Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review of Methods and Approaches of Data Security using Steganography

Arshdeep Kaur
M.Tech Student,
Department of CSE, GZSPTU,
Bathinda, Punjab, India

Jyoti Rani
Assistant Professor,
Department of CSE, GZSPTU,
Bathinda, Punjab, India

Abstract— By the advancement of information transformation, the security of information is top concern of any organization. Main objective of Steganography is to hide the information in cover object and make the presence of information undetectable so that it cannot be accessed by unauthorized person. Many Steganography approaches are used to conceal the data in other information for secure data transmission. This paper provide an overview of steganography and give brief description of current major steganography techniques in spatial domain and transform domain like LSB Substitution, PIT, PVD, Edge Based, DCT, DFT, DWT etc. so the initiators who are going to explore this area can get basic knowledge of steganography and its existing techniques.

Keywords— Data Security, Stegangraphy, Embedding data, Cover object, stego object, robustness, imperceptibility.

I. INTRODUCTION

As the invention of computer and internet the world becomes connected with each other and there remains no barrier to the communication between two people. Now-a-days people can share and transfer their information by telecommunication services like telephone and internet etc. Internet is the quick and easy way for information communication. But as the increase in the ease of information transformation, the security of information is top concern of any organization. There are also some unwanted people exits who want to access private and personal data for some illegal purpose. So there is a requirement to protect and secure the information when it is transferring to other person.

Cryptography has been created on the concept of encryption and decryption that scrambles the information and makes its cipher text in order to keep the content of information secret. But in some cases it may also be necessary to keep the existence of message secret. This science is called Steganography.

Steganography is the art of hiding the information into other information. Steganography derived from Greek words "stegos" means "cover" and "graphia" means "writing" defining it as "covered writing" [1]. To send the information in a secure manner the secret information is concealed into cover object and sent to other party in such a way that no one can imagine there is any communication takes place. Main objective of Steganography is to hide the message and make the presence of message undetectable so that it is also called covert communication [13]. Steganography built from cryptography, they work as different ways but both are used for similar purpose to protect the information from outsider and attacker. Many steganograpy approaches and techniques have been developed by the researchers. The aim of this paper is to give a brief description of steganographic terms and techniques to the fresher who want to discover more in this field. Throughout the history, people used some tricks and methods for secret communication. For example, to send a secret message the head of a person was shaved and tattooed an image or a message on his head. After the hair grew back, the message would be undetected until the head was shaved again [1]. Invisible inks also used early in World War II for invisible writing. As the advancement of technology, the way of sending secrets become digital. In digital steganography the sender embed the secret information into cover object by using embedding process and create a stego object which is transmitted to receiver who extracts the hidden information by extraction process with a secret key that is used for authorization purpose as shown in fig 1. The cover object is a file that is used to store the secret information. A cover object can be in the form of an image, binary file, audio, video etc.

This paper is structured as follows: Section 2 describe various types of steganography based on cover objects. Section 3 reviews the study of existing methods and approaches of steganography. Section 4 represent different criteria's and performance measures for evaluating steganography techniques and Section 5 presents the conclusion of the paper.

