International Journal of Advanced Research and Development
ISSN: 2455-4030; Impact Factor: RJIF 5.24
Received: 17-06-2019; Accepted: 19-07-2019
www.advancedjournal.com
Volume 4; Issue 5; September 2019; Page No. 129-131

Review paper on Steganographic methods

Jyoti Kumari
Assistant Professor, Department of Computer Science, Keshav Mahavidyalaya, University of Delhi, New Delhi, India

Abstract
Steganography is characterized as the investigation of imperceptible correspondence. Steganography for the most part manages the methods for concealing the presence of the imparted information so that it stays private. It keeps up secrecy between two conveying parties. In image steganography, secrecy is accomplished by inserting information into cover image and producing a stego-image. There are various kinds of steganography methods each have their qualities and shortcomings. In this paper, we survey the distinctive security and information hiding methods that are utilized to implement a steganography, for example, LSB, ISB, MLSB and so forth.

Keywords: steganography, cryptography, LSB, BPCP, PVD, DCT, PSNR

1. Introduction
In this day and age, the communication is the essential need of each developing region. Everybody needs the secrecy and well-being of their imparting information. In our everyday life, we utilize many secure pathways like web or phone for moving and sharing data, yet it's not protected at a specific level. So as to share the information in a hid way two systems could be utilized. These methods are cryptography and steganography. In cryptography, the message is adjusted in an encoded structure with the assistance of encryption key which is known to sender and recipient as it were. The message can't be gotten to by anybody without utilizing the encryption key. In any case, the transmission of encoded message may effortlessly stimulate attacker's doubt, and the encoded message may along these lines be captured, attacked or decoded savagely. So as to defeat the inadequacies of cryptographic methods, steganography methods have been created. Steganography is the art and study of imparting so that it hides the presence of the communication. Along these lines, steganography hides the presence of information with the goal that nobody can distinguish its quality. In steganography the way toward hiding data content inside any interactive media substance like image, sound, video is alluded as an "Embedding". For expanding the classification of imparting information both the methods might be joined. The rest of the paper comprise of following area: II. Steganography III. End and Future Work.

2. Steganography
Steganography is a Greek word which means disguised composition. "steganos" signifies "covered " and "graphical" signifies "writing". Accordingly, steganography isn't just the specialty of hiding information yet in addition hiding the reality of transmission of secret information. Steganography conceals the secret information in another document so that lone the beneficiary knows the presence of message. In old time, the information was secured by hiding it on composing tables, the back of wax, on the scalp of the slaves or stomach of hares. In any case, the present the majority of the individuals transmit the information as content, images, video, and sound over the medium. So as to securely transmission of classified information, the sight and sound article like sound, video, images are utilized as a spread source to hide the information.

2.1 Types of steganography
a. Text steganography: It comprises of hiding data inside the content documents. In this technique, the secret information is taken cover behind each nth letter of each expression of instant message. Quantities of strategies are accessible for hiding information in content document. These techniques are I) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.
b. Image steganography: Hiding the information by taking the spread item as image is alluded as image steganography. In image steganography pixel powers are utilized to hide the information. In digital steganography, images are generally utilized cover source in light of the fact that there are number of bits exhibits in digital representation of an image.
c. Audio steganography: It includes hiding information in sound documents. This strategy shrouds the information in WAV, AU and MP3 sound records. There are various strategies for sound steganography. These strategies are I) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.
d. Video steganography: It is a method of hiding any sort of documents or information into digital video group. For this situation video (combination of images) is utilized as bearer for hiding the information. For the most part discrete cosine transform (DCT) adjust the values (e.g., 8.667 to 9) which is utilized to hide the information in every one of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the arrangements utilized by video steganography.
e. Network or protocol steganography: It includes hiding the data by taking the network protocol, for example, TCP, UDP, ICMP, IP and so forth, as spread article. In the OSI layer network model there exist incognito channels where steganography can be utilized.

2.2 Steganography terminology

Steganography comprises of two terms that is message and cover image. Message is the secret information that necessities to stow away and cover image is the transporter that shrouds the message in it.

