International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

A Study of Various Techniques and Methods of Steganography

Harpreet Singh

Department of CSE, BBSBEC, Fatehgarh Sahib, Punjab, India

Abstract: ***In order to secure delicate data, frequent and intensive internet transmission of data needs security methods. Steganography is one of many safety methods consisting of concealing data within a suitable multimedia (e.g. picture, video, audio. Steganography technologies such as capability (information size integrated) and imperceptibility (detectability level) face many diffculties. These two elements are inversely proportional to each other, resulting in a dilemma of data hiding.This article provides a review of the steganography techniques used in latest years and a critical assessment based primarily on measuring ability and, secondly, measuring imperceptibility and steganography.***

Keywords: Steganography, ability, steganography characteristics, steganography types

1. Introduction

Recent years have seen an increase in the use of intensive information transmission through government channels such as the internet. When the data is deemed sensitive, protecting it from unauthorized parties is very crucial.

Therefore, a powerful system of safety is engaged. Steganography is one of these mechanisms of safety used to ensure transmission between sender and receiver.

2. Steganography

Steganography is a science of hiding information within a suitable container (which can be used as a text file, picture, video, audio, etc.) in a manner that prohibits unintended recipients from detecting confidential data[1]. If the secret message is not disclosed, a good steganography scheme will be deemed; otherwise it will be broken. The most significant elements of any steganographic technique are the elevated level of imperceptibility (also called undetectability) and the quantity of secret information (also called capacity) to be embedded in the multimedia carrier[2]. The carrier is changed in the embedding phase in the common type of digital steganography called container modification and then sent to the receiver extracting the information.

2.1 Terminology of steganography

StegoObject: The outcome should be that the cover object be comes a stegoobject after confidential information is embed ded into the cover object.

Embedding: is the method of hiding a hidden message within a digital medium.

Extraction: The inverse embedding method is considered, so that the integrated message is retrieved from the object to be read.

Message / data: refers to the confidential data to be incorporated in the cover object for safe sender-to-receiver communication.

3. Types of Steganography

Text Steganography: it includes hiding information within text files. In this Technique, secret data is concealed in each letter at the bottom of each text message phrase. There are many techniques accessible to hide information in the text file. These techniques are linguistic method, format-based method, random and statistical method.

3.1 Steganography image

Steganography image is the most widely used technique. Using an embedding method, the hidden text is integrated as a shield in a digital picture. This method results in a stego-image that will be sent to the line of transmission. The receiver uses a particular removal algorithm to obtain the signal. The unauthorized parties can only notice the transmission of an image throughout the transmission of the stego-image, but they can't assume the presence of a hidden message.

3.2Audio Steganography

Steganography for sound: it includes protecting information from video documents. This technique protects information from audio records in WAV, AU, and MP3. There are various techniques of steganography of sound. These techniques are i) Low Bit Encoding ii) Phase Coding iii) Spread diffusion

3.3Video Steganography

Hiding information or documents in a digital video folder is a method. In this technique in which the clip is deemed a "picture mix" is used as a courier to hide the hidden information. In this sector, too, many methods are used.

4. Steganographic Techniques

In the sector of steganography, there are many methods that are displayed. Their ranking or categorization is distinct, and a distinctive ranking is not claimed.

1) Spatial Domain Methods

The hidden information is straight integrated in the pixel strength in this technique. It implies that while storing information, some pixel sizes of the picture are altered immediately. Spatial domain methods are categorized as follows: : i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labelling or connectivity method vii) Pixel intensity based.

LSB: Most frequently, this technique is used to hide information. The embedding is performed in this technique by combining the least important parts of picture pixels with hidden data bits. The picture acquired after embedding is nearly comparable to the initial picture because the image pixel shift in the LSB does not cause too many variations in the picture.

BPCP- In this image segmentation, its difficulty is measured. To determine the loud row, complexity is used. This technique replaces loud bit scheme frames with binary models traced from a hidden information.

PVD: Two successive colors are chosen to embed the information in this technique. Payload is determined by inspecting the distinction between two successive pixels and is used to determine whether the two pixels belong to an border region or are flat.

2) Statistical Technique

Embedded in the text of the method by altering several cover characteristics. It includes dividing the paper into sections and then embedding each section with one signal piece. The cover block will only be modified if the message bit size is one otherwise no change will be required.