The basic architecture of steganography is as under:-

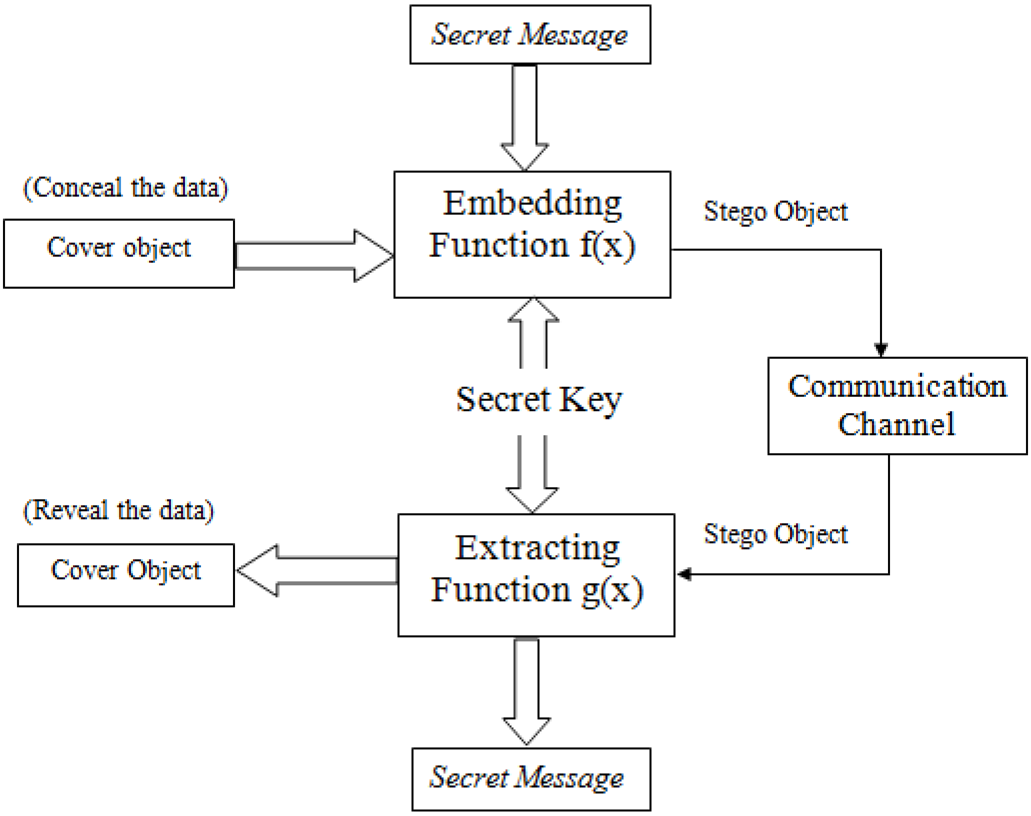

Fig 1: Basic Architecture of Steganography

II. TYPES OF STEGANOGRAPTY

Different types of steganography are:

A. Text Steganography: Text files are used as a cover object and message can be in text form. In text steganography the words and lines are altered in order to hide the data. Different techniques for text Steganography are line shifting, word shifting and feature coding etc.

B. Image Steganography: Images in different formats like JPEG, BMP, and GIF etc. are used as a cover media. An image is more preferred media for Steganographic purpose because it can be easily spread out and transmitted by digital means and there is wide area in pixel bits for conceal the data. Image Steganography methods take the benefits of limited human visual perception of color images.

C. Audio Steganography: Audio files are used as a cover media like WAV files, MP3 etc. Different methods of audio Steganography are LSB coding, spread spectrum method, phase coding etc. Audio files have limited payload capacity than other types of Steganography.

D. Video Steganography: Video files like MP4, AVI, MPEG etc. are used as a cover media. Data can be hidden in frames and audio file so that large amount data can be embedded.

E. Protocol Steganography: Network protocols like TCP, UDP, IP, ICMP etc. are used as a cover object. Some header part of TCP/IP packets is optional and can be used as a means of secret communication. But if the firewall configuration of a system is on then there is chances of data lost.

III. STEGANOGRAPHY TECHNIQIES

Many data hiding techniques have been developed by past few years and many research activities are going on to ensure the data security. The Steganography techniques are divided into following fields:

A. Spatial Domain techniques

In this technique the secret data is embedded directly into the pixels. The basic principle of spatial domain technique is to manipulating the pixels values. Spatial domain techniques are as below:

1) LSB Substitution: Least significant bits substitution is simple and mostly used approach for embedding data. The message is converted into binary form and is embedded on LSB bits of image pixels either sequential or in selected pixels. For 24 bits color images 3bits of data is embedded in each pixel. For example it takes 3 pixels to embed S alphabet in 24 bits image. Suppose the values of 3 pixels are:

(00101101 00110010 11010010)
(10110011 11010001 00110010)
(01100101 10011010 01110011)

Binary representation of S is (01010011). After embedding values of pixels are:
(0010110**0** 0011001**1** 11010010)
(10110011 1101000**0** 00110010)
(01100101 1001101**1** 01110011)

Only 4 bits are changed from original bits values. As the changes are negligible, it creates little visual distortion in original image. There are more similar techniques are also developed like Stego1Bits, Stego2Bits, Stego3Bits, Stego4Bits and StegoColourcycle which replace 1, 2, 3 and 4 LSB bits of one of RGB value of pixel with secret data. StegoColourcycle involve cycling method to embed the data on RGB Color palette in pixels. But LSB substitution is easily detected by steganalysis tools and has less robustness. [1], [4]

2) Pixel Indicator Technique (PIT): PIT is extended technique of previous LSB substitution technique. This approach is work only on 24-bits RGB color images. In this method 2 LSB's of one channel is taken as indicator of the presence of secret data in the other two channels. The order of indicator channel and embedding channel can be taken as: RGB, RBG, GBR, GRB, BRG and BGR. This method gives better security and data capacity by effecting 6 bits of one pixel. [5]

3) Pixel Value Differencing (PVD): Pixel Value Differencing method is edge based LSB Steganography. The rate of data insertion depends upon whether the pixel is an edge or a smooth area [6]. In PVD approach first divide the image into non overlapping blocks of 2 consecutive pixels labeled as Pn and Pn+1.

