IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Analysis and Review of the Steganographic Techniques

H.A. Patil[1*], P. Saxena[2]

[1,2] Computer Science & Engineering , Jaipur National University, Rajasthan, India

[*]*Corresponding Author: pharshal2288@gmail.com, Tel.: +91-9833161531*

Available online at: www.ijcseonline.org

Accepted: 18/Nov/2018, Published: 30/Nov/2018

***Abstract*—** Nowadays, the security associated with information over the web has turned into a significant issue. With the aim to take care of the issue, two fundamental procedures are utilized cryptography and Steganography. The two strategies are utilized for information security reason. Cryptography changes the type of the information and Steganography totally hides its core from the clients, aside from the proposed recipient. The steganography implies secured script while cryptography implies mystery composing. In this paper, a strategy is defined which joins these two techniques to give a more productive and successful outcome. In this paper, different steganographic methods have been analyzed. These methods include text hiding, audio hiding, file hiding and image hiding. This paper reviews and analyzes many existing digital image steganographic methods in both the spatial and transform domains.

***Keywords*—**Steganography, Data hiding, Cryptography, spatial domain, transform domain

I. INTRODUCTION

In general, clients on the web need to send, share or get private data. Because of fast improvement in both PC advances and Web, the security of data is viewed as a standout amongst the most crucial components of Information Technology and association. Steganography has developed as an incredible and effective instrument which gives abnormal state of security especially when it is joined with encryption. Steganography is a Greek word it implies disguised composition. "Steganos" signifies "secured" and "graphical " signifies "stating" . Genenerally, it is known as "Hidden Communication".

Hence, steganography isn't just the craft of concealing information yet additionally concealing the verity of transmission of covert information. Steganography shrouds the secure information in another document so that only the beneficiary knows the presence of message. In antiquated time, the information was secured by concealing it on the back of wax, composing tables. In any case, the present a large portion of the general population transmit the information as content, pictures, video, and sound over the medium. With the aim to securely transmit the classified information, the interactive media objects like sound, video, pictures are utilized as a cover sources to shroud the information.

Steganography system is utilized to install and conceal important information into another kind of information for security purposes. Various carter record activities can be utilized yet advanced pictures are the most well known ones in light of their recurrence on the Web. The primary objective of image steganography is to conceal the presence of the information message from illicit goal. For concealing the secure data in pictures, there exist a variety of steganography procedures based on spatial domain, transform domain, spread spectrum techniques, distortion techniques, masking, and filtering.

One of the most important areas which attracted by peoples are security is related to internet and also related to communication. At present, security for hiding data is most popular technique which receives more attention than cryptography. Various methods are used for hidden communication. The major benefit of Steganography over other coding techniques is that it hiding the data inside other data in such a way that no other person recipient, even know the existence of it.

Steganography is categorised among three types which are pure, symmetric and asymmetric. Symmetric and asymmetric steganography are used when encryption is applied by means of providing secure data transmission where a secret key (stego-key) is needs to be exchanged before transmission of the data. Similarly, no key is exchanged in pure steganography. When both cryptographic and steganography

techniques are used to protect data, a high security level will be provided.The data is doubly secured by encrypting the message in a cover medium before it is hidden.
In particular, the steganography technique consists of covers that are used to hide data inside and secret data that is referred to as data or messages that are hidden inside the covers. The combination of the media and secret data is known as stego-media. It can be recognized as steganography. In addition to these components, Stego-key may be used when data is encrypted using cryptography techniques before concealing data by stenographic techniques.
As illustrated in Figure 1, same stego-key must be used in the receiver of the message to conduct steganalysis process to extract the embedded secret data from the stego-media

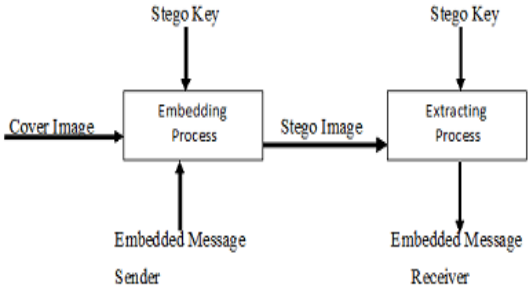

Fig 1: Image Steganography

Figure 1 depicts the process of inserting the secret data through the steganography process using the stego-key to produce stego-media into the cover media. Stego-media will then be sent to destination. The receiver requires a stego-key to extract the secret information from the stego-media during the process of steganalysis. During the steganography process, users must ensure that stego-media looks the same as the media cover.