3) Transform Domain Technique:

The hidden signal is integrated in the cover's flip or frequency domain in this method. This is a more complicated method to hide an picture signal. The picture uses various algorithms and changes to conceal messages in it. Techniques for transforming domains are widely categorized as: i) Discrete technique of Fourier transformation (DFT) ii) Discrete technique of cosine conversion (DCT) iii) Discrete technique of wavelet conversion (DWT) iv) Lossless or reversible process (DCT) iv) Embedding in coefficient parts.

4) Masking and Filtering:

By labeling an picture, these methods conceal data. Steganography covers data only when it becomes a potion of the picture as watermarks. These methods embed the data rather than storing it in the noise level in the most important fields.

5) Data Embedding ALGO

Literature provided algorithms. This article focuses on optimization and methods used to increase ability and imperceptibility. Algorithms concentrating on enhancing safety and robustness fell outside the reach of this article, but a lot of work has been undertaken on enhancing these last two characteristics in distinct steganography kinds. The writers suggested methods in the sound form (like in [6], [7] and [8]) that prioritize the robustness of information embedded in video coats. In the picture form, as in ([9], [10], [11] and [12]), a more safe scheme was created in contrast with the picture form. Previous studies on picture steganography and audio style plays such as plays in ([13], [14] and [15]) demonstrated improvement in the safety of the integrated text and robustness against assaults.

Are subsequently evaluated, accompanied by those intended to provide excellent imperceptibility. In[16] by building four designs, the author attempted to provide a definite performance measurement of various designs of concealing picture and/or writing information in picture steganography.

In [17], the authors proposed a method for enhancing capacity and security in the spatial domain, which consists of dividing the image into two parts; one is reserved for embedding the secret data, the other is used to indicate which change is applied in the first part to each pixel.

In [18], the writers suggested a reversible steganography system in encrypted pictures relying on function mining with enhanced plaintext capability. The writers used two encryption of multigranularity and remaining switching of histograms.

In [19], the writers used a temporal domain method to implement a LSB technique consisting of placing the hidden signal using a vibrant image pixel replacement in the LSB instead of sequentially protecting the signal

[20] The fresh multi-secret and incorrect digital image steganography idea was submitted. The concept is to embed more than one signal in a single carrier. One (or more) of the hidden secrets is / are a true signal, while the other posts are incorrect.

In [21], the author suggested a fresh technique in the frequency domain for MP3 steganography. The goal is to use the Modified Discrete Cosine Transform (MDCT) technique to compress these properties to emphasize the robustness of data embedding based on the MP3 statistical properties.

In [22], the writers provided a fresh image steganography algorithm centered on the algorithm monitoring various objects and Hamming instructions. This algorithm involves four phases: Secret Message Pre-Processing Stage: the hidden signal is a text file, the author used a button for encryption after changing all letters to ASCII code in a binary set. The encrypted range is split into sections of 11-bit. Then, the Hamming keys encode each set. Motion-Multiple Object Tracking Stage: This phase detects each shifting image within a single image and then combines these detections throughout all the screen sequences. The technique of subtraction of the context is used to identify shifting items.

Data Embedding Stage: Video images identify the movement areas and track them. In each frame, the region of interest changes based on the size and number of objects

moving. The algorithm is used to forecast all shifting items ' trajectories

In [23], the author suggested a technique in image steganography that would transform the image images into YCbCr color space and then embed a secret signal into a specific area of concern. Using the skin tracking algorithm, the specific region of concern is chosen. The secret message is embedded in a frame with the least MSE in the selected region of interest.

In [24], the author used a multilevel easy embedding technique depending on an integrated domain method. In this strategy, the primary concept is to use three video steganography techniques on a given audio file rather than using a separate technique.

This document suggested transmitting three emails through three stages in one audio file.

An efficient data hiding algorithm for audio documents was suggested by the writers in[25]. For each image, the primary method is to create a skin chart using an integrated skin tracking algorithm that decreases the amount of false positives. The skin map is then transformed to a skin block chart to eliminate the error-prone skin pixels that can lead to inefficient recovery of the concealed information. The writers used the wavelet quantization method to improve the robustness of the embedding method over the trigger and black streams of the target variables.