Then take the difference Dn of two pixels into the block as:

$$Dn=|Pn+Pn+1|$$

Categorize each block according to the three levels as lower, medium and higher level. If the block has higher difference value then it will fall under higher level and more number of data bits can be embedded into block of pixels. The range of levels can be categorized as:

Table I. Pixel range table

Levels	**Range**
Lower level	R=(0~15)
Middle level	R=(16~31)
Higher level	R=(32~255)

This method has high payload capacity and imperceptibility but has one drawback that range of levels is also needed to send for retrieval process. [7]

4) Edge based techniques (EBT): Along with PVD, various edge based techniques are developed for steganography. The main idea behind these techniques is that edges can bear more variation than smooth areas without being detected. Edge based algorithms like first filter algorithm that uses edge detection filters like Laplace formula and sobal filter. Other algorithms are adaptive filtering based image steganography, random edge LSB, hybrid edge detection, canny edge detector etc. These techniques based on the concept that changes or modification in features of image is less recognized by human eyes. High frequency components of spatial image are used to hide the data in image and give better PSNR and capacity. [7]

Four neighbor, diagonal neighbor and 8 neighbor method utilize the information of neighbor pixels. The relationship of a pixel with its neighbor pixels decides whether it is smooth or edge based area. The amount of data to be embedded into a pixel depends upon its surrounding area.

B. Transform Domain Techniques

In this technique the image is mathematically transform into frequency domain and data is embedded into transform coefficients of image. This method is complex but has more robustness than spatial domain methods. Various transform domain techniques are:

1. Discrete Cosine Transformation (DCT)
2. Discrete Fourier Transformation (DFT)
3. Discrete Wavelet Transformation (DWT)

1) Discrete Cosine Transformation: DCT is widely used technique. It separates the image into high, middle and low frequency components [4]. There are different algorithms are developed that are used the DCT transformation like Jsteg, Outguess, F5.

Jsteg algorithm is known to be first algorithm that is used for JPEG images. The image is transform into frequency domain by DCT transformation and data is embedded into LSB of DCT coefficients. But Jsteg is easily detected by steganalysis tools like chi-square attack [8].

Jsteg algorithm has drawback that it embed secret data in LSB's of DCT coefficients sequentially, outguess algorithm this drawback and uses a Pseudo-random-number-generator (PRNG) for randomly selection of DCT coefficients skipping the 0 and 1 value [3].

F5 algorithm is different from other algorithms in a manner that it does not alter or overwrite the LSB of DCT coefficients. It just increment/decrement the LSB's of DCT coefficients based upon situations. F5 is more secure and has better payload capacity [3].

2) Discrete Fourier Transformation (DFT): In Fourier transformation image is decomposed into a weighed sum of 2-D sinusoidal form. After converting the image into frequency domain data is embedded. Inverse Fourier Transformation is applied for retrieval of original image.

3) Discrete Wavelet Transformation (DWT): DWT is better than DCT transformation because DWT separate the low frequency components and high frequency components on a pixel by pixel basis [9].

IV. PERFORMANCE MEASURES FOR STEGANOGRAPHY TECHNIQUES

There are some criteria's for evaluating the Steganography techniques. However it is difficult to have all characteristics in same algorithm because there is some trade-off between these characteristics.

A. Payload Capacity: The amount of data or information that can be embedded in cover object. Capacity of data embedding depends upon cover object and type of secret data to be embedded.

B. Robustness: It can be defined as if image undergoes any operation like transformation, rotating, scaling, cropping, blurring or compression, the embedded data should not be damaged and remain intact by these attacks [4].

C. Imperceptibility: This is the main feature of Steganography algorithm. It is the ability of Steganography techniques to make the message undetectable and hidden. The difference between original image and stego image should be insignificant. This can be achieved by making little distortion on original image and hide the data on noisy areas.

D. Security: The level of security depends upon complexity of algorithm and secret key which is used for security of information so that in case if attackers detect the presence of hidden information he could not reveal the information by any steganalysis tool.

The parametric evaluation of different steganography methods is represented in table II on the basis of data capacity, data security and imperceptibility by three levels as low, medium and high.