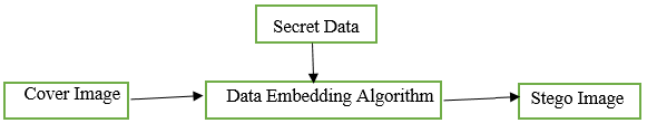

Fig 1: Steganography Diagram

2.3 Steganography Methods

a. Spatial domain method: In this technique the secret information is implanted legitimately in the power of pixels. It implies some pixel estimations of the image are changed straightforwardly during hiding information. Spatial domain methods are ordered into following classifications: i) Least significant bit (LSB) ii) Edges based information embedding technique (EBE) iii) Pixel value differencing (PVD) iv) Random pixel embedding method (RPE) v) Labeling or availability technique vi) Mapping pixel to hidden information technique vii) Pixel intensity based.
   1. LSB: this technique is most regularly utilized for hiding information. In this strategy the embedding is done by supplanting the least significant bits of image pixels with the bits of secret information. The image got in the wake of embedding is practically like original image in light of the fact that the adjustment in the LSB of image pixel does not get an excessive amount of contrasts in the image.
   2. PVD: In this strategy, two sequential pixels are chosen for embedding the information. Payload is dictated by checking the contrast between two successive pixels and it fills in as reason for recognizing whether the two pixels has a place with an edge area or smooth area.
   3. BPCP: In this division of image are utilized by estimating its complexity. Complexity is utilized to decide the noisy block. In this technique noisy blocks of bit plan are supplanted by the binary patterns mapped from a secret information.

b. Spread spectrum method: The idea of spread spectrum is utilized in this method. In this strategy the secret information is spread over a wide recurrence data transfer capacity. The proportion of signal to noise in each recurrence band must be little to the point that it become hard to distinguish the nearness of information. Regardless of whether parts of information are expelled from several bands, there would be still enough data is available in different bands to recuperate the information. Along these lines it is hard to evacuate the information totally without annihilating the cover. It is a strong procedure for the most part utilized in military communication.

c. Statistical Method: In the method message is embedded by changing a few properties of the cover. It includes the parting of cover into blocks and afterward embedding one message bit in each block. The cover block is altered just when the size of message bit is one, otherwise no change is required.

d. Transform Domain Method: In this method, the secret message is embedded in the change or recurrence area of the cover. This is a progressively intricate method for hiding message in a image. Various algorithms and changes are utilized on the image to hide message in it. Transform domain methods are comprehensively arranged as following: i) Discrete Fourier transformation strategy (DFT) ii) Discrete cosine transformation strategy (DCT) iii) Discrete Wavelet transformation strategy (DWT) iv) Lossless or reversible strategy (DCT) iv) Embedding in coefficient bits

e. Distortion Methods: In this method, the secret message is put away by twisting the signal. An arrangement of adjustment is connected to the cover by the encoder. The decoder estimates the contrasts between the first cover and the twisted cover to identify the succession of alterations and therefore recuperate the secret message.

f. Masking and Filtering: These methods shroud data by denoting an image. Steganography just hides the data whereas watermarks turns into an elixir of the image. These systems embed the data in the more significant areas as opposed to hiding it into the noise level. Watermarking methods can be connected without the dread of image annihilation because of lossy compression as they are increasingly incorporated into the image. This method is essentially utilized for 24-bit and grey scale images.

2.4 Variables affecting a steganographic method

The viability of any steganographic technique can be controlled by contrasting stego-image and the cover image. There are a few factors that decides the productivity of a system. These variables are:

a. Robustness: Robustness alludes to the capacity of embedded information to stay unblemished if the stego-image experiences changes, for example, linear and non-linear filtering, honing or obscuring, expansion of irregular noise, cropping or decimation, rotations and scaling, lossy compression.

b. Intangibility: The indistinctness implies imperceptibility of a steganographic algorithm. Since it is the as a matter of first importance necessity, since the quality of steganography lies in its capacity to be unnoticed by the human eye.

c. SNR (Signal to Noise Ratio): It is the proportion between the signal power and the noise control. It looks at the degree of an ideal signal to the degree of background noise.

