, the security of information is regarded as one of the most important factors of Information Technology and communication. Steganography has emerged as a powerful and efficient tool which provides high level for security particularly when it is combined with encryption. Steganography, hides the existence of message such that intruder can't even guess that communication is going on and thus provides a higher level of security.

II. STEGANOGRAPHY

The term Steganography was first introduced by Johannes Trithemiu in 1499. Steganography is a combination of two words Stegano + Graptos. Stegano means "Covered" and Graptos means "Writing" which exactly means "cover writing". So Steganography means covered writing. Steganography is a exclusive technique of hiding data in some medium so that it doesn't awaken doubt to the hackers. The key concept behind Steganography is that message to be transmitted is not detectable to the casual eye.. In this, the sender embedded its message into the text, image, video, or audio file so that hackers will not be aware of the message. This is not a new technique, it is very old. The most well-liked Steganographic methods used by spies contain invisible ink and microdots. People used design messages in wooden tablets and covered with wax. They used tattooing a shaved messenger's head, letting his hair grow back and then saving it again when he arrived at his contact point to reveal the message.

III.VISUAL CRYPTOGRAPHY

Visual Cryptography scheme was introduced by Naor & Shamir in 1994. Visual Cryptography is a technique which allows visual information (pictures, text, etc.) to be encrypted in the way that decryption becomes a mechanical operation. Visual Cryptography contains two transparent images.

- One image contains random or noisy pixels.
- Other image contains the secret data. It is almost impossible to retrieve the secret information from encrypted images.

Both transparent images and layers are essential to disclose the information. In order to implement a Visual Cryptography, the easiest way is to print the two layers onto one transparent sheet.

The main advantage of visual cryptography scheme is :

- it eliminates computation problem during decryption process, and the secret image can be restored by stack operation. This property makes the visual cryptography especially useful for the low computation method. It is a secret sharing scheme with good security for binary image.
- It decodes directly during human vision.

IV. NEED OF STEGANOGRAPHY

Currently, the use of internet increasing quickly. One of the most important area which attracted by people is security is related to internet and also related to communication. At present, security for hiding data is most popular technique which receives more attention than cryptography. Various methods such as cryptography, coding Steganography, etc. are used for hidden communication. The major benefit of Steganography over other coding techniques is that it hiding the data inside other data in such a way that no other person recipient, even know the existence of it. Terms used in Steganography are**:**

- *Cover Image*: The medium in which information is to be hidden. It may be an audio, video, image or a text file.
- *Key:* It's a secret value which help in encoding or extraction of data, without which data cannot be encode and extract.
- *Stego-image*: A medium within which information is hidden.
- *Messag***e**: The data to be hidden or to be extracted.

DOI 10.17148/IJARCCE.2016.54203

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016.

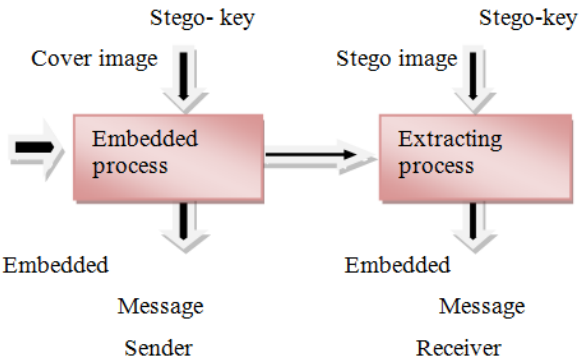


Figure 1: General Block Diagram of Steganography

For Steganography, the size of cover image can be of any size -8 bit, 24 bit, 32 bit, 36 bit. The image can be in any format either jpeg, gif, bmp, etc. we have a key which is used to select the random pixels in which data is to hide. Therefore Stego image is generated which is send to another person. Now on the receiver side the Stego image is processed and extraction of message can be done with the help of secret key. The key is the one by which receiver knows the position of the pixel on which message is rooted.