The research in[26] concentrated on capability efficiency using three techniques: Alphabet Letter Patterns (CALP), Vertical Straight Line (VERT), and Quadruple Categorization (QUAD), respectively. These techniques use concealed text files and this hidden text is transformed to binary bits before being used in the embedding phase. Letters by tracing the hidden text binary sequence by changing patterns of several cover code documents during the embedding phase. Using some unnecessary ASCII number system letters, these model modifications were integrated. By choosing English characters separated into two communities, the writer used the VERT technique. The documents comprise a direct row recognized as a G1 band hiding 1 piece of concealed information. Whereas a text comprising more than one row or not a vertical plain row is recognized as a band of G2 and hides concealed information of 0 bits.

[27] recommends a fresh technique of sms steganography to hide text messages in SQL providers. This technique is regarded a generation-based method that uses a dictionary of phrases organized into 65 classifications without common words to generate SQL queries from the hidden text. These classifications constitute 65 distinct personalities, including 26 English letters, 10 decimal numbers and 29 unique characters. features. The term to produce is selected from the dictionary, so this would lead in a distinct SQL query when altering the dictionary material.

Using Huffman coding, a writing steganography technique was suggested in[28]. In the forward email system, the confidential information is concealed. The authors used the range of symbols used in the email I d to refer to the secret data bits and took the secret data processed, adding the characters to the email I d to optimize the use of a number of characters.

5. Literature Discussion

By studying and analyzing the various articles in this and other literature, we notice that most of the above techniques and methods have enhanced (or attempted to enhance) one estate at the cost of other characteristics, although the other characteristics have shown some enhancement.

Is obviously small compared to the paper-focused enhancement of the primary estate. Most of these surveyed articles were directed at improving capability assets; however, nearly all of them accomplished a capability range of less than 20 percent, with the exception of three articles in which they expanded ability to 50 percent as in[19], 52 percent in[17] and 55 percent as in[21].

Some have mildly improved capability compared to their prior publications from other documents as in[16, 27, 28, 32, 35], some documents have mildly maintained ability and imperceptibility as in[18, 24]. 25, 26, 29] proved healthy ability, safety and robustness efficiency. The writers attained excellent imperceptibility in[20, 22, 23, 30].

Because these study concerns in capability ownership, we discovered in these checked articles that their highest quantity of integrated information is less than 56 percent where the two largest dimensions are 55 percent and 52 percent respectively in the form of sound and picture form. In addition, nearly all of these documents have a prevalent capability deficiency which is embedding the entire volume of confidential information in the display press. This document therefore attempts to perform a new method to solve this deficiency as well as the trade-off between the two characteristics (capability and imperceptibility)

6. Conclusions

This article shows ideas of common methods and algorithms in steganography. There are distinct kinds of techniques accessible for steganography. There is no restriction on the amount of techniques. Methods that focus on the capability estate and secondly on imperceptibility are provided significance here. Other characteristics of a "robustness and safety" steganogrpahic scheme are shortly stated in the chapter on literature. According to this document, 55% and 52% respectively in[21] and[17] are the highest volume of integrated information achieved by prior studies in this literature survey. This method involves transforming the hidden information on the cover foundation into a tiny portion

Considered a reference series. This series is the topic in place of the initial confidential information to be integrated. The initial volume of confidential information is considerably decreased from the preliminary job and integrated without distortion.

