A Survey on Image Steganography Techniques

Ankit Dhar[1] Kinjal Rathod[2] Nageswar Kamble[3] Ajay Dhruv[4]
[1,2,3,4]Vidyalankar Institute of Technology, Wadala, Mumbai-400037

Abstract— With the increase in new technology there are many ways of communication over a network, the security of information is a major concern. Steganography and cryptography are two different technologies which are associated with techniques of hiding the data. Steganography hides messages inside some other digital media. Cryptography, on the other hand encrypts the content of the message. Using cryptography data can be encrypted after that data is embedded. The process revolves around encryption and hiding of data, this is the whole summary regarding steganography.

Key words: Steganography Techniques, Cryptography

I. INTRODUCTION

World has evolved in the field of technology hence security of data is the main focus in the industry and thus encrypting the data is the best alternative. Steganography techniques are used for inscription of digital copyrights management, protect information, and conceal secrets. Data hiding techniques provide a riveting provocation for digital forensic investigators. To ensure that data security is achieved and does not infers into others privacy new technologies came into the picture. Digital data when delivered over the network there is a possibility of few errors.

II. LITERATURE SURVEY

In ancient time there used to be a secret communication which was carried out using different steganography techniques. The Greek historian Herodotus recorded two stories for steganography techniques used at that time. Suppose one individual wants to send any secret message to the another individual then the former used to shave the head and write message on the scalp of a person. When the person's hair grew back, he was sent to the latter, then the person head was again shaved to read the secret message.

A. Spatial And Transform Domain

In this paper [1],the author has considered color image as cover and two grey scale images as secret information. The content used to implant particulars is called as cover object. The cover along with the hidden information is called as stego object. The design of a stenographic system can be categorized into spatial domain methods and transform domain methods. In spatial domain methods, the action is applied on the image pixel values directly. The advantage of these methods are its intelligibility. The disadvantage is low ability to bear signal processing operations. Least Significant Bit Insertion methods, Pallet based methods come under this category. In transform domain methods, the first step is to modify the cover image into different domain. Then the modified coefficients are processed to hide the secret information. These modified coefficients are transformed back into spatial domain to get stego image. The advantage of transform domain methods is the excessive ability to face signal processing operations. However, methods of this type are computationally complex.

B. Frequency Domain

In this paper [2], the author demonstrates a unique technique which can be used along steganography to increase the level of security and those techniques are Watermarking and fingerprinting. These are the two other technologies that are closely related to steganography. Watermarking is a protecting technique which protects the owner's property right for digital media (by the means of some hidden watermarks. Therefore, the steganography goal is the secret message while the watermarking goal is the cover object itself. Fingerprint algorithm maps a large bulb of data to a much shorter bit string.

This technique is mainly used for data de duplication. During steganography using frequency domain method the message to be sent is first converted in the binary form of frequency domain.

C. Pangram And Image Mediums

In this paper [3], hiding information in plain text can be done in many different ways. Some techniques consist of altering the outline of the carrier text such as adding white spaces or altering the case of certain characters so as to represent secret text. Others, consist of relating the characters to hide with the characters of the carrier text, creating a reference dictionary that maps words from the secret text with words from the carrier text. These include techniques like The Pangram Sentence and the Carrier Image

A pangram sentence is a statement which consists of all the alphabets in a sentence and it is used to match characters from the secret. The process used for matching the alphabets from the secret message with the pangram sentence is a linear search algorithm. The pangram statement is usually of 512 char. The matching process i.e. linear search algorithm starting from a random seed index denoted by SEED till an offset index denoted by OFFSET representing the distance from the SEED index to the actual position of the matching character in PAN. In The Carrier Image technique first the image is converted into RGB format and then the SEED and OFFSET value is set.

D. Steganography And Dynamic Video Generation

In this paper [4], the author proposed architecture is a blend of dynamic video generation and Digital Steganography thus providing a secure and authentic transmission of data over a network. The sender and the receiver will have a database consisting of the 16 same images. Each image will have a 4 bit combination allocated to it. This same 16 images and their analogous 4 bit code can be exchanged between the users by meeting face to face or by simply transmitting it over the network securely. First input to the proposed algorithm is 4 integer values. The next input by the user will be the data file which is transformed into bytes. The whole data is divided into small. Now the data from the 4 byte chunk is transformed into bits leading to 32 bits of data. Then the 4 bits are selected based on the 4 integer values supplied by the user.

The image analogous with this 4 bit code is picked .Now using the key 28 pixels are dynamically selected and these bits are concealed into the respective pixels. Thus each image consists of 4 byte of data hidden in it. The rest chunks are steganographed in the similar manner. Then all the images are combined to form a video which is then transmitted over the network and at the receiver end this video file is split back into images. An image comparison algorithm is used to compare the images in the video and find out their respective codes. The bits are placed back in the right position by using the passkey supplied. Even the hidden data in the rest of the image retrieved using the passkey. Thus the data file is regenerated

III. CONCLUSION

This paper shows the survey of image steganography and below explains all the four paper that are surveyed.

A. Comparison Study Of Techniques Surveyed

Name of the paper	Methodology Used	Advantages
A secure and high capacity image steganography technique.	Spatial domain methods and transform domain methods.	Confidentiality, integrity, Consistency.
A Review on Image Steganography using Frequency Domain.	The image is converted to binary form or frequency domain	Security, Integrity, Consistency.
A Text Steganography Method Using Pangram and Image Mediums.	The First Medium – The Pangram Sentence The Second Medium – The Carrier Image	Confidentiality, integrity, Consistency.
Data Hiding Technique using Steganography and Dynamic Video Generation	Video is generated as a result of steganography.	Consistency, Security, Confidentiality, integrity,

Table 1.1. Comparison

REFERENCES

[1] Hemalatha S1, U Dinesh Acharya2, Renuka A3, Priya R. Kamath4, "A SECURE AND HIGH CAPACITY IMAGE STEGANOGRAPHY TECHNIQUE", Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, February 2013

[2] Arzoo Dahiya1 Vandana 2 1Assistant Prof. 2P. G. Student, "A Review on Image Steganography using Frequency Domain", IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 02, 2014 | ISSN (online): 2321-0613

[3] Youssef Bassil, "A Text Steganography Method Using Pangram and Image Mediums", International Journal of Scientific & Engineering Research (IJSER), ISSN: 2229-5518, Vol. 3, No. 12, December 2012

[4] Abhishek Mangudkar, Prachi Kshirsagar, Vidya Kawatikwar, Umesh Jadhav, "Data Hiding Technique using Steganography and Dynamic Video Generatio", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June 2012.