Table II. Parametric evaluation of steganography methods

Method	**Parametric evaluation (in three levels)**		
	Data Capacity	**Data Security**	**Imperceptibility**
LSB	High	Low	High
PIT	High	Medium	Medium
PVD	Medium	Medium	High
EBT	Medium	High	High
DCT	Medium	Low	High
DFT	Medium	High	High
DWT	Medium	High	High

V. CONCLUSION

Steganography is science of secret communication. Basic property of steganography is to conceal the actual information into other information so that unwanted people cannot access the information. However like any other science steganography can be used for ill purposes as there are more useful applications of steganography or it can be misused. It is the perception of human who can use it as some positive manner or any negative manner. This paper provides the review and analysis of steganography and its major techniques mainly in spatial domain and transform domain so that the initiator who wants to explore this field can take the basic requirements and an overview of existing steganography techniques. The main problem of most common steganography methods is that they can be easily detected or more complex and struggle with their drawbacks. So there is a need to develop such an undetectable and advanced algorithm that is resistant to image processing operation like cropping, transformation, compression and noise impulse and contain proper balance of steganography parameters. Many steganalysis tools and techniques are developed to fail the existing steganography techniques which are based on LSB, DCT etc. and these steganalysis techniques easily detect the presence of message in cover object. So to advance this field there is need to design some efficient steganography techniques and methods that concentrate on two basic requirements of steganography that is capacity and level of security and such a method that barely affect the quality of original image and prevent the contents of information.

REFERENCES

[1] Johnson N. F., Jajodia S., *"Exploring steganography: Seeing the unseen."* 1998 IEEE Computer, pp.26-34, February 1998.

[2] Chanu Y. J., Tuithung T., Singh Kh. M., *"A short survey on image steganography and steganalysis techniques."* Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on, pp. 52-55. IEEE, March 2012.

[3] Roy R., Changder S., Sarkar A, Debnath N. C., *"Evaluating image steganography techniques: Future research challenges."* In Computing, Management and Telecommunications (ComManTel), 2013 International Conference on, pp. 309-314. IEEE, 2013.

[4] Kaur S., Bansal S., Bansal R. K., *"Steganography and classification of image steganography techniques."* In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on, pp. 870-875. IEEE, 2014.

[5] Gutub, Adnan Abdul-Aziz., *"Pixel indicator technique for RGB image steganography."* Journal of Emerging Technologies in Web Intelligence, Vol. 2, no. 1 (2010) pp. 56-64, Feb 2010.

[6] Wu H. C., Wu N.I., Tsai C. S., Hwang M. S., *"Image steganographic scheme based on pixel-value differencing and LSB replacement methods."* IEE Proceedings-Vision, Image and Signal Processing, Vol. 152, no. 5 (2005), pp. 611-615, 2005.

[7] Singla D., Juneja M., *"An analysis of edge based image steganography techniques in spatial domain."* In Engineering and Computational Sciences (RAECS), 2014 Recent Advances in, pp. 1-5. IEEE, March 2014.

[8] Cheddad A., Condell J., Curran K., Kevitt P.M., *"Digital image steganography: Survey and analysis of current methods."* Signal processing, Vol. 90, no. 3 (2010), pp. 727-752 March 2010.

[9] Kaur R., Singh B., *"Survey and Analysis of various steganographic techniques"*, Internal Journal of Engineering Science & Advanced Technology, Vol 2, Issue 3, pp. 561-566, May-June 2012.

[10] Bairagi A., Mondal S., Ddebnath R., *"A Robust RGB Channel Based Image Steganography Technique Using A Secret Key"* IEEE 16th International Conference Of Computer And Information Technology,pp. 81-87, March 2014

[11] Hossain M., Haque S. A., Sharmin F., *"Variable rate steganography in gray scale digital images using neighborhood pixel information."* In Computers and Information Technology, 2009. ICCIT'09. 12th International Conference on, Vol. 7, pp. 267-272. IEEE, 2009.

[12] Goswami. S, Goswami J., Mehra R., *"An efficient algorithm of steganography using JPEG colored image."* In Recent Advances and Innovations in Engineering (ICRAIE), 2014, pp. 1-5. IEEE, May 2014.

[13] Garg M., Wasson V., *" Data Security with Image Clustering using Hopping Neighbour Technique"* International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 9,pp.628-634, September 2014

[14] Raja K. B., Chowdary C. R., Venugopal K. R., Patnaik L. M., *"A secure image steganography using LSB, DCT and compression techniques on raw images."* In Intelligent Sensing and Information Processing, 2005. ICISIP 2005. Third International Conference on, pp. 170-176. IEEE, 2005.