INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Global Advanced Research Publication House Journal

Home page: www.ijaite.co.in

Data Hiding Using Image Steganography Techniques

[1]Sonali Shevatkar, [2]Dr. C. N. Deshmukh

[1,2]Department of Electronics and Telecommunication, Prof. Ram Meghe Institute of Technology and Research Badnera, Amravati, Maharashtra, India

[1]sonali.shevatkar@gmail.com, [2]cn_desh111@yahoo.co.in

Article History

Received on: 10 Oct 2021

Final Revised on: 28 Oct 2021

Published on: 30 Nov 2021

Keywords:

Steganography, Data hiding, Steganalysis, Message Embedding

e-ISSN: 2455-6491

Production and hosted by
www.garph.org

ABSTRACT

Steganography is the technique of hiding the fact that communication is taking place, by hiding data in other data. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques. Steganalysis, the detection of this hidden information, is an inherently difficult problem. In this paper we have critically analyzed various steganographic techniques and also have covered steganography overview its major types, classification.

1. INTRODUCTION

In today's highly competitive and dynamic world, it is the data and information that fuels the engine of the computer communication and global economy. With the boost in computer power, the internet and with the development of digital signal processing (DSP), steganography has gone "digital". In order to ensure that data is secured and does not go to unintended destination, the concept of data hiding has attracted researchers to come up with creative solutions to protect a piece of information from falling into wrong hands. This idea of data hiding is not a novelty but it has been used for centuries all across the world under different regimes which is a tool for hiding information so that it does not even appear to exist. Over the past decade methods, techniques and technologies to conceal digital evidence and communicate covertly have increased alarmingly. Thus, people have adapted different means of concealing information.

Digital data provides easy way of editing and modifying of data which can be copied without any loss in quality and content. Digital data can be delivered over computer networks from one place to another without any errors and often without interference. The distribution of digital data raised a concern over the years as the data are attacked and manipulated by unauthorized person. Digital content is now posing formidable challenges to content developers, aggregators, distributors and users. Now a day, a lot of applications are internet-based and in some cases, it is desired that the communication be made secret. The Internet provides a way of communication to distribute information to the masses. Since the rise of the internet, one of the most important factors of information technology and communication has been the security of information. This is because of the fact that data are being transmitted or exchanged over some public communication channel. Therefore, the confidentiality and data integrity are required to be protected against unauthorized access and use. Therefore, how to achieve safe secret communication is an important field of research. Techniques for data hiding are increasing day by day with more sophisticated approach. The digital media which are used for secret communication includes text, images, audio and videos which provide excellent carriers for hidden information. Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. Data hiding techniques provide an interesting challenge for digital forensic investigators. One of the main concerns in this field is the ability to privately exchange information and hide the data of interest throughout the transmission process.

