International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 6, Issue 1 (January 2017), PP.68-71

Survey Paper on Steganography

Namrata Singh
Computer Science and Engineering ABES Engineering College, Ghaziabad A.K.T.U

Abstract: Steganography is an art for hiding the secret information inside other information which are digitally cover. The definition of steganography can also be given as study of unseen communication that usually deals with existence of communicated message. The hidden message can be text, audio, image or video accordingly to that it can be cover from either image or video. In steganography, hiding information achieved to insert a message into cover image which generates a stego image. In this paper, we have analyze various steganography methods and also covered classification and applications.
Keywords: Steganography, Data Hiding, Encryption, Stego-File, Video, Image

I. INTRODUCTION

In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. In order to share the information in a concealed manner two techniques could be used. These mechanisms are cryptography and steganography. . In cryptography, the message is modified in an encrypted form with the help of encryption key which is known to sender and receiver only. The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arouse attacker's suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, steganography techniques have been developed. Steganography is the art and science of communicating in such a way that it hides the existence of the communication. Thus, steganography hides the existence of data so that no one can detect its presence. In steganography the process of hiding information content inside any multimedia content like image, audio, video is referred as a "Embedding". For increasing the confidentiality of communicating data both the techniques may be combined. The remaining paper consist of following section: II. Steganography III. Conclusion and Future Work.

II. STEGANOGRAPHY

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos, meaning "covered, concealed, or protected", and graphein meaning "writing".

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

The Steganography Method Used should have:

a) Imperceptibility: The video with data and original data source should be perceptually identical.
b) Robustness: The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.
c) Capacity: Maximum data embedding rate.
d) Secrecy: Extraction of hidden information from the video must not happen without prior permission of intended user having password.
e) Accuracy: The extraction of the hidden data from the medium should be accurate and reliable.

III. TERMINOLOGIES STEGANOGRAPHY

- Message: The Secret message which is meant to be sent/transmitted safely is known as Message.[3]
  - Cover-object: Cover Object is basically the object in which the data is to be hidden. It may be image, video and Audio.
  - Stego-object: The object carrying the secret message is known as stego object.
  - Stego-key: Key used for encrypting and decrypting the secret message..
  - Embedding algorithm: Algorithm used to hide the message In the cover.
  - Extracting algorithm: An algorithm used to unhide/uncover the message from the stego object.

IV. TYPES OF STEGANOGRAPHY

Depending on the type of the cover object there are many suita)e stenographic techniques which are in order to obtain security.[1][4]

a) Image Steganography: The process of concealing the secret message in an image file is known as image steganography. It has certain limitations like you cannot embed a large amount of data in an image because it may distort which may arise suspicion that the image might contain any information.

b) Video Steganography: The process of concealing the secret message in an Video file is known as Video steganography. Video Steganography is far more safe and efficient as compared to that of the image steganography as you can embed large amount of data in audio and frames of the video.

c) Network Steganography: Network Steganography method uses modification of a single network protocol. The protocol modification may be applied to the PDU (Protocol Data Unit), time relation**s** between exchanged PDUs, or both (hybrid methods). It is Highly secure and robust.

d) Audio Steganography: In Audio Steganography audio is used as the cover to hide the secret information it is also very robust in nature but with limitation of the amount of data one can hide.

e) Text Steganography: Secret Data is hided in a text file. This method lacks robustness and is not that much efficient in hiding the data. It can be easily detected by the eyes of intruders.

IV. STEGANOGRAPHY MEASURES

a) Imperceptibility: A steganographic process is imperceptible when human eye cannot distinguish between the cover image and the stego image.

b) Payload: It indicates the amount of secret information that can be embedded in the cover image. The embedding rate is given in absolute measurement such as the length of the secret message.

c) Statistical Attacks: The process of extracting the secret information from the stego object is known as statistical attack. The algo used for steganography must be robust to statistical attacks.

d) Security: Security of a steganographic system is defined in terms of undetectability, which is assured when the statistical tests cannot distinguish between the cover and the stego-image.

e) Computational Cost: Data hiding and Data retrieval are the two parameters used to figure computational cost of any steganography approach. Information concealing time alludes to the time required to implant information inside a cover video edge and information recovery alludes to extraction time of mystery message from the stego outline.

f) Perceptual Quality: Increasing the payload degrade the quality of the video so approach should be used such that the quality should remain intact to avoid it from getting in sight.

