International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 3951 -3959

Study and Analysis Of Steganalysis Techniques: A Systematic Review

Darpan Anand[1], Surender Singh[2], Saurabh[3]
darpan.e8545@cumail.in
[1]Associate Professor, [2]Associate Professor, [3]Assistant Professor,
Chandigarh University, Garuha , Punjab, India

Abstract

Web has become a wellspring of correspondence through which the data is transmitted, get inside such a messages, text, pictures, recordings, sounds and so forth. Presently a day's JPEG pictures are generally used in our everyday life. Correspondence that is happening between clients are regularly secure by utilizing Cryptography procedures which correspondence are frequently implanted by utilizing Steganography. Anyway Steganography will use in advanced conveys like content, picture, sound or video record for conceal insider facts reports. Presently every day Steganalysis might be another way to deal with search out and investigate the significant data which is concealing utilizing the steganography strategy. The steganalysis for JPEG kind pictures gets significant and significant. Steganalysis in pictures upheld DCT renovated locale, prepared to recognize the premier far reaching steganography calculations happening on web . Anyway execution of any calculation relying on affectability of alternatives and amount of information covered up during an image. This paper is gives an outline about steganography procedures and steganayisis strategies for computerized pictures to search out signal against to where to appear for concealed information in pictures, conversation about various steganayisis algorithmic projects, steganayisis grouping techniques, constraint and qualities of different steganayisis strategy.

INTRODUCTION

Steganography is that the cycle that shroud significant data and structure two kinds of data that is spread and stego[1]. While in cryptography the messages are scrambled, which message are frequently decoded by expected beneficiary. In Steganography procedures are wont to shroud data like picture, sound with another data all together that lone sender and recipient can see the concealed data. Though steganayisis is that the way toward identifying that concealed data and the process of detecting that hidden information. There are various kinds of steganography have been available in literature. The upcoming sections are discussing some important terminologies.

[A] IMAGE STEGANOGRAPHY:- Steganography is that the way toward concealing data into another data. an image with a mystery message covered up is named as stego picture though a quick picture is named as spread picture. These methods are regularly utilized with fluctuated degrees of achievement on contrasting sorts of picture documents.

[B] IMAGE STEGANALYSIS:- Important data are covered up by Steganography. Inside the picture presence of the message are hides. In Steganography extraction and change procedures are utilized for discovery yet in steganayisis the stego object and non stego object are allude in dazzle steganalysis technique. While not past information of strategy won't to cover the information [3].The picture during

ISSN: 2233 -7857 IJFGCN

which the key information is covered up is perceived as stego picture. The location of shrouded implanted information inside the picture without earlier information about information concealing calculation is that the fundamental focus on dazzle picture Steganalysis. An outsized number of steganalysis methods are accessible for the identification of steganography inside the picture [11].
Steganalysis method can be divided into two different categories as per the detecting presence of any hidden messages.

TYPE OF STEGANALYSIS:-
Some circumstance the steganalysis technique is trusted Steganography calculation. Be that as it may, in some circumstance Steganalysis utilize own technique for distinguishing presence of concealed message bases consequently Steganalysis are arranged in two unique classes.

1) Specific steganalysis.
2) Blind steganalysis

SPECIFIC STEGANALYSIS: In this specific and explicit steganalysis procedure there is a Steganalysis calculation that is wont to distinguish the concealed data by Analyzing the factual properties that are upheld the exact steganalysis technique. As we get the exact outcomes once we utilize explicit steganalysis strategy . There ought to be explicit information on the calculation that is utilized for recognition subsequently, it's the most impediment of this framework.