Section I contains the introduction of steganography, Section II contain classification of steganography, Section III contain some approaches to classify the techniques of steganography, Section IV contain the related work done in the field of data hiding, section V concludes the research work.

II. STEGANOGRAPHY CLASSIFICATION

Depending on the type of the cover object, many appropriate steganographic classifications are used to obtain security
a) Image Steganography:
This Steganography conceals the message in the images. This is the most popular technique because no apparent changes occur. Most commonly used image cover methods are least significant bits (LSB). The substitution of the cover pixel in the LSBs is changed to hide the payload and more data can be hidden in the edges.

b) Video Steganography:
Video steganogrphy is a technique for hiding data or files in digital video format. Video is hidden information carrier. Generally discrete cosine transforms (DCT) correct values used to hide the information in each of the images in the video that the human eye does not notice. H.264, Mp4 and MPEG, AVI or other video designs are used for video steganography.

c) Audio Steganography:
When audio is used as a carrier to hide information, it is known as audio steganography It has become a very important medium due to the popularity of voice over IP (VOIP). Audio steganogrphy uses digital audio formats for steganography, like WAVE MIDI, AVI MPEG, etc.

d) Text Steganogrphy:
Number of tabs, white spaces and capital letters, like Morse code, etc. are the general technique used to hide information in text steganography.
Steganographic measurements are described below

i. High capacity: the maximum data size can be integrated into the image.
ii. Perceptual Transparency: After the process of hiding into the cover image, the perceptual quality is degraded to the stego image in comparison with the cover.
iii. Robustness: Data should remain intact after embedding if the stego image enters into some transformation, such as cropping, scaling, filtering and adding noise.
iv. Temperature resistance: the message should be difficult to change once it has been embedded in the stego image
v. Computing Complexity: How costly is it to embed and extract a hidden message in a computer?

.

III, STEGANOGRAPHY TECHNIQUES

There are some approaches to classify the techniques of steganography:
1. Substitution Technique (Spatial Domain):
These techniques attempt to encode secret data by replacing small portions of the cover image with secret data bits. It includes many techniques such as minor bit substitution, pseudorandom permutation, etc. The most common and simplest method of steganography is the least important method of insertion (LSB). In this technique, the smallest bits of the pixels are replaced by the message bits before embedding. Most steganography software hides information by replacing only the smallest bits (LSB) of an image with hidden bits from the file. Generally, this technique is called LSB encoding. One of the most common steganography techniques

The following example shows how the letter A can be hidden in a 24-bit image in the first 8 bytes of 3 pixels.
Pixels:

(10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)

Secret message: 01000001

Result:

(1010111**0** 11101001 10101000)
(1010011**0** 01011000 1110100**0**)
(11011000 10000111 01011001)

The three bold bits are actually the only three bits that have been changed. Since the 8-bit letter A requires only 8 bytes to hide it, the ninth byte of the three pixels can be used to hide the next hidden message character. A minor change in this technique allows the message to be embedded in two or more of the least important bits per byte. This increases the cover object's hidden information capacity, but the cover object is further degraded and therefore more detectable.

2. Transform Domain Technique:
These techniques conceal messages in an important part of the cover image that makes them more attackable. It includes DCT, DWT methods.

3. Spread Spectrum Technique:
In this technique, it attempts to spread a secret message over a cover so that it can not be recognized. It's difficult to delete the embedded message using this technique. It contains two types of methods: -one is the direct sequence method and the second is the hopping frequency.
4. Distortion Technique:
This technique requires the knowledge in the decoding process of the original cover. Most hiding methods based on texts are distortion-type.

IV. RELATED WORK

LSB Steganography Detection Algorithm Gradient Energy-Flipping Rate (CEFR) has been proposed by Zlii, Yang and Xian[1]. The analysis of gradient energy variation, LSB color and gray scale image, detects the secret message embedded in the target image, and estimates the length of the embedded message in this method.

In Anindya Sarkar .al.'s paper[2] proposes a steganography based on Matrix Embedding with Repeat Accumulate (ME-RA), in which the host coefficients are minimally disturbed so that the transmitted bits fall into a linear code coset and the syndrome transmits the hidden bits. For error correction, a powerful repeat accumulate code is used. The authors compared the methods QIM (quantification index modulation) and ME-RA. Comparisons with a slight modification of the ME-RA (puncture and non-shrinkage) methods are also tabulated with different decoding methods. The authors emphasize that the use of ME instead of QIM within the YASS(another steganographic scheme) provides improved steganalysis performance but complexity of software is more important

In article[3] by Jasvinder Kaur et.al., the authors analyze various steganographic techniques based on digital logic and propose a new improved steganographic technique based on this. The carrier image depends on the information to be carried. This technology uses digital operations based on logic gates and shift operators to incorporate / derive the hidden information from image data. The carrier image is divided into rows depending on the size of the information to be embedded and the data is embedded by digital operation.