V. STEGANOGRAPHY TECHNIQUES

Steganography techniques can be divided into following domains : [2]

a) Frequency 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 frequency domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested frequency domain are broadly classified into :

- Discrete Fourier transformation technique: The Discrete Fourier Transform to get frequency component for each pixel value. The Discrete Fourier Transform (DFT) of spatial value f(x, y) for the image of size M x N is defined in equation for frequency domain transformation.
- Discrete cosine transformation technique: The discrete cosine transform (DCT) is a technique for converting a signal into elementary frequency components. It is widely used in image compression.
- Discrete Wavelet transformation technique: A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled.

b) Spatial Domain Methods:

There are many versions of spatial steganography' a directly change some bits in the image pixel values in hiding data A directly change some bits in the image pixel values in hiding data. Spatial domain techniques are broadly classified into:

- **Least significant Bit :** The least significant bit is the lowest bit in a series of numbers in binary the LSB is located at the far right of a string. For example, in the binary number: 10111001, the least significant bit is the far right 1. Here the secret information is stored in the LSB of the image.
- **Pixel value differencing :** The pixel-value differencing (PVD) scheme provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels.
- **Edge based data embedding method:** In ELSB, we use all the edge pixels in an image. Here, we first calculate the masked image by masking the two LSB bits in the cover image. Then we identify the edge pixels by using the Canny Edge detection method. After obtaining the edge pixels we hide the data in the LSB bits of the edge pixels only and send the stego object to the receiver.
- **Random pixel embedding method:** random pixels are used to embed and send the stego object to the receiver.

VI. COMPARISON TABLE

Encryption	Watermarking	Steganography	Criterion/Method
usually text based, with some extensions to image files	mostly image/audio files	any digital media	Carrier
plain text	watermark	payload	Secret data
necessary	optional	optional	Key
one	at least two unless in self-embedding	at least two unless in self-embedding	Input files
blind	usually informative (i.e., original cover or watermark is needed for recovery)	blind	Detection
full retrieval of data	usually achieved by cross correlation	full retrieval of data	Authentication
data protection	copyright preserving	secrete communication	Objective
cipher-text	watermarked-file	stego-file	Result
robustness	robustness	delectability/ capacity	Concern
cryptanalysis	image processing	steganalysis	Type of attacks
always	sometimes	never	Visibility
de-ciphered	it is removed/replaced	it is detected	Fails when
N/A	usually becomes an attribute of the cover image. The cover is more important than the message.	not necessarily related to the cover. The message is more important than the cover.	Relation to cover
N/A	cover choice is restricted	free to choose any suitable cover	Flexibility
modern era	modern era	very ancient except its digital version	History

VII. CONCLUSION

This paper gave an overview of different steganographic techniques its major types and classification of steganography which have been proposed in the literature during past few years.

ACKNOWLEDGMENT

This Paper is completed by referring various research papers on steganography techniques and their overview and I really appreciate the hard work and dedication done by the authors of the papers

REFERENCES

[1]. Volume-2, Issue-5, May-2015 ISSN: 2349-7637 (Online) RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ) Research Paper Available online at: www.rhimrj.com 2015, RHIMRJ, All Rights Reserved Page 1 of 5 ISSN: 2349-7637 (Online) A Survey Paper on Steganography and Cryptography Z. V. Patel1st Student, M.Tech. C. U. Shah College of Engineering and Technology, Surendranagar, Gujarat (India) S. A. Gadhiya2nd Head, B.E.(IT) C. U. Shah College of Engineering and Technology, Surendranagar, Gujarat (India)

[2]. Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques Mukesh Garg* A.P. Gurudev Jangra M.Tech. Scholar H.O.D in CSE Department Jind Institute of Engineering & Technology Jind Institute of Engineering & Technol

[3]. Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques Mukesh Garg* A.P. Gurudev Jangra M.Tech. Scholar H.O.D in CSE Department Jind Institute of Engineering & Technology Jind Institute of Engineering & Technology Jind, Haryana 126102, India Jind, Haryana 126102, India

[4]. International Journal of Innovative Research in Computer and Communication Engineering (A High Impact Factor, Monthly, Peer Reviewed Journal) Vol. 4, Issue 1, January 2016 Copyright to IJIRCCE DOI: 10.15680/IJIRCCE.2016. 0401158 721 A Survey Paper on Steganography Techniques Dr. Rajkumar L Biradar1 , Ambika Umashetty2 Associate Professor, Dept. of Electronics and Telematics, G. Narayanamma Institute of Technology & Science, Hyderabad, India1 Dept. of Computer Science & Engineering, Appa Institute of Engineering & Technology, Kalaburagi, India2