BLIND / UNIVERSAL STEGANALYSIS: As we there is no requirement of knowledge of which embedding algorithm to be used , so this is the best method to detect the presence of the hidden information. This provide less accurate results as compared to specific steganalysis technique. But it is a power full technique because we are not dependent on specific algorithm.
In general the classification of the steganography is illustrated in figure-1. The details of each type can be explained as:-

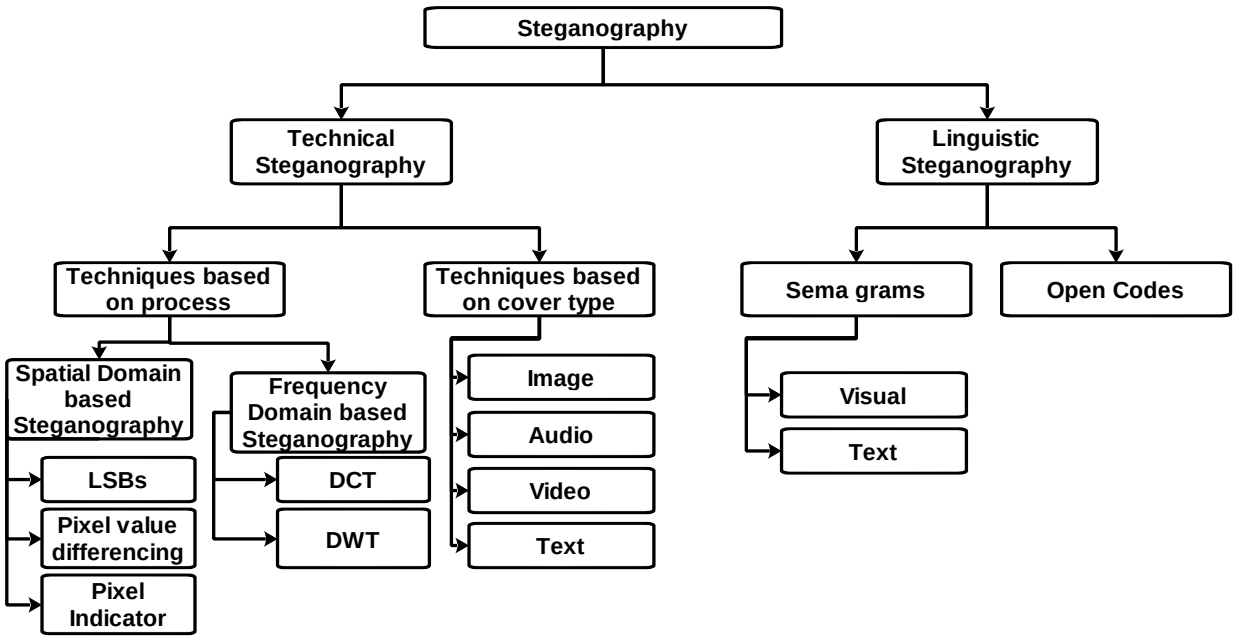

Figure 1: Classification of Steganography

ISSN: 2233 -7857 IJFGCN

LINGUISTIC STEGANOGRAPHY: This type of steganography is very much useful for hiding the message through the cover text used in this technique. While, it is not an obvious technique because outside cannot imperceptible the presence of messages. Further this technique can be classified as the following techniques.

A) Semagrams:- The semagrams is the specific type of steganography technique in which the various signs and symbols are used to hide the secret information. Further, this type of technique can be classified as:-

1. **Visual Semagrams:** As name reflected for visual semagrams, the physical objects are to be used to convey the messages. These objects are being used in this technique should be from the objects addressed by the user every day like the positioning of items on a particular website.
2. **Text Semagrams:** The text semagrams are the specific type of steganography technique used to hide the secrete message through a process of modification over the appearance of the carrier text. This technique further used the technique to change the font size, font type add extra space between sentences & words, or any other formatting means and technique.

B) Open Code: - The Open code technique is a specific type of linguistic steganography in which the secrete message is inserted/embedded in paragraph, paraphrase of the language used to cover it. This process should be processed in such a way that it appears not obvious to an unsuspecting observer. There are various ways to achieve this hiding through Open Code technique as Jargon and Cipher. Jargon is only understand by the specific group of people while other i.e. Cipher can extracted and processed only through some important feature 'secrete key'.