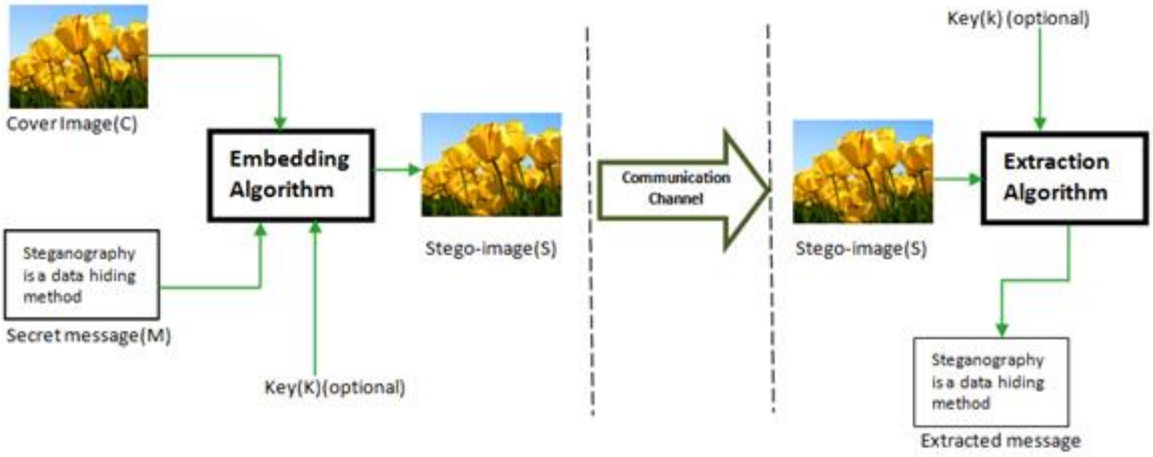

Figure 1: Image Steganographic System

A steganographic system involves two parties: the sender who embeds the secret message in the cover medium and the receiver who extracts the message from the cover. The sender takes the “host” object, which represents the cover-object, and embeds a secret binary message produce a stego-object that is perceptually identical to the cover. The stego-object is then communicated along a public channel to the receiver. At the receiver the stego-object is used to extract the secret binary message. The public channel may be monitored by an active warden whose goal is to detect the presence of any covert communication taking place. The key (k) is optional as it may be included in embedding process. The key is specific to the steganography algorithm which ensures that only recipient who knows the corresponding extraction key will be able to decode the message from a stego-image. A steganographic system scenario is presented in figure 1. If a sender wants to send the secret message M to some recipient over the insecure communication line, the sender embeds secret-message (M) into cover-image (C) by some embedding method to produce stego-image (S). The key K (optional) may be used to find out the location in C to hide the message. Then the stego-image (S) is sent to recipient. Upon receipt, the recipient uses extraction algorithm to retrieve M (extracted message).

2. Related Work

Kordov K. et. al. (2021), approach for hiding secret text message in color images is presented, combining steganography and cryptography. The location and the order of the image pixels chosen for information embedding are randomly selected using chaotic pseudorandom generator. Encrypting the secret message before embedding is another level of security designed to misguide the attackers in case of analyzing for traces of steganography. Evaluating the proposed stego algorithm. The standard statistical and empirical tests are used for randomness tests, key-space analysis, key-sensitivity analysis, visual analysis, histogram analysis, peak signal-to-noise ratio analysis, chi-square analysis, etc. The obtained results are presented and explained in the present article.

G. Mallikharjuna Rao (2020), proposed to have a combination of cryptography and image steganography techniques. This scheme will enable the security, secret message and image cannot be extracted. The International Data Encryption Algorithm (IDEA) cryptographic algorithms and Discrete Cosine Transform (DCT) based steganography algorithm is chosen for the functionality. Cryptography is used to encrypt and decrypt the document. Steganography to hide document inside an image with increasing payload for the secure transmission of confidential data across the internet. In this study present a single application to hide the information by the sender, which is so important document and confidential in the form of files, it will be invisible to unauthorized person. The results of a suggested scheme with respect to PSNR of 90.06 dB with a payload of 52,400 bytes of information in an image.

Jemima Dias et. al. (2020), proposed research involves an image encryption algorithm, it uses a secret key from Lorenz chaotic system. It's a network consisting of weights with which the Y channel of the plain image is XORed with and the cipher image will be formed. These weights are unique and are non-identical to each other. The results have proved that the decrypted plain image has a similarity index of 0.96 to the original plain image.

Serdar Solak et. al. (2019) proposed adaptive least-significant-bit (LSB)+3 type I and adaptive LSB+3 type II methods to hide encrypted data in the cover image. The image quality of the stego image obtained from the proposed adaptive LSB+3 method is better than the traditional three-bit LSB methods. When maximum data are embedded in the cover image, a peak signal-to-noise ratio (PSNR) greater than 41 dB is reached. Experimental studies show that adaptive LSB+3 type I and adaptive LSB+3 type II methods are higher PSNR values (3.48% and 5.73%) than the standard three-bit LSB substitution methods.

Swati Bhargava et. al. (2019) proposed securing the image by way of encryption is completed by LSB bits, DWT and RSA algorithm. This study additionally presents new strategies wherein cryptography and steganography are mixed to scramble the information and in addition to cover the insights in some other medium through image processing (IP). The encrypted picture can be hiding in some other image by way of the use of LSB bits, DWT strategies so that the secret's message exists. RSA algorithm applied; receiver will use his/her private key because the secret data have been encrypted by recipient public key. Hide encrypted image in the cover image by DWT. Extract encrypted image from cover image and decrypt text by DWT. The proposed scheme is implemented in MATLAB platform the use of preferred cryptography and steganography set of regulations. Calculate PSNR and MSE. Also calculate the entropy of cover image and stego image. This method is secure for communication in the digital world with the digital data transmission.