In Mamta Juneja al's[4] research paper proposesan adaptive steganography based on a robust, secure approach to information security. It presents two component-based LSB (Least Significant Bit) methods for the integration of secret data into the blue components of the LSB and partial green components of random pixel locations at the edges of the image.

In rajesh shah et.al[5] method data is embedded in the red image plane and a random number generator is used to select the pixel. The changes in the images are almost impossible to notice. In order to select pixel locations a stego key is used to seed the PRNG (Pseudo Random Number Generator).

In article[6] of M.B.Ould MEDENI et.al., the authors use error correction codes in steganographic protocols. An optimal code is the maximum embeddable code (MLE). The method known as matrix encoding requires the sender and the receiver to agree on a parity control matrix H in advance. The cover media is processed to extract a TE symbol sequence, which is which is changed in s to embed,s is sometimes referred to as the stego data, and modifications on s are translated into the cover medium to obtain the stego. The relationship between algorithms of steganography and error correction codes is discussed.

In[7] Rajkumar Yadav et. present a study of a new method of inserting messages into an image.To insert and retrieve messages, the last two bits of pixel value are used. If the last two bits of pixel value are 00 or 10, we can insert 0, otherwise we can insert 0 by adding / subtracting 1 to the pixel value. Likewise, if the last two bits are 01 or 11, 1 is inserted.

Parul et al.,[8] introduced a modified, high - capacity, secure steganography scheme to hide a large secret image into a small cover image. The transformation arnold is carried out

to scramble the secret image. Discrete Wavelet Transformation (DWT) is carried out in both images and followed by Alpha mixing. The Inverse Discrete Wavelet Transformation (IDWT) is then used to obtain the image of the stego.

C.H.Yang[9]. proposes a predictive method for enhancing the histogram-based reversible data hiding approach**.** Two predictive interleaving stages are used. The majority of pixels are predicted in the column-based and chess-board approach by their two neighborhood pixels and four neighboring pixels.The difference between the original image and the stego image of each pixel remains within ± 1. Pixels in strange columns are predicted by pixels in even columns, or vice versa, in interleaving predictions. Predictive error values of strange columns are used in the embedding process to generate a histogram for embedding secret data. To get the stego image, the predictive error values are converted.
A session-based encryption and cross-fold transposition are used for embedding by authors. The secret text is converted to its binary form and fold-over is carried out[10].

Fahim Irfan et. paper[11] suggests noise filtering before embedding at the beginning. ARQ (Automatic Repeat Request) is used to detect and correct errors after extraction at the receiving end. In order to ensure safe data transmission, encryption and data hiding are combined in one step.

In Keith.L. Haynes article [12] author studies the use of image steganography to infringe the physical and cyber defenses of an organization. The proposed method uses computer vision and machine learning techniques to produce undetectable messages which can not be decrypted without key compromises when intercepted. DWT (Discrete Wavelet Transform) is used to prevent detection. The objective of a computer vision system is to enable machines to analyze an image and to decide the content of the image. Computer vision can be classified as model - based & appearance-based, using example images and machine learning techniques to identify important areas or aspects of images that are important for the discrimination of image objects. Machine learning is different from learning with human knowledge. A computer must decide whether a face is present on the basis of the numbers in a 2D matrix. The feature is identified by selecting the hair feature. The aim is to identify the set of characteristics that best distinguish images in different classes. The proposed method does not contain a secret message in the cover image, but rather the classification of the image results in a hidden message. Since the proposed algorithm uses ordinary unmodified images, no inherent hidden communication indicators exist.

In 2014, Sunny Dagar[13] proposed a new approach to image steganography in his paper. In which it uses two secret keys to randomize the process of hiding. This selection of two keys increases the level of secret information security. This approach uses a pixel's red, green and blue values and calculates them. Based on this calculation, secret information bits are placed in the pixel random position. This approach maintains a high capacity for data hiding, such as LSB substitution, but maintains a much better level of security than simple LSB substitution, because we know that LSB substitution is predictable.