TECHNICAL STEGANOGRAPHY: It is a special type of steganography which is used to hide the secrete message through the special devices, hardware, tools, and scientific methods like use of microdots, invisible ink, various computer based techniques or hide the message to kept in secrete place, etc.

A) COVER: The cover message of object is very important for steganography because it is working as carrier of the secrete message. It may be an image, audio, video, text or any other digital media.

These digital objects are divided in to small blocks and bits of message which will use for hiding the secrete message in each identified block. The secrete message is embedded or encoded through changing of various features and properties of the cover image. The cover blocks remain unchanged if message block is zero.

a. Text Steganography: Random character sequences will be generated through context-free grammars or changing the formatting. In this methodology the spread content is delivered by creating arbitrary character successions, changing words inside a content, utilizing setting free sentence structures or by changing the organizing of a current book to cover the message. The spread content produced by this methodology can fit the bill for phonetic steganography if text is phonetically determined. Despite the fact that these content based strategies has its own novel qualities for spread content however experiences different issues from both an etymological and security angle [9] [10].
b. Image Steganography:- This Steganography method is more famous in ongoing year than other steganography conceivably in view of the surge of electronic picture data accessible

ISSN: 2233 -7857 IJFGCN

with the coming of computerized cameras and rapid web conveyance. It can include concealing data in the normally happened commotion inside the picture. Most sorts of data contain some sort of clamor. Commotion alludes to the blemishes characteristic during the time spent delivering a simple picture as a computerized picture. In Image steganography we can shroud message in pixels of a picture. A picture steganographic conspire is one sort of steganographic frameworks, where the mystery message is covered up in a computerized picture with some concealing technique [11]. Somebody would then be able to utilize an appropriate unraveling method to recuperate the concealed message from the picture. The first picture is known as a spread picture in steganography, and the message-inserted picture is known as a stego picture [12] [13]. Different techniques for picture steganography are:

i. **Data Hiding Method:** hiding the data, a username and password are required prior to use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image. This method is used to hiding the existence of a message by hiding information into various carriers. This prevents the detection of hidden information.

ii. Data Embedding Method: For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. The process of embedding the message inside the image, a secret key is needed for retrieving the message back from the image, the secret message that is extracted from the system is transfer into text file and then the text file is compressed into the zip file and zip text file is converting it into the binary codes [15].

iii. Data Extracting Method: It is used to retrieve an original message from the image; a secret key is needed for the verification. And for extracting method, a secret key is needed to check the key is correct with the decodes from the series of binary code. If key is matched, the process continues by forming the binary code to a zipped text file, the unzip the text file and transfer the secret message from the text file to retrieve the original secret message

c. Audio Steganography:- Audio steganography, the hiding of messages in audio “noise” (and in frequencies which humans can’t hear), is another area of information hiding that relies on using an existing source as a space in which to hide information. Audio steganography can be problematic and can be useful for transmitting covert information in an innocuous cover audio signal. There are various types of audio steganography based on features of audio as:-

i. Echo Hiding based audio Steganography:- This method embeds data or text into audio signals by adding a small echo to the host signal. The Nature of the echo is a resonance added to the host audio. Then the data is invisible by varying three echo parameters: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded

ISSN: 2233 -7857 IJFGCN

ii. Phase Coding based audio Steganography:- One of the most effective coding methods in terms of the signal-to perceived noise ratio. In this phase components of sound are not as perceptible to the human ear as noise is. It can be done by substituting the phase of an initial audio segment with a reference phase that represents the data. It encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio subsequent segments is then adjusted store the relative phase between segments. Disadvantage: It is a complex method and has low data transmission rate

iii. Parity Coding based audio Steganography:- This method breaks a signal down into different regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of selected region does not match the secret bit to be encoded, Disadvantage: This method like LSB coding is not robust in nature. Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner

iv. Spread Spectrum based audio Steganography:- This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. It is used to encode a category of information by spreading the encoded data across frequency spectrum. This allows the signal reception, even if there is interference on some frequencies. Disadvantage: It can introduce noise into a sound file

v. Tone insertion based audio Steganography:- In this inaudibility of lower power tones in the presence of significantly higher ones. Tone insertion method can resist to attacks such as low-pass filtering and bit truncation addition to low embedding capacity, embedded data could be maliciously extracted since inserted