Amit Khare et. al. (2018), proposed the OUTGUESS algorithm. Outguess is one of the embedding algorithms which embeds messages in the DCT domain. Outguess goes about the embedding process in two separate steps. First it identifies the redundant DCT and then depending on the information obtained in the first step, chooses bits in which it would embed the message. Digital Image Steganography system is a standalone application that combines steganography and encryption to enhance the confidentiality of intended message. The user's intended message is first encrypted to create unintelligible cipher text. Then the cipher text will be hidden within an image file in such a way as to minimize the perceived loss in quality. The recipient of the image is able to retrieve the hidden message back from the image with Digital Image Steganography system.

3. STEGANOGRAPHY TECHNIQUES

It has been observed that all digital file formats can be used as digital carrier for steganography, but the formats those are with a high degree of redundancy are more suitable since the redundant bits can be replaced with secret information without the embedded information being perceivable. The redundant bits of an object are those bits that can thus be altered without the alternation being detected easily. Image, Text, Audio, Video and Network Protocol often have redundant data present in their binary representation and comply with the requirement of steganography. Each of these file format categories uses different techniques for hiding information based on the unique characteristics of the file format and the redundancy created in the digital representation of the file.

A. Text Steganography

In text-based steganography data hiding takes place by introducing changes in the structure of the document without making a notable change in the concerned output. Text steganography is the art or process of hiding one text into another text for the purpose of secure communication so that the unauthorized user cannot get trace of the secret message.

B. Format based

Format based methods used physical text formatting of text as a place in which to hide information. They do not change any word or sentence, so it does not harm the value of the cover-text. Format Based Method is of four types.

1. Line shifting method

In the line shifting method, the lines of the text are vertically shifted to some degree and information is hidden by creating a unique shape of the text. In a typical implementation, a line is moved up or down, while the line immediately above or below (or both) is left unmoved. The unmoved adjacent lines serve as reference locations in the decoding process. Though the human eye is particularly adapted at noticing deviations from uniformity, each vertical line can be shifted 1/300 inch up or down and such changes less go unnoticed by human eye.

2. Word shifting method

In word shifting method, the horizontal alignment of some words is shifted by changing distances between words to embed information in the text and is acceptable for text where the distance between words is varied. Readers accept a wide variation in text setting within a line and each horizontal words can be shifted 1/150 inch and such changes less go unnoticed by human eye. In such process, a word is altered left or right, while the words immediately adjacent are left unmoved and these words serve as reference locations in the extracting process.

3. Feature coding

In feature coding method, some of the features of the text are chosen and altered depending on the message to be inserted. Such feature alterations can be a change to a character’s height or its position within a given font relative to other characters. In such case document will have the same content and some character features are left unchanged to facilitate decoding process. Feature coding method also involves the alterations of vertical lines of the individual characters and the length of those lines may be modified in a way that is imperceptible to the ordinary readers

4. White/null /open space

In the open spaces method, extra white/null spaces are added into the text of the cover message for hiding the secret message. These whitespaces can be placed at the end of each line, at the end of each paragraph or sentence or between the words. This method can be implemented on any arbitrary text and does not raise attention of the reader. Although a little amount of data can be hidden in a document, this method can be applied to almost all kinds of text without revealing the existence of the hidden data.

5. Random and statistical generation methods

Random and statistical generation methods are used to generate cover-text automatically according to the statistical properties of language. This method uses example grammars to produce cover-text in a certain natural language and is based on character sequences and words sequences. A probabilistic context-free grammar (PCFG) is used to generate word sequences by starting with the root node and recursively applying randomly chosen rules. The sentences are constructed according to the secret message to be hidden in it. The quality of the generated stego-message depends directly on the quality of the grammars used.