In Gaikwad, D.P. et. al.'s paper[14]the authors propose a technique for image restoration in steganography. The image is blurred before the message image is hidden with a special point spreading function and a random key. In this project, sequential LSB embedding in the R plane is carried out. In the first row of the cover image the number of rows and columns of the message image are encrypted. The original message image is blurred using the specific PSF (Point Spread Function) before inserting. The parameters used to blur with PSF are used as de-blurring keys. The secret key values are transmitted via a safe channel (Tunneling). The secret image is recovered using both keys and a third key, which is generated randomly and depends on the content of the message.
In article by Hemalatha .S et. al. [15],Integer Wavelet Transform (IWT) has been suggested that several secret images and keys be hidden in a more efficient color cover image. The cover picture is shown in YCbCr color space. Two keys are obtained through IWT, encrypted and hidden in the cover image.

V. CONCLUSION

The analysis shows that the transform domain techniques are best suited for an attack-resistant system with relatively lower data capacity and greater complexity, while the spatial domain is best suited for limited complexity systems and also offers greater options for selecting techniques for systems with limited computer power.

REFERENCES

[1] S Zlii Li,Yang S. A. F. , Xian Y (2003)," A LSB Steganography Detection Algorithm", The 14th IEEE 2003 International Symposium on Persona1,Indoor and Mobile Radio Communication Proceedings.pp.2780-2783.

[2] Anindya Sarkar, Member, IEEE, Upamanyu Madhow, Fellow,IEEE, and B.S.Manjunath, Fellow, IEEE, (2010) "Matrix Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography", IEEE Transactions on Information Forensics and Security, Vol.5.No.2, pp.225-239.

[3] Jaswinder Kaur, Inderjeet & Manoj Duhan, (2009) "A Comparative Analysis of Steganographic Techniques", International Journal of Information Technology and Knowledge Management, Vol. 2, No. 1, pp 191-194
[4] Mamta Juneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.
[5] Rajesh Shah and Yashwant Singh Chouhan, "*Encoding of Hindi Text Using Steganography Technique*", International Journal of Scientific Research in Computer Science and Engineering, Vol.2, Issue.1, pp.22-28, 2014 .
[6] M.B.Ould MEDENI and El Mamoun SOUIDI, (2010) "Steganography and Error Correcting Codes", IJCSIS, Vol.8.No.8, pp147-149..
[7] Rajkumar Yadav, (2011) "A Novel Approach For Image Steganography In Spatial Domain Using Last Two Bits of Pixel Values", International Journal of Security, Vol.5 Iss. 2 pp. 51-61
[8] Parul, Manju, Dr. Harish Rohil, "Optimized Image Steganography using Discrete Wavelet Transform (DWT)", International Journal of Recent Development in Engineering and Technology, ISSN 2347– 6435, Volume 2, Issue 2, February 2014). pp. 75-81.
[9] C.-H. Yang and M.-H. Tsai, (2010) "Improving Histogram-based Reversible Data Hiding by Interleaving Predictions", IET Image Processing, Vol.4. Iss. 4 pp. 223-234
[10] Tanmay Bhattacharya, Manas Paul & Arindam Dasgupta (2009) "A Novel session Based Text Encryption & Hiding Technique Using Bit Level Cross Fold Transposition & Genetic Algorithm", International Journal of Information Technology and Knowledge Management, Vol. 2, No.2, pp.419-423.
[11] Fahim Irfan et. Al.s (2011) "An Investigation into Encrypted Message Hiding through Images Using LSB ", International Journal of EST.
[12] Keith L.Haynes, (2011) "Using Image Steganography to Establish Covert Communication Channels", International Journal of Computer Science and Information Security, Vol 9, No.9, pp. 1- 7.
[13] Sunny Dagar, "Highly Randomized Image Steganography using Secret Keys", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.
[14] D.P.Gaikwad and S.J.Wagh, (2010) "Colour Image Restoration For An Effective Steganography", I-mar‟s Journal on Software Engineering, Vol.4 .No.3, pp.654
[15] Hemalatha.S, U.Dinesh Acharya and Renuka.A, (2013) "Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCBCR domains", International Journal of Advanced Information Technology, Vol.3, No.3, pp.1-9.

Authors Profile

Mr.H. A. Patil pursed Master of Engineering from University of Mumbai in 2014. He is currently pursuing Ph.D in Computer Science from JNU Jaipur.

Prof. Prashant Sahai Saxena , Joint Director, JNU Jaipur is Ph.D in Computer Sciences. He has more than 23 years of experience in IT infrastructure management, Projects handling and Academic Administration. Prof. Saxena has successfully coordinated several projects on behalf of the state Government and other agencies such as WHO, World Bank etc. As Resource Person, he has participated in many Workshops, Symposia and Conferences.