B) Steganography Techniques based on process:- In spatial domain, images are represented by pixels. Simple watermarks could be embedded by modifying the pixel values or the least significant bit (LSB) values [20]. It directly loads the raw data into the image pixels. Some of its algorithms are LSB, SSM Modulation based technique.

a. Steganography based on Spatial Domain: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms.

i. Least Significant Bit (LSB): This is the most common, simple approach for embedding data in a cover image. The least significant bit (8th bit) of one or all of the bytes inside an image is changed to a bit of the secret message.

ii. Pixel Value Differencing: It provides both high embed-ding capacity and outstanding imperceptibility for the stego-image; this segments the cover image into non overlapping [8] blocks containing two connecting pixels and it modifies the pixel difference in each pair for data embedding.

iii. Pixel Indicator: This method gives the stego images of better quality than the traditional method while maintaining a high embedding capacity and it also uses concept of hiding the data using the difference between the pixel values [20]. It’s

ISSN: 2233 -7857 IJFGCN

more complex way of hiding information in an image. Transformations are used on the image to hide information in. Transform domain embedding can be termed as a domain of embedding techniques in frequency domain; image is represented in terms of its frequencies.

b. Steganography based on Frequency Domain:
    i. Discrete Cosine Transformation:- These methods convert the uncompressed image into JPEG compressed type[22]It is based on data hiding used in the JPEG compression algorithm to transform successive 8x8- pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain. [23]The main advantage of this method is its ability to minimize the block like appearance resulting when boundaries between the 8x8 sub-images become visible.
    ii. Discrete Wavelet Transformation: It gives the best result of image transformation .it splits the signal into set of basic functions .there are two types of wavelet transformation one is continuous and other is discrete [24] This is the new idea in the application of wavelets, in this the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. It also performs local analysis and multi-resolution analysis. DWT transforms the object in wavelet domain and then processes the coefficients and performs inverse wavelet transform to show the original format of the stego object [25].

There is a requirement of features to identify the steganography specially for the classification. There are various features available for steganography listed in literature. These features are also very important to evaluate the quality of the steganography. Some of important features are listing in this manuscript as:-

- Transparency: The steganography should not affect the quality of the original image after steganography.
- Robustness: Steganography could be removed intentionally or unintentionally by simple image processing operations like contrast or enhancement brightest gamma correction, steganography should be robust against variety of such attacks.
- Data payload or capacity: This property describes how much data should be embedded as a steganography to successfully detect during extraction.
- Imperceptibility: The imperceptibility means invisibility of a steganographic algorithm. Because it is the first and Secret Data Cover Image Data Embedding Algorithm Stego- Image foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.
- Payload Capacity: It refers to the amount of secret information that can be hidden in the cover source. Watermarking usually embed only a small amount of copyright information, whereas, steganography focus at hidden communication and therefore have sufficient embedding capacity.
- PSNR (Peak Signal to Noise Ratio): It is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between the original and a compressed image. The higher value of PSNR represents the better quality of the compressed image.
- MSE (Mean Square Error): It is defined as the average squared difference between a reference image and a distorted image. The smaller the MSE, the more efficient the image steganography

ISSN: 2233 -7857 IJFGCN

technique . MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

- SNR (Signal to Noise Ratio): It is the ratio between the signal power and the noise power. It compares the level of a desired signal to the level of background noise.

II. LITERATURE REVIEW

Yiqin Zhang and Fenlin Liu, et.al [1] in this paper proposes a feature selection based on Fisher criterion. Supported the principle that "The within-class variance ought to be smaller and between-class variance ought to be larger". Within the experimental analysis wealthy model SRM that may be won't to find typical fashionable steganography Victor-Marie Hugo.