6. Linguistic method

The final category is linguistic method which specifically considers the linguistic properties of generated and modified text, frequently uses linguistic structure as a place for hidden messages. Linguistic steganography is defined as a technique of data hiding that embeds the secret message within texts based on some linguistic knowledge. They are basically of two types

7. Semantic method

In the semantic method, the synonyms of certain words are used for hiding information in the text. The synonym substitution may represent a single or multiple bit combination for the secret information. The semantic transformation method is the most sophisticated approach for linguistic steganography and perhaps impractical given the current state-of the- art for NLP technology.

8. Syntactic method

In this approach the syntactic structure of the text is used to embed the secret message into text file. Syntactic method is a linguistic steganography method where some punctuation signs like comma (,) and fullstop (.) are placed in proper places in the document to embed data. Syntactic method is based on the fact that a given sentence may be represented into various syntactic structures without any essential change in meaning. Syntactic methods include changing the diction and structure of text without significantly altering the meaning.

C. Network Steganography

Network steganography allows users to communicate secretly by embedding information within other messages and network control protocols used by common applications. This is possible because inserting hidden data into a chosen carrier remains unnoticeable for users not involved in steganographic communication. Data hiding within network protocols were based on the discovery of covert channels and embedding took place in TCP/IP packets also in application layer protocols. Hidden communication network steganography utilizes network protocols and/or relationships between them as a secret message carrier.

Some of the Network Steganography methods are as follows:

1. Steganophony

Voice over IP (VoIP) is a real-time service, which enables users to make phone calls through data networks that use an IP protocol. A steganographic technique applied to VoIP traffic steganophony that involves information hiding techniques in any layer of the TCP/IP protocol-stack. According to them, for VoIP systems, four possible hidden communication scenarios may be considered. In the first method, the sender and the receiver perform VoIP conversation while simultaneously exchanging secret messages. In the rest three methods only a part of the VoIP end-to-end path is used for hidden communication and thus the sender and/or receiver are unaware of the steganographic data exchange.

2. LACK

In case of VoIP, when a packet does not reach the destination point or when it is delayed excessive amount of time, it is considered as packet lost and then discarded. This feature is used to create new steganographic technique called LACK (Lost Audio Packets Steganographic Method). LACK is a hybrid steganographic method which modifies both packets and their time dependencies. Firstly, one packet is selected from the RTP stream and its voice payload is substituted with bits of the secret message. At the transmitter, some selected audio packets are intentionally delayed by a certain time before transmitting. If the delay of such packets at the receiver is considered excessive, the packets are discarded by a receiver which is not aware of the steganographic procedure. If the receiver knows about the hidden communication, then instead of deleting the packet the receiver extracts the payload.

3. SCTP Steganography

Steganographic methods may be applied to Stream Control Transmission Protocol (SCTP) which is a transport layer protocol and its main role is similar to both popular protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The information hiding methods for TCP and UDP protocols may be utilized due to several similarities between these transport layer protocols and SCTP. It provides ensuring reliability and transport of messages with congestion control. SCTP specific steganographic methods can be divided in three groups- methods that modify content of SCTP packets, methods that modify how SCTP packets are exchanged and methods that modify both content of SCTP and the way they are exchanged i.e., hybrid methods.

4. Multi-Level Steganography

First, the upper-level method uses covert traffic as a secret data carrier. The second, the lower-level method, uses the way the upper-level method operates as a carrier. The indirect carriers for lower-level methods are still packets from covert communication, but the direct carrier is another (upper-level) method. In MLS the bandwidth of the lower-level method is a fraction of the bandwidth of the upper-level method. Also, the lower-level method is potentially harder to detect than the upper-level one. It results from the fact that the lower-level method functioning entirely depends on upper-level one. Thus, the adversary has to detect the upper-level method first in order to look for the lower-level one.