V. CLASSIFICATION OF STEGANOGRAPHY

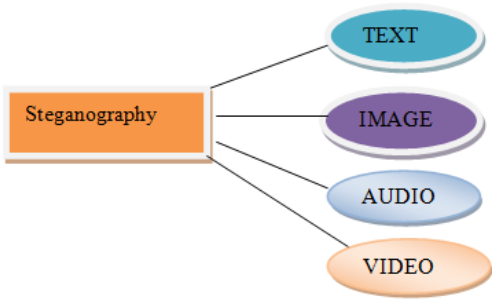
- Text based Steganography.
- Image based Steganography.
- Audio based Steganography.
- Video based Steganography.

A. *Text-based Steganography*
In this, the message that is to be sent is rooted firstly in a text file by formatting. The format it based on line-shift coding, word-shift coding, feature coding etc. Reformatting of the text destroys the rooted content hence the technique is not robust.

B. *Audio Steganography*
This Alters audio files so that they contain hidden messages. The techniques are LSB manipulation, phase coding and echo hiding.

C. *Image Steganography*
This Steganography hides the message in the images. This is the most popular technique because of the fact that almost no perceivable changes occur. Some of the commonly used methods of embedding payload in cover image are least Significant Bits (LSB) substitution in which the LSBs of cover image pixel are altered to hide the payload and more data can be hidden in edges.

D. Video Steganography
Video Steganography is a technique to hide files or information into digital video format. Video is used as carrier for hidden information. Generally discrete cosine transforms (DCT which is used to hide the information in each of the images in the video, which is not visible by the human eye. Video Steganography uses such as H.264, Mp4, MPEG, AVI or other video format.



VI. STEGANOGRAPHY TECHNIQUES

There are some approaches in classifying the Steganography techniques are given below:

E. *Substitution Technique*:
These techniques try to encode secret data by substituting insignificant parts of the cover image by secret data bits. It consists of many techniques such as least significant bit substitution, pseudorandom permutation etc.

F. *Transform Domain Technique:* -
These techniques conceal message in a significant area of the cover image which makes them stronger to attack. It consists of DCT, DWT methods.

G. *Spread Spectrum Technique*: -
In this technique, it tries to extend a secret message over a cover, in order to make it impossible to recognize. By this technique, it is hard to remove the embedded message. It includes two types of methods: -one is direct sequence method and second is frequency hopping.

H. *Distortion Technique*: -
This technique requires the knowledge of original cover in the decoding process. Most text based hiding methods are of distortion type.

VII. FACTORS AFFECTING ON STEGANOGRAPHY

Some factors that determine how efficient and Powerful a technique is are as follows:

I. *Robustness*:
Robustness refers to the ability of embedded data to remain unbroken if the stego image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations.

J. *Imperceptibility:*
The invisibility of a Steganographic algorithm is the first and foremost requirement, since the strength of Steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

K. *Payload Capacity*:
It refers to the amount of secret information that can be hidden in the cover source. Watermarking needs to embed

DOI 10.17148/IJARCCE.2016.54203

only a small amount of copyright information, on the other side, Steganography aims at hidden communication and therefore requires sufficient embedding capacity.

L. *PSNR (Peak Signal to Noise Ratio):*
It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the reliability of its representation. This ratio is mainly used as a quality measurement between the original and compressed image. The higher the PSNR, the better the quality of the compressed image

M. *MSE (Mean Square Error):*
Mean Squared Error is the average squared difference between a reference image and a distorted image. An Image Steganography technique is able if it gives low MSE.

N. *SNR (Signal to Noise Ratio)***:** It compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power.

VIII. APPLICATION OF STEGANOGRAPHY

O. Secret Communication
By using Steganography, two parties can communicate secretly without anyone knowing about the communication and in Cryptography, only encode the message but its presence is not hidden. Thus draws unwanted attention. On the other hand, Steganography hides the existence of message in some cover media.

P. *Copyright Protection*
In this, secret message is embedded in the images which serves as the watermark and thus identify it as an intellectual property which belongs to a particular owner. This is basically related to watermarking.

Q. Feature Tagging
Features such as captions, annotations, name of the individuals in a photo or location in a map can be embedded inside an image. Copying the stego image also copies all of the embedded features and only parties who possess the decoding stego key will be able to extract and view the features .