Madhavi B. Desai the author describe et.al [2] in their paper proposes based on Fisher Criterion and multivariate analysis techniques. These methods contain dimensional unified feature set for universal image steganalysis. The planned algorithmic rule achieves overall 97% detection accuracy against various steganography techniques.

Punam Bedi, et.al [3] in their paper proposes a feature selection technique that works for a unique feature choice algorithmic rule (FS-SDS) for steganalysis. FS-SDS may be a wrapper-type feature selection algorithmic rule that selects reduced feature set based on mistreatment random Diffusion Search.

Z. X. &. X. W, et.al [4] in their paper proposes the models for the messages embedded by spatial least vital bit (LSB) matching as freelance noises to the duvet image, and divulges that the bar chart of the variations between element grey values is smoothened.

Zhihua Xia, et.al [5] in their paper proposes the models for the learning-based steganalysis and detection technique to attack patial domain least vital bit (LSB) matching steganography in grayscale pictures.

Xiao feng Song et.al [6] in their paper describe about the 2D Gabor filters that bound the optimum joint localization properties within the spatial domain and within the spatial frequency domain. The experimental results show that the detection error EOOB is given for quality factors 75% and 95%.

Madhavi B. Desai, et.al [7] in their paper describe about the value the performance of DWT feature based mostly steganalysis algorithms against varied state-of-art steganography ways and variable message embedding rates. This paper additionally presents the comparative performance of individual algorithms against totally different classification ways.

Yi Zhang, et.al [8] in their paper describe about strategies to boost the detection performance for content-adaptive JPEG steganography. The planned technique generates filtered pictures comprising wealthy texture and edge data victimization Gauss partial filter bank, and histograms of absolute values of filtered sub pictures.

Daniel Majercak et.al in their paper proposes Feature-based Steganalysis strategies method. [9] The objective is performance testing of Feature-based Steganalysis strategies for detection of steganography tools that area unit used for activity a secret message in still pictures. Feature extraction during this paper was applied in spatial domain and conjointly directly in transformation domain of DCT in JPEG files what helps to obtained relevant applied mathematics information.

Oswaldo Juarez-Sandoval et.al in their paper discuss about strategies proposes Feature-based Steganalysis strategies method. [10] The author propose a compact image steganalysis technique for the LSB-matching steganography, during which a feature vector composed by solely twelve parts is extracted from the image. By practical they Achieving 99.626% steganalyzer sensitivity on 0.25bpp stego images of the dataset by only two analysis dimensions.

APPLICATION OF STEGANEOGRAPHY:-

i) Confidential Communication and Secret Data Storing

ISSN: 2233 -7857 IJFGCN

ii) Protection of Data Alteration
iii) Access Control System for Digital Content Distribution
iv) E-Commerce
v) Media
vi) Database Systems.
vii) digital watermarking.

CONCLUSION

In this paper, we review the various fundamental concepts and different steganalysis techniques, so that we can say that steganalysis is meant to reverse of steganography. In the steganalysis, we use two different methods feature extraction and classification for detecting the steganography algorithm. For improving the accuracy rate there is requirement of efficient feature selection technique that reduces the redundant features and improves the accuracy rate. So by identifying a minimum number of features we can develop a better image steganalysis algorithm. It will provide better classification result. Blind image steganalysis has an advantage over Specific steganalysis, because in blind image steganalysis there is no requirement of any prior knowledge about data hiding methods. Therefore, it could be applicable to any type of image and file format. After finding the reduced feature sets we can use different classification techniques like Bayesian, ANN, SVM. By comparing their results, we get to know that which methods are given high accuracy.

REFERENCES

[1] H. j. J. L. a. C. Y. Yiqin Zhang and Fenlin Liu, "Compact Image Steganalysis for LSB-Matching Steganography", International Conference on Advanced Computational Intelligence (ICACI), pp. 187-192, 2018.

[2] S. V. P., B. P. Madhavi B. Desai, "ANOVA and Fisher Criterion based Feature Selection for Lower Dimensional Universal Image Steganalysis", IJIP, 2016.