Table 1: Comparison of Steganography with Cryptography and Watermarking

Characteristic	Watermarking	Cryptography	Steganography
Medium	Mostly with image and can also be with video and audio	Mostly text-based with some extension to image	any digital media (image, audio, video, text, network protocol)
Operation/work	Embeds watermark in cover-medium	Rearranges secret text in a way that it appears unintelligible	Fully embeds the secret data into the cover-media
Perceptivity	Mostly visible	Fully visible	Invisible
Key	Optional	Essential	Optional

Deals with	Robustness	Protection	Security and invisibility
Protects from	manipulations of data	Readability of secret data	
Input	Two files	One file	Two files
Output	Watermarked-file	Cipher-text	Stego-file
Structure of secret data	does not alter	Alters the position of the secret data	does not alter the structure of secret data
Parameters used in testing output data	optional	optional	Statistical and structural methods are used
Detection method	Target	Blind	Blind
Replacement	Replaces watermark with redundant part of cover media	Replace the plain-text character with ciphertext	Replaces secret data with redundant part of cover media
Authentication	usually achieved by cross correlation	full retrieval of data	full retrieval of data
Attacks	signal processing	cryptanalysis	steganalysis
Relation to cover medium	The cover is more important than the secret data	N/A	The secret data is more important than the cover.
Application	Data authentication	Mainly used in ecommerce and network applications.	Wide range of application
Readability of secret data	Partially readable	Fully readable	Not readable without extraction

CONCLUSION

Steganography is the art and science of communicating in a way which hides the existence of the communication. Though Cryptography gives good security, the attacker can come to know that communication is taking place. But in Steganography, attacker does not have any knowledge of communication. The information can be revealed in such cases in which attacker knows that information is hidden in cover text, video, image etc. Therefore, security of steganography can be increased by combining it with cryptographic techniques. For future research in steganography can be done using image processing techniques such as edge detection algorithm.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

FUNDING SUPPORT

The author declare that they have no funding support for this study.

REFERENCES

[1] [1] Kordov K, Zhelezov S. 2021. Steganography in color images with random order of pixel selection and encrypted text message embedding. PeerJ Comput. Sci. 7:e380 DOI 10.7717/peerj-cs.380

[2] Serdar Solak and Umut Altınışık "Image steganography based on LSB substitution and encryption method: adaptive LSB+3," Journal of Electronic Imaging 28(4), 043025 (13 August 2019). https://doi.org/10.1117/1.JEI.28.4.043025

[3] A. Soria-Lorente, S. Berres, "A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information", Security and Communication Networks, vol. 2017, Article ID 5397082, 14 pages, 2017. https://doi.org/10.1155/2017/5397082

[4] Swati Bhargava and Manish Mukhija: Hide Image and Text Using LSB, DWT And RSA Based on Image Steganography, ICTACT Journal on Image and Video Processing, Volume: 09, Issue: 03, February 2019 DOI: 10.21917/ijivp.2019.0275

[5] Hayfaa Abdulzahra Atee, Robiah Ahmad and Norliza Mohd Noor, "Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding", Middle-East Journal of Scientific Research 23 (7): 1450-1460, 2015. DOI: 10.5829/idosi.mejsr.2015.23.07.22361

[6] Amit Khare, Neha Khare, 2014, Integrity Verificationn of Secret Information in Image Steganography, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICONET – 2014 (Volume 2 – Issue 04),

[7] G. Mallikharjuna Rao, "Information Security using Cryptography and Image Steganography", International Journal of Recent Technology and Engineering (IJRTE), Volume-9 Issue-2, July 2020.

[8] Jemima Dias, Dr. Ajit Danti, "Image Steganography based Cryptography", International Journal of Scientific & Engineering Research, Volume 11, Issue 3, March-2020.

[9] M. Padmaa and Y. Venkataramani, 2014. Encrypted Secret Blend with Image Steganography for Enhanced Imperceptibility and Capacity. Research Journal of Information Technology, 6: 342-355. DOI: 10.3923/rjit.2014.342.355.

[10] Kamaldeep Joshi, Swati Gill, Rajkumar Yadav, "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image", Journal of Computer Networks and Communications, vol. 2018, Article ID 9475142, 10 pages, 2018. https://doi.org/10.1155/2018/9475142

[11] De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Christy Atika Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption", Journal of Applied Intelligent System, Vol. 2 No. 1, April 2017, pp. 1 – 11

[12] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au and Y. Y. Tang, "Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, March 2016, doi: 10.1109/TCSVT.2015.2416591.

[13] Mohammed Mahdi Hashim, Mohd Shafry Mohd Rahim, "Image Steganography Based on Odd/Even Pixels Distribution Scheme and Two Parameters Random Function", Journal of Theoretical and Applied Information Technology. Vol.95. No 22, 30th November 2017.