R. Use by terrorists
Steganography can also be used by terrorists in order to hide their secret messages in innocent, cover sources to spread terrorism across the country. Rumours were spread about terrorists using Steganography when the two articles titled “Terrorist instructions hidden online” and “Terror groups hide behind Web encryption” were published in newspaper.

S. *Digital Watermarking*
This is the most important applications of Steganography. It basically embeds a digital watermark inside an image. This Watermark is used to verify the authenticity or integrity of the carrier signal. It is highly used for tracing copyright infringements and for banknote authentication.

IX. RELATED WORK

Authors have proposed a latest method designed for securing the online payment system using visual cryptography and text based Steganography. The planned text based Steganography is derived from Vedic Numeric Code which uses characters of English language. In this Paper, there are 3 users are considered Customer, Online merchant. The customer is provided by a unique authentication password related to the bank which is encrypted using text based steganography and visual cryptography. And one share obtained by this process is kept in CA‟s database and other by the customer. During online shopping the online merchant directs the customer to the certified authority portal. In this portal the customer submits his share and the merchant submit his account details. Then the CA combines the customer submitted share with its own share and obtains the original image. The CA forwards the cover text and the merchant bank details to the bank where the authentication password is recovered from the cover text. The CA then sent the customer authentication information to the merchant. When the bank receives the authentication password it will compared with the bank database and verify. If the verification is successful the fund is transferred from the customer account to the merchant account. Certified authority(C A). Nadeem Akhtar [3], planned the variation in plain LSB algorithm by using bit inversion technique. In this RC4 algorithm is used in order to achieve the randomization of message bits before hiding the message bits into the cover image. The result shows improvement in security as well as quality. In 2013, Mamta Juneja et al.[3], introduced an approach to insert the text into gray scale image using RC4 stream cipher method and after that it stored the text in non sequential pixel in image by use of variable hop value power. In this approach, robustness increases due to multilevel security architecture along with faster embedding and extraction process. Zaidoon Kh. et al**.** [4], have given a general overview of Steganography types, general Steganography systems, and characterization of Steganography systems and categorization of Steganography techniques.

A. M. Hamid and M. L. M. Kiah [5], authors have proposed a data hiding technique, this method used LSB technique in order to finds out the shady area of the image to hide the data. It converts the binary image and labels each object using 8 pixel connectivity schemes for hiding data bits. This method required high computation to find shady area. and has not tested on high texture type of image. Its hiding ability totally depends on texture of image.

Hamid et al.[6], have proposed a texture based image steganography. In this technique, the texture area is divided into two groups by texture analysis, Simple texture area and Complex texture area. In Simple texture, it is used to hide the 3-3-2 LSB (3 bits for Red, 3 bits for Green, 2 bits for Blue channels) method and in Complex texture area 4 LSB embedding technique is applied for information hiding. The above method used the both (2 to

4 LSB for each channel) methods depending on texture classification for better visual quality. Proposed method has high hidden capacity with considering the perceptual transparency measures e.g. PSNR etc .H. Motameni [7] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a Stego-key. This private Stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in Stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for colour image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

X. CONCLUSION

In this paper, an overview on Steganography is described and basic working of Image Steganography along with various insertion techniques used in Image Steganography. This paper also deals with Steganography Software and Applications. The target of this paper is to implement two techniques like Steganography and Cryptography for confidential communication between the two entities and also deals with security and privacy.

REFERENCES

[1] Souvik Roy, P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," 2014 IEEE Students" Conference on Electrical, Electronics and Computer Science.

[2] Nadeem Akhtar, Pragati Johri and Shahbaaz Khan, "Enhancing the Security and Quality of LSB Based Image Steganography", Proceedings of IEEE International Conference on Computational Intelligence and Communication Networks, pp.385-390 September 2013,

[3] Mamta Juneja and Parvinder S. Sandhu, "An improved LSB based Steganography with Enhanced Security and Embedding/ Extraction", Proceedings of IEEE International Conference on Intelligent Computational Systems, , pp. 29-34 January 2013.

[4] Zaidan, B.B Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography", Journal of Computing, pp.158-165 vol.2, March 2010,

[6] A. M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, (2009).

[7] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, (2007).

DOI 10.17148/IJARCCE.2016.54203