[3] V. B. N. M. a. T. C. Punam Bedi, "FS-SDS: Feature Selection for JPEG Steganalysis using Stochastic Diffusion Search", IEEE, pp. 3797-3802, 2014.

[4] Z. X. &. X. W. &. X. S. &. Q. L. &. N. Xiong, "Steganalysis of LSB matching using differences between nonadjacent pixels", Springer, 2014.

[5] f. l. C. Y. Xiaofeng Song, "Steganalysis of Adaptive JPEG Steganography Using 2D Gabor Filters, IJRITCC, 2015.

[6] S. V. P. Madhavi B. Desai, "Performance Analysis of Image Steganalysis against Message Size, Message Type and Classification Methods", IEEE, 2016.

[7] F. L, C. Y, X. L. X. S. J. L. Y. Yi Zhang, "Steganalysis of contentadaptive JPEG steganography based on Gauss partial derivative filter bank",Journal of Electronic Imagin , 2017.

[8] Daniel Majercak, Vladimir Banoci, Martin Broda, Gabriel Bugar, Dusan Levicky"Performance Evaluation of Feature-based Steganalysis in Steganography", Conference Radioelektronika 2013, April 16-17.

[9] M. C.-H. Oswaldo Juarez-Sandoval, "Compact Image Steganalysis for LSB-Matching Steganography", IEEE, 2015.

[10] J.Anita christaline, R.Ramesh, D.Vaishali "Steganalysis with classifier combinations",ARPR-2014, pg. no-2858-2863.

[11] S.K.Sabnisa,R.N.Awaleb" Statistical Steganalysis of High Capacity Image Steganography with Cryptography",Elsevier2016,321-327.

ISSN: 2233 -7857 IJFGCN

[12] Zohaib Khan, Atif Bin Mansoor "An Analysis of Quality Factor on Image Steganalysis" ,IEEE-Conference Paper · April 2010.
[13] Sruthi Das N1, Rasmi P S"A Survey on Different Image Steganalysis Techniques",IJMTER-2015,533-536.
[14] S.Geetha, shiva s.shivtha sandhu, N. kamraj"blindimagesteganalysis based on contentindependentstatisticalmeasures maximizing the specificity and sensitivity of system", Elsevier-2006, pg N0683-697.
[15] Ismail Avcıbas¸Mehdi Kharrazi,Nasir Memon,B¨ulent Sankur"Image Steganalysis with Binary Similarity Measures",EURASIP Journal on Applied Signal Processing 2005:17, 2749–2757.
[16] Yi Zhang, Fenlin Liu ,Chunfang Yang ,Xiangyang Luo,Xiaofeng Song, Jicang Lu"Steganalysis of content-adaptive JPEG steganography based on Gauss partial derivative filter bank",Journal of Electronic Imaging-2017.
[17] Manisha Saini, Rita Chhikara "performance Evaluation of DCT and DWT Features for Blind Image Steganalysis using Neural Networks" International Journal of Computer Applications- March 2015 (0975 – 8887).
[18] Dr. Monisha Sharma1 and Mrs. Swagota Bera" a review on blind still image steganalysis techniques using features extraction and pattern classification method", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.3. Vol.2, No.3.June 2012.
[19] Rita Chhikara, Latika Singh" A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted", International Journal of Engineering and Innovative Technology (IJEIT) - October 2013Volume 3, Issue 4.
[20] K. Nandhini1, B. Gomathi" Implementation of LSB Based Steganography Algorithms in FPGA", IJSRNSC, Volume-6, Issue5, June 2017.
[21] Rajesh Shah, Yashwant Singh Chouhan "Encoding of Hindi Text Using Steganography Technique", ISROSET- Int. J. Sci. Res. in Computer Science & Engineering Vol-2, Issue-1, PP (22-28), Feb 2014.
[22] P. Kaur, S. Chatterjee, and D. Singh, "Neural network technique for diabetic retinopathy detection," Int. J. Eng. Adv. Technol., vol. 8, no. 6, pp. 440–445, 2019.

ISSN: 2233 -7857 IJFGCN