d. Payload Capacity: It alludes to the measure of secret data that can be covered up in the cover source. Watermarking typically embed just a limited quantity of copyright data, while, steganography center at hidden communication also, along these lines have adequate embedding capacity.

e. MSE (Mean Square Error): It is characterized as the normal squared contrast between a reference image and a contorted image. The littler the MSE, the more proficient the image steganography method. MSE is figured pixel-by-pixel by including the squared contrasts of the considerable number of pixels and separating by the complete pixel count.

f. PSNR (Peak Signal to Noise Ratio): It is characterized as the proportion between the most extreme conceivable intensity of a signal and the intensity of defiling noise that influences the loyalty of its portrayal. This proportion estimates the quality between the unique and

a compressed image. The higher estimation of PSNR speaks to the better nature of the compressed image.

2.5 Steganographic applications

Confidential Communication and Secret Data Storing, E-Commerce, Database Systems, Media, Protection of Data Alteration, digital watermarking, Access Control System for Digital Content Distribution.

3. Conclusion and future work

In this exploration work we assessed on numerous papers on steganography methods. These papers are sufficient and have wide future degree. By assessing on these papers, we saw that the greater part of the steganography work is done in the year 2012 and 2013. In these years, LSB is the most broadly utilized method for steganography. A few specialists have additionally utilized the methods like watermarking, distortion methods, spatial methods, ISB, MSB in their work and gave a strong method for secure data transmission. The vast majority of the papers that are examined here are taken from IEEE Explore, AICCSA, IJET, IJCSE, IJCA and so forth. These papers give a great deal of assistance to the initiator for beginning their work in this field. This survey paper is sufficient for them to begin their work in this field. The distinctive security and information hiding procedures are utilized to execute steganography utilizing LSB, ISB, MLSB. In further look into we are going to utilize progressively advance plans like steganography with some mixture cryptographic algorithm for improving the information security.

4. References

1. Babu KS, Raja KB, Kiran Kumar K, Manjula Devi TH, Venugopal KR, Pataki LM. Authentication of secret information in image steganography, IEEE Region 10 Conference, TENCON, 2008, 1-6.
2. Chaumont M, Puech W. DCT-Based Data Hiding Method to embed the Color Information in a JPEG Grey Level Image", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, 2006, 4-8.
3. Amirtharajan R, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq, *et al*. Colour Guided Colour Image Steganography Universal Journal of Computer Science and Engineering Technology, 2010, 16-23, 2219-2158.
4. Yang, Chunfang, Liu, Fenlin, Luo, Xiangyang, Zeng, Ying. Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography, IEEE Transactions on Information Forensics and Security. 2013; 8:1.
5. Swati Malik, Ajit. Securing Data by Using Cryptography with Steganography International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3:5.
6. Ishwarjot Singh, Raina JP. Advance Scheme for Secret Data Hiding System using Hop field & LSB" International Journal of Computer Trends and Technology (IJCTT). 2013; 4:7.
7. Manikandan G, Sairam N, Kamarasan M. A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme, Research Journal of Applied Sciences, Engineering and Technology. 2012; 4(6): 608-614.
8. Shabir Parah A, Javaid Sheikh A, Bhat GM. Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique, International Conference on Emerging Trends in Science, Engineering and Technology, 2012, 192-197.
9. Michel Kulhandjian K, Dimitris Pados A, Ming Li, Stella Batalama N, Michael Medley J. Extracting spread-spectrum hidden data from digital media, IEEE transactions on information forensics and security. 2013; 8:7.
10. Fadhil Salman Abe. A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography, IJAIEM. 2013; 2:4.
11. Bailey K, Curran K. An Evaluation of Image Based Steganography Methods, Journal of Multimedia Tools and Applications. 2006; 30(1):55-88.
12. Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh. Triple-A Secure RGB Image Steganography Based on Randomization, International Conference on Computer Systems and Applications (AICCSA-), 2009, 400-403, 10-13.
13. Anil Kumar, Rohini Sharma. A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique, International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3:7.
14. Gutub A, Al-Qahtani A, Tabakh A. Secure RGB image steganography based on randomization, Computer Systems and Applications, AICCSA 2009, IEEE/ACS, 2009, 400-403.