References

[1] Subhedar, Mansi S., and Vijay H. Mankar. "Current status and key issues in image steganography: A survey." Computer science review 13 (2014): 95-113.
[2] Barni, Mauro. "Steganography in Digital Media: Principles, Algorithms, and Applications (Fridrich, J. 2010) [Book Reviews]." IEEE Signal Processing Magazine 28.5 (2011): 142-144.
[3] Cheddad, Abbas. Digital Image Steganography: Concepts, Algorithms, and Applications. VDM Publishing, 2009.
[4] Solanki, Roshni, Monika Chuahan, and Madhavi Desai. "SURVEY OF IMAGE STEGANOGRAPHY TECHNIQUES.", IJARESM, ISSN: 2394-1766.
[5] Anandpara, Dimple, and Amit Kothari. "Working and comparative analysis of various spatial based image steganography techniques." International Journal of Computer Applications 113.12 (2015).
[6] Bazyar, Mohsen, and Rubita Sudirman. "A Robust Data Embedding Method for MPEG Layer III Audio Steganography." International Journal of Security and Its Applications 9.12 (2015): 317-327.
[7] Kamalpreet Kaur and Er. Deepankar Verma, "Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Encoding and Advanced LSB Technique", International Journal of Advanced Research in Computer Science, Volume 4, No. 9, July- August 2013
[8] Dieu, Huynh Ba, and Nguyen Xuan Huy. "An improved technique for hiding data in audio." Digital Information and Communication Technology and its Applications (DICTAP), 2014 Fourth International Conference on. IEEE, 2014.
[9] Lwin, Thandar, and SUWAI PHYO. "Information Hiding System Using Text and Image Steganography." International Journal of Scientific Engineering and Technology Research 3.4 (2014): 1972- 1977.
[10] Manjula, Y., and K. B. Shivakumar. "Enhanced secure image steganography using double encryption algorithms." Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on. IEEE, 2016.
[11] Mohan Megha, and Anitha Sandeep. "Multiple security enhancements for image steganography." Inventive Computation Technologies (ICICT), International Conference on. Vol. 1. IEEE, 2016.
[12] Verma, Vaidehi, and Trapti Ozha. "Enhancing the Security and Quality of Image Steganography Using a Novel Hybrid Technique." International Conference on Smart Trends for Information Technology and Computer Communications. Springer, Singapore, 2016.
[13] Ramalingam, Mritha, and Nor Ashidi Mat Isa. "A data-hiding technique using scene-change detection for video steganography." Computers & Electrical Engineering 54 (2016): 423-434.
[14] Zhang, Hong, Yun Cao, and Xianfeng Zhao. "Motion vector-based video steganography with preserved local optimality." Multimedia Tools and Applications 75.21 (2016): 13503-13519.
[15] Sharma, Shikha, and Devendra Somwanshi. "A DWT based Attack Resistant Video Steganography." Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. ACM, 2016.
[16] Ouyang, Linqiang, Jin H. Park, and Harbhinder Kaur. "Performance of Efficient Steganographic Methods for Image and Text." Journal of Advances in Information Technology Vol 7.1 (2016).
[17] Marghny H. Mohamed, Loay M. Mohamed, "High Capacity Image Steganography Technique based on LSB Substitution Method", Applied Mathematics & Information Sciences 10(1):259-266• January 2016.
[18] Zhaoxia Yin, Wien Hong, Jin Tang and Bin Luo "High capacity reversible steganography in encrypted images based on feature mining in plaintext domain", Int. J. Embedded Systems, Vol. 8, Nos. 2/3, 2016.
[19] Rashid, Aqsa, and Muhammad Khurrum Rahim. "Critical Analysis of Steganography "An Art of Hidden Writing"." International Journal of Security and Its Applications 10.3 (2016): 259-281.
[20] Ogiela, Marek R., and Katarzyna Koptyra. "False and multi-secret steganography in digital images." Soft Computing 19.11 (2015): 3331-3339.Mathematics & Information Sciences 10(1):259-266• January 2016.
[21] Bazyar, Mohsen, and Rubita Sudirman. "A Robust Data Embedding Method for MPEG Layer III Audio Steganography." International Journal of Security and Its Applications 9.12 (2015): 317-327
[22] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes." Machine Learning and Applications (ICMLA), 2015 IEEE 14th International Conference on. IEEE, 2015
[23] Khupse, Sneha, and Nitin N. Patil. "An adaptive steganography technique for videos using Steganoflage." Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on. IEEE, 2014
[24] Kaur, Ramandeep, et al. "Enhanced Steganographic Method Preserving Base Quality of Information Using LSB, Parity and Spread Spectrum Technique." Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on. IEEE, 2015
[25] Sadek, Mennatallah M., Amal S. Khalifa, and Mostafa GM Mostafa. "Robust video steganography algorithm using adaptive skin-tone detection." Multimedia Tools and Applications 76.2 (2017): 3065-3085.
[26] Osman, Baharudin, Roshidi Din, and Mohd Rushdi Idrus. "Capacity performance of steganography method in text based domain." ARPN Journal of Engineering and Applied Sciences 10.3 (2015): 1345-1351.
[27] Bassil, Youssef. "A Generation-based Text Steganography Method using SQL Queries." arXiv preprint arXiv: 1212.2067 (2012).
[28] Kumar, Rajeev, et al. "A high capacity email based text steganography scheme using Huffman compression." Signal Processingand Integrate