Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Various Steganography Techniques

Gurwinder Kaur
Student
AIET, Faridkot, India

Navdeep Singh Sethi
Assistant Professor
AIET, Faridkot, India

Harinderpal Singh
Assistant Professor
AIET, Faridkot, India

Abstract: ***In this paper we tend to review completely different Steganography techniques for concealment the information. Steganography may be a technique of concealment the information in any media in such how that it remains confidential. This paper explores the various methods of information hiding that are image steganography, audio steganography, video steganography, text steganography, steganography in abstraction domain, remodel domain and reconciling steganography. The various aspects on that the steganography technique depends are: strength, capacity, undetectability and physical property.***

Keywords: Biometric, DCT, DWT, PSNR, Steganography.

I. INTRODUCTION

Steganography is a Greek work which suggests the coated writing. Steganography is an art of concealing information in a coated media (image, audio, video, text). In Steganography, we tend to hide the mere presence of that it'll be undetectable. The covered media is chosen in such a way that it's capability to cover the information and strength that has quality to the stego image. As within the coming years the requirement of information concealing, copyright protection, and confidentiality will increase, steganography plays a vital role during this field thanks to its some distinctive options. During this paper, we tend to target the different steganography strategies. This review paper provides some vital info concerning steganography methods that may facilitate in future researches in steganography and information concealing field. This paper is split into completely different sections within which we tend to make a case for steganography system, connected work, completely different steganography strategies and conclusion.

II. SCOPE OF STEGANOGRAPHY

With the boost in pc power, the web and with the event of digital signal process (DSP), scientific theory and cryptography theory, steganography has gone ‘‘digital’’. Within the realm of this digital world, steganography has created an environment of company vigilance that has spawned numerous fascinating applications, so its continued evolution is bonded. Cyber-crime is believed to learn from this digital revolution. Therefore an instantaneous concern is to search out absolute best attacks to hold out steganalysis, and at the same time, checking out techniques to strengthen existing stenography techniques against in style attacks like steganalysis.

A. Steganography System

From the traditional times, Steganography is employed to cover the key knowledge. The information was hidden on the rear of wax, writing tables, abdomen of rabbits or on the scalp of the slaves. And currently on a daily basis, hacking is employed for associate unauthorized access of data so, to stay the information confidential, sender uses totally different strategies. Steganography is one among the strategy during which the data is hidden within the cowl object with the utilization of secret key. The extractor ought to have secret key to extract the information. The secret key designed in such a way that it can’t be verify by associate uncommon user. In Steganography systems following terms are used:
Cover Media: The cover media is the medium in which message is embedded to hide the presence of secret data.
Stegno: The media through which the data is hidden.
Secret data: The data to be hidden or extract.
Steganalysis: The process by which secret data is to be extracted.

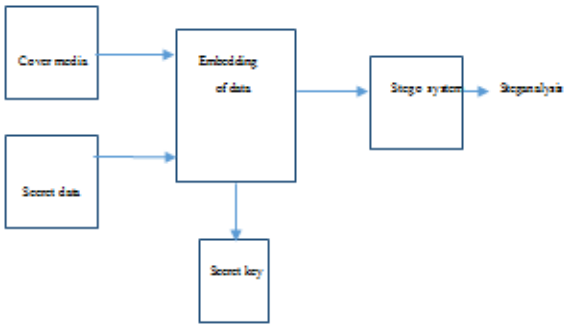

Figure 1:Steganography system

III. LITERATURE SURVEY

In related work, LSB is the most common method used to hide the message developed by Chandramouli [1] by applying the filtering, masking and transformation on the cover object. LSB matching revisited image steganography and edge adaptive scheme to which can select the embedding region Weigi Luo [2] according to the size of secret data.Hassan Mathkour [3] use a new image steganography scheme based on LSB replacement technique and pixel value differencing. Chen Ming [4] discussed different steganography algorithms and tools into spatial domain, transform domain, document based and other categories such as spread spectrum technique and video compressing encoding. Mankun Xu [10] proposed a model based steganography technique which is based on least square method to estimate the embedding rates of secret information.

Anjali A. Shejul [7] proposed a DWT based approach for steganography using biometric features. Here, the secret data is embedded in skin region of image that provides secure location for data hiding. Secret data is hidden in one of the high frequency sub band of DWT by tracing skin pixels. All the steps of data hiding are applied on the cropped image. This provides security to the method and PSNR is used to determine the quality of stegno image after embedding the secret data.

IV. STEGANOGRAPHY TECHNIQUES

Steganography is differentiated on the basis of the media in which we hide the data. These are: text, image, audio and video. The Steganography methodology uses the text media to cover the info referred to as text Steganography. There square measure totally different techniques to implant the key information in text files.

- Format primarily based methodology
- Random and Statistical based method
- Linguistics methodology

- Format based Method: This methodology modifies the prevailing text to cover the info in such a way that it involves the insertion of areas, resizing the text, modification the fashion of text.
- Random and Statistical Method: during this technique characters square measure hidden that appeared in random sequence. Applied mathematics method determines the statistics like mean, variance and chi sq. text that live the quantity of redundant information to be hidden inside the text.
- Linguistics Method: it's the mixture of syntax and linguistics. Syntactical steganalysis make sure the correct structure as the text is generated from descriptive linguistics. In linguistics technique price is appointed to synonyms and information may be encoded to the actual word of text.

1. Audio Steganography

When secret information is embedded into digital sound, the technique is understood as audio steganography. This technique embeds the secret message in WAV, AU and MP3 sound files. There square measure totally different ways through that audio steganography explored:

- Low Bit secret writing
- Phase Coding
- Spread Spectrum

Low Bit Encoding: This technique is employed by pitch amount prediction is conducted throughout low bit speech secret writing. Thus, maintaining synchronization between data activity and speech secret writing.

2. Frequency Domain Steganography:

In frequency domain, secret information is hidden in important areas of lined image, which makes information invigorate to attacks like compression, cropping or image process ways than LSB approach. This provides associate degree increased security level to steganography technique and result in the event of algorithms. This technique transforms embrace DCT, DWT and DFT. A lossless and reversible theme are introduced that use every block of quantal DCT constant in JPEG image for secret information [6]. The tactic ends up in high stego image quality and achieves changeableness. DCT coefficients of a picture used for embedding information bits. F5 embeds information in DCT constant by miscalculation the quantal coefficients to the closest information bit. It conjointly uses matrix secret writing for reducing the embedded noise within the signal. F5 is one among the foremost in style embedding schemes in DCT domain. Wave rework (WT) converts spatial domain data to the frequency domain information. Wavelets square measure employed in image as a result of wave individually partitions the high frequency and low frequency information picture element by picture element. This theme chiefly addresses the capability and hardiness of the information activity system.

V. CONCLUSION

As described in this paper, we represent various steganography techniques which can be used to hide the message (text or image) into cover image. In the past few years, Steganography has become AN interested field of information concealment techniques.

This paper provides an overview of various steganography strategies that satisfy the foremost vital factors of steganography style. These are undetectability, capability and lustiness.

REFERENCES

[1] N. F. Johnson, S. Jajodia, "*Exploring Steganography: Seeing the Unseen*", IEEE Computer vol. 31, issue 2, pp. 26-34, 1998.

[2] J. C. Judge, "*Steganography: Past, Present, Future",* SANS Institute Publications, 2001.

[3] Artz D., "*Digital Steganography: Hiding Data within Data*", Internet Computing IEEE, vol. 5, issue 3, pp. 75-80, 2001.

[4] Jar no Mielikainen, "*LSB Matching Revisited*", Signal Processing letters, IEEE, vol. 13, issue 5, pp. 285-287, May 2006.

[5] L-C. Lin, "*Hiding Data in Spatial Domain with Distortion Tolerance*", Computer Standard & Interfaces 31, pp. 458-464, (2009).

[6] C-C. Chang, "*Reversible Hiding in DCT based Compressed Images*", Information Sciences 177, pp. 2768-2786, (2007).

[7] Anjali A. Shejul, Prof. U. L. Kulkarni, "*A DWT based Approach for Steganography using Biometric*", International Conference on Data Storage and Data Engineering, IEEE, pp. 39-43, 2010.

[8] Provos N. and Honeyman P, "*Hide and Seek: An Introduction to Steganography*", IEEE Security and Privacy, vol. 01, issue 3, pp. 32-44, May-June 2003.

[9] Shaveta Mahajan, Arpinder Singh, "*A Review of Methods and Approach for Secure Steganography",* International Journal of Advanced Research Computer Science and Software Engineering, vol 2, issue 10, pp. 67-70, October 2012.

[10] K. Gopalan. , "*Audio steganography using bit modification*", IEEE International Conference on Acoustics, Speech, and Signal